Group Structure in Correlations and its Applications in Cryptography

Guru-Vamsi Policharla, Manoj Prabhakaran, Rajeev Raghunath, and Parjanya Vyas

IIT Bombay

February 11, 2021

Abstract

Correlated random variables are a key tool in cryptographic applications like secure multiparty computation. We investigate the power of a class of correlations that we term *group correlations*: A group correlation is a uniform distribution over pairs $(x, y) \in G^2$ such that $x + y \in S$, where G is a (possibly non-abelian) group and S is a subset of G. We also introduce bi-affine correlations, and show how they relate to group correlations. We present several structural results, new protocols and applications of these correlations. The new applications include a completeness result for black box group computation, perfectly secure protocols for evaluating a broad class of black box "mixed-groups" circuits with bi-affine homomorphisms, and new information-theoretic results. Finally, we uncover a striking structure underlying OLE: In particular, we show that OLE over $\mathbb{F}_{2^n}$, is isomorphic to a group correlation over $\mathbb{Z}_4^n$.

1 Introduction

A central concept in secure multiparty computation (MPC) is that of correlated random variables. If Alice and Bob are given correlated random variables, they can later use them to securely compute any function, with information-theoretic security [20, 22]. This model has been a key ingredient in many theoretical and practical results in MPC. While the class of 2-party correlations that information-theoretically secure computation *can be* based on (i.e., "complete" correlations) is well-understood [23, 24], not all complete correlations *are* used in practical protocols. Instead, several "standard" correlations which have additional structure, like Oblivious Transfer (OT), Oblivious Linear function Evaluation (OLE) and Beaver's Multiplication Triplets (BMT) [3] are used in practice. The main motivation in this work is to systematically study the additional structure that protocols can exploit, and develop a deeper and broader foundation for such correlations.

Apart from uncovering the beautiful mathematical structures from which these correlations derive their power, another motivation for our work is to expand the applicability of correlated random variables to secure computation involving black-box algebraic structures which can be less structured than finite fields or rings. Consider the following seemingly disparate problems of information-theoretically secure 2-party computation:

- **Blackbox Group Computation:** If the function is given as a circuit over a blackbox (non-abelian) group, how can two parties securely compute it with *perfect security*? The complete

correlation proposed in [10] (namely, oblivious transfer of group elements), yielded only statistical security.

- **Generating and Processing Correlations over a Blackbox Ring:** If correlated random variables over a blackbox ring (e.g., OLE) are acquired by a pair of parties from a trusted server, can they be efficiently *rerandomized* (e.g., for "forward security" against future corruption of the server)? Efficiency relates to both the use of correlations as well as communication and number of rounds.
  How efficiently can such correlations be generated, using a less structured primitive like string OT?
- **Circuits Using Alternate Algebraic Structures:** Traditionally, MPC literature has considered algebraic circuits to be over fields or rings, and these protocols breakdown if the algebraic structure underlying the circuit has less structure. Can alternate protocols be devised for computation over (say) distributive near-rings or non-associative algebras, or when multiple such algebraic structures are used in the same circuit?

We introduce *bi-affine correlations* as an abstraction of a broad class of cryptographically interesting correlations, and address all of the above problems in terms of them. Perhaps more importanly, we undertake a study of the fundamental properties of bi-affine correlations and the underlying mathematical structure of bi-affine homomorphisms, without being confined to immediate applications. This leads us to the definition of *Group Correlations* and *Subgroups Correlations* as a generalization of bi-affine correlations, that brings out additional hidden structure of bi-affine correlations.

Interestingly, while "additive correlations" (the abelian version of group correlations) and "bilinear correlations" (a special case of bi-affine correlations) have been explicitly considered before in various applications, most notably in the rich line of work on function/homomorphic secret-sharing (F/HSS) and pseudorandom correlation generators (PCG) [5, 6, 7, 8, 9],[1] it was not realized that the former is a generalization of the latter, underlining the need for studying them abstractly.

1.1 Our Contributions

We develop a theory of *group correlations* and *subgroups correlations*, with a focus on the subclass of bi-affine correlations. A group correlation, specified by a group G and a subset $S \subseteq G$, is simply an additive secret-sharing of a random element in S, or equivalently, a uniform distribution over $\{(x, y) \mid x, y \in G, x + y \in S\}$. A subgroups correlation is a restriction of such a group correlation correlation to the universe $G_1 \times G_2$ where G_1 and G_2 are subgroups of G, with a regularity condition on S (so that the resulting correlation has uniform marginal distributions). Within this simple framework, a rich variety of structures arise based on how the groups and the set S are defined. Our contributions include the following:

- **A Theory of Group Correlations**: This includes several new definitions of structures and properties, as well as connections between them. (Section 3).
- **Information-Theoretic Results**: We give new results on information theoretic quantities (specifically, *residual information*) that can be used to analyze the optimality of secure protocols. (Section 4).

[1] In these works, bi-linear correlations were often termed *simple bi-linear correlations*. For consistency with the terminology in the current work, we avoid this term. What was termed (general) bi-linear correlations there would correspond to correlations of the form $\mathsf{BA}_{\sigma\langle 2\rangle}$ in this work.

- **New Protocol Building-Blocks**: We present a suite of protocols for various functionalities involving bi-affine correlations, with applications to 2-Party secure computation. (Section 5).
- **Applications**: The above building-blocks can be put together to yield various information-theoretically secure computation protocols. In particular, we show:
  - There exists a *complete correlation* for 2-party *perfectly* passive-secure evaluation of a black-box (non-abelian) group circuit – called the Zero Alternating Sum (ZAS) correlation (Section 6.2). ZAS is a bi-affine correlation, and hence this could seen as a special case of the following results. In contrast, previously the complete correlation proposed in [10] (namely, OT with group elements), yielded only statistical security.
    When the circuit has logarithmic depth, or is in the form of polynomial-sized formula, we obtain a 2-round UC secure protocol.
  - A GMW-style 2-Party protocol for evaluating a black-box "mixed-group circuit" with homomorphism and bi-affine homomorphism gates, which requires 2 rounds of interaction per layer.
  - 2-Party protocols for rerandomizing and testing bi-affine correlations obtained from a semi-trusted source (who will not collude with either party until after the protocol is over) (Section 5.1, Section 5.4). We also discuss how this can be viewed as a solution to sampling correlations in the single-server version of the commodity based model [2]. (Section 6.3).
  - A 2-Party protocol for securely sampling bi-affine correlations using string OTs, generalizing a protocol of Gilboa [19]. Using our information-theoretic results, we establish its optimality for a class of bi-affine correlations (including the ones considered in [19]). (Section 5.3).
- **A Surprising Structure.** Finally, we uncover a striking structure underlying OLE. In particular, we show that OLE over $\mathbb{F}_{2^n}$, is isomorphic to a group correlation over $\mathbb{Z}_4^n$. Given that OLE has been widely studied and used, it is remarkable that such a structure has remained hidden so far. (Section 7).

Discussion

Here we elaborate on some of the above contributions.

Hidden Structures. We point out two instances of hidden structure in well-studied objects that are revealed by our abstractions. OLE and BMT are two correlations that have been extensively studied both in terms of their applications, and in terms of protocols generating them. However, while abstracting them as bi-linear correlations (see Footnote 1), they are treated somewhat differently. For instance, in [7], PCGs for bi-linear correlations are given, which directly applies to OLE; and then a PCG for BMT is provided by reducing BMT to OLE. However, a consequence of our results is that BMT is already a (simple) bi-linear correlation, but with a bi-linear operator different from that of OLE: while OLE uses a map $\sigma(a, b) = ab$, BMT uses $\sigma((a, b), (c, d)) = ad + bc$ (all variables belonging to a ring). This results in a more efficient protocol since reducing one BMT to two OLE correlations is wasteful (a reduction in the opposite direction is not possible).

The second instance of a hidden structure is that of OLE which has a complicated structure due to the interaction of field multiplication with the addition structure of the field. As such, one may not expect OLE (over large fields) to be a group correlation. But we show that every symmetric bi-affine correlation (of which OLE is an example) is in fact a group correlation. Even more surprisingly, for the special case of OLE over the field $\mathbb{F}_{2^n}$, the underlying group turns out to be $\mathbb{Z}_4^n$. Thus OLE over $\mathbb{F}_{2^n}$ can be seen as sampling an element uniformly from a (non-obvious)

set $S \subseteq \mathbb{Z}_4^n$, and then simply additively secret-sharing it coordinate-wise. While we do not offer any immediate applications of this particular structure, as a fundamental property of an extremely useful cryptographic primitive, it is an interesting result.

ZAS: A Bi-Affine Correlation in a Group. An interesting application we present is that of a complete correlation for 2-party secure computation over a black-box group, with *perfect security*. In contrast to the prior approach which relied on OT with group elements, and only obtained statistically secure protocols [10], we rely on a deceptively simple correlation, called the Zero Alternating Sum (ZAS) correlation. In a ZAS correlation over a (non-abelian) group G, Alice and Bob get random pairs $(a, c) \in G^2$ and $(b, d) \in G^2$ such that $a + b + c + d = 0$.

Note that defining ZAS does not require anything more than the group operation. This demonstrates the generality of bi-affine homomorphisms, compared to bi-linear maps. While bi-linear maps are used to capture the multiplication operation in a *ring*, bi-affine homomorphisms can equally well capture the alternating sum structure in a group. Concretely, the function $\sigma : G^2 \to G^{\text{op}}$, defined as

$$\sigma(x, y) = -(x + y)$$

where G^{op} is the *opposite group* of G (whose group operation is the same as that of G, but applied to the operands in the opposite order), is a bi-affine homomorphism w.r.t. the subgroups $T = G \times \{0\}$ and $U = \{0\} \times G$ of the group G^2.

Optimality of Gilboa's Reduction. As a corollary of our information-theoretic results pertinent to bi-affine correlations, we show that Gilboa's reduction from OLE over $\mathbb{F}_{2^n}$ to string OT [19] is optimal in the number of string OTs used (n string OTs per OLE instance), and cannot be improved upon even with amortization. In fact, this extends to OLE over $\mathbb{F}_{p^n}$ if Gilboa's protocol is modified to use 1-out-of-p string OTs.

Mixed-Groups Circuit with Bi-Affine Homomorphism Gates. Conventionally, MPC literature has considered boolean or arithmetic circuits over a given ring or field. A variant of this considers the underlying algebraic structure to be given as a black box to the protocol (e.g., [11, 21] for rings and [10, 16, 17] for groups). Motivated by practical applications, MPC protocols for computation that uses multiple representations has received attention (e.g., the ABY framework [15] and subsequent works). More recently, circuits with bi-linear gates over multiple black box groups has been considered in [5].

Our applications use a similar circuit paradigm as [5], and use two types of gates (1) group operations (2) gates for group homomorphisms and bi-affine homomorphisms. Bi-Affine Homomorphisms are quite general, and can correspond to multiplication in distributive near-rings or non-associative rings, or even (negated) addition in a non-abelian group. As such, this is a powerful computational model that subsumes arithmetic circuits over a ring. Nevertheless, the bi-affine homomorphism structure lets us build perfectly secure 2-party protocols for all such circuits, using bi-affine correlations for the corresponding bi-affine homomorphisms (if necessary, along with "Zero Alternating Sum" correlations for the non-abelian groups).

1.2 Related Work

Correlations have received much attention in cryptography, especially since Beaver's proposal of using them as cryptographic commodities [4] and the emergence of the pre-processing model as a common approach to theoretically and practically efficient MPC. They have been put to great use for MPC, both in the passive and active corruption settings, in theory and practice (see. e.g.,

the SPDZ family of protocols [13] and subsequent work). All these works develop and use several building blocks like self-reduction and self-testing for their correlations.

The recent line of works on Pseudorandom Correlation Generators and Function Secret Sharing [5, 6, 7, 8, 9], which consider bi-linear and additive correlations are most closely related to our work. Briefly, they answer two important questions. (1) how to perform secure computation over bi-linear gates (2) how to efficiently generate these correlations. In contrast to our work, these results were focussed on exploiting computational hardness, and restricted themselves to bi-linear correlations and abelian groups.

Secure Multi Party Computation over non-abelian Black-Box groups has been well studied in the honest-majority setting [10, 16, 17]. In the two-party setting Cohen et al. [10] gave a passive statistically secure protocol for evaluating circuits over black-box groups in the OT hybrid model and used the IPS compiler [20] to achieve security against active corruption. In this work, we use a stronger primitive – namely Zero Alternating Sum correlations – but are able to obtain a simple perfectly secure protocol against active adversaries without the use of expensive compilers for log-depth circuits.

Protocols for rerandomization and testing of correlations have appeared previously in the literature but their focus has remained on specific correlations such as BMT, squaring tuples etc., [14]. The commodity based model first introduced by Beaver in [2] has been revisited recently in [12, 27] to sample OLE and BMT correlations.

1.3 Technical Overview

In this section we present the highlights of our results, informally. Several additional technical details and generalizations are deferred to the subsequent sections.

1.3.1 Definitions

We consider several classes of *flat* correlations – i.e., distributions that are uniform over their support. Below we use support and distribution interchangeably.

Group Correlations and Subgroups Correlations. A group correlation defined w.r.t a group G and a subset $S \subseteq G$ is the uniform distribution over all pairs $(g_1, g_2) \in G^2$ such that $g_1 + g_2 \in S$. A subgroups correlation *embedded in* this group correlation is obtained by requiring $g_1 \in G_1$ and $g_2 \in G_2$, where G_1, G_2 are subgroups of G with the property that the marginal distributions of g_1 and g_2 are both uniform. This subgroups correlation is said to be *compact* if $|G| < |G_1||G_2|$.

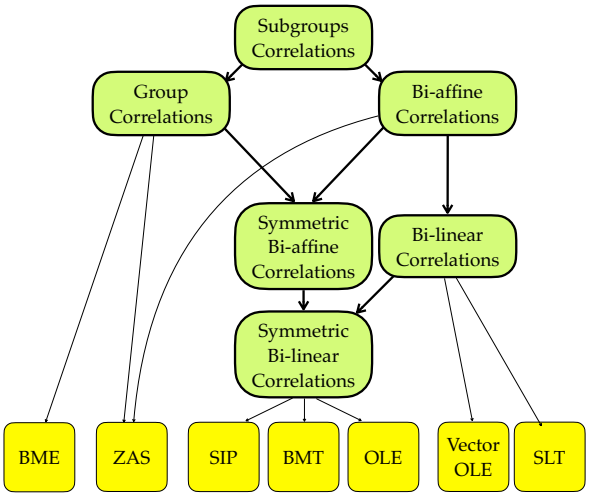

Figure 1: A taxonomy of correlations.

Bi-Affine Homomorphisms. A linear function (or a group homomorphism) $\phi : G \to H$ satisfies $\phi(a+b) = \phi(a)+\phi(b)$ (where the addition and subtraction are in the appropriate groups). An "affine" function ψ is such that ϕ defined by $\phi(x) := \psi(x) - \psi(0)$ is linear; i.e., $\psi(a+b) = \psi(a) - \psi(0) + \psi(b)$.

A bi-affine function could be defined as a function of two inputs, which is affine in each of them; i.e., for groups groups T, U, H, a function $e : T \times U \to H$ such that

$$e(t, u + u') = e(t, u) - e(t, 0) + e(t, u') \quad \text{and} \quad e(t + t', u) = e(t, u) - e(0, u) + e(t', u). \tag{1}$$

Note that if we required $e(t, 0) = e(0, u) = 0$, then the conditions above would collapse to e being *bi-linear*. Examples of functions that satisfy (1) but are not bi-linear include $e : G \times G \to G$ defined as $e(a, b) = a + b$ or as $e(a, b) = -a - b$.

For notational simplicity in our results, we define a *bi-affine homomorphism* as a *unary* function $\sigma : Q \to H$, (Q, H being groups) with respect to subgroups $T, U \leqslant Q$ so that $e : T \times U \to H$ defined as $e(t, u) := \sigma(t + u)$ satisfies (1). An equivalent definition, in terms of group homomorphisms, is given in Definition 7.

Bi-Affine Correlation. Given a bi-affine homomorphism σ as above, the support of the corresponding bi-affine correlation correlation $\mathsf{BA}_\sigma \subseteq (T \times H) \times (U \times H)$ is defined as

$$\mathsf{BA}_\sigma = \{((t, a), (u, b)) \mid \sigma(t + u) = a + b\}$$

Examples. As shown in Figure 1, the most commonly used correlations indeed fall under the class of bi-affine correlations.

- Oblivious Linear Evaluation (OLE): Defined over a ring A as $\big((t, a), (u, b)\big)$ such that $a + b = tu$, OLE is isomorphic to a bi-affine correlation with $\sigma(t, u) = tu$, where $\sigma : A^2 \to A$ is a bi-affine homomorphism with respect to $T = A \times \{0\}$ and $U = \{0\} \times A$.
- Beaver's Multiplication Triples (BMT): Defined over a ring A as $\big((t_1, u_1, a), (t_2, u_2, b)\big)$ such that $a + b = (t_1 + t_2)(u_1 + u_2)$, BMT is isomorphic to a bi-affine correlation with $\sigma((t_1, u_1), (t_2, u_2)) = t_1u_2 + t_2u_1$, where $\sigma : A^4 \to A$ is a bi-affine homomorphism with respect to $T = A^2 \times \{0\}^2$ and $U = \{0\}^2 \times A^2$.
- Zero Alternating Sum (ZAS): Defined over a (possibly non-abelian) group D as $\big((a, c), (b, d)\big)$ such that $a + b + c + d = 0$, ZAS is isomorphic to a bi-affine correlation BA_σ, where $\sigma : D^2 \to D^{\mathrm{op}}$ defined as $\sigma(c, d) = -(c + d)$ is a bi-affine homomorphism with respect to $T = D \times \{0\}$ and $U = \{0\} \times D$.

Powers of a Bi-Affine Homomorphism. Given a bi-affine homomorphism $\sigma : Q \to H$ w.r.t. subgroups T, U, we can define new bi-affine homomorphisms as "powers" of σ. As it turns out, there are a few different useful notions of such powers that emerge in the sequel, namely, σ^n, $\sigma^{(n)}$ and $\sigma^{\langle n \rangle}$.

$\sigma^n : Q^n \to H^n$ is simply the coordinate-wise application of σ. $\sigma^{(n)} : Q^n \to H^n$ corresponds to a "vector" variant of σ, generalizing how string-OT or vector-OLE are vector variants of OT and OLE respectively; it is in fact the same as σ^n, but considered as a bi-affine homomorphism w.r.t. T^n and $U^{(n)} = \{(u, \ldots, u) | u \in U\} \subseteq U^n$. $\mathsf{BA}_{\sigma^{(n)}}$. $\sigma^{\langle n \rangle} : Q^n \to H$ is an *inner-product* version of σ. It turns out that BMT is isomorphic to $\mathsf{BA}_{\sigma^{\langle 2 \rangle}}$ where σ is the multiplication in a ring (so that BA_σ corresponds to OLE over that ring).

✯ There exists a non-interactive, UC-secure protocol (Lemma 10) to securely sample one instance of $\mathsf{BA}_{\sigma^{\langle \ell, m \rangle}}$ from $\ell + m$ instances of BA_σ. A special case of this protocol is the reduction of a BMT correlation to two OLE correlations.

1.3.2 Connections

We uncover some surprising connections between the different classes of correlations mentioned above.

- ✯ Every symmetric bi-affine correlation is a group correlation. In particular, OLE over a ring A is isomorphic to a group correlation w.r.t the group $\mathbb{K}_A$ over $A \times A$ whose group operation is defined as $(a, b) \odot (c, d) = (a + c, b + d - ac)$, and subset $S = \{(a, 0) \mid a \in A\}$.
- ✯ Every bi-affine correlation is a *compact* subgroups correlation. Note that an asymmetric bi-affine correlation, like a vector OLE, cannot be a group correlation. But this result shows that it is a subgroups correlation compactly embedded in a group correlation. In particular, n-dimensional vector OLE over a ring A is embedded in the group correlation over the group $A^n \times A \times A^n$ with subset $S = \{(\boldsymbol{t}, u, \boldsymbol{t}u) | \boldsymbol{t} \in A^n, u \in A\}$. Interestingly, when instantiated for OLE ($n = 1$), it shows that OLE is embedded in the BMT correlation.
- ✯ If σ is a semi-abelian bi-affine homomorphism, then BA_σ is embedded in $\mathsf{BA}_{\sigma\langle 2\rangle}$ (Theorem 1). This serves as an alternate way of viewing the embedding of OLE in BMT, since OLE is BA_σ and BMT is $\mathsf{BA}_{\sigma\langle 2\rangle}$ where σ is the multiplication operation in the (possibly non-commutative) ring.

As mentioned above OLE over a ring is a group correlation, over the group $\mathbb{K}_\cdot$. We explore this group and discover more unexpected structure:

- When A has an element η such that $\eta + \eta = 1$, $\mathbb{K}_\sigma$ is isomorphic to the group $A \times A$ (considering only the addition operation in the ring).
- When A is $\mathbb{F}_{2^n}$ then $\mathbb{K}_\sigma$ is isomorphic to $\mathbb{Z}_4^n$. (See Section 1.3.5).

1.3.3 Information-Theoretic Results

Wyner residual information (RI_{w}) (6) is an information theoretic measure which describes how "correlated" two random variables are. This measure is a monotone and cannot be increased through communication. Concretely, Prabhakaran et. al. [25] showed that if m independent instances of one type of correlation (C) can be reduced to n independent instances of another type of correlation (C'), then $m \cdot RI_{\mathrm{w}}(C) \leq n \cdot RI_{\mathrm{w}}(C')$ (Proposition 1).

In this work, we compute the Wyner Residual Information for a subset of bi-affine correlations which satisfy the *non-defective* property (Definition 7). A consequence of our results is that, for any field F, $RI_{\mathrm{w}}(\mathrm{OLE}_F^n) = \log |F|$. In fact, the above result extends to *domains* rather than fields. (A domain is a ring with the "zero-product property," i.e., if $ab = 0$ then $a = 0$ or $b = 0$.) These results play a crucial role in later sections where we prove optimality of reductions from bi-affine correlations to oblivious transfer. Furthermore, we show that the bi-partite graph of a group correlation is a single connected component iff the set $\{s - s' \mid s, s' \in S\}$ is a generating set for the group G by appealing to the Gács-Körner common information (Lemma 5).

1.3.4 Constructions

We present several constructions (Section 5), which relate to various conditional sampling functionalities that *complete* a bi-affine correlation. As an example, the deterministic function-evaluation version of OLE can be interpreted as sampling an OLE correlation, conditioned on certain variables

being fixed. Below, three such functionalities are defined – depending on how many variables are fixed – for bi-affine correlations in general.

Conditional Sampling Functionalities $\mathcal{F}_{\sigma|\mathrm{U}}$, $\mathcal{F}_{\sigma|\mathrm{TU}}$ and $\mathcal{F}_{\sigma|\mathrm{TAU}}$
(where $\sigma : Q \to H$ is a bi-affine homomorphism w.r.t. $T, U \leqslant Q$)

Inputs: t, a from Alice, and $u \in U$ from Bob, where

$$t = a = \perp \text{ for } \mathcal{F}_{\sigma|\mathrm{U}} \qquad t \in T, a = \perp \text{ for } \mathcal{F}_{\sigma|\mathrm{TU}} \qquad t \in T, a \in H \text{ for } \mathcal{F}_{\sigma|\mathrm{TAU}}.$$

Outputs: $(\tilde{t}, \tilde{a})$ to Alice and $(\tilde{u}, \tilde{b})$ to Bob, where $((\tilde{t}, \tilde{a}), (\tilde{u}, \tilde{b})) \leftarrow \mathsf{BA}_\sigma$ conditioned on $\tilde{u} = u$, $\tilde{t} = t$ if $t \neq \perp$, and $\tilde{a} = a$ if $a \neq \perp$.

We present various protocols:

- ✯ UC secure protocols for $\mathcal{F}_{\sigma|\mathrm{U}}$, $\mathcal{F}_{\sigma|\mathrm{TU}}$ and $\mathcal{F}_{\sigma|\mathrm{TAU}}$ in the $\mathcal{F}_\sigma$-hybrid model (Figure 3). The protocols remain secure even if $\mathcal{F}_\sigma$ is replaced by an "adversarially controlled" version $\widetilde{\mathcal{F}}_\sigma$ (which still only provides instances in the support of the correlation BA_σ).
  - These protocols, denoted as $\mathsf{Comp}_{\sigma|\mathrm{U}}$, $\mathsf{Comp}_{\sigma|\mathrm{TU}}$ and $\mathsf{Comp}_{\sigma|\mathrm{TAU}}$, can be used for multiple purposes. In particular, it allows for *rerandomizing* a sample, and also as a tool for non-destructively checking the validity of a sample (in the protocols TRSamp_σ and $\mathsf{altTRSamp}_\sigma$ below). Our protocols are optimal in multiple ways: there is only one message (or in the case of $\mathsf{Comp}_{\sigma|\mathrm{TAU}}$, two messages) and a single instance of the correlation is "consumed" per instance produced. For the basic forms of these tasks (without the extension to $\widetilde{\mathcal{F}}_\sigma$), similar constructions have been previously developed, but only for specific correlations like OLE, BMT etc., [14].
- ✯ We also develop a new set of protocols for realizing the above functionalities using a "tamperable" version $\widehat{\mathcal{F}}_\sigma$ (which, when the two parties are honest, allows the adversary to specify arbitrary pairs, possibly outside the support of BA_σ), instead of $\widetilde{\mathcal{F}}_\sigma$. We present two such protocols, trading-off generality with efficiency.
  - The first protocol, TRSamp_σ (Figure 6) works for all bi-affine homomorphisms σ, but consumes $\omega(\log \lambda)$ (purported) samples of BA_σ to produce a single (good) instance. This protocol relies on an *error-preservation property* of the protocol $\mathsf{Comp}_{\sigma|\mathrm{TAU}}$, whereby it can be checked if two purported samples have identical "error," by consuming only one of them. This allows checking that a set of samples all have the same error, while leaving one of them unconsumed. This still admits the possibility that *all of the samples* have the same non-zero error. To detect this (except with negligible probability), a cut-and-choose step is employed.
  - The second protocol, $\mathsf{altTRSamp}_\sigma$ (Figure 8) achieves a rate of $1/2$, but relies on additional algebraic structure in the groups underlying σ. The main component of this protocol is an *error rerandomization* step (Figure 7), which we instantiate (Figure 9) for a variety of bi-affine homomorphisms $\sigma : Q \to H$, where:
    - σ corresponds to multiplication in a vector space over a large field (or more generally, a module of appropriate complexity),
    - H is abelian and its order has no small prime factors,
    - H is non-abelian and $|\{r + x - r \mid r \in H\}$ is large for all $x \neq 0$.

✯ We give a semi-honest secure protocol (Figure 5) for efficiently sampling a bi-affine correlation BA_σ from string-OTs. This protocol relies on additional structure in the groups underlying the σ, and requires (slight) non-blackbox access to them. The additional structure is used to represent every group element as a small sum of elements from a "basis." The protocol is a generalization of a protocol by Gilboa [19] for sampling OLE over a ring using string OTs, to bi-affine correlations over a wide range of groups. We also show, using our results on residual information from above, that when the basis allows a tight representation of the group elements, then, with some additional constraints on σ, the protocol is *optimal in the number of string-OTs used* (Lemma 12).

1.3.5 A Surprising Structure for OLE.

It is easy to see that OT (i.e., OLE over $\mathbb{F}_2$) can be written as a group correlation over $\mathbb{Z}_4$, by "drawing" the correlation as a bipartite graph and observing that it forms a cycle (see Figure 2). A surprising result we obtain is that OLE over $\mathbb{F}_{2^n}$ is in fact a group correlation over $\mathbb{Z}_4^n$. This is illustrated in Figure 12 for $n = 2$.

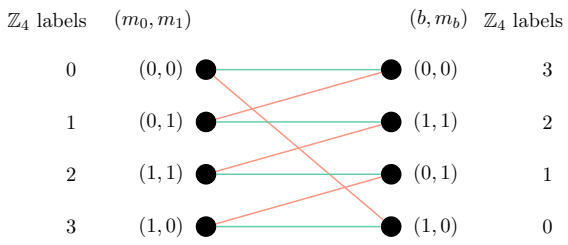

Figure 2: Bipartite graph of the OT correlation.

We give a detailed proof in Section 7 but provide a high level overview here. To show that $\text{OLE}_{\mathbb{F}_{2^n}}$ is a group correlation we give an isomorphism $\boldsymbol{\phi}$ from $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ to $\mathbb{Z}_4^n$ along with a subset $S \subset \mathbb{Z}_4^n$ and show that field elements $(t, a), (u, b)$ form an OLE correlation ($a + b = tu$) iff the sum of elements $g_1 = \boldsymbol{\phi}(t, a), g_2 = \boldsymbol{\phi}(u, b)$ lies within S. The isomorphism itself is highly non-trivial as it needs to handle the interaction of multiplicative and additive operations of the field in a purely additive sense. The isomorphism and subset are given by

$$\boldsymbol{\phi}(x, y) = [x] - 2 \cdot \left[\sqrt{\sum_{i:x_i=1} \xi^{(i)}(x)_i} \right] + 2 \cdot [\sqrt{y}]$$

$$S = \{[x] - 2 \cdot \left[\sqrt{\sum_{i:x_i=1} \xi^{(i)}(x)_i} \right] \mid x \in \mathbb{F}_{2^n}\}$$

where $[x]$ denotes the embedding from $\mathbb{F}_{2^n}$ to $\mathbb{Z}_4^n$, obtained by interpreting $x \in \{0, 1\}^n$ as $x \in \{0, 1, 2, 3\}^n$, $\{\xi^{(i)}\}_{i\in[0,n-1]}$ is an arbitrary basis of $\mathbb{F}_{2^n}$ with $\xi^{(0)} = 1$, and $(x)_i$ is the field element obtained by zeroing out all coordinates greater than or equal to i.

1.3.6 Applications

Using our constructions from Section 5 we show how to perform secure 2-Party computation of "mixed-groups" circuits in the semi-honest setting. The mixed-groups circuit model uses wires which carry group elements and group/bi-affine homomorphism gates in addition to gates implementing standard group operations.

✯ The first setting is semi-honest 2-Party computation in the $\mathcal{F}_\sigma$, $\mathcal{F}_{ZAS}$ hybrid model, where σ is the bi-affine homomorphism corresponding to the bi-affine homomorphism gate being evaluated (Section 6.2). Throughout the evaluation we maintain the invariant that all wires are secret shared

between the two parties. At each bi-affine gate, two bi-affine correlations and one ZAS correlation (in the group of the output wire) is consumed and at most two rounds of communication are needed to evaluate each level of the circuit. We achieve perfect security in this setting.

- As a corollary, we show that the ZAS correlation is complete for passively secure 2-Party secure computation over black-box groups (Section 6.2). This is immediate as all group operations can be implemented using ZAS correlations only.
- For the special case of formulas (or log-depth circuits) we present a two round perfectly secure protocol where the communication is proportional to the number of terms in the formula (Figure 10). Note that a formula can be written as an alternating sum of Alice and Bob's private inputs $f(x_1, \ldots, x_n, y_1, \ldots, y_n) = \sum_{i=1}^{n}(x_i + y_i)$. Alice pads each term of the formula with randomness and sends terms which contain her input in the clear. Alice and Bob invoke $\mathcal{F}_{ZAS}$ to compute terms containing Bob's inputs. Bob then sums up the terms sent by Alice and his output from $\mathcal{F}_{ZAS}$ invocations to compute $f(x_1, \ldots, x_n, y_1, \ldots, y_n) = \sum_{i=1}^{n}(x_i + y_i)$.
- We also show how the same task can be achieved in a different manner using the Function Secret Sharing based approach of Boyle et al. [5] (Section 6.2, Appendix F).

✯ The second setting we consider is the commodity based model introduced by Beaver [2]. Here a semi-trusted server which provides Alice and Bob with (possibly incorrect) correlations and is guaranteed to not collude with either party. Incorrect correlations are identified by using either TRSamp_σ or $\mathsf{altTRSamp}_\sigma$, after which the computation can be done in a manner identical to the previous setting.

2 Preliminaries

All the sets (and in particular, groups, rings and fields) we consider in this work are finite. For groups, we typically use additive notation. When several groups are used together, we often assign different symbols like $\odot$, $\oplus$ and $+$ for their operators. The unary negation symbol $(-x)$ is used across all groups to indicate the inverse; also, the binary subtraction symbol $(x-y)$ is used to denote $x+(-y)$, when the group operation is $+$. We use upright capital letters to denote random variables, as X, Y etc. Through out the paper, 2-party secure computation, unless otherwise qualified, refers to information-theoretic security against passive corruption.

We recall that given a subgroup T of a group $(G, +)$, its right and left cosets containing an element $g \in G$ are defined as $T + g = \{t + g \mid t \in T\}$, $g + T = \{g + t \mid t \in T\}$. We define "shifted groups" over these cosets, by redefining the group operation.

Definition 1 (Shifted Group Operation)**.** Given a group $(G, +)$, and $g \in G$, the operation $+_g$ is defined as $x +_g y = x - g + y$. ◁

It can be seen that $+_g$ is associative, as $(x +_g y) +_g z = x +_g (y +_g z) = x - g + y - g + z$. For any subgroup $T \subseteq G$, it can be verified that $(T + g, +_g)$ and $(g + T, +_g)$ are both groups with identity element g and the inverse of x given by $g - x + g$. They are both subgroups of $(G, +_g)$.

Definition 2 (Flat Correlation)**.** A flat correlation over sets X, Y is defined to be the uniform distribution over a set $C \subseteq X \times Y$. It is said to be *regular* if there are integers d_X, d_Y such that $\forall x \in X$, $|C \cap (\{x\} \times Y)| = d_X$ and $\forall y \in Y$, $|C \cap (X \times \{y\})| = d_Y$. ◁

Above, C is called the *support* of the correlation, and is also used to denote the correlation itself. Given a flat correlation over X, Y with support C, its graph $\mathbb{G}_C$ is defined as the bipartite graph with vertices $X \dot\cup Y$ (disjoint union) and the set of edges C.

Definition 3 (Isomorphic Correlations)**.** Flat correlations $C \subseteq X \times Y$ and $C' \subseteq X' \times Y'$ are said to be *isomorphic* to each other if there exist bijections $\alpha : X \to X'$ and $\beta : Y \to Y'$ such that $C' = \{\big(\alpha(x), \beta(y)\big) \mid (x, y) \in C\}$. $\triangleleft$

Definition 4 (Sampling Functionalities $\mathcal{F}_C$, $\widetilde{\mathcal{F}}_C$, $\widehat{\mathcal{F}}_C$)**.** For a flat correlation C, we define three functionalities as follows.

- **Sampling Functionality** $\mathcal{F}_C$: Uniformly samples a pair $(x, y) \leftarrow C$, and gives x to Alice and y to Bob.
- **Biasable Sampling Functionality** $\widetilde{\mathcal{F}}_C$: If Alice is corrupt, then it takes $x \in X$ from Alice, and outputs $y \leftarrow \{y' | (x, y') \in C\}$ to Bob; similarly, if Bob is corrupt, it takes y from Bob and outputs $x \leftarrow \{x' | (x', y) \in C\}$ to Alice. But if both parties are honest then it lets the adversary specify a *valid* sample, i.e., $(x, y) \in C$, instead of sampling one itself.
- **Tamperable Sampling Functionality** $\widehat{\mathcal{F}}_C$: It behaves like $\widetilde{\mathcal{F}}_C$, but if both Alice and Bob are honest, then it lets the adversary specify an arbitrary pair (x, y) (rather than only a valid pair).

$\triangleleft$

3 Definitions and Connections

3.1 Group Correlations and Subgroups Correlations

Definition 5 (Group Correlation)**.** A flat correlation $C \subseteq X \times Y$ is said to be a *group correlation* if there exists a group G and a subset $S \subseteq G$ such that C is isomorphic to the flat correlation $C' \subseteq G \times G$ given by $C' = \{(x, y) \mid x + y \in S\}$. In this case, we say that C is a group correlation of the form $\mathrm{GC}^{G,S}$. A group correlation of the form $\mathrm{GC}^{G,S}$ is said to be *abelian* if the group G is abelian. $\triangleleft$

Regularity. Let G_1, G_2 be subgroups of G, and $S \subseteq G$. S is said to be *regular* with respect to (G_1, G_2) if, for all $g_2, g_2' \in G_2$, we have $|S \cap (G_1 + g_2)| = |S \cap (G_1 + g_2')|$, and for all $g_1, g_1' \in G_1$, we have $|S \cap (g_1 + G_2)| = |S \cap (g_1' + G_2)|$. We call $\deg_L = |S \cap (g_1 + G_2)|$ and $\deg_R = |S \cap (G_1 + g_2)|$ the left and right degree of the subgroups correlation respectively.

We say that a group correlation $\mathrm{GC}^{G,S}$ is regular w.r.t. a pair of subgroups (G_1, G_2) of G if S is regular w.r.t. (G_1, G_2).

Definition 6 (Subgroups Correlation)**.** A flat correlation $C \subseteq X \times Y$ is said to be a *subgroups correlation* if there exists a group correlation C' that is regular w.r.t. a pair of subgroups (G_1, G_2), and C is isomorphic to the correlation $C'' \subseteq G_1 \times G_2$ defined as $C'' = C' \cap (G_1 \times G_2)$.

In this case, we say C is of the form $\mathrm{GC}^{G,S}_{G_1,G_2}$, and is *embedded in* C'.

Further, if $|G| < |X||Y|$, we say that C is a *compact* subgroups correlation. $\triangleleft$

If C is a *regular* flat correlation, then it can be seen to be a (non-compact) subgroups correlation of the form $\mathrm{GC}^{G,S}_{G_1,G_2}$ where, identifying X and Y with arbitrary groups of the same sizes (say $\mathbb{Z}_{|X|}$ and $\mathbb{Z}_{|Y|}$), we let $G = X \times Y$, $G_1 = X \times \{0_Y\}$, $G_2 = \{0_X\} \times Y$, and $S = C$. Conversely, a subgroups

correlation is a regular flat correlation. Hence, without restricting to being compact, subgroups correlations and regular flat correlations are the same. A compact subgroups correlation entails more structure than just being regular.

3.2 Bi-Affine Correlations

We start by defining a generalization of the notion of a homomorphism, called *bi-affine homomorphism*. Note that the definition below refers to homomorphisms between "shifted" groups, using the shifted group operation (Definition 1).

Definition 7 (Bi-Affine Homomorphism)**.** For groups $(Q,+)$ and $(H,\oplus)$, and subgroups $T,U \leqslant Q$, a function $\sigma : Q \to H$ is said to be a *bi-affine homomorphism w.r.t.* (T,U), if the following are group homomorphisms

$$\sigma|_{T+u} : (T+u, +_u) \to (H, \oplus_{\sigma(u)}) \qquad \forall u \in U$$
$$\sigma|_{t+U} : (t+U, +_t) \to (H, \oplus_{\sigma(t)}) \qquad \forall t \in T.$$

Further, σ is said to be *semi-abelian* if H is an abelian group; it is said to be *abelian* if both Q and H are abelian. It is said to be *symmetric* if it is semi-abelian and $Q = D \times D, T = D \times \{0\}, U = \{0\} \times D$ for some group D. If either $\sigma|_{T+u}$ is surjective for every $u \in U$, or $\sigma|_{t+U}$ is surjective for every $t \in T$, σ is called a *surjective* bi-affine homomorphism. If there is no pair $(t,u) \in (T \setminus \{0\}) \times (U \setminus \{0\})$ such that $\sigma(t+u) = \sigma(t) - \sigma(0) + \sigma(u)$, σ is said be to non-defective[2]. $\triangleleft$

These homomorphism conditions over the shifted groups can be equivalently written as, $\forall t, t' \in T, u, u' \in U$,

$$\sigma(t+t'+u) = \sigma(t+u) \oplus -\sigma(u) \oplus \sigma(t'+u)$$
$$\sigma(t+u+u') = \sigma(t+u) \oplus -\sigma(t) \oplus \sigma(t+u').$$

(where we used $(t+u) +_u (t'+u) = t+t'+u$ and $(t+u) +_t (t+u') = t+u+u'$).

Definition 8 (Bi-Affine Correlation)**.** Given groups $(Q,+)$ and $(H,\oplus)$, and a bi-affine homomorphism $\sigma : Q \to H$ w.r.t. (T,U), the correlation $\mathsf{BA}_\sigma \subseteq (T \times H) \times (U \times H)$ is defined as

$$\mathsf{BA}_\sigma = \{((t,a),(u,b)) \mid \sigma(t+u) = a \oplus b\}$$

A flat correlation C is said to be a *bi-affine correlation* if there exists σ as above such that it is isomorphic to BA_σ. Further, C is said to be *semi-abelian*, *abelian* or *symmetric* if σ has the corresponding property. $\triangleleft$

Bi-linear correlations. It is instructive to compare bi-affine homomorphisms with bi-linear maps. For groups $(T,+)$, $(U,+)$ and $(H,\oplus)$, where the last one is abelian, a function $e : T \times U \to H$ is said to be a bi-linear map if e left and right distributes over the group operations: i.e., for all $t_1, t_2 \in T$ and $u_1, u_2 \in U$, $e(t_1+t_2, u_1) = e(t_1,u_1) \oplus e(t_2,u_1)$, and $e(t_1, u_1+u_2) = e(t_1,u_1) \oplus e(t_1,u_2)$.

It is easy to see that a bi-linear map is a special case of a bi-affine homomorphism: Let $Q = T \times U$, $T' = T \times \{0_U\}$ and $U' = \{0_T\} \times U$. Then, $e : Q \to H$ is a bi-linear map iff it is a semi-abelian bi-affine homomorphism w.r.t. (T',U'), with the additional property that $e(x) = 0$ for all $x \in T' \cup U'$.

[2]This condition corresponds to $K_{2,2}$ freeness of the bi-affine correlation. We prove this in Appendix C.

If a bi-affine homomorphism σ is a bi-linear map, then we say that a correlation of the form BA_σ is a *bi-linear correlation*. For bi-linear σ, non-defective reduces to not having non-zero $t \in T, u \in U$ such that $\sigma(t+u) = 0$. An example of such a bi-affine correlation is given by OLE (or vector OLE) over a *domain*. A domain is a ring with the "zero-product property," i.e., if $ab = 0$ then $a = 0$ or $b = 0$ (with fields being a special case of domains).

3.3 Powers of Bi-Affine Homomorphisms

Given a bi-affine homomorphism σ, one can define related bi-affine homomorphisms as various "powers". In this section, we describe some standard transformations to do this, and in Section 3.5 give some important examples of correlations in the literature that illustrate these transformations. Let $\sigma : Q \to H$ be a bi-affine homomorphism w.r.t subgroups T, U.

- We define $\sigma^n : Q^n \to H^n$ as simply the coordinate-wise application of σ. That is,
$$\sigma^n(q_1, ..., q_n) = (\sigma(q_1), ..., \sigma(q_n)).$$
If σ is a bi-affine homomorphism w.r.t. subgroups $T, U \leqslant Q$, then σ^n is readily seen to be a bi-affine homomorphism w.r.t. subgroups $T^n, U^n \leqslant Q^n$.
- It is interesting to view σ^n as a bi-affine homomorphism w.r.t. other subgroups within T^n, U^n. In particular, we define $\sigma^{(n)}$ to be the same as σ^n but considered as a bi-affine homomorphism w.r.t. $T^n, U^{(n)}$, where
$$U^{(n)} = \{(u, \ldots, u) | u \in U\} \subseteq U^n.$$
- When H is abelian, we also define an aggregating version $\sigma^{\langle \ell, m \rangle} : Q^{\ell+m} \to H$, as
$$\sigma^{\langle \ell, m \rangle}(q_1, \ldots, q_\ell, q'_1, \ldots, q'_m) = \sum_{i=1}^{\ell} \sigma(q_i) \oplus \sum_{i=1}^{m} \sigma(-q'_i)$$
where the summations refer to the operation $\oplus$ in the group H. $\sigma^{\langle \ell, m \rangle}$ can be seen to be a bi-affine homomorphism w.r.t. $(T^\ell \times U^m, U^\ell \times T^m)$. We shall simply write $\sigma^{\langle n \rangle}$ for the symmetric bi-affine homomorphism $\sigma^{\langle \lceil n/2 \rceil, \lfloor n/2 \rfloor \rangle}$.

In Appendix B, we prove that these powers of a bi-affine homomorphism are indeed bi-affine homomorphisms.

Lemma 1. *For groups $(Q, +)$ and $(H, \oplus)$, and subgroups $T, U \leqslant Q$, let $\sigma : Q \to H$ be a* bi-affine homomorphism w.r.t. (T, U). *Then:*

1. *$\sigma^n : Q^n \to H^n$ is a bi-affine homomorphism w.r.t T^n, U^n for all $n \geq 1$.*
2. *$\sigma^{(n)} := \sigma^n$ is a bi-affine homomorphism w.r.t $T^n, U^{(n)} := \{(u, ..., u) | u \in U\}$ for all $n \geq 1$.*
3. *If H is abelian, then $\sigma^{\langle \ell, m \rangle} : Q^{\ell+m} \to H$ is a bi-affine homomorphism w.r.t $(T^\ell \times U^m, U^\ell \times T^m)$ for all $\ell, m \geq 1$.*

Bi-Affine Correlations using the powers of σ We shall define BA_{σ^n}, $\mathsf{BA}_{\sigma^{(n)}}$ and $\mathsf{BA}_{\sigma^{\langle n \rangle}}$ as the bi-affine correlations defined on the corresponding bi-affine homomorphism σ^n, $\sigma^{(n)}$ and $\sigma^{\langle n \rangle}$ respectively.

$\mathsf{BA}_{\sigma^{(n)}}$ is a "vector" variant of BA_σ, generalizing how string-OT or vector-OLE are vector variants of OT and OLE respectively. $\mathsf{BA}_{\sigma^{\langle n \rangle}}$ could be considered an "inner-product" version of BA_σ. Further, it turns out that BMT is isomorphic to $\mathsf{BA}_{\sigma^{\langle 2 \rangle}}$ (where σ is the multiplication in a ring, so that BA_σ corresponds to OLE over that ring). We explore these examples in Section 3.5.

3.4 Group Structure of Bi-Affine Correlations

In this section we show connections between (sub)group correlations and bi-affine correlations, which can be summarized as follows:

Theorem 1. *For any bi-affine homomorphism σ,*

1. BA_σ *is a compact subgroups correlation;*
2. *if σ is symmetric, then BA_σ is a group correlation;*
3. *if σ is semi-abelian, then BA_σ is embedded in $\mathsf{BA}_{\sigma^{\langle 2\rangle}}$, and more generally, $\mathsf{BA}_{\sigma^{\langle \ell,m\rangle}}$ is embedded in $\mathsf{BA}_{\sigma^{\langle 2m'\rangle}}$ for all $m' \geq \max(\ell, m)$.*

We present the key ingredients of the above connections here. Details omitted from here are included in Appendix B.

Groups $\mathbb{J}$ and $\mathbb{K}$. To capture the structure of bi-affine correlations as (sub)group correlations, we define two groups. If $\sigma : Q \to H$ is a bi-affine homomorphism w.r.t. (T, U), the group $\mathbb{J}_\sigma$ is defined as the direct product $T \times U \times H$. Then it is easy to see the following:

Lemma 2. *If $\sigma : Q \to H$ is a bi-affine homomorphism w.r.t. (T, U), then BA_σ is a subgroups correlation of the form $\mathrm{GC}^{G,S}_{G_1,G_2}$ where $G = \mathbb{J}_\sigma$ and $S = \{(t, u, \sigma(t + u)) \mid t \in T, u \in U\}$, with $G_1 = T \times \{0\} \times H, G_2 = \{0\} \times U \times H$.*

This is a compact subgroups correlation because $|G_1||G_2| = |T||U||H|^2 > |T||U||H| = |G|$. While this group structure is direct, a surprising group structure exists for *symmetric* bi-affine correlations, that shows that they are all group correlations. To describe this, we define the following group:

Definition 9. If $\sigma : D \times D \to H$ is a symmetric bi-affine homomorphism, then $\mathbb{K}_\sigma$ is defined as $(D \times H, \odot)$, where $\odot$ is given by

$$(d, h) \odot (d', h') = \left(d + d', h \oplus h' \oplus \sigma(d, 0) \oplus \sigma(0, d') \oplus -\sigma(d, d')\right). \tag{2}$$

◁

It can be verified that $\mathbb{K}_\sigma$ is indeed a group. An interesting special case is when σ is bi-linear, in which case the terms $\sigma(d, 0)$ and $\sigma(0, d')$ vanish. In particular, if $\sigma : A \times A \to A$ for a ring A, with $\sigma(a, b) = ab$ (multiplication in the ring), then the operation $\odot$ defined as $(t, a) \odot (u, b) = (t+u, a+b-tu)$. This group, which we denote as $\mathbb{K}_A$, encodes both the addition and multiplication operations in the ring (as $(0, a) \odot (0, a') = (0, a + a')$, and $(a, 0) \odot (a', 0) = (a + a', -aa')$). Given that $\mathbb{K}_\sigma$ is a group, the following claim is easy to verify.

Lemma 3. *A bi-affine correlation of the form BA_σ, where $\sigma : D \times D \to H$ is a symmetric bi-affine homomorphism, is a group correlation of the form $\mathrm{GC}^{\mathbb{K}_\sigma, S}$, where $S = \{(d+d', \sigma(d, 0) \oplus \sigma(0, d')) | d, d' \in D\}$.*

Finally, we show that $\mathsf{BA}_{\sigma^{\langle \ell,m\rangle}}$ is embedded in $\mathsf{BA}_{\sigma^{\langle 2m'\rangle}}$ for all $m' \geq \max(\ell, m)$. Note that from Lemma 3, $\sigma^{\langle 2m'\rangle}$ is a symmetric bi-affine homomorphism, hence $\mathsf{BA}_{\sigma^{\langle 2m'\rangle}}$ is isomorphic to a group correlation $\mathrm{GC}^{G,S}$ with $G = \mathbb{J}_{\sigma^{\langle 2m'\rangle}}$ and

$$S = \{(\boldsymbol{t_1}, \boldsymbol{u_1}, \boldsymbol{u_2}, \boldsymbol{t_2}, h) \mid \sigma^{\langle 2m'\rangle}(\boldsymbol{t_1} + \boldsymbol{u_1}, \boldsymbol{u_2} + \boldsymbol{t_2}) = h;\ \boldsymbol{t_1}, \boldsymbol{t_2} \in T^{m'},\ \boldsymbol{u_1}, \boldsymbol{u_2} \in U^{m'},\ h \in H\}.$$

We then give subgroups $G_1, G_2 \leqslant G$

$$G_1 = \big(T^\ell \times \{0\}^{m'-\ell}\big) \times \big(U^m \times \{0\}^{m'-m}\big) \times \{0\}^{m'} \times \{0\}^{m'} \times H,$$

$$G_2 = \{0\}^{m'} \times \{0\}^{m'} \times \big(U^\ell \times \{0\}^{m'-\ell}\big) \times \big(T^m \times \{0\}^{m'-m}\big) \times H.$$

such that $\mathsf{BA}_{\sigma\langle\ell,m\rangle}$ is isomorphic to the subgroups correlation $\mathrm{GC}^{G,S}_{G_1,G_2}$. See Appendix B for full proof.

3.5 Some Noteworthy Examples

Here we consider several cryptographically interesting examples and show that they are (sub) group correlations and also explore connections between them. More examples can be found in Appendix A. See Table 1 for a summary.

3.5.1 OLE and Beaver Multiplication Triples

Oblivious Linear function Evaluation (OLE) and Beaver's Multiplication Triple (BMT) over an arbitrary ring A are defined as follows:

$$\textsc{ole}_A := \{\big((p,a),(q,b)\big) \mid a+b = pq\},$$

$$\textsc{bmt}_A := \{\big((a_1,b_1,c_1),(a_2,b_2,c_2)\big) \mid c_1+c_2 = (a_1+a_2)(b_1+b_2)\}.$$

Consider the symmetric bi-affine homomorphism $\sigma : A \times A \to A$ defined with respect to subgroups $T = A \times \{0\}$ and $U = \{0\} \times A$ as $\sigma(a,b) = ab$. It can be seen that the bi-linear correlation BA_σ is isomorphic to $\textsc{ole}_A$. Since σ is symmetric, $\textsc{ole}_A$ is a group correlation (Theorem 1).

It is straightforward to see that BMT is a group correlation with $G = A \times A \times A$ and $S = \{(a,b,ab) \mid a,b \in A\}$. In fact, it can be shown that BMT is isomorphic to the bi-linear correlation

$$\mathsf{BA}_{\sigma\langle 2\rangle} := \{\big((\tilde{a}_1,0),(0,\tilde{b}_2),\tilde{c}_1\big),\big((0,\tilde{b}_1),(\tilde{a}_2,0),\tilde{c}_2\big) \mid \tilde{a}_1\tilde{b}_1 + \tilde{a}_2\tilde{b}_2 = \tilde{c}_1 + \tilde{c}_2\},$$

by defining isomorphisms

$$\alpha(a_1,b_1,c_1) = \big((a_1,0),(0,b_1),c_1 - a_1b_1\big),$$

$$\beta(a_2,b_2,c_2) = \big((0,b_2),(a_2,0),c_2 - a_2,b_2\big).$$

It can now be checked that $\big((a_1,b_1,c_1),(a_2,b_2,c_2)\big) \in \textsc{bmt}_A \Leftrightarrow \big(\alpha(a_1,b_1,c_1),\beta(a_2,b_2,c_2)\big) \in \mathsf{BA}_{\sigma\langle 2\rangle}$. Hence, the following statement holds true.

Lemma 4. *$\textsc{bmt}_A$ defined over a ring A, is a bi-linear correlation of the form $\mathsf{BA}_{\sigma\langle 2\rangle}$, where $\sigma : A \times A \to A$ is a bi-affine homomorphism with respect to subgroups $T = A \times \{0\}$ and $U = \{0\} \times A$ defined as $\sigma(a,b) = ab$.*

While the group correlation structure of BMT and the bi-linear correlation structure of OLE are evident from their definitions, the fact that BMT is also a bi-linear correlation and that OLE is a group correlation (corresponding to the group $\mathbb{K}_A$ over $A \times A$ with addition given by $(a,b) \odot (c,d) = (a+b, c+d-ab)$) was not immediate. Indeed, the intriguing group $\mathbb{K}_A$ calls for further investigation which we take up in Section 7.

3.5.2 Shared Inner Product and Linear Transformation.

The Shared Inner Product (SIP) correlation corresponds to a secret sharing of the inner product of two vectors over a ring A. Formally, it is a flat correlation over $A^{m+1} \times A^{m+1}$ with support:

$$\textsc{sip}_A^m := \{\big((\boldsymbol{x}, a), (\boldsymbol{y}, b)\big) \mid \langle \boldsymbol{x}, \boldsymbol{y} \rangle = a + b\},$$

where the vectors $\boldsymbol{x}, \boldsymbol{y}$ are m-dimensional. It can be seen that $\textsc{sip}_A^m$ is isomorphic to $\mathsf{BA}_{\sigma^{\langle m,0\rangle}}$, where bi-affine homomorphism $\sigma : A \times A \to A$ w.r.t subgroups $T = A \times \{0\}$ and $U = \{0\} \times A$ is defined as $\sigma(t, u) = tu$. Since $\sigma^{\langle m,0\rangle}$ is a symmetric bi-linear homomorphism, it follows from Lemma 3 that $\textsc{sip}_A^m$ is a group correlation.

One may also consider the vector variant of this correlation, which we shall call the Shared Linear Transformation (SLT) correlation. SLT is a correlation over $X \times Y$, where $X = A^{mn} \times A^n$, $Y = A^m \times A^n$, defined as follows (considering elements in A^{mn} as $n \times m$ matrices, and the vectors as column vectors),

$$\textsc{slt}_A^{m,n} = \{((M, \boldsymbol{x}), (\boldsymbol{z}, \boldsymbol{y})) \mid M\boldsymbol{z} = \boldsymbol{x} + \boldsymbol{y}\}.$$

SLT is isomorphic to a bi-linear correlation with $\sigma : A^{mn} \times A^m \to A^n$ defined w.r.t subgroups $T = A^{mn} \times \{0\}^n$ and $U = \{0\}^{mn} \times A^n$ as $\sigma\big(M, \boldsymbol{z}\big) = M\boldsymbol{z}$.

3.5.3 Zero-Alternating Sum Correlation

We introduce an important correlation, called Zero Alternating Sum (ZAS) correlation over any (non-abelian) group $(D, +)$. ZAS is a flat correlation $\textsc{zas}_D \subseteq D^2 \times D^2$, defined as

$$\textsc{zas}_D := \{\big((a, c), (b, d)\big) \mid a + b + c + d = 0\}.$$

We remark that if D is an abelian group, then $\textsc{zas}_D$ is a trivial correlation.[3]

$\textsc{zas}_D$ as a Bi-Affine Correlation. Somewhat surprisingly, ZAS turns out to be a bi-affine correlation. We define the corresponding bi-affine homomorphism $\sigma : D \times D \to H$, where $H = D^{\text{op}}$, the *opposite group* of D (i.e., H has the same elements as D and has a group operation $\oplus$ defined by $a \oplus b = b + a$). We let $\sigma(x, y) = -(x + y)$. Then, clearly, ZAS is isomorphic to the flat correlation $\{((c, a), (d, b)) \mid \sigma(c, d) = a + b\}$. To show that ZAS is of the form BA_σ it remains to verify that σ is a bi-affine homomorphism w.r.t. (T, U) where $T = D \times \{0\}$, $U = \{0\} \times D$. We illustrate that $\sigma|_{t+U}$ is a homomorphism from $(t + U, +_t)$ to $(H, \oplus_{\sigma(t)})$ for any $t = (a, 0) \in T$ (the case of $\sigma|_{T+u}$ being analogous). Consider $u = (0, b)$ and $u' = (0, b')$. Then,

$$\begin{aligned}
\sigma((t + u) +_t (t + u')) &= \sigma(t + u + u') = \sigma(a, b + b') = -(a + b + b') = -b' - b - a \\
\sigma(t + u) \oplus_{\sigma(t)} \sigma(t + u') &= \sigma(a, b) \oplus -\sigma(a) \oplus \sigma(a, b') \\
&= -(a + b') + a - (a + b) = -b' - b - a.
\end{aligned}$$

We shall later refer to the bi-affine homomorphism σ defined above as σ_D^{ZAS}.

$\textsc{zas}_D$ as a Group Correlation. When D is not abelian, σ defined above is not semi-abelian, and hence $\textsc{zas}_D$ is *not* symmetric. As such, Lemma 3 *does not* apply to $\textsc{zas}_D$. Nevertheless, we

[3] A secure protocol for sampling from $\textsc{zas}_D$, when D is abelian, is as follows: Alice samples $x \leftarrow D$ to Bob; Alice then picks a random $a \leftarrow D$ and outputs $(a, x - a)$; Bob samples $b \leftarrow D$ and outputs $(b, -x - b)$.

can see that ZAS_D over any group D is a group correlation of the form $\text{GC}^{G,S}$, where the group G is D^2, with coordinate-wise addition, and $S = \{(g, -g) \mid g \in D\}$. To see this, we note that

$$\begin{aligned}((a,c),(b,d)) \in \text{ZAS}_D &\Leftrightarrow a+b+c+d=0 \Leftrightarrow a+b=-(c+d)\\ &\Leftrightarrow (a+b,c+d) \in S \Leftrightarrow (a,c)+(b,d) \in S.\end{aligned}$$

4 Information Theoretic Results

In this section, we collect a set of information-theoretic results about (sub)group correlations and bi-affine correlations. These will later be used in Section 5.3 to prove optimality of our reduction from bi-affine correlations to string OT.

Common-Information. For a pair of correlated random variables (X, Y), two important information-theoretic measures of correlation are the well-known quantity of *mutual information* $I(\mathrm{X};\mathrm{Y})$ [26] and the lesser known notions of *common information*. Specifically, there are two measures of common information due to Gács and Körner [18] and due to Wyner [28], which can defined as below:

$$CI_{\text{GK}}(\mathrm{X};\mathrm{Y}) = I(\mathrm{X};\mathrm{Y}) - RI_{\text{GK}}(\mathrm{X};\mathrm{Y}) \tag{3}$$

$$CI_{\text{W}}(\mathrm{X};\mathrm{Y}) = I(\mathrm{X};\mathrm{Y}) + RI_{\text{W}}(\mathrm{X};\mathrm{Y}) \tag{4}$$

$$RI_{\text{GK}}(\mathrm{X};\mathrm{Y}) = \inf_{\mathrm{Q}} I(\mathrm{X};\mathrm{Y}|\mathrm{Q}), \text{ such that } H(\mathrm{Q}|\mathrm{X}) = H(\mathrm{Q}|\mathrm{Y}) = 0 \tag{5}$$

$$RI_{\text{W}}(\mathrm{X};\mathrm{Y}) = \inf_{\mathrm{Q}} I(\mathrm{Y};\mathrm{Q}|\mathrm{X}) + I(\mathrm{X};\mathrm{Q}|\mathrm{Y}), \text{ such that } I(\mathrm{X};\mathrm{Y}|\mathrm{Q}) = 0 \tag{6}$$

where the infimum is over all random variables Q that are jointly distributed with (X, Y). Here RI_{GK} and RI_{W} are (respectively) Gács-Körner and Wyner *residual information*.

We shall write $RI_{\text{W}}(C)$ etc. as a short hand for $RI_{\text{W}}(\mathrm{X};\mathrm{Y})$, where the random variables (X, Y) are uniformly distirbuted over C. Residual information (of either kind) provides a fundamental measure of the cryptographic quality of a correlated random variable (and are special instances of a more general measure called tension [25]).

We will use the following proposition that is a special case of a "monotonicity" result in [25].

Proposition 1 ([25])**.** *If m independent instances of $\mathcal{F}_C$ can be securely computed using n independent instances of $\mathcal{F}_{C'}$, then $m \cdot RI_{\text{W}}(C) \leq n \cdot RI_{\text{W}}(C')$.*

Also, C is a trivial correlation – i.e., there exists an information theoretically secure 2-party protocol to sample from C – iff $RI_{\text{W}}(C) = 0$ (or equivalently, $RI_{\text{GK}}(C) = 0$).

Lemma 5. *Suppose C is a group correlation of the form $\text{GC}^{G,S}$. Then:*

1. *C is trivial iff S is a (left or right) coset of a subgroup of G.*
2. *$CI_{\text{GK}}(C) = 0$ iff the set $\{s - s' \mid s, s' \in S\}$ is a generating set for the group G.*
3. *If for all $s_1, s_2, s_3, s_4 \in S$, $s_1 - s_2 + s_3 - s_4 = 0 \Rightarrow \{s_1, s_3\} = \{s_2, s_4\}$, then $RI_{\text{W}}(C) = \log|S|$ viz. C is $K_{2,2}$ free.*

Now, we state our main technical result in this section. Recall that in a non-defective bi-affine homomorphism, there is no pair $(t, u) \in (T \setminus \{0\}) \times (U \setminus \{0\})$ such that $\sigma(t+u) = \sigma(t) - \sigma(0) + \sigma(u)$.

Lemma 6. *If σ is a non-defective bi-affine homomorphism w.r.t. (T, U), then $RI_{\text{W}}(\mathsf{BA}_\sigma) = \log\min(|T|, |U|)$.*

An example of a non-defective bi-affine homomorphism is given by multiplication in a *domain*. A domain is a ring with the "zero-product property," i.e., if $ab = 0$ then $a = 0$ or $b = 0$ (with fields being a special case of domains).

Lemma 7. *If A is a domain, then $RI_{\mathrm{W}}(\mathrm{OLE}_A^n) = \log |A|$.*

See Appendix C for full proofs of lemmas.

5 Protocols for Bi-Affine Correlations

In this section, we present several protocols pertinent to bi-affine correlations which will form the building blocks of the various applications in Section 6. These protocols realize several basic functionalities related to "completing" the correlations (i.e., sampling from a correlation conditioned on certain parts being fixed), given access to a random instance of the same correlation which could be obtained from a semi-trusted source modeled by the biasable sampling functionality. The same protocols can also be used to "rerandomize" for forward security. This is carried out for bi-affine correlations in Section 5.1. Next, in Section 5.2 we give a reduction for inner-product bi-affine correlations to the corresponding bi-affine correlation. In Section 5.3, we present an extension of Gilboa's protocol [19] to sample bi-affine correlations in the string OT hybrid model. Finally in Section 5.4, we present protocols for "self-testing" correlations acquired from an adversarially controlled functionality (tamperable sampling) to sample an unbiased instance of the bi-affine correlation.

In the following, $\sigma : Q \to H$ is a bi-affine homomorphism from a group $(Q, +)$ to group $(H, \oplus)$ w.r.t subgroups $T, U \leqslant Q$.

5.1 Completing a Bi-Affine Correlation

We first define the conditional sampling functionality that *completes* a bi-affine correlation, by sampling an instance of the correlation conditioned on its inputs.

Conditional Sampling Functionalities $\mathcal{F}_{\sigma|\mathrm{U}}$, $\mathcal{F}_{\sigma|\mathrm{TU}}$ and $\mathcal{F}_{\sigma|\mathrm{TAU}}$
(where $\sigma : Q \to H$ and $T, U \leqslant Q$)

Inputs: $t \in T, a \in H$ from Alice, and $u \in U$ from Bob, where

$$t = a = \perp \text{ for } \mathcal{F}_{\sigma|\mathrm{U}} \qquad t \in T, a = \perp \text{ for } \mathcal{F}_{\sigma|\mathrm{TU}} \qquad t \in T, a \in H \text{ for } \mathcal{F}_{\sigma|\mathrm{TAU}}.$$

Outputs: $(\tilde{t}, \tilde{a})$ to Alice and $(\tilde{u}, \tilde{b})$ to Bob, where $((\tilde{t}, \tilde{a}), (\tilde{u}, \tilde{b})) \leftarrow \mathsf{BA}_\sigma$ conditioned on $\tilde{u} = u$, $\tilde{t} = t$ if $t \neq \perp$, and $\tilde{a} = a$ if $a \neq \perp$.

Functionalities $\mathcal{F}_{\sigma|\mathrm{T}}$ and $\mathcal{F}_{\sigma|\mathrm{TUB}}$ are defined symmetric to $\mathcal{F}_{\sigma|\mathrm{U}}$ and $\mathcal{F}_{\sigma|\mathrm{TAU}}$, respectively. All functionalities allow the adversary to selectively abort output delivery to honest parties (after seeing its own output, if any).

Figure 3 contains UC secure protocols for the functionalities $\mathcal{F}_{\sigma|\mathrm{U}}$, $\mathcal{F}_{\sigma|\mathrm{TU}}$ and $\mathcal{F}_{\sigma|\mathrm{TAU}}$ in the $\widetilde{\mathcal{F}}_\sigma$ hybrid model (with only one invocation of $\widetilde{\mathcal{F}}_\sigma$). The first two protocols require one round of communication while $\mathsf{Comp}_{\sigma|\mathrm{TAU}}$ needs two rounds of communication.

Lemma 8. *$\mathsf{Comp}_{\sigma|\mathrm{U}}$ and $\mathsf{Comp}_{\sigma|\mathrm{TU}}$ (Figure 3) UC-securely realize the functionalities $\mathcal{F}_{\sigma|\mathrm{U}}$ and $\mathcal{F}_{\sigma|\mathrm{TU}}$, respectively in the $\widetilde{\mathcal{F}}_\sigma$ hybrid.*

Lemma 9. $\mathsf{Comp}_{\sigma|\text{TAU}}$ *(Figure 3) UC-securely realizes the functionality* $\mathcal{F}_{\sigma|\text{TAU}}$ *in the* $\widetilde{\mathcal{F}}_\sigma$ *hybrid.*

We prove these lemmas in Appendix D.1. Here, we point out that if both parties are honest, then Alice and Bob output (t, a) and (u, b) such that:

$$\begin{aligned} a \oplus b &= [\sigma(t + \Delta_u) \oplus -\sigma(t)] \oplus [\tilde{a} \oplus \tilde{b}] \oplus [-\sigma(\tilde{u}) \oplus \sigma(\Delta_t + \tilde{u})] \\ &= [\sigma(t + \Delta_u) \oplus -\sigma(t)] \oplus [\sigma(\tilde{t} + \tilde{u})] \oplus [-\sigma(\tilde{u}) \oplus \sigma(\Delta_t + \tilde{u})] \\ &= [\sigma(t + \Delta_u) \oplus -\sigma(t)] \oplus [\sigma((\tilde{t} + u) +_u (\Delta_t + \tilde{u})] \\ &= \sigma((t + \Delta_u) +_t (t + \tilde{u})) \\ &= \sigma(t + u) \end{aligned}$$

where, we use the properties of σ (Definition 7) and the fact that $\tilde{a} \oplus \tilde{b} = \sigma(\tilde{t} + \tilde{u})$. Also note that to prove Lemma 9, it is sufficient to show that Π_σ is a secure realization of $\mathcal{F}_{\sigma|\text{TAU}}$ (and then appeal to Lemma 8 and the UC theorem to implement $\mathcal{F}_{\sigma|\text{TU}}$ with protocol $\mathsf{Comp}_{\sigma|\text{TU}}$ in the $\widetilde{\mathcal{F}}_\sigma$ hybrid model). Correctness of Π_σ, when the parties are honest, follows from the fact that $a \oplus b = a \oplus \Delta_a \oplus \tilde{b} = \tilde{a} \oplus \tilde{b} = \sigma(t + u)$. UC security follows from the observation that in Π_σ, the inputs to $\mathcal{F}_{\sigma|\text{TU}}$ and the message that Alice sends to Bob can be arbitrary and would still correspond to valid input choices of the parties (or aborting).

5.2 Inner-Product Bi-Affine Correlations from Bi-Affine Correlations

If Alice and Bob hold $\ell + m$ instances of any semi-abelian bi-affine correlation BA_σ (in appropriate directions), they can non-interactively extract an instance of $\mathsf{BA}_{\sigma^{\langle \ell+m \rangle}}$.

The correctness of the protocol in Figure 4 can be seen as follows. Recall that the bi-affine correlation corresponding to $\sigma^{\langle \ell, m \rangle}$ is defined as $\big((t_1, \ldots, t_\ell, u'_1, \ldots, u'_m, h_1), (u_1, \ldots, u_\ell, t'_1, \ldots, t'_m, h_2)\big)$ such that

$$\sigma^{\langle \ell, m \rangle}(t_1 + u_1, \ldots, t_\ell + u_\ell, u'_1 + t'_1, \ldots, u'_m + t'_m) = h_1 \oplus h_2 \tag{7}$$

Note that the L.H.S of (7) can be expanded as

$$\begin{aligned} \sum_{i=1}^{\ell} \sigma(t_i + u_i) + \sum_{i=1}^{m} \sigma(-t'_i - u'_i) &= \sum_{i=1}^{\ell} \sigma(r_i + s_i) + \sum_{i=1}^{m} \sigma(r'_i + s'_i) \\ &= \sum_{i=1}^{\ell} (x_i + y_i) + \sum_{i=1}^{m} (x'_i + y'_i) \\ &= h_1 \oplus h_2 \end{aligned}$$

Lemma 10. *The protocol in Figure 4 is a non-interactive UC-secure secure protocol for reducing* $\mathsf{BA}_{\sigma^{\langle \ell, m \rangle}}$ *to* $\ell + m$ *instances of* BA_σ.

5.3 Bi-Affine Correlations from String OT

In this section we present a protocol to generate arbitrary bi-affine correlations in the OT^ℓ hybrid model. We do this by first constructing a protocol for $\mathcal{F}_{\sigma|\text{TAU}}$ in the string OT hybrid model. This implies a semi-honest secure protocol for $\mathcal{F}_\sigma$ when Alice and Bob sample their inputs uniformly at

Protocols $\mathsf{Comp}_{\sigma|\mathrm{U}}$ and $\mathsf{Comp}_{\sigma|\mathrm{TU}}$ in the $\widetilde{\mathcal{F}}_\sigma$ hybrid model

- **Inputs:** Bob receives $u \in U$. In $\mathsf{Comp}_{\sigma|\mathrm{TU}}$, Alice receives $t \in T$, as well.
- **Invocation of $\widetilde{\mathcal{F}}_\sigma$:** Alice gets $(\tilde{t}, \tilde{a})$ and Bob gets $(\tilde{u}, \tilde{b})$ from $\mathcal{F}_\sigma$, s.t. $\tilde{a} \oplus \tilde{b} = \sigma(\tilde{t} + \tilde{u})$.
- In $\mathsf{Comp}_{\sigma|\mathrm{U}}$, Alice sets $t = \tilde{t}$.
- **Alice $\leftrightarrow$ Bob:**
  - Alice sends Δ_t to Bob, where $\Delta_t := -\tilde{t} + t$. (In $\mathsf{Comp}_{\sigma|\mathrm{U}}$, $\Delta_t = 0_T$ and this message can be omitted.)
  - Bob sends Δ_u to Alice, where $\Delta_u := u - \tilde{u}$.
- **Output:** Alice outputs (a, t) where $a := \sigma(t + \Delta_u) \oplus -\sigma(t) \oplus \tilde{a}$, and Bob outputs (u, b) where $b := \tilde{b} \oplus -\sigma(\tilde{u}) \oplus \sigma(\Delta_t + \tilde{u})$. (In $\mathsf{Comp}_{\sigma|\mathrm{U}}$, $b = \tilde{b}$.)

Protocol Π_σ in the $\mathcal{F}_{\sigma|\mathrm{TU}}$ hybrid model

- **Inputs:** Alice receives $(t, a) \in T \times H$, and Bob receives $u \in U$.
- **Invocation of $\mathcal{F}_{\sigma|\mathrm{TU}}$:** Alice inputs t, Bob inputs u to $\mathcal{F}_{\sigma|\mathrm{TU}}$, and receive outputs $(t, \tilde{a})$ and $(u, \tilde{b})$ respectively s.t. $\tilde{a} \oplus \tilde{b} = \sigma(t + u)$.
- **Alice $\rightarrow$ Bob:** Alice sends Δ_a to Bob, where $\Delta_a := -a \oplus \tilde{a}$.
- **Output:** Alice outputs (t, a) and Bob outputs (u, b), where $b := \Delta_a \oplus \tilde{b}$.

Protocol $\mathsf{Comp}_{\sigma|\mathrm{TAU}}$ in the $\widetilde{\mathcal{F}}_\sigma$ hybrid model

$\mathsf{Comp}_{\sigma|\mathrm{TAU}}$ is obtained by composing Π_σ with $\mathsf{Comp}_{\sigma|\mathrm{TU}}$ (as an implementation of $\mathcal{F}_{\sigma|\mathrm{TU}}$).

Figure 3: UC-secure protocols for $\mathcal{F}_{\sigma|\mathrm{T}}$, $\mathcal{F}_{\sigma|\mathrm{TU}}$ and $\mathcal{F}_{\sigma|\mathrm{TAU}}$ in the $\widetilde{\mathcal{F}}_\sigma$ hybrid model. All protocols use a single invocation to the functionality $\widetilde{\mathcal{F}}_\sigma$. The first two protocols have a single round of message exchange, while the latter requires two rounds.

Protocol to sample $\mathsf{BA}_{\sigma\langle\ell,m\rangle}$ in the $\mathcal{F}_\sigma$ hybrid model

- **Invocation of $\mathcal{F}_\sigma$:**
  - $\mathcal{F}_\sigma$ is invoked ℓ times, at the end of which Alice holds $(r_1, \ldots, r_\ell, x_1, \ldots, x_\ell)$ and Bob holds $(s_1, \ldots, s_\ell, y_1, \ldots, y_\ell)$ such that $\sigma(r_i + s_i) = x_i \oplus y_i$ where $r_i \in T, s_i \in U$ and $x_i, y_i \in H$ for all $i \in [\ell]$.
  - $\mathcal{F}_\sigma$ is invoked m times in the opposite direction, at the end of which Alice receives $(s'_1, \ldots, s'_m, y'_1, \ldots, y'_m)$ and Bob receives $(r'_1, \ldots, r'_m, x'_1, \ldots, x'_m)$, such that $\sigma(r'_i + s'_i) = x'_i \oplus y'_i$ where $r'_i \in T, s'_i \in U$ and $x'_i, y'_i \in H$ for all $i \in [m]$.
- **Outputs:** Alice outputs $t_i = r_i, u'_j = -s'_j, h_1 = \sum_{k=1}^{\ell} x_k \oplus \sum_{k=1}^{m} y'_k$ and Bob outputs $t'_j = -r'_j, u_i = s_i, h_2 = \sum_{k=1}^{\ell} y_k \oplus \sum_{k=1}^{m} x'_k$ for all $i \in [\ell]$, $j \in [m]$.

Figure 4: A protocol for sampling $\mathsf{BA}_{\sigma\langle\ell,m\rangle}$ in the $\mathcal{F}_\sigma$, $\mathcal{F}_{ZAS|\mathrm{TU}}$ hybrid model.

random. Our construction subsumes the OLE_A generation protocol proposed by Gilboa [19], where A is an arbitrary ring which has a bit decomposition. Furthermore, we show that Gilboa's protocol

is optimal in the number of string-OTs used when sampling a correlation from $\text{OLE}_{\mathbb{F}_{2^n}}$.

As the first step in a protocol for $\mathcal{F}_{\sigma|\text{TAU}}$, Alice and Bob agree upon a *generator matrix* M_U of dimensions $k \times d$ such that every element $u \in U$ can be expressed as $u = \sum_{i=1}^{k} M_U(i, c_i)$ where $M_U(i, j)$ denotes the element in the i-th row and j-th column and the vector $\boldsymbol{c}$ is the decomposition of element u w.r.t the generator matrix M_U. Given such an generator matrix, our protocol needs k instances of $\binom{d}{1}$-OT^{ℓ} string OTs.[4] Figure 5 describes the protocol for $\mathcal{F}_{\sigma|\text{TAU}}$ in the string OT hybrid model.

Protocol $\mathsf{Comp}_{\sigma|\text{TAU}}$ in the $\binom{d}{1}$-OT^{ℓ} Hybrid model

Parameters: Groups $(T, +), (U, +), (H, \oplus)$ and a generator matrix of U, $M_U \in U^{k \times d}$.

- **Inputs:** Alice has input $t \in T, a \in H$ and Bob has input $u \in U$.
  - Alice samples $\{r_i\}_{i \in [2,k]} \leftarrow H$ and sets $r_1 = a$.
  - For each $i \in [k-1]$, Alice and Bob invoke $\binom{d}{1}$-OT^{ℓ}. Alice's input is the tuple $\{-r_i \oplus \sigma(t + M_U(i,j)) \oplus -\sigma(t) \oplus r_{i+1}\}_{j \in [d]}$ and Bob's input is a choice integer $c_i \in [d]$. Bob receives $m_i = -r_i \oplus \sigma(t + M_U(i, c_i)) \oplus -\sigma(t) \oplus r_{i+1}$.
  - For $i = k$, Alice's input is the tuple $\{-r_k \oplus \sigma(M_U(i,j))\}_{j \in [d]}$ and Bob's input is a choice integer $c_i \in [d]$. Bob receives $m_k = -r_k \oplus \sigma(t + M_U(k, c_k))$.
- Bob combines the messages he received to compute $b = \sum_{i=1}^{k} m_i$

Figure 5: A semi-honest secure protocol realising $\mathcal{F}_{\sigma|\text{TAU}}$ in the $\binom{m}{1}$-OT^{ℓ}-Hybrid model.

Lemma 11. $\mathsf{Comp}_{\sigma|\text{TAU}}$ *(Figure 5) is a semi-honest secure protocol realising* $\mathcal{F}_{\sigma|\text{TAU}}$.

We prove Lemma 11 in Appendix D.3. Note that $|U| \leq d^k$ since every element in U can be represented as the summation of k elements, each chosen from a d-dimensional row of M_U. The following lemma considers the case when this representation is tight.

Lemma 12. *If σ is non-defective and $|U| = d^k \leq |T|$, then $\mathsf{Comp}_{\sigma|\text{TAU}}$ is optimal in the number of instances of $\binom{d}{1}$-OT^{ℓ} used (for any length ℓ) for semi-honest securely realizing one instance of BA_{σ}.*

Lemma 12 follows from the fact that $RI_{\text{W}}(\binom{d}{1}\text{-OT}^{\ell}) \leq \log(d)$.[5] Also, by Lemma 6, $RI_{\text{W}}(\mathsf{BA}_{\sigma}) \leq \log|U| = k \log d$. Then, by Proposition 1, at least k instances of $\binom{d}{1}$-OT^{ℓ} are needed to securely sample one instance of BA_{σ}, proving the lemma.

More General Generator Matrix. The number of elements in each column of the generator matrix was fixed to be d, however, this is not necessary. By choosing a different d_i for each column $i \in [k]$, one could obtain cheaper protocols by using string OTs with fewer choice bits. Lemma 12 generalizes accordingly.

[4] Effectively, we require oblivious transfer over group elements and hence the length of strings must be long enough to send the description of an element.

[5] An upperbound on $\binom{d}{1}$-OT^{ℓ} can be computed by setting $\text{Q} = \text{Y}$ in (6), where $\text{X} = (m_1, \ldots, m_d)$ and $\text{Y} = (b, m_b)$. Then $I(\text{Y}; \text{Y}|\text{X}) = H(\text{Y}|\text{X}) = \log(d)$ since the only remaining entropy in Y given X is the d different choices of b.

Sampling Bi-Affine Correlation. Observe that in $\mathsf{Comp}_{\sigma|\text{TAU}}$, if Alice and Bob randomly sample their inputs instead of receiving them from the environment, they effectively sample a bi-affine correlation. More formally, they realise $\mathcal{F}_\sigma$ described in Section 2.

Comparison with Gilboa's protocol. In [19], Gilboa gave a protocol to generate OLE correlations over a ring A. This protocol is a special case of Figure 5. Gilboa requires the ring to have a bit-decomposition which is equivalent to demanding the existence of a generator matrix M_A of dimension $\log|A| \times 2$. When $A = \mathbb{F}_{(2^n)}$, Gilboa's protocol uses n instances of $\binom{2}{1}$-OT^ℓ. By appealing to Lemma 18, Proposition 1 and the fact that $RI_{\text{W}}(\binom{2}{1}\text{-OT}^\ell) = 1$, it can be argued that this is the minimum number of OTs that must be invoked (in either direction and per correlation if amortised) to obtain an information-theoretically secure 2-Party protocol that samples $\text{OLE}_{\mathbb{F}_{2^n}}$ correlations.

5.4 Biasable Correlations from Tamperable Correlations

The protocol TRSamp_σ in Figure 6 gives a secure protocol for $\widetilde{\mathcal{F}}_\sigma$ in the $\widehat{\mathcal{F}}_\sigma$ hybrid model. With no assumptions on the structure of the correlation, Alice and Bob can consume $\log(\lambda)$ correlations and output one correlation which they are guaranteed is correct with overwhelming probability. The main insight in our tamper resistant protocols is to use the following error preservation property of $\mathsf{Comp}_{\sigma|\text{TAU}}$ to check correlations against each other in a "tournament" style and thereby amplify the probability of catching incorrect correlations.

Error-Preservation Property: When $\mathsf{Comp}_{\sigma|\text{U}}$, $\mathsf{Comp}_{\sigma|\text{TU}}$ and $\mathsf{Comp}_{\sigma|\text{TAU}}$ are instantiated in the $\widehat{\mathcal{F}}_\sigma$-hybrid, errors in the correlation output by parties is related to the error in the correlation which parties receive from $\widehat{\mathcal{F}}_\sigma$. Recall that when both Alice and Bob are honest, $\widehat{\mathcal{F}}_\sigma$ allows the adversary to feed an arbitrary pair $((\hat{t},\hat{a}),(\hat{u},\hat{b}))$ to the parties. Suppose, $\hat{a} \oplus \hat{b} = \sigma(\hat{t}+\hat{u}) \oplus \hat{e}$. In this case, the outputs (t,a) and (b,u) are such that $a \oplus b = \sigma(t+u) \oplus e$, where $e = x \oplus \hat{e} \oplus -x$ (for $x = -\sigma(t+\hat{u}) \oplus \sigma(\hat{t}+\hat{u})$). In particular, $e = 0_H$ iff $\hat{e} = 0_H$; further, when H is abelian, $e = \hat{e}$. We shall refer to this as the error preservation guarantee of $\mathsf{Comp}_{\sigma|\text{T}}$, $\mathsf{Comp}_{\sigma|\text{TU}}$ and $\mathsf{Comp}_{\sigma|\text{TAU}}$ in the $\widehat{\mathcal{F}}_\sigma$-hybrid model.

Lemma 13. TRSamp_σ *(Figure 6) securely realizes the functionality* $\widetilde{\mathcal{F}}_\sigma$ *against passive corruption, with statistical security.*

We prove security in Appendix D.4.

A More Efficient Version. While applicable to all bi-affine correlations, TRSamp_σ has a *rate* of $o(1/\log\lambda)$, which depends on the security parameter. Here we present a template which can be used to obtain much better constant rate (in our instantiations, 1/2, without resorting to amoritization) in many common examples of bi-affine correlations over large groups. This template is in the form of a passive-secure protocol for $\widetilde{\mathcal{F}}_\sigma$ in the $(\widehat{\mathcal{F}}_\sigma, \mathcal{E}_\sigma)$-hybrid, where $\mathcal{E}_\sigma$ is an "error randomization" functionality. Then, $\mathcal{E}_\sigma$ itself is securely realized in the $\widehat{\mathcal{F}}_\sigma$-hybrid, depending on the specifics of the map σ. We implement this latter step only for large groups which satisfy one of three different structural properties.

Error Randomization Functionality. The error randomization functionality $\mathcal{E}_\sigma$ outputs two instances of the correlation $((t_1,a_1),(u_1,b_1))$ and $((t_2,a_2),(u_2,b_2))$ such that either the latter is a valid correlation in BA_σ, or the former has a "high min-entropy error". Relying on this $\mathsf{altTRSamp}_\sigma$ checks one correlation against the other and catches erroneous correlations with overwhelming probability. In our instantiations of $\mathcal{E}_\sigma$, the latter is obtained through an invocation of $\widehat{\mathcal{F}}_\sigma$ and the former is a

Protocol TRSamp_σ in the $\widehat{\mathcal{F}}_\sigma$ hybrid model

Parameter: Let $n := \omega(\log \lambda)$.

- **Invocation of $\widehat{\mathcal{F}}_\sigma$:** Alice gets $\{(t^i, a^i)\}_{i\in[n]}$ and Bob gets $\{(u^i, b^i)\}_{i\in[n]}$ from n invocations of $\widehat{\mathcal{F}}_\sigma$.
- **[Cut-and-Choose] Bob $\to$ Alice:**
  - Bob samples a random permutation $\sigma \in S_n$, and sends σ to Alice. Both reorder their correlations as per σ: in the following, we let $t_i := t^{\sigma(i)}$, etc.
  - Bob sends $\{(u_i, b_i)\}_{1\le i\le \frac{n}{2}}$ to Alice. Alice aborts if for any $i \le \frac{n}{2}$, $((t_i, a_i), (u_i, b_i)) \notin C$.
- **[Consistency Check]** For each i such that $\frac{n}{2} + 1 < i \le n$, Alice and Bob check the instances i and $i-1$ for consistency:
  - Alice and Bob invoke $\mathsf{Comp}_{\sigma|_{\mathrm{TAU}}}^{(t_{i-1},a_{i-1}),(u_{i-1},b_{i-1})}$ on inputs (t_i, a_i) and u_i respectively, and Bob gets output b_i^*.
  - Bob aborts if $b_i^* \neq b_i$.
- **Output**: Alice outputs (t_n, a_n) and Bob outputs (u_n, b_n).

Figure 6: A passive secure protocol for $\widetilde{\mathcal{F}}_\sigma$ in the $\widehat{\mathcal{F}}_\sigma$ hybrid model.

"randomised" version of the latter such that the new error (if non-zero) has large min-entropy. For details of the error randomization functionality and protocols see Figure 7 and Figure 9. Depending on the structure of the bi-affine homomorphism $\sigma : Q \to H$, the instantiations need different algebraic properties from the group H:

- **Modules:** A group H is said to be a right-module of a ring R if there is a bi-linear map $\sigma : H \times R \to H$ (i.e., $\sigma((h + h'), r) = \sigma(h, r) + \sigma(h', r)$ and $\sigma(h, (r + r')) = \sigma(h, r) + \sigma(h, r')$) with the additional properties that $\sigma(\sigma(h, r), r') = \sigma(h, (rr'))$ (where the multiplication rr' is from the ring) and $\sigma(h, 1) = h$, where 1 stands for the multiplicative identity in R. Let units(R) denote the set of ring elements $r \in R$ that have a multiplicative inverse in the ring. We define minimg$_R(H)$ to be the minimum size of the image of units(R) under the map $r \mapsto x \cdot r$, over all non-zero elements x in the module H. i.e.,

$$\text{minimg}_R(H) = \min_{x\in H\setminus\{0_H\}} |\{x \cdot r | r \in \text{units}(R)\}|.$$

  We require that minimg$_R(H)$ is super-polynomial in the security parameter. An example is the case when R is a large enough field and H is a vector-space over R, then minimg$_R(H) = |R| - 1$.
- **Semi-Abelian Bi-affine correlations:** For a group H, we define minord(H) as the order of the smallest non-trivial subgroup of H. Consequently, for all $0 < k <$ minord(H), for all $h \in H \setminus \{0_H\}$, we have $\underbrace{h + \cdots + h}_{k \text{ times}} \neq 0$. minord$(H)$ equals the smallest prime factor of the order of H. For security we require that minord(H) is super-polynomial in the security parameter. An example is a large prime order group H, where minord$(H) = |H|$.
- **Surjective Bi-affine Correlations:** For a (non-abelian) group D, we define minorbit(D) to be

the size of the smallest conjugacy class of D, excluding $\{0\}$. That is,

$$\text{minorbit}(D) := \min_{x \in D \setminus \{0\}} |\{r + x - r | r \in D\}|.$$

This instantiation requires the minorbit(D) must be super-polynomial in security parameter. As an example consider the group $\text{SL}(2, 2^n)$ [6] – i.e., 2×2 matrices over $\mathbb{F}_{2^n}$, with determinant 1, where $\text{minorbit}(\text{SL}(2, 2^n)) \geq 2^n$ [1].

Functionality $\mathcal{E}_\sigma$

Parameters: $\ell = \omega(\log \lambda)$, groups $(H, \oplus), (Q, +)$ and $T, U \subseteq Q$, bi-affine $\sigma : Q \to H$ w.r.t T, Q

- If Alice and Bob are both honest:
  - Adversary specifies a distribution $\mathcal{D}$ over $(T \times H) \times (U \times H)$, and a pair $\big((\tilde{t}, \tilde{a}), (\tilde{u}, \tilde{b})\big)$.
  - Define the distribution E_{u_0}, for each $u_0 \in U$, as

$$E_{u_0} := \{-x \oplus e \oplus x\}_{\big((t,a),(u,b)\big) \leftarrow \mathcal{D}, e := -\sigma(t+u) \oplus a \oplus b, x := \sigma(t+u_0)}.$$

    - If $\big((\tilde{t}, \tilde{a}), (\tilde{u}, \tilde{b})\big) \in \mathsf{BA}_\sigma$ or, $\forall u_0 \in U$, $\text{H}_\infty(E_{u_0}) \geq \ell$, then let $\big((t_2, a_2), (u_2, b_2)\big) := \big((\tilde{t}, \tilde{a}), (\tilde{u}, \tilde{b})\big)$.
    - Else sample $\big((t_2, a_2), (u_2, b_2)\big) \leftarrow \mathsf{BA}_\sigma$.
  - Sample $\big((t_1, a_1), (u_1, b_1)\big) \leftarrow \mathcal{D}$.
- If Alice is corrupt:
  - Adversary specifies (t_1, a_1) and $(t_2, a_2) \in T \times H$ along with a function $\xi : T \times H \to T \times H$
  - Sample $u_2 \leftarrow U$ and let $b_2 := -a_2 \oplus \sigma(t_2 + u_2)$. Compute $(u_1, b_1) = \xi(u_2, b_2)$.
  - Check if $\big((t_1, a_1), (u_1, b_1)\big) \in \mathsf{BA}_\sigma$. If not, then sample $u_1 \leftarrow U$ and set $b_1 = -a_1 \oplus \sigma(t_1 + u_1)$
- If Bob is corrupt:
  - Adversary specifies (u_1, b_1) and $(u_2, b_2) \in U \times H$ along with a function $\xi : U \times H \to U \times H$
  - Sample $t_2 \leftarrow T$ and let $a_2 := \sigma(t_2 + u_2) \oplus -b_2$. Compute $(t_1, a_1) = \xi(t_2, a_2)$.
  - Check if $\big((t_1, a_1), (u_1, b_1)\big) \in \mathsf{BA}_\sigma$. If not, then sample $t_1 \leftarrow T$ and set $a_1 = \sigma(t_1 + u_1) \oplus -b_1$
- Send (t_1, a_1) and (t_2, a_2) to Alice and (u_1, b_1) and (u_2, b_2) to Bob.

Figure 7: The error randomization functionality for bi-affine homomorphism σ.

Lemma 14. $\mathsf{altTRSamp}_\sigma$ *(Figure 8) passive-securely realizes the functionality $\widetilde{\mathcal{F}}_\sigma$, in the $\widehat{\mathcal{F}}_\sigma$, $\mathcal{E}_\sigma$ hybrid model*

Lemma 15. *The protocols in (Figure 9) passive-securely realize the functionality $\mathcal{E}_\sigma$, in the $\widehat{\mathcal{F}}_\sigma$ hybrid model, provided the stated security conditions are satisfied.*

We prove both these lemmas in Appendix D.4.

[6] Every element in the group also has a succinct representation using $O(n)$ bits.

Protocol $\mathsf{altTRSamp}_\sigma$ in the $\widehat{\mathcal{F}}_\sigma$, $\mathcal{E}_\sigma$ hybrid model

- **Invocation of $\widehat{\mathcal{F}}_\sigma$:** Alice gets (t_0, a_0) and Bob gets (u_0, b_0) from $\widehat{\mathcal{F}}_\sigma$.
- **Error-Rerandomization:** Alice and Bob invoke $\mathcal{E}_\sigma$ and receive (t_1, a_1), (t_2, a_2) and (u_1, b_1), (u_2, b_2) respectively.
- **Verification:**
  - Alice and Bob invoke $\mathsf{Comp}_{\sigma|_{\mathrm{TAU}}}^{(t_0,a_0),(u_0,b_0)}$ on inputs (t_1, a_1) and u_1 respectively, and Bob gets output b^*.
  - Bob aborts if $b^* \neq b_1$.
- **Output**: Alice outputs (t_2, a_2) and Bob outputs (u_2, b_2).

Figure 8: A passive-secure protocol for $\widetilde{\mathcal{F}}_\sigma$ in the $\widehat{\mathcal{F}}_\sigma$, $\mathcal{E}_\sigma$ hybrid model.

6 Applications

6.1 Evaluating Log-Depth Circuits over Black-Box groups

For the case of log-depth black-box group circuits we give a 2 round perfectly secure protocol (Figure 10). Later, we show that the ZAS correlation is in fact complete for passively secure black-box group computation (Section 6.2).

A depth d circuit can be expanded into a *formula* of size $O(2^d)$, simply by recursively expanding the sub-circuits for the two input wires to a top-level gate into two formulas and concatenating them. Since all the operators in this formula are the group operation, which is associative, one can remove all the parentheses in the formula. Thus a log-depth circuit can be "flattened" into a polynomial length summation of the input variables. Further, adjacent input variables in this summation that are available with one party can be aggregated into a single variable locally. Hence, it is enough to securely compute the *alternating sum functionality*, $\mathcal{F}_{D,n}^{\mathrm{altsum}}$ defined as $f(x_1, \ldots, x_n, y_1, \ldots, y_n) = \sum_{i=1}^{n}(x_i + y_i)$, where x_i are Alice's inputs and y_i are Bob's inputs, only Bob receives the output, and the summation is in the group D (in the given order). Our protocol is in the $\mathcal{F}_{\sigma_D^{\mathrm{ZAS}}|_{\mathrm{TAU}}}$ hybrid model, where $\sigma_D^{\mathrm{ZAS}} : D \times D \to D^{\mathrm{op}}$ defined as $\sigma_D^{\mathrm{ZAS}}(t, u) = -(t + u)$, is the bi-affine homomorphism corresponding to the ZAS correlation (Section 3.5.3). The protocol description and proof can be found in Figure 10 and Appendix E, respectively.

Alternate Summation Functionality $\mathcal{F}_{D,n}^{\mathrm{altsum}}$

Inputs: Alice has inputs $(x_1, \ldots, x_n) \in D^n$ and Bob has inputs $(y_1, \ldots, y_n) \in D^n$.
Output: Bob receives output $\sum_{i=1}^{n}(x_i + y_i)$.

Theorem 2. *The protocol in Figure 10 is a UC-secure protocol for the Alternate Summation functionality $\mathcal{F}_{D,n}^{\mathrm{altsum}}$ over a non-abelian group D, in the $\mathcal{F}_{\sigma_D^{\mathrm{ZAS}}|_{\mathrm{TAU}}}$ hybrid model.*

Protocols for error-randomization in the $\widehat{\mathcal{F}}_\sigma$ hybrid model

We present 3 error randomization protocols, for $\sigma : Q \to H$ w.r.t $T, U \subseteq Q$:

1. **Modules:** R is a ring and H is a right module of R. $\sigma : H \times R \to H$ is the scalar multiplication operation $\cdot$ of the module. $T = H \times \{0\}$ and $U = \{0\} \times H$.
   Security Condition: $\text{minimg}_R(H)$ is super-polynomial in λ.
   - **Invocation of $\widehat{\mathcal{F}}_\sigma$:** Alice gets (t, a) and Bob gets (u, b) from $\widehat{\mathcal{F}}_\sigma$.
   - Bob samples $r \leftarrow \text{units}(R)$ and sends it to Alice.
   - Alice outputs $(t_1, a_1) = (t \cdot r, a \cdot r)$ and $(t_2, a_2) = (t, a)$. Bob outputs $(u_1, b_1) = (u, b \cdot r)$ and $(u_2, b_2) = (u, b)$.
2. **Semi-abelian Bi-Affine Correlations:** Groups $(Q, +), (H, \oplus)$ with a bi-affine homomorphism $\sigma : Q \to H$ w.r.t $T, U \subseteq Q$ where H is abelian.
   Security Condition: $\text{minord}(H)$ is super-polynomial in λ.
   - **Invocation of $\widehat{\mathcal{F}}_\sigma$:** Alice gets (t, a) and Bob gets (u, b) from $\widehat{\mathcal{F}}_\sigma$.
   - Alice samples $k \leftarrow \mathbb{Z}_{\text{minord}(H)}$ and sends k to Bob.
   - Alice outputs $(t_1, a_1) = (kt, ka)$, $(t_2, a_2) = (t, a)$ and Bob outputs $(u_1, b_1) = (u, kb \oplus -(k-1)\sigma(u))$, $(u_2, b_2) = (u, b)$.
3. **Surjective Bi-Affine Correlations:** Groups $(Q, +), (H, \oplus)$ with a surjective bi-affine homomorphism $\sigma : Q \to H$ w.r.t $T, U \subseteq Q$.
   Security Condition: $\text{minorbit}(H)$ is super-polynomial in λ.
   - **Invocation of $\widehat{\mathcal{F}}_\sigma$:** Alice gets $(\tilde{t}, \tilde{a})$ and Bob gets $(\tilde{u}, \tilde{b})$ from $\widehat{\mathcal{F}}_\sigma$.
   - Alice and Bob invoke $\mathsf{Comp}_{\sigma|_U}^{(\tilde{t},\tilde{a}),(\tilde{u},\tilde{b})}$ with Bob using a freshly sampled $u \leftarrow U$ as his input. Let Alice's outputs be (t_1, a_1) and Bob's be (u_1, b_1).
   - Alice outputs (t_1, a_1) and $(t_2, a_2) := (\tilde{t}, \tilde{a})$ and Bob outputs (u_1, b_1) and $(u_2, b_2) := (\tilde{u}, \tilde{b})$

Figure 9: Error randomization protocols

6.2 2-Party Secure Computation

In this section, we present applications of protocols from Section 5 in the context of secure two party computation. We put forth a *mixed-group circuit model* for functions, and present protocols for them. Then we present two comparable, but different flavors of perfectly secure protocols ("GMW-style" and "FSS-style").

Mixed-Group Circuit Model We define an algebraic circuit model in which different wires may belong to *different groups*. The computation gates can be of the following kinds:

1. Group operations: Addition gates $(+) : G \times G \to G$ and Inverse gates $(-) : G \to G$
2. Homomorphism gates $\phi : G_1 \to G_2$ which apply a given homomorphism ϕ on the input wire.
3. Bi-Affine Homomorphism gates $g_\sigma : T \times U \to H$ such that $g_\sigma(t, u) = \sigma(t + u)$ where $\sigma : Q \to H$ is a bi-affine homomorphism with respect to $T, U \leqslant Q$.
4. Direct product gates $(\otimes) : G_1 \times G_2 \to G_3$ where $G_3 = G_1 \times G_2$ such that $a \otimes b = (a, b)$.

Protocol for $\mathcal{F}_{D,n}^{\text{altsum}}$ in the $\mathcal{F}_{\sigma_D^{\text{ZAS}}|\text{TAU}}$-hybrid model

- **Inputs:** Alice's input is $(x_1, x_2, \ldots, x_n)$ and Bob's is $(y_1, y_2, \ldots, y_n)$.
- **Alice's Randomness:** Alice samples $\{r_i, s_i\}_{i\in[n-1]}$ i.i.d. uniformly from D, but with $r_1 = s_n = 0$.
- **Invocation of $\mathcal{F}_{\sigma|\text{TAU}}$:** Alice and Bob invoke $n-1$ instances of $\mathcal{F}_{\sigma_D^{\text{ZAS}}|\text{TAU}}$ (in parallel). In the i^{th} instance, Alice inputs $(-s_i, r_{i+1})$ and Bob inputs (y_i), and Bob receives $y'_i := -(-s_i + y_i + r_{i+1})$ as the output.
- **Alice $\to$ Bob:** Alice sends $\{x'_i\}_{i\in[n]}$ to Bob where $x'_i := -r_i + x_i + s_i$ for each $i \in [n]$.
- **Output:** To evaluate the alternating sum function, Bob simply computes $(\sum_{i\in[n-1]}(x'_i - y'_i)) + x'_n + y_n$.

Figure 10: A UC-secure protocol for the Alternate Summation functionality over non-abelian groups. Note that the roles of Alice and Bob could also be reversed with Alice receiving the output.

In a black box group model, only the "wiring" of the circuit and the type of the gates are specified, and the actual groups associated with each wire is left unspecified (beyond the restrictions implied by the wiring and the gate types).

In both the protocols below, the computation proceeds by evaluating the gates in a topologically sorted order. The wire values will either be kept additively secret-shared in the corresponding group (in the first protocol) or kept masked with a pad chosen by a dealer in a pre-processing phase (in the second protocol). In both cases, homomorphism and direct product gates are "free" and can be applied locally. Addition and inverse also come for free where the group is abelian but is non-trivial otherwise.

2PC Given Random Correlations. Alice and Bob evaluate the circuit layer-wise, while maintaining the invariant that every wire is secret shared. As we shall see below, evaluating each layer takes at most two rounds. We focus on showing how Alice and Bob can evaluate Bi-Affine Homomorphism, Inverse and Addition gates given an additive secret sharing of the input wires to then obtain an additive secret sharing of the output wire. Details of these protocols can be found in Figure 11.

In evaluating an addition gate, Alice and Bob hold shares (x_a, y_a) and (x_b, y_b) respectively, and would like shares of $(x_a + x_b) + (y_a + y_b)$. Let $\sigma_H^{\text{ZAS}} : H \times H \to H^{\text{op}}$ be as defined in Section 3.5.3, so that ZAS corresponds to $\mathsf{BA}_{\sigma_H^{\text{ZAS}}}$ (i.e., $\sigma_H^{\text{ZAS}}(t, u) = -(t + u)$). Addition can now be achieved by invoking $\mathcal{F}_{\sigma_H^{\text{ZAS}}|\text{TU}}$: Alice and Bob send $-y_a$ and $-x_b$, respectively to $\mathcal{F}_{\sigma_H^{\text{ZAS}}|\text{TU}}$. They receive y'_a and x'_b such that $y'_a + x'_b = x_b + y_a$. Alice and Bob then output $x_a + y'_a$ and $x'_b + y_b$, respectively.

To evaluate the inverse gate, observe that Alice and Bob hold x_a, x_b and want to obtain y_a, y_b such that $y_a + y_b = -(x_a + x_b)$, which is exactly the ZAS correlation. Thus, by invoking $\mathcal{F}_{\sigma_H^{\text{ZAS}}|\text{TU}}$ on inputs x_a and x_b, they obtain desired outputs.

When evaluating the bi-affine homomorphism gate, the idea is to decompose the function into pieces that can either be locally evaluated or terms for which a secret sharing can be obtained by invoking the conditional sampling functionality $\mathcal{F}_{\sigma|\text{TU}}$. At the end of this, Alice and Bob are left with an alternate sum comprising of four terms. This can be converted into a secret sharing of two terms by invoking $\mathcal{F}_{\sigma_D^{\text{ZAS}}|\text{TU}}$ similar to the case of addition gates. [7]

To evaluate a single bi-affine gate, we require two rounds of simultaneous messages, whereas

[7] When the group of the output wire is abelian, a weaker correlation $\mathsf{BA}_{\sigma\langle 2\rangle}$ can be used instead of two instances

the addition and inverse gates, only require one round of simultaneous messages. However, we note that n rounds of simultaneous message exchanges can be converted to $n+1$ rounds with only one party sending a message in each round. Thus, a circuit with n layers would only need $2n+1$ rounds where a single party sends messages.

Protocols for evaluating computation gates

1. **Bi-Affine Homomorphism gate** g_σ
   - **Inputs:** Alice's input is (t_a, u_a) and Bob's input is (t_b, u_b)
   - Alice and Bob invoke $\mathcal{F}_{\sigma|\text{TU}}$ and $\mathcal{F}_{\sigma|\text{UT}}$ on inputs t_a, u_b and t_b, u_a to obtain α_1, β_1 and α_2, β_2 such that $\sigma(t_b + u_a) = \alpha_2 \oplus \beta_2$ and $\sigma(t_a + u_b) = \alpha_1 \oplus \beta_1$.
   - Alice and Bob invoke $\mathcal{F}_{\sigma_H^{\text{ZAS}}|\text{TU}}$ where Alice's input is $-(-\sigma(t_a) \oplus \alpha_1)$ and Bob's input is $-(\beta_2 \oplus -\sigma(t_b) \oplus \sigma(0))$ to obtain outputs α_3 and β_3 respectively.
   - **Outputs:** Alice outputs $h_a = \sigma(t_a + u_a) \oplus -\sigma(u_a) \oplus \alpha_2 \oplus \alpha_3$ and Bob outputs $h_b = \beta_3 \oplus \beta_1 \oplus -\sigma(u_b) \oplus \sigma(t_b + u_b)$.
2. **Inverse gates**
   - **Inputs:** Alice holds x_a and Bob holds x_b.
   - Alice and Bob sample random elements r_a and r_b from G. respectively.
   - Alice and Bob invoke $\mathcal{F}_{\sigma_H^{\text{ZAS}}|\text{TU}}$ where Alice's input is x_a and Bob's input is x_b and obtain outputs y_a and y_b respectively.
   - **Outputs:** Alice outputs y_a and Bob outputs y_b.
3. **Addition gates**
   - **Inputs:** Alice has input (x_a, y_a) and Bob has input (x_b, y_b)
   - Alice and Bob invoke $\mathcal{F}_{\sigma_H^{\text{ZAS}}|\text{TU}}$ with input $-y_a$ and $-x_b$, respectively and obtain y'_a and x'_b as output.
   - **Outputs:** Alice outputs $x_a + y'_a$ and Bob outputs $x'_b + y_b$.

Figure 11: Secure protocols for evaluation of computation gates in when wire values are additively secret shared.

2PC in the Pre-Processing Model. Recently, Boyle et. al. [5] proposed a protocol for secure computation of circuits with bi-linear gates with the assistance of a trusted dealer who provides circuit dependent correlations. We now show how an analogous evaluation can be done for circuits using bi-affine homomorphism gates over non-abelian groups.

We first define the three party functionality $\mathcal{G}_{\sigma|\text{TAU}}$ and give our protocol in the $\mathcal{G}_{\sigma|\text{TAU}}$ hybrid. In Appendix F we show how to implement $\mathcal{G}_{\sigma|\text{TAU}}$.

Conditional Sampling Functionality $\mathcal{G}_{\sigma|\text{TAU}}$
(where $\sigma : Q \to H$ and $T, U \leqslant Q$)

Inputs: Alice, Bob have common input $(t_1, u_1) \in T \times U$ and Carol has input $(t_2, u_2, b) \in T \times U \times H$.
Output: a to Alice, Bob such that $\sigma(t_1 + t_2 + u_1 + u_2) = a \oplus b$.

of BA_σ. This is akin to using a BMT correlation for evaluating multiplication gates instead of two OLE correlations.

All wire values in the circuit are public but masked by a random value which is sampled by a dealer. Evaluation is done in a topologically ordered manner, where at each gate, the input wires are 'unmasked', the gate is evaluated and the output wire is 'masked' again, in a secure manner. Thus, maintaining the invariant that all wires are public. To evaluate a bi-affine homomorphism gate Alice and Bob have a common input (t, u) where the dealer has chosen random masks[8] (t_r, u_r) for the input wire and h_r for the input wire of the next gate corresponding to the output wire of this gate. Alice-Bob and Dealer(Charlie) invoke $\mathcal{G}_{\sigma|\text{TAU}}$, where the common input of Alice and Bob is (t, u) and the Dealer's input is $(-t_r, -u_r, h_r)$ such that Alice-Bob receive $h = \sigma(t+-t_r+u+-u_r) \oplus -h_r$. While it looks like each gate requires interaction between the dealer and parties, in our implementation (Figure 13), the only communication from dealer to the parties is an additive secret sharing of h_r which is the mask on the input wire to the next gate. This can be sent to the parties all at once at the beginning of the protocol after which the dealer can go offline.

Completeness of ZAS for 2PC over Black-Box Groups As a consequence of the 2-party secure computation protocol we see that the ZAS correlation is complete for 2-party secure computation in the black-box group setting. These functions are represented as circuits in which all the wires correspond to group variables, the gates carry out the group operation, and the inputs are group elements distributed between Alice and Bob. Any circuit over the group $(D, +)$ is written in terms of the addition and inverse gates. From Figure 11, both these operation can be performed given ZAS correlations. Thus, any function over black-box groups can be evaluated using only ZAS correlations, hence making the correlation complete.

6.3 Single-Server Commodity-Based Cryptography

Commodity-based cryptography was introduced by Beaver in [2]. The setup consists of at least two (or more) clients and at least one server. The clients use these servers to sample correlations that will then allow them to perform secure computation. Beaver [2] showed how to sample an Oblivious Transfer correlation in the commodity model where the servers had an honest majority and the adversary was semi-honest. The only communication allowed between clients and servers is a two round protocol where clients make a request in the first round and servers respond in the second round. Recently, this model was revisited by Damgård et al. [12] and Smart et al. [27] where they showed how to sample OLE and BMT correlations in the commodity model and allowed active corruption of servers and parties.

In this work, we focus on a different adversarial model with a single actively corrupt server that does not collude with clients, with the goal of sampling bi-affine correlations. This has been considered before in the context of specific correlations like BMT, squaring tuples etc., [14].

Sampling Bi-affine Correlations. Using our results from Section 5.4 we show how to sample a much more general class of bi-affine correlations in the single-server commodity model and achieve statistical security with abort. For arbitrary bi-affine correlations, Alice and Bob invoke TRSamp_σ with the server realizing the functionality $\widehat{\mathcal{F}}_\sigma$. The communication required to sample one bi-affine correlation is $\omega(\log \lambda)$ where λ is the security parameter. However, when the bi-affine correlation satisfies one of the three different structural properties discussed in Section 5.4, Alice and Bob can invoke $\mathsf{altTRSamp}_\sigma$. In this case, the communication per bi-affine correlation generated is a constant

[8] Without loss of generality we assume all masks are on the right side of the underlying secret.

number of field elements. We note that the communication in our protocols is identical to that of [14] for the specific correlations considered.

Re-randomization for Forward-Security. The $\mathsf{Comp}_{\sigma|\text{TAU}}$ protocol can be used as a tool for re-randomization of correlations obtained from a server. Even if the server colludes with one of the parties in the future (after the rerandomization protocol has been invoked and its state erased), the other party is assured of security. It also remains secure if one of the parties (not colluding with the server) is corrupt during the rerandomization phase itself (upto letting that party choose its own side of the correlation).

7 Group Structure of OLE

While Lemma 3 gives an explicit group $\mathbb{K}_A$ such that OLE over a ring A is a group correlation of the form $\text{GC}^{\mathbb{K}_A,V}$, where $V = A \times \{0\}$, the group operation in $\mathbb{K}_A$, namely $(t,h)\odot(t',h') = (t+t', h+h'-tt')$ can be quite complex, as it involves multiplication in A. We now present non-obvious group isomorphisms between $\mathbb{K}_A$ and standard groups. Firstly, for commutative rings A which have an element $\frac{1}{2}$, we show that $\mathbb{K}_A$ is isomorphic to $\mathbb{G}_A \times \mathbb{G}_A$, where $\mathbb{G}_A$ is the abelian group corresponding to the addition operation in A. In particular, for odd primes p, $\mathbb{K}_{\mathbb{F}_{p^n}}$ is isomorphic to the group $\mathbb{Z}_p^{2n}$ (since $\mathbb{G}_{\mathbb{F}_{p^n}}$ is simply $\mathbb{Z}_p^n$). This leaves out the important case of $\mathbb{F}_{2^n}$; for this case we show that $\mathbb{K}_{\mathbb{F}_{2^n}}$ is isomorphic to the group $\mathbb{Z}_4^n$. Note that the $\mathbb{F}_{2^n}$ case does not follow the same pattern as $\mathbb{F}_{p^n}$. It is isomorphic to the group $\mathbb{Z}_{2^2}^n$ instead of Z_2^{2n} unlike one might expect, thus exposing a fundamental structural difference between OLE over $\mathbb{F}_{2^n}$ and $\mathbb{F}_{p^n}$.

7.1 OLE over a ring with an element $\frac{1}{2}$

Given a ring A, recall that $\mathbb{G}_A$ is an abelian group with same set of elements as A with its group operation being the addition operation in A.

Lemma 16. *Suppose A is a commutative ring with an element η such that $\eta+\eta = 1$. Then there is a group isomorphism $\mathbb{K}_A \to \mathbb{G}_A \times \mathbb{G}_A$, which maps $A \times \{0\}$ to $S = \{(x, \eta x^2) | x \in A\}$.*

Proof: The group isomorphism $\boldsymbol{\phi}$ is such that $\boldsymbol{\phi}(x,y) = (x, y+\eta x^2)$. To see that this is a homomorphism, note that

$$\begin{aligned}
\boldsymbol{\phi}((x,y)\odot(x',y')) &= \boldsymbol{\phi}(x+x', y+y'-xx') \\
&= (x+x', y+y'-xx'+\eta(x+x')^2) \\
&= (x+x', y+y'+\eta x^2+\eta x'^2) \qquad (\text{since } \eta+\eta=1) \\
&= \boldsymbol{\phi}(x,y) + \boldsymbol{\phi}(x',y').
\end{aligned}$$

$\boldsymbol{\phi}$ is injective as its kernel is $\{(0,0)\}$: $\boldsymbol{\phi}(x,y) = (0,0) \Rightarrow (x, y+\eta x^2) = (0,0) \Rightarrow (x,y) = (0,0)$. Then, since $|\mathbb{K}_A| = |\mathbb{G}_A \times \mathbb{G}_A|$, $\boldsymbol{\phi}$ is an isomorphism.

Also, clearly it maps elements of the form $(x,0)$ to $(x, \eta x^2) \in S$. Since $\boldsymbol{\phi}$ is a bijection, and $|S| = |A|$, the image of $A \times \{0\}$ under $\boldsymbol{\phi}$ is exactly S. □

7.2 OLE over $\mathbb{F}_{2^n}$

We shall establish an isomorphism between the groups $\mathbb{K}_{\mathbb{F}_{2^n}}$ and $\mathbb{Z}_4^n$. First, we shall setup some notation for $\mathbb{F}_{2^n}$ and $\mathbb{Z}_4^n$.

We fix a representation of the elements of $\mathbb{F}_{2^n}$ as $\{0,1\}^n$, using an arbitrary *basis*, $\xi^{(0)}, \cdots, \xi^{(n-1)}$, where $\xi^{(0)} = 1$, the multiplicative identity. Then, $x \in \{0,1\}^n$ is identified with the element $\sum_{i=0}^{n-1} x_i \cdot \xi^{(i)}$ in $\mathbb{F}_{2^n}$ (where $x_i \in \{0,1\}$ is interpreted as the corresponding field element). We define $(x)_i$ as the field element obtained by zeroing out all coordinates greater than or equal to i. That is,

$$(x)_i = \sum_{j=0}^{i-1} x_j \cdot \xi^{(j)}.$$

Elements in $\mathbb{Z}_4^n$ are naturally represented as n-ary vectors with elements in $\{0,1,2,3\}$. Let $\lfloor x \rceil$ denote the embedding from $\mathbb{F}_{2^n}$ to $\mathbb{Z}_4^n$, obtained by interpreting $x \in \{0,1\}^n$ as $x \in \{0,1,2,3\}^n$. Further, for a single bit x_i, we let $[x_i]$ denote this bit as an element in $\mathbb{Z}_4$.

Note that in $\mathbb{F}_{2^n}$, every element has a unique square root.[9] We use it to define $\boldsymbol{f} : \mathbb{F}_{2^n} \to \mathbb{Z}_4^n$ and $\boldsymbol{g} : \mathbb{F}_{2^n} \to \mathbb{Z}_4^n$ as follows (using $\cdot$ to indicate multiplication of a vector in $\mathbb{Z}_4^n$ with a scalar in $\mathbb{Z}_4$):

$$\begin{aligned} \boldsymbol{f}(x) &= 2 \cdot \lfloor \sqrt{x} \rceil \\ \boldsymbol{g}(x) &= \lfloor x \rceil - \boldsymbol{f}\Big(\sum_{i : x_i = 1} \xi^{(i)} (x)_i \Big) \end{aligned} \tag{8}$$

We note that $\boldsymbol{f}(0) = \boldsymbol{g}(0) = 0$, and further, $\forall x \in \mathbb{F}_{2^n}$, $2 \cdot \boldsymbol{f}(x) = 0$. Also, $\boldsymbol{g}(\xi^{(i)}) = \lfloor \xi^{(i)} \rceil$ (since $(\xi^{(i)})_i = 0$), and so, $\lfloor x \rceil = \sum_{i=0}^{n-1} [x_i] \, \boldsymbol{g}(\xi^{(i)})$.

Lemma 17. *There is a group isomorphism $\boldsymbol{\phi} : \mathbb{K}_{\mathbb{F}_{2^n}} \to \mathbb{Z}_4^n$, which maps V to $S := \{\boldsymbol{g}(x) \mid x \in \mathbb{F}_{2^n}\}$.*

Proof: Recall that the group $\mathbb{K}_{\mathbb{F}_{2^n}}$ is of the form $(\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}, \odot)$ where $(x,y) \odot (x',y') = (x + x', y + y' + xx')$. Here, we have written subtraction in $\mathbb{F}_{2^n}$ as addition; the product xx' refers to multiplication in $\mathbb{F}_{2^n}$. The claimed group isomorphism is given by

$$\boldsymbol{\phi}(x,y) = \boldsymbol{g}(x) + \boldsymbol{f}(y)$$

where $\boldsymbol{f}$ and $\boldsymbol{g}$ are as defined in (8). Below, we prove the lemma by Claim 3 and Claim 4. Towards this, first we prove the following claims about $\boldsymbol{f}$ and $\boldsymbol{g}$.

Claim 1. *For all $x, y \in \mathbb{F}_{2^n}$, $\boldsymbol{f}(x+y) = \boldsymbol{f}(x) + \boldsymbol{f}(y)$.*

Proof: This follows from the facts that in $\mathbb{F}_{2^n}$, $\sqrt{x+y} = \sqrt{x} + \sqrt{y}$ (because $z + z = 0$, and hence $(\sqrt{x} + \sqrt{y})^2 = x + y + \sqrt{xy} + \sqrt{xy} = x + y$), and the map $x \mapsto 2 \cdot [x]$ is a group homomorphism from $\mathbb{F}_{2^n}$ to $\mathbb{Z}_4^n$. □

Claim 2. *For all $x, y \in \mathbb{F}_{2^n}$, $\boldsymbol{g}(x) + \boldsymbol{g}(y) - \boldsymbol{g}(x+y) = \boldsymbol{f}(xy)$.*

[9] For $a, b \in \mathbb{F}_{2^n}$, we have $a^2 = b^2 \Rightarrow (a+b)(a-b) = 0$. In $\mathbb{F}_{2^n}$, $a + b = a - b$. Also, this being a field, we have $(a-b)^2 = 0 \Rightarrow a = b$. Thus squaring is a permutation in $\mathbb{F}_{2^n}$, and square root is its inverse.

Proof: Let $z = x+y$. We shall show that $\boldsymbol{g}(z) = \boldsymbol{g}(x)+\boldsymbol{g}(y)-\boldsymbol{f}(xy)$. Note that $(z)_i = (x)_i+(y)_i$ (all operations being in the field $\mathbb{F}_{2^n}$), and $[z_i] = [x_i]+[y_i]-2\,[x_i y_i]$ (the additions and the multiplication by 2 being in $\mathbb{Z}_4$). Then we have,

$$
\begin{aligned}
\boldsymbol{g}(z) &= \big[z\big] - \boldsymbol{f}\Big(\sum_{i:z_i=1} \xi^{(i)}(z)_i\Big) = \sum_{i=0}^{n-1} [z_i] \cdot \big(\boldsymbol{g}(\xi^{(i)}) - \boldsymbol{f}(\xi^{(i)}(z)_i)\big) \\
&\overset{(a)}{=} \sum_{i=0}^{n-1} \big([x_i] + [y_i] - 2\,[x_i y_i]\big) \cdot \big(\boldsymbol{g}(\xi^{(i)}) - \boldsymbol{f}(\xi^{(i)}(x)_i) - \boldsymbol{f}(\xi^{(i)}(y)_i)\big) \\
&\overset{(b)}{=} \boldsymbol{g}(x) + \boldsymbol{g}(y) - \sum_{i=0}^{n-1} \Big([x_i] \cdot \boldsymbol{f}(\xi^{(i)}(y)_i) + [y_i] \cdot \boldsymbol{f}(\xi^{(i)}(x)_i) + 2\,[x_i y_i] \cdot \boldsymbol{g}(\xi^{(i)})\Big) \\
&\overset{(c)}{=} \boldsymbol{g}(x) + \boldsymbol{g}(y) - \sum_{i=0}^{n-1} \Big([x_i] \cdot \boldsymbol{f}(\xi^{(i)}(y)_i) + [y_i] \cdot \boldsymbol{f}(\xi^{(i)}(x)_i) + [x_i y_i] \cdot \boldsymbol{f}({\xi^{(i)}}^2)\Big) \\
&\overset{(d)}{=} \boldsymbol{g}(x) + \boldsymbol{g}(y) - \boldsymbol{f}\left(\sum_{i=0}^{n-1} x_i \cdot \xi^{(i)}(y)_i + y_i \cdot \xi^{(i)}(x)_i + x_i y_i \cdot {\xi^{(i)}}^2\right) \\
&= \boldsymbol{g}(x) + \boldsymbol{g}(y) - \boldsymbol{f}\left(\sum_{i=0}^{n-1} x_i \cdot \xi^{(i)}\Big(\sum_{j=0}^{i-1} y_j \cdot \xi^{(j)}\Big) + y_i \cdot \xi^{(i)}\Big(\sum_{j=0}^{i-1} x_j \cdot \xi^{(j)}\Big) + x_i y_i \cdot {\xi^{(i)}}^2\right) \\
&\overset{(e)}{=} \boldsymbol{g}(x) + \boldsymbol{g}(y) - \boldsymbol{f}(xy),
\end{aligned}
$$

where, we used Claim 1 in steps (a) and (d); step (b) used the fact that $2\boldsymbol{f}(\alpha) = 0$; in step (c), we used the fact that $\boldsymbol{f}({\xi^{(i)}}^2) = 2 \cdot \left[\sqrt{{\xi^{(i)}}^2}\right] = 2\big[\xi^{(i)}\big] = 2\boldsymbol{g}(\xi^{(i)})$; for step (e), we used the expansion of x and y as $x = \sum_{i=0}^{n-1} x_i \cdot \xi^{(i)}$, $y = \sum_{i=0}^{n-1} y_i \cdot \xi^{(i)}$. □

Now we are ready to prove the following claims, which complete the proof of the theorem.

Claim 3. *$\boldsymbol{\phi}$ is a group isomorphism from $\mathbb{K}_{\mathbb{F}_{2^n}}$ to $\mathbb{Z}_4^n$.*

Proof: Firstly, we note that it is a group homomorphism:

$$
\begin{aligned}
\boldsymbol{\phi}((x,y) \odot (x',y')) &= \boldsymbol{\phi}(x+x', y+y'+xx') \\
&= \boldsymbol{g}(x+x') + \boldsymbol{f}(y+y'+xx') \\
&= \boldsymbol{g}(x) + \boldsymbol{g}(x') - \boldsymbol{f}(xx') + \boldsymbol{f}(y+y'+xx') \text{[by Claim 2]} \\
&= \boldsymbol{g}(x) + \boldsymbol{f}(y) + \boldsymbol{g}(x') + \boldsymbol{f}(y') \text{[by Claim 1]} \\
&= \boldsymbol{\phi}(x,y) + \boldsymbol{\phi}(x',y').
\end{aligned}
$$

To see that this homomorphism is injective, we shall verify that its kernel consists only of $\{(0,0)\}$. If $\boldsymbol{g}(x) + \boldsymbol{f}(y) = 0$, then we have $\big[x\big] + \boldsymbol{f}(w) = 0$ for some w (using the definition of $\boldsymbol{g}$ and the homomorphism of $\boldsymbol{f}$). Considering this equation modulo 2 (coordinate-wise), we get $x = 0$ (since $\boldsymbol{f}(w)$ is 0 modulo 2 for any w). Since $\boldsymbol{g}(0) = 0$, it implies $\boldsymbol{f}(y) = 0$, and hence $y = 0$. Thus, indeed, $\boldsymbol{\phi}(x,y) = 0$ iff $(x,y) = (0,0)$.

Finally, since $|\mathbb{K}_{\mathbb{F}_{2^n}}| = (2^n)^2 = |\mathbb{Z}_4^n|$, this injective homomorphism is an isomorphism. □

Claim 4. $(x, y) \in V$ *iff* $\boldsymbol{\phi}(x, y) \in S$.

Proof: We have $(x, y) \in V \Rightarrow y = 0 \Rightarrow \boldsymbol{\phi}(x, y) = \boldsymbol{g}(x) \Rightarrow \boldsymbol{\phi}(x, y) \in S$. Since $\boldsymbol{\phi}$ is a bijection, this implies that $|S| \geq |V|$. On the other hand, $|S| \leq 2^n = |V|$. Hence, $|S| = |V|$ and $(x, y) \in V \Leftrightarrow \boldsymbol{\phi}(x, y) \in S$. □

This completes the proof of Lemma 17. □

Theorem 3. $\text{OLE}_{\mathbb{F}_{2^n}}$ *is a group correlation of the form* $\text{GC}^{\mathbb{Z}_4^n, S}$*, where* $S = \{\boldsymbol{g}(x) \mid x \in \mathbb{F}_{2^n}\}$.

Proof: By Lemma 3, $\text{OLE}_{\mathbb{F}_{2^n}}$ is a group correlation of the form $\text{GC}^{\mathbb{K}_{\mathbb{F}_{2^n}}, V}$, where $V = \mathbb{F}_{2^n} \times \{0\}$. The theorem follows from Lemma 17, which shows a group isomorphism $\phi : \mathbb{K}_{\mathbb{F}_{2^n}} \to \mathbb{Z}_4^n$, which maps V to S. □

References

[1] Edith Adan-Bante and John M Harris. "On conjugacy classes of GL (n, q) and SL (n, q)". In: *arXiv preprint arXiv:0904.2152* (2009).

[2] Donald Beaver. "Commodity-based cryptography". In: *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*. 1997, pp. 446–455.

[3] Donald Beaver. "Efficient multiparty protocols using circuit randomization". In: *Annual International Cryptology Conference*. Springer. 1991, pp. 420–432.

[4] Donald Beaver. "Foundations of Secure Interactive Computing". In: 1991, pp. 377–391.

[5] Elette Boyle, Niv Gilboa, and Yuval Ishai. "Secure computation with preprocessing via function secret sharing". In: *Theory of Cryptography Conference*. Springer. 2019, pp. 341–371.

[6] Elette Boyle et al. *Correlated Pseudorandom Functions from Variable-Density LPN*. Cryptology ePrint Archive, Report 2020/1417. 2020.

[7] Elette Boyle et al. "Efficient Pseudorandom Correlation Generators: Silent OT Extension and More". In: *CRYPTO*. Vol. 11694. Springer, 2019, pp. 489–518.

[8] Elette Boyle et al. "Efficient Pseudorandom Correlation Generators from Ring-LPN". In: *CRYPTO*. Springer. 2020, pp. 387–416.

[9] Elette Boyle et al. "Homomorphic secret sharing: optimizations and applications". In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. 2017, pp. 2105–2122.

[10] Gil Cohen et al. "Efficient multiparty protocols via log-depth threshold formulae". In: *Annual Cryptology Conference*. Springer. 2013, pp. 185–202.

[11] Ronald Cramer et al. "Efficient Multi-party Computation over Rings". In: *EUROCRYPT*. 2003, pp. 596–613.

[12] Ivan Damgård et al. "Commodity-based 2PC for arithmetic circuits". In: *IMA International Conference on Cryptography and Coding*. Springer. 2019, pp. 154–177.

[13] Ivan Damgård et al. "Multiparty computation from somewhat homomorphic encryption". In: *Annual Cryptology Conference*. Springer. 2012, pp. 643–662.

[14] Ivan Damgård et al. “Practical covertly secure MPC for dishonest majority–or: breaking the SPDZ limits”. In: *European Symposium on Research in Computer Security*. Springer. 2013, pp. 1–18.

[15] Daniel Demmler, Thomas Schneider, and Michael Zohner. “ABY - A Framework for Efficient Mixed-Protocol Secure Two-Party Computation”. In: *NDSS*. The Internet Society, 2015.

[16] Yvo Desmedt, Josef Pieprzyk, and Ron Steinfeld. “Active security in multiparty computation over black-box groups”. In: *International Conference on Security and Cryptography for Networks*. Springer. 2012, pp. 503–521.

[17] Yvo Desmedt et al. “Graph Coloring Applied to Secure Computation in Non-Abelian Groups”. In: *J. Cryptology* 25.4 (2012), pp. 557–600.

[18] P. Gács and J. Körner. “Common information is far less than mutual information”. In: *Problems of Control and Information Theory* 2.2 (1973), pp. 149–162.

[19] Niv Gilboa. “Two Party RSA Key Generation”. In: *CRYPTO*. 1999, pp. 116–129.

[20] Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. “Founding Cryptography on Oblivious Transfer - Efficiently”. In: *CRYPTO*. 2008, pp. 572–591.

[21] Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. “Secure Arithmetic Computation with No Honest Majority”. In: *TCC*. 2009, pp. 294–314.

[22] Joe Kilian. “Founding Cryptography on Oblivious Transfer”. In: *STOC*. 1988, pp. 20–31.

[23] Joe Kilian. “More general completeness theorems for secure two-party computation”. In: pp. 316–324.

[24] Hemanta Maji, Manoj Prabhakaran, and Mike Rosulek. “A Unified Characterization of Completeness and Triviality for Secure Function Evaluation”. In: *INDOCRYPT*. 2012, pp. 40–59.

[25] Vinod M Prabhakaran and Manoj M Prabhakaran. “Assisted common information with an application to secure two-party sampling”. In: *IEEE Transactions on Information Theory* 60.6 (2014), pp. 3413–3434.

[26] Claude Shannon. “A Mathematical Theory of Communications”. In: *Bell System Technical Journal* 27 (July 1948), pp. 379–423.

[27] Nigel P Smart and Titouan Tanguy. “TaaS: Commodity MPC via Triples-as-a-Service”. In: *Proceedings of the 2019 ACM SIGSAC Conference on Cloud Computing Security Workshop*. 2019, pp. 105–116.

[28] A. D. Wyner. “The common information of two dependent random variables”. In: *IEEE Transactions on Information Theory* 21.2 (1975), pp. 163–179.

Appendix

A More Examples

Smallest Non-Trivial Group Correlation. The smallest non-trivial group correlation is what we call the *binary mutual erasure* (BME) correlation, in which a uniformly random "message" bit b is sampled to be given to both parties, but at most one party's message is replaced with $\perp$. For each choice of the message bit b, the three possibilities (b, b), $(b, \perp)$ and $(\perp, b)$ are equally likely. It can be seen that BME is a group correlation of the form $\mathrm{GC}^{\mathbb{Z}_3,\{0,1\}}$, using the maps $\alpha(0) = 0$, $\alpha(1) = 1$ and $\alpha(\perp) = 2$ and $\beta(\perp) = 0$, $\beta(0) = 1$ and $\beta(1) = 2$.

We remark that a group correlation of the form $\mathrm{GC}^{\mathbb{Z}_m,\{0,1\}}$ can be associated with the so-called "noisy typewriter" channel over $\mathbb{Z}_m$, which maps an input x to a uniform element in $\{x, x+1\}$ (or, upto relabeling, $\{-x, -x+1\}$).

OLE. In Figure 12, we draw the bi-partite graph corresponding to $\mathrm{OLE}_{\mathbb{F}_{2^n}}$ along with the corresponding labelling of nodes to show that it is a group correlation of the form $\mathrm{GC}^{\mathbb{Z}_4^2,S}$, where $S = \{(0,0),(0,1),(1,0),(3,3)\}$.

Vector OLE. An n-dimensional *vector OLE correlation* over a ring A is a flat correlation over $A^{2n} \times A^{n+1}$ with support:

$$\mathrm{OLE}_A^n := \{\big((\boldsymbol{p}, \boldsymbol{a}), (q, \boldsymbol{b})\big) \mid \boldsymbol{a}, \boldsymbol{p}, \boldsymbol{b} \in A^n, q \in A, \boldsymbol{a} + \boldsymbol{b} = \boldsymbol{p}q\}$$

When $A = \mathbb{Z}_2$, it is called Oblivious Transfer (or String Oblivious Transfer, for $n > 1$). So we shall write OT instead of $\mathrm{OLE}_{\mathbb{Z}_2}$ and OT^n instead of $\mathrm{OLE}_{\mathbb{Z}_2}^n$. Note that OLE_A^n is isomorphic to $\mathsf{BA}_{\sigma^{(n)}}$ where $\sigma : A \times A \to A$ w.r.t subgroups $A \times \{0\}$ and $\{0\} \times A$ is $\sigma(t, u) = tu$. From Lemma 2, OLE_A^n is a subgroups correlation embedded in a group correlation of the form $\mathrm{GC}^{\mathbb{J}_{A,n},S}$, where $S = \{(\boldsymbol{t}, u, \boldsymbol{h}) | \boldsymbol{t}u = \boldsymbol{h}\}$. And from Lemma 3, OLE_A is a group correlation of the form $\mathrm{GC}^{\mathbb{K}_A,S}$, where $S = A \times \{0\}$.

It is instructive to note that the group correlation that OLE_A^n is embedded in corresponds to a vector version of Beaver's Multiplication Triplet correlation:

$$C := \{\big((\boldsymbol{a_1}, b_1, \boldsymbol{c_1}), (\boldsymbol{a_2}, b_2, \boldsymbol{c_2})\big) \mid \boldsymbol{c_1} + \boldsymbol{c_2} = (\boldsymbol{a_1} + \boldsymbol{a_2})(b_1 + b_2)\}.$$

This follows from Theorem 1.

Correlation	Structure
Binary Mutual Erasure Correlation: BME $\{(a,b) \in \{0,1,\perp\}^2 \mid \ \lvert\{a,b\} \cap \{0,1\}\rvert = 1\}$.	Group correlation of the form $\mathrm{GC}^{\mathbb{Z}_3,\{0,1\}}$.
Flat Regular Correlation: $C \subseteq A \times B$ is the support such that $\forall a \in A \ \lvert\{b \mid (a,b) \in C\}\rvert = d_B$ and $\forall b \in B \ \lvert\{a \mid (a,b) \in C\}\rvert = d_A$ for some fixed d_A, d_B and A, B are arbitrary sets.	Subgroup correlation of the form $\mathrm{GC}^{G_A \times G_B, C}_{G_A \times \{0\}, \{0\} \times G_B}$, where G_A and G_B could be any groups of size $\lvert A\rvert$ and $\lvert B\rvert$ respectively.
OLE over a ring A: OLE_A $\{(p,a),(q,b) \mid a + b = pq\}$.	Symmetric bi-linear correlation BA_σ, where $\sigma : A^2 \to A$, $T = A \times \{0\}$, $U = \{0\} \times A$ and $\sigma(p,q) = pq$.
Beaver's Mult. Triple over a ring A: BMT_A $\{(a_1,b_1,c_1),(a_2,b_2,c_2) \mid (a_1+a_2)(b_1+b_2) = (c_1+c_2)\}$.	Group correlation of the form $\mathrm{GC}^{\mathbb{Z}_A^3,S}$ where $S = \{(a,b,ab)\}$ and $\mathbb{Z}_A$ is the additive group of ring A. Aliter: Lemma 3. Symmetric bi-linear correlation BA_σ, where $\sigma : A^4 \to A$, $T = A^2 \times \{0\}^2$, $U = \{0\}^2 \times A^2$ and $\sigma((a_1,b_1,a_2,b_2)) = a_1b_2 + a_2b_1$.
Vector OLE over a ring A: OLE^n_A $\{(\boldsymbol{p},\boldsymbol{a}),(q,\boldsymbol{b}) \mid \boldsymbol{a} + \boldsymbol{b} = \boldsymbol{p}q\}$.	Bi-linear correlation BA_σ, where $\sigma : A^n \times A \to A^n$, $T = A^n \times \{0\}$, $U = \{0\}^n \times A$ and $\sigma(\boldsymbol{p},q) = \boldsymbol{p} \cdot q$ where $\cdot$ is scalar multiplication in A^n as a right A-module.
Vector BMT over a ring A: BMT^n_A $\{(a_1,\boldsymbol{b_1},\boldsymbol{c_1}),(a_2,\boldsymbol{b_2},\boldsymbol{c_2}) \mid (a_1+a_2)(\boldsymbol{b_1}+\boldsymbol{b_2}) = (\boldsymbol{c_1}+\boldsymbol{c_2})\}$.	Bi-linear correlation BA_σ, where $\sigma : A \times A^n \times A \times A^n \to A^n$, $T = A \times A^n \times \{0\}^2$, $U = \{0\}^2 \times A \times A^n$ and $\sigma((a_1,\boldsymbol{b_1},a_2,\boldsymbol{b_2})) = a_1 \cdot \boldsymbol{b_2} + a_2 \cdot \boldsymbol{b_1}$ where $\cdot$ is scalar multiplication in A^n as a right A-module.
Shared Inner Product over a ring A: SIP^m_A $\{((\boldsymbol{x},a),(\boldsymbol{y},b)) \mid \langle \boldsymbol{x},\boldsymbol{y}\rangle = a + b\}$ where $\boldsymbol{x},\boldsymbol{y} \in A^m$.	Symmetric bi-linear correlation BA_σ where $\sigma : A^n \times A^n$, $T = A^n \times \{0\}$, $U = \{0\} \times A^n$ and $\sigma(\boldsymbol{x},\boldsymbol{y}) = \langle \boldsymbol{x},\boldsymbol{y}\rangle$.
Shared Linear Transformation over a ring A: $\mathrm{SLT}^{m,n}_A$ $\{((M,\boldsymbol{x}),(\boldsymbol{z},\boldsymbol{y})) \mid M\boldsymbol{z} = \boldsymbol{x} + \boldsymbol{y}\}$ where $M \in A^{n \times m}$, $\boldsymbol{z} \in A^m$, $\boldsymbol{x},\boldsymbol{y} \in A^n$.	Bi-linear correlation BA_σ where $\sigma : A^{n \times m} \times A^m$, $T = A^{n \times m} \times \{0\}$, $U = \{0\} \times A^m$ and $\sigma(M,\boldsymbol{z}) = M\boldsymbol{z}$.
Zero Alternating Sum over a group G: ZAS_G $\{\big((a,c),(b,d)\big) \mid a + b + c + d = 0\}$.	Group correlation of the form $\mathrm{GC}^{G^2,S}$, where $S = \{(g,-g)\}$. Aliter: Lemma 2. Bi-affine correlation BA_σ, where $\sigma : D^2 \to D^{\mathrm{op}}$, $T = D \times \{0\}$ $U = \{0\} \times D$, and $\sigma(a,b) = -(a+b)$.

Table 1: Summary of cryptographically interesting correlations and their corresponding (sub)group and bi-affine structure.

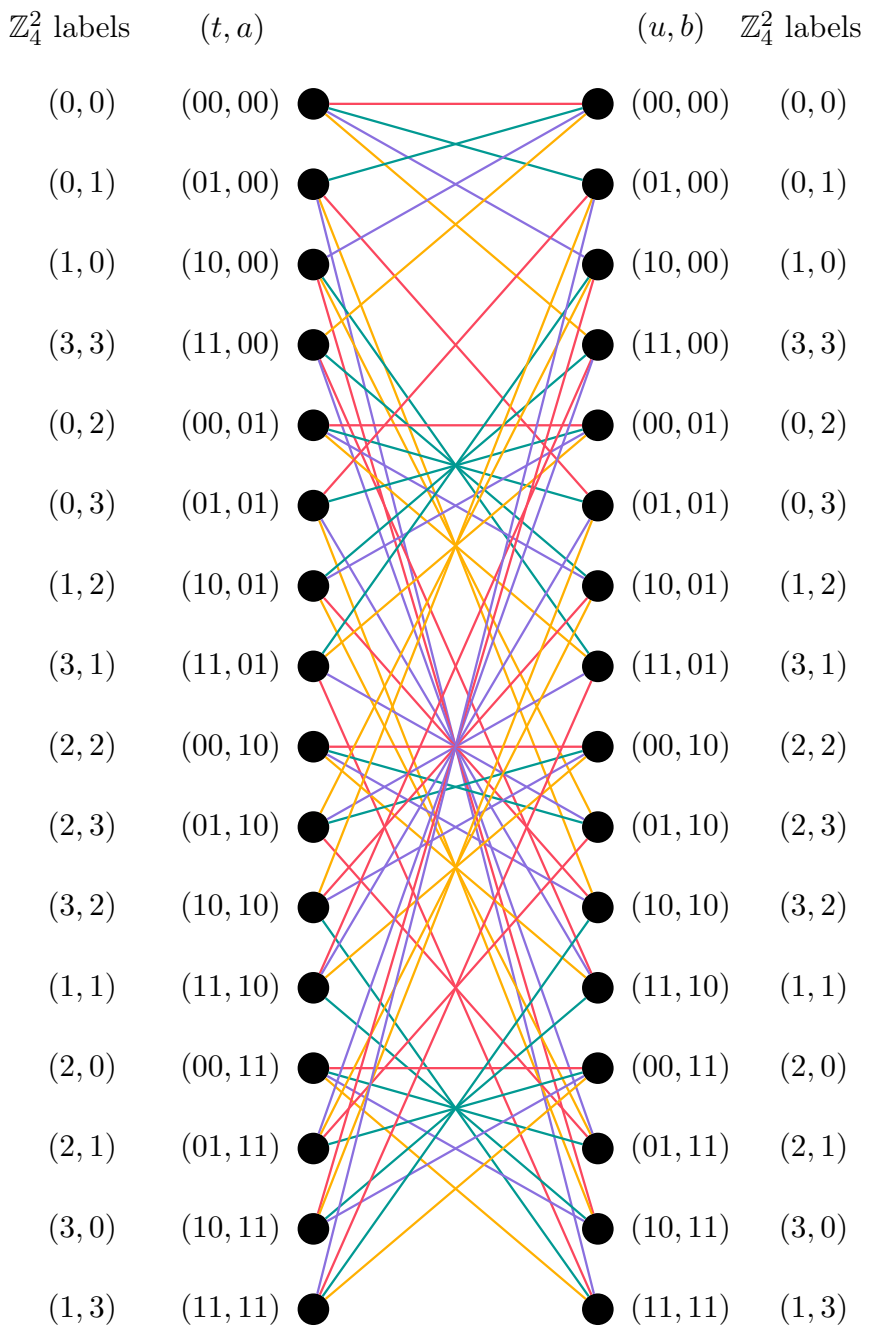

Figure 12: Bipartite graph $\mathbb{G}_{\text{OLE}}$ of the OLE correlation over the field $\mathbb{F}_4$. The edges correspond to $a + b = t * u$ in the field $\mathbb{F}_4$ (consisting of 2-bit strings, addition being bit-wise XOR, and the multiplication operator $*$ fully defined by $00 * z = 00, 01 * z = z$, $10 * 11 = 01$, and $z * z = z^{-1}$), as well as $x + y \in S$ in $\mathbb{Z}_4^2$.

B Details Omitted from Section 3

Lemma 1 (Restated)**.** *For groups $(Q,+)$ and $(H,\oplus)$, and subgroups $T,U \leqslant Q$, let $\sigma : Q \to H$ be a* bi-affine homomorphism w.r.t. (T,U)*. Then:*

1. *$\sigma^n : Q^n \to H^n$ is a bi-affine homomorphism w.r.t T^n, U^n for all $n \geq 1$.*
2. *$\sigma^{(n)} := \sigma^n$ is a bi-affine homomorphism w.r.t $T^n, U^{(n)} := \{(u,...,u) | u \in U\}$ for all $n \geq 1$.*
3. *If H is abelian, then $\sigma^{\langle \ell, m \rangle} : Q^{\ell+m} \to H$ is a bi-affine homomorphism w.r.t $(T^\ell \times U^m,\ U^\ell \times T^m)$ for all $\ell, m \geq 1$.*

Proof: To prove that these powers are bi-affine homomorphisms, we will show that they satisfy the homomorphism conditions from Definition 7. For σ^n note that

$$\begin{aligned}
\sigma^n\big((t_1,\dots,t_n)+(t'_1,\dots,t'_n)+(u_1,\dots,u_n)\big) =& \big(\sigma(t_1+u_1),\dots,\sigma(t_n+u_n)\big) \oplus -\big(\sigma(u_1),\dots,\sigma(u_n)\big) \\
& \oplus \big(\sigma(t'_1+u_1),\dots,\sigma(t'_n+u_n)\big) \\
=& \sigma^n\big((t_1,\dots,t_n)+(u_1,\dots,u_n)\big) \oplus -\sigma^n\big((u_1,\dots,u_n)\big) \\
& \oplus \sigma^n\big((t'_1,\dots,t'_n)+(u_1,\dots,u_n)\big)
\end{aligned}$$

$$\begin{aligned}
\sigma^n\big((t_1,\dots,t_n)+(u_1,\dots,u_n)+(u'_1,\dots,u'_n)\big) =& \big(\sigma(t_1+u_1),\dots,\sigma(t_n+u_n)\big) \oplus -\big(\sigma(t_1),\dots,\sigma(t_n)\big) \\
& \oplus \big(\sigma(t_1+u'_1),\dots,\sigma(t_n+u'_n)\big) \\
=& \sigma^n\big((t_1,\dots,t_n)+(u_1,\dots,u_n)\big) \oplus -\sigma^n\big((t_1,\dots,t_n)\big) \\
& \oplus \sigma^n\big((t_1,\dots,t_n)+(u'_1,\dots,u'_n)\big)
\end{aligned}$$

hence, σ^n is a bi-affine homomorphism w.r.t T^n, U^n. Similarly, it can be shown that $\sigma^{(n)}$ is a bi-affine homomorphism wr.t. $T^n, U^{(n)}$.

We now show that $\sigma^{\langle \ell, m \rangle}$ is bi-affine homomorphism w.r.t $(T^\ell \times U^m,\ U^\ell \times T^m)$. Let $\boldsymbol{t} = (t_1,...,t_\ell,u_1,...,u_m)$, $\tilde{\boldsymbol{t}} = (t'_1,...,t'_\ell,u'_1,...,u'_m)$ and $\boldsymbol{u} = (u''_1,...,u''_\ell,t''_1,...,t''_m)$, then we have:

$$\begin{aligned}
\sigma^{\langle \ell, m \rangle}\big(\boldsymbol{t}+\tilde{\boldsymbol{t}}+\boldsymbol{u}\big) &= \sigma^{\langle \ell, m \rangle}\big((t_1,...,t_\ell,u_1,...,u_m)+(t'_1,...,t'_\ell,u'_1,...,u'_m)+(u''_1,...,u''_\ell,t''_1,...,t''_m)\big) \\
&= \sigma^{\langle \ell, m \rangle}\big((t_1+t'_1+u''_1),...,(t_\ell+t'_\ell+u''_\ell),(u_1+u'_1+t''_1),...,(u_m+u'_m+t''_m)\big) \\
&= \sum_{i=1}^{\ell} \sigma(t_i+t'_i+u''_i) + \sum_{j=1}^{m} \sigma(-(u_j+u'_j+t''_j)) \\
&= \sum_{i=1}^{\ell} \big(\sigma(t_i+u''_i) - \sigma(u''_i) + \sigma(t'_i+u''_i)\big) \\
&\quad + \sum_{j=1}^{m} \big(\sigma(-t''_j-u'_j) - \sigma(-t''_j) + \sigma(-t''_j-u_j)\big) \\
&= \sum_{i=1}^{\ell} \sigma(t_i+u''_i) + \sum_{j=1}^{m} \sigma(-t''_j-u_j) - \sum_{i=1}^{\ell} \sigma(u''_i) - \sum_{j=1}^{m} \sigma(-t''_j) \\
&\quad + \sum_{i=1}^{\ell} \sigma(t'_i+u''_i) + \sum_{j=1}^{m} \sigma(-t''_j-u'_j)
\end{aligned}$$

$$= \sigma^{\langle \ell,m \rangle}\big(\boldsymbol{t}+\boldsymbol{u}\big) - \sigma^{\langle \ell,m \rangle}\big(\boldsymbol{u}\big) + \sigma^{\langle \ell,m \rangle}\big(\tilde{\boldsymbol{t}}+\boldsymbol{u}\big)$$

Similarly, it can be shown that

$$\sigma^{\langle \ell,m \rangle}\big(\boldsymbol{t}+\boldsymbol{u}+\tilde{\boldsymbol{u}}\big) = \sigma^{\langle \ell,m \rangle}\big(\boldsymbol{t}+\boldsymbol{u}\big) - \sigma^{\langle \ell,m \rangle}\big(\boldsymbol{t}\big) + \sigma^{\langle \ell,m \rangle}\big(\boldsymbol{t}+\tilde{\boldsymbol{u}}\big)$$

Thus, $\sigma^{\langle \ell,m \rangle}$ is a bi-affine homomorphism. □

Lemma 2 (Restated)**.** *If $\sigma : Q \to H$ is a bi-affine homomorphism w.r.t. (T,U), then BA_σ is a subgroups correlation of the form $\mathrm{GC}^{G,S}_{G_1,G_2}$ where $G = \mathbb{J}_\sigma$ and $S = \{(t,u,\sigma(t+u)) \mid t \in T, u \in U\}$, with $G_1 = T \times \{0\} \times H, G_2 = \{0\} \times U \times H$.*

Proof: Let $(Q,+)$ and $(H,\oplus)$ be the groups between which σ is defined. Note that the correlation $\mathsf{BA}_\sigma \subseteq (T \times H) \times (U \times H)$ is a regular correlation. So, to show that it is a subgroups correlation of the form $\mathrm{GC}^{G,S}_{G_1,G_2}$, for a group $(G,\odot)$ and $G_1, G_2 \leqslant G$, it is enough to show that there are bijections $\alpha : (T \times H) \to G_1$ and $\beta : (U \times H) \to G_2$ such that $(x,y) \in \mathsf{BA}_\sigma$ iff $\alpha(x) \odot \alpha(y) \in S$.

Consider the group $(G,\odot)$ to be $\mathbb{J}_\sigma$. Note that $G_1 = T \times \{0_{_U}\} \times H$ and $G_2 = \{0_{_T}\} \times U \times H$ are both closed under the group operation $\odot$, and hence form subgroups of G.

Define $\alpha : (T \times H) \to G_1$ as $\alpha(t,h) = (t, 0_{_U}, h)$ and $\beta : (U \times H) \to G_2$ as $\alpha(u,h) = (0_{_T}, u, h)$. Consider $S = \{(t,u,\sigma(t+u)) \mid t \in T, u \in U\}$. Then, $\alpha(t,a) \odot \beta(u,b) \in S$ iff $(t,u,a \oplus b) \in S$ iff $\sigma(t+u) = a \oplus b$, or equivalently, $((t,a),(u,b)) \in \mathsf{BA}_\sigma$. □

Lemma 3 (Restated)**.** *A bi-affine correlation of the form BA_σ, where $\sigma : D \times D \to H$ is a symmetric bi-affine homomorphism, is a group correlation of the form $\mathrm{GC}^{\mathbb{K}_\sigma,S}$, where $S = \{(d + d', \sigma(d,0) \oplus \sigma(0,d')) | d,d' \in D\}$.*

Proof: By definition of a symmetric bi-affine homomorphism, $\sigma : D \times D \to H$ is a bi-affine homomorphism w.r.t. subgroups $T = D \times \{0\}$ and $U = \{0\} \times D$. Let $\alpha : T \times H \to D \times H$ and $\beta : U \times H \to D \times H$ be given by $\alpha(d,0,h) = (d,h)$ and $\beta(0,d,h) = (d,h)$. Clearly, these are bijections from T and U respectively to $\mathbb{K}_\sigma$.

Consider $t = (d,0) \in T$ and $u = (0,d') \in U$. $((t,a),(u,b)) \in \mathsf{BA}_\sigma$ iff $a \oplus b = \sigma(t+u) = \sigma(d,d')$, or equivalently, $(d,a) \odot (d',b) \in S$. That is, $((t,a),(u,b)) \in \mathsf{BA}_\sigma$ iff $\alpha(t,a) \odot \beta(u,b) \in S$. □

$\mathbb{K}_\sigma$ is a group: We verify that $\mathbb{K}_\sigma$ satisfies all the group axioms:

- $\odot$ has an identity, namely $(0, -\sigma(0,0))$
- Every element (d,h) has an inverse under $\odot$. It is enough to separately verify that (d,h) has a right inverse as well as a left inverse. (By associativity and the nature of identity, it follows that the two inverses should be equal.) We note that $(d,h) \odot (d',h') = (0, -\sigma(0,0))$ if we set $d' = -d$ and $h' = -h \oplus -\sigma(0,0) \oplus -(\sigma(t,0) \oplus \sigma(0,-d) \oplus -\sigma(d,-d))$; similarly $(d'',h'') \odot (d,h) = (0,-\sigma(0,0))$ is we set $d'' = -d$ and $h'' = -h \oplus -\sigma(0,0) \oplus -(\sigma(t,0) \oplus \sigma(0,-d) \oplus -\sigma(d,-d))$.
- We now verify that $\odot$ is associative. We have $((d_1,h_1) \odot (d_2,h_2)) \odot (d_3,h_3) = (d_1+d_2+d_3, h_1 \oplus h_2 \oplus h_3 \oplus w)$ and $(d_1,h_1) \odot ((d_2,h_2) \odot (d_3,h_3)) = (d_1+d_2+d_3, h_1 \oplus h_2 \oplus h_3 \oplus w')$, where

$$\begin{aligned} w =& \sigma(d_1,0) \oplus \sigma(0,d_2) \oplus -\sigma(d_1,d_2) \oplus \sigma(d_1+d_2,0) \oplus \sigma(0,d_3) \oplus -\sigma(d_1+d_2,d_3) \\ =& \sigma(d_1,0) \oplus \sigma(0,d_2) \oplus -\sigma(d_1,d_2) \oplus \sigma(d_1,0) \oplus -\sigma(0,0) \oplus \sigma(d_2,0) \oplus \sigma(0,d_3) \\ & \oplus -\sigma(d_1,d_3) \oplus \sigma(0,d_3) \oplus -\sigma(d_2,d_3) \\ w' =& \sigma(d_1,0) \oplus \sigma(0,d_2+d_3) \oplus -\sigma(d_1,d_2+d_3) \oplus \sigma(d_2,0) \oplus \sigma(0,d_3) \oplus -\sigma(d_2,d_3) \end{aligned}$$

$$=\sigma(d_1,0)\oplus\sigma(0,d_2)\oplus-\sigma(0,0)\oplus\sigma(0,d_3)\oplus-\sigma(d_1,d_2)\oplus\sigma(d_1,0)\oplus-\sigma(d_1,d_3)$$
$$\oplus\sigma(d_2,0)\oplus\sigma(0,d_3)\oplus-\sigma(d_2,d_3)$$

By comparing the terms, the two expressions can be verified to be equal. Here we relied on the group H being abelian.

Theorem 1 (Restated)**.** *For any bi-affine homomorphism σ,*

1. BA_σ *is a compact subgroups correlation;*
2. *if σ is symmetric, then BA_σ is a group correlation;*
3. *if σ is semi-abelian, then BA_σ is embedded in $\mathsf{BA}_{\sigma^{\langle 2\rangle}}$, and more generally, $\mathsf{BA}_{\sigma^{\langle \ell,m\rangle}}$ is embedded in $\mathsf{BA}_{\sigma^{\langle 2m'\rangle}}$ for all $m'\geq\max(\ell,m)$.*

Proof: From Lemma 2, every bi-affine correlation is a compact subgroups correlation. Point 2 follows from Lemma 3. We now show that $\mathsf{BA}_{\sigma^{\langle \ell,m\rangle}}$ is embedded in $\mathsf{BA}_{\sigma^{\langle m',m'\rangle}}$ for all m' such that $m'\geq\max(\ell,m)$. First, note that $\mathsf{BA}_{\sigma^{\langle 2m'\rangle}}$ is isomorphic to a group correlation with group G and subset S defined as:

$$G=\mathbb{J}_{\sigma^{\langle 2m'\rangle}}$$

$$S=\{(\boldsymbol{t_1},\boldsymbol{u_1},\boldsymbol{u_2},\boldsymbol{t_2},h)\mid\sigma^{\langle 2m'\rangle}(\boldsymbol{t_1}+\boldsymbol{u_1},\boldsymbol{u_2}+\boldsymbol{t_2})=h;\,\boldsymbol{t_1},\boldsymbol{t_2}\in T^{m'},\,\boldsymbol{u_1},\boldsymbol{u_2}\in U^{m'},\,h\in H\}$$

Consider subgroups $G_1,G_2\leqslant G$ defined as

$$G_1=\left(T^\ell\times\{0\}^{m'-\ell}\right)\times\left(U^m\times\{0\}^{m'-m}\right)\times\{0\}^{m'}\times\{0\}^{m'}\times H,$$
$$G_2=\{0\}^{m'}\times\{0\}^{m'}\times\left(U^\ell\times\{0\}^{m'-\ell}\right)\times\left(T^m\times\{0\}^{m'-m}\right)\times H.$$

It can be seen that S is regular with respect to G_1 as $|S\cap(G_1+g_2)|=|T|^\ell|U|^m=|S\cap(G_1+g_2')|$ for all $g_2,g_2'\in G_2$. Similarly, S is regular with respect to G_2. Thus, $\mathrm{GC}^{G,S}_{G_1,G_2}$ is a valid subgroup correlation embedded in $\mathsf{BA}_{\sigma^{\langle 2m'\rangle}}$. We now show that $\mathsf{BA}_{\sigma^{\langle \ell,m\rangle}}$ is isomorphic to $\mathrm{GC}^{G,S}_{G_1,G_2}$. Note that all correlations in the support of $\mathrm{GC}^{G,S}_{G_1,G_2}$ satisfy the following condition:

$$\sigma^{\langle \ell,m\rangle}\big((\boldsymbol{t_1}+\boldsymbol{u_1},\{0\}^{m'-\ell}),(\boldsymbol{u_2}+\boldsymbol{t_2},\{0\}^{m'-m})\big)=h_1\oplus h_2$$

with

$$g_1=\big((\boldsymbol{t_1},\{0\}^{m'-\ell}),(\boldsymbol{u_2},\{0\}^{m'-m}),\{0\}^{m'},\{0\}^{m'},h_1\big),$$
$$g_2=\big(\{0\}^{m'},\{0\}^{m'},(\boldsymbol{u_1},\{0\}^{m'-\ell}),(\boldsymbol{t_2},\{0\}^{m'-m}),h_2\big).$$

Defining isomorphisms

$$\alpha\big((\boldsymbol{t_1},\{0\}^{m'-\ell}),(\boldsymbol{u_2},\{0\}^{m'-m}),\{0\}^{m'},\{0\}^{m'},h_1\big)=(\boldsymbol{t_1},\boldsymbol{u_2},h_1\oplus-(2m'-\ell-m)\sigma(0))$$

$$\beta\big(\{0\}^{m'},\{0\}^{m'},(\boldsymbol{u_1},\{0\}^{m'-\ell}),(\boldsymbol{t_2},\{0\}^{m'-m}),h_2\big)=(\boldsymbol{u_1},\boldsymbol{t_2},h_2)$$

it is easy to check that $g_1+g_2\in S\Leftrightarrow(\alpha(g_1),\beta(g_2))\in\mathsf{BA}_{\sigma^{\langle \ell,m\rangle}}$ for all $g_1\in G_1$, $g_2\in G_2$. □

C Proofs of Results in Section 4

Lemma 5 (Restated). *Suppose C is a group correlation of the form $\mathrm{GC}^{G,S}$. Then:*

1. *C is trivial iff S is a (left or right) coset of a subgroup of G.*
2. *$CI_{\mathrm{GK}}(C) = 0$ iff the set $\{s - s' \mid s, s' \in S\}$ is a generating set for the group G.*
3. *If for all $s_1, s_2, s_3, s_4 \in S$, $s_1 - s_2 + s_3 - s_4 = 0 \Rightarrow \{s_1, s_3\} = \{s_2, s_4\}$, then $RI_{\mathrm{w}}(C) = \log |S|$ viz. C is $K_{2,2}$ free.*

Proof: W.l.o.g, we consider $C \subseteq G \times G$ such that $C = \{(a, b) \mid a + b \in S\}$ (omitting the bijections α, β).

Part 1: Firstly, if $|S| = 1$, then C is trivial (it is a matching) and S is also a coset of the trivial subgroup $\{0\}$. So, suppose $|S| \geq 2$.

We use the fact that C is trivial iff it is of the form $\bigcup_i A_i \times B_i$, where the A_is are mutually disjoint as are the B_is. Consider the set A_i containing 0. Since $(0, s) \in C$ iff $s \in S$, we have $B_i = S$. Define the set $H \subseteq G$ as $H := S - b$.

We claim that H is a subgroup of G. For this we show that H is closed under addition. Indeed, if $h_1, h_2 \in H$, we can write $h_1 = s_1 - b$ and $h_2 = s_2 - b$ for $s_1, s_2 \in S$. Then $h_1 + h_2 = s_1 - b + s_2 - b$. Now, since $((s_1 - b), b) \in C$, we have $s_1 - b \in A_i$. Further, since $s_2 \in S = B_i$, we must have $((s_1 - b), s_2) \in C$, or equivalently, $s_1 - b + s_2 \in S$. Thus $h_1 + h_2 = s - b$ for some $s \in S$, and hence $h_1 + h_2 \in H$. Hence H is a subgroup of G. Since $S = H + b$, S is a coset of the H, as claimed.

(Symmetrically, starting with B_i containing 0, S can be written as $a + H$ for a subgroup H.)

Part 2: We use the fact that $CI_{\mathrm{GK}}(C) = 0$ iff the characteristic bipartite graph of C is connected.

Note that if for two distinct elements $a_0, a_1 \in G$, there exists $b \in G$ such that $(a_0, b), (a_1, b) \in C$ iff $a_1 = (s' - s) + a_0$ for $s, s' \in S$ (by taking $b = -a_0 + s = -a_1 + s'$). More generally, there is a path of the form $a_0, b_1, a_1, \cdots, a_n$ – i.e., we have $a_{i-1} + b_i = s_i \in S$ and $a_i + b_i = s'_i \in S$ – iff $a_n = (s'_n - s_n) + \cdots + (s'_1 - s_1) + a_0$. That is, every element $a \in G$ has a path from 0 (both as nodes on the left part of the characteristic bipartite graph) iff every element $a \in G$ can be written as $a = x_n + \cdots + x_1$ for some $x_1, \cdots, x_n \in \{(s' - s) \mid s, s' \in S\}$. The former condition is equivalent to the graph being connected (as there are no isolated nodes).

Part 3: We observe that the condition that there is no $s_1, s_2, s_3, s_4 \in S$ such that $\{s_1, s_3\} \neq \{s_2, s_4\}$ but $s_1 - s_2 + s_3 - s_4 = 0$ is the same as the characteristic bipartite graph of C not having the bipartite clique $K_{2,2}$ as a subgraph.

To see this, suppose $A = \{a, a'\}$ and $B = \{b, b'\}$ are such that $A \times B \subseteq C$ and $|A| = |B| = 2$. Then, writing

$$s_1 = a + b, s_2 = a' + b, s_3 = a' + b', s_4 = a + b',$$

it holds that $s_1 - s_2 + s_3 - s_4 = 0$, where each $s_i \in S$; further, since $|A| = |B| = 2$, we have $\{s_1, s_3\} \cap \{s_2, s_4\} = \emptyset$ (otherwise, e.g., $s_1 = s_2 \Rightarrow |A| = 1$). Conversely, given the summation condition $s_1 - s_2 + s_3 - s_4 = 0$, $s_i \in S$, then, for any $a \in G$, the sets $A = \{a, s_2 - s_1 + a\}$ and $B = \{-a + s_1, -a + s_4\}$ are such that $A \times B \subseteq C$ – i.e., $x + y \in \{s_1, s_2, s_3, s_4\}$ for all $x \in A$ and $y \in B$. Further, $|A| = |B| = 2$, as otherwise we require $\{s_1, s_3\} = \{s_2, s_4\}$ (if $|A| = 1$, then we have $s_1 = s_2$, and then by the summation condition, $s_3 = s_4$; , if $|B| = 1$ we have $s_1 = s_4$ and $s_2 = s_3$).

The statement then follows by Lemma 18. □

Lemma 18. *If C is a regular correlation then $RI_{\mathrm{w}}(C) \leq \log \min(\deg_L(C), \deg_R(C))$. Further, if C is $K_{2,2}$-free, then $RI_{\mathrm{w}}(C) = \log \min(\deg_L(C), \deg_R(C))$.*

Proof: Let the random variables (X, Y) be jointly distributed uniformly over the set of pairs in C. Firstly, we note that there exists a random variable Q jointly distributed with (X, Y) such that $I(\mathrm{X}; \mathrm{Y}|\mathrm{Q}) = 0$ and $I(\mathrm{Y}; \mathrm{Q}|\mathrm{X}) + I(\mathrm{X}; \mathrm{Q}|\mathrm{Y}) = \log(\deg_R(C))$. Specifically, let Q be the same as X, so that $I(\mathrm{Y}; \mathrm{Q}|\mathrm{X}) + I(\mathrm{X}; \mathrm{Q}|\mathrm{Y}) = 0 + H(\mathrm{X}|\mathrm{Y})$. Since C is regular, $H(\mathrm{X}|\mathrm{Y}) = \log(\deg_R(C))$. Hence $RI_{\mathrm{w}}(C) \leq \log(\deg_R(C))$. Similarly, by considering $\mathrm{Q} = \mathrm{Y}$, we obtain that $RI_{\mathrm{w}}(C) \leq \log(\deg_L(C))$.

Now, we need to prove that if C is $K_{2,2}$-free, then this is the smallest possible value of $I(\mathrm{Y}; \mathrm{Q}|\mathrm{X}) + I(\mathrm{X}; \mathrm{Q}|\mathrm{Y})$ among all Q such that $I(\mathrm{X}; \mathrm{Y}|\mathrm{Q}) = 0$. The condition on Q requires that for each possible value q of Q, the pair $(\mathrm{X}_q, \mathrm{Y}_q)$ should be independent of each other conditioned, where the subscript q denotes that the corresponding random variables are conditioned on $\mathrm{Q} = q$. To be independent, we require the support of $(\mathrm{X}_q, \mathrm{Y}_q)$ to be a Cartesian product $A \times B$. However, since C is $K_{2,2}$-free, it must be the case that either $|A| = 1$ or $|B| = 1$. In other words, $(\mathrm{X}_q, \mathrm{Y}_q)$ is a distribution over $\{(a_q, b) \mid b \in G\}$ for some fixed a_q or over $\{(a, b_q) \mid a \in G\}$ for some b_q (its support could be a proper subset of one of these sets). In these cases, we shall say that $(\mathrm{X}_q, \mathrm{Y}_q)$ is of the *type* $(a_q, \cdot)$ or $(\cdot, b_q)$ respectively.

Next we claim that w.l.o.g, we may assume that for Q minimizing $I(\mathrm{Y}; \mathrm{Q}|\mathrm{X}) + I(\mathrm{X}; \mathrm{Q}|\mathrm{Y})$, there are no two distinct values q_1, q_2 in the support of Q such that $(\mathrm{X}_{q_1}, \mathrm{Y}_{q_1})$ and $(\mathrm{X}_{q_2}, \mathrm{Y}_{q_2})$ are both of the same type. To see this, suppose there is a set W in the support of Q such that $|W| > 1$ and for all $q \in W$, $(\mathrm{X}_q, \mathrm{Y}_q)$ have the same type, say $(a, \cdot)$. Then consider Q' defined as a function of Q as follows: it takes the same value as Q, except whenever Q takes a value in W, its value is a new symbol q^*. We note that $I(\mathrm{X}; \mathrm{Y}|\mathrm{Q}') = 0$, because conditioned on all values q for Q', it is still the case that $(\mathrm{X}_q, \mathrm{Y}_q)$ is of the *type* $(a_q, \cdot)$ or $(\cdot, b_q)$ respectively – for $q = q^*$ this follows from the fact that $(\mathrm{X}_{q^*}, \mathrm{Y}_{q^*})$ is a convex combination of $(\mathrm{X}_{q'}, \mathrm{Y}_{q'})$ for $q' \in W$. On the other hand, since Q' is a function of Q, $I(\mathrm{Y}; \mathrm{Q}'|\mathrm{X}) + I(\mathrm{X}; \mathrm{Q}'|\mathrm{Y}) \leq I(\mathrm{Y}; \mathrm{Q}|\mathrm{X}) + I(\mathrm{X}; \mathrm{Q}|\mathrm{Y})$. So, w.l.o.g., we may replace Q with Q'. We then repeat this argument for each type.

Given the above claim, among Q such that $I(\mathrm{X}; \mathrm{Y}|\mathrm{Q}) = 0$, there is one that minimizes $I(\mathrm{Y}; \mathrm{Q}|\mathrm{X}) + I(\mathrm{X}; \mathrm{Q}|\mathrm{Y})$ whose support is contained in the set $\mathcal{Q} = \{q^{(a,\cdot)} | a \in A\} \cup \{q^{(\cdot,b)} | b \in B\}$, where the superscript of each symbol indicates the type associated with it. Note that $I(\mathrm{X}; \mathrm{Q}|\mathrm{Y}) + I(\mathrm{Y}; \mathrm{Q}|\mathrm{X}) = H(\mathrm{X}|\mathrm{Y}) + H(\mathrm{Y}|\mathrm{X}) - \big(H(\mathrm{X}|\mathrm{Y}, \mathrm{Q}) + H(\mathrm{Y}|\mathrm{X}, \mathrm{Q})\big)$. Since $H(\mathrm{X}|\mathrm{Y}) + H(\mathrm{Y}|\mathrm{X}) = \log \deg_R(C) + \log \deg_L(C)$ is fixed (irrespective of Q), we focus on Q that maximizes $H(\mathrm{X}|\mathrm{Y}, \mathrm{Q}) + H(\mathrm{Y}|\mathrm{X}, \mathrm{Q})$.

For each $(a, b) \in C$, note that conditioned on $(\mathrm{X}, \mathrm{Y}) = (a, b)$, Q takes a value in $\{q^{(a,\cdot)}, q^{(\cdot,b)}\}$. This is because these are the only two values q of Q such that (a, b) is in the support of $(\mathrm{X}_q, \mathrm{Y}_q)$. Let $\pi_{a,b} := \Pr[\mathrm{Q} = q^{(a,\cdot)} | \mathrm{X} = a, \mathrm{Y} = b]$; then, $\Pr[\mathrm{Q} = q^{(\cdot,b)} | \mathrm{X} = a, \mathrm{Y} = b] = 1 - \pi_{a,b}$. Also, let $p_{\mathrm{QXY}}(q, a, b)$ denote $\Pr[\mathrm{Q} = q, \mathrm{X} = a, \mathrm{Y} = b]$, $p_{\mathrm{QX}}(q, a)$ denote $\Pr[\mathrm{Q} = q, \mathrm{X} = a]$, etc. Then,

$$
\begin{aligned}
H(\mathrm{Y}|\mathrm{X}, \mathrm{Q}) &= \sum_{a \in A, q \in \mathcal{Q}} p_{\mathrm{QX}}(q, a) \cdot H(\mathrm{Y}|\mathrm{X} = a, \mathrm{Q} = q) \\
&= \sum_{a \in A} p_{\mathrm{QX}}(q^{(a,\cdot)}, a) \cdot H(\mathrm{Y}|\mathrm{X} = a, \mathrm{Q} = q^{(a,\cdot)}) \qquad \text{(other terms are 0)} \\
&\leq \log \deg_L(C) \sum_{a \in A} p_{\mathrm{QX}}(q^{(a,\cdot)}, a) \\
&= \log \deg_L(C) \sum_{a \in A, b \in B} p_{\mathrm{QXY}}(q^{(a,\cdot)}, a, b) \\
&= \log \deg_L(C) \sum_{a \in A, b \in B} p_{\mathrm{XY}}(a, b) \pi_{a,b}
\end{aligned}
$$

$$\leq \max(\log \deg_L(C), \log \deg_R(C)) \sum_{a\in A, b\in B} p_{\mathrm{XY}}(a,b)\pi_{a,b}.$$

Similarly,

$$H(\mathrm{X}|\mathrm{Y},\mathrm{Q}) \leq \max(\log \deg_L(C), \log \deg_R(C)) \sum_{a\in A, b\in B} p_{\mathrm{XY}}(a,b)(1-\pi_{a,b}).$$

Summing the two, we get

$$H(\mathrm{X}|\mathrm{Y},\mathrm{Q}) + H(\mathrm{Y}|\mathrm{X},\mathrm{Q}) \leq \max(\log \deg_L(C), \log \deg_R(C)).$$

Since $\max(\alpha,\beta) = \alpha+\beta-\min(\alpha,\beta)$, and $I(\mathrm{X};\mathrm{Q}|\mathrm{Y}) + I(\mathrm{Y};\mathrm{Q}|\mathrm{X}) = \log \deg_L(C) + \log \deg_R(C) - (H(\mathrm{X}|\mathrm{Y},\mathrm{Q}) + H(\mathrm{Y}|\mathrm{X},\mathrm{Q}))$, we get that $I(\mathrm{X};\mathrm{Q}|\mathrm{Y}) + I(\mathrm{Y};\mathrm{Q}|\mathrm{X}) \geq \min(\log \deg_L(C), \log \deg_R(C))$, as desired. □

If C is a bi-affine correlation of the form BA_σ, then $\deg_L(C) = |U|$ and $\deg_R(C) = |T|$, where σ is a bi-affine homomorphism w.r.t. (T,U). Thus, Lemma 18 implies that $RI_{\mathrm{w}}(C) \leq \min(\log|U|, \log|T|)$ and if C is $K_{2,2}$-free, then equality holds. The following lemma gives a class of examples where this holds.

Lemma 19. *A bi-affine correlation of the form BA_σ where σ is a bi-affine homomorphism w.r.t. (T,U) is $K_{2,2}$-free iff σ is non-defective.*

Proof: Consider a bi-affine correlation C of the form BA_σ as in the lemma statement. It is easy to see that if σ does not satisfy the condition in the statement – i.e., if there exists a pair $(t,u) \in (T\setminus\{0\}) \times (U\setminus\{0\})$ such that $\sigma(t+u) = \sigma(t) - \sigma(0) + \sigma(u)$, then $\{(0,0),(t,\sigma(t)-\sigma(0))\} \times \{(0,\sigma(0)),(u,\sigma(u))\} \subseteq C$. Here, we relied on the above condition on (t,u) to ensure that $((t,\sigma(t)-\sigma(0)),(u,\sigma(u))) \in C$.

In the other direction, we shall show that if C is not $K_{2,2}$-free then there must be such a pair (t,u). Suppose a copy of $K_{2,2}$ in C is $\{(t_0,\alpha),(t_1,\beta)\}\times\{(u_0,\gamma),(u_1,\gamma)\}$, where $t_0,t_1 \in T$, $u_0,u_1 \in U$ and $\alpha,\beta,\gamma,\delta \in H$. Let $t = t_1 - t_0$ and $u = -u_0 + u_1$, so that $t_1 = t + t_0$ and $u_1 = u_0 + u$. Then the conditions on the four edges in $K_{2,2}$ being contained in C translate to

$$\alpha+\gamma = \sigma(t_0+u_0) \qquad \alpha+\delta = \sigma(t_0+u_0+u)$$
$$\beta+\gamma = \sigma(t+t_0+u_0) \qquad \beta+\delta = \sigma(t+t_0+u_0+u).$$

Note that if $t=0$, then $\alpha=\beta$, and two nodes of the copy of $K_{2,2}$ (t_0,α) and (t_1,β) collapse to the same node; hence $t\neq 0$. Similarly, $u\neq 0$. Now, since $\beta+\delta = \beta+\gamma-(\alpha+\gamma)+\alpha+\delta$, we get

$$\sigma(t+t_0+u_0+u) = \sigma(t+t_0+u_0) - \sigma(t_0+u_0) + \sigma(t_0+u_0+u).$$

Expanding the expressions using the properties of bi-affine homomorphism, we get

$$\begin{aligned}\sigma(t+t_0+u_0+u) &= \sigma(t+t_0+u_0) - \sigma(t+t_0) + \sigma(t+t_0+u)\\ &= \sigma(t+t_0+u_0) - [\sigma(t)-\sigma(0)+\sigma(t_0)] + [\sigma(t+u)-\sigma(u)+\sigma(t_0+u)]\\ &= \sigma(t+t_0+u_0) - \sigma(t_0) + \sigma(0) - \sigma(t) + \sigma(t+u) - \sigma(u) + \sigma(t_0+u)\end{aligned}$$

Also,

$$\sigma(t+t_0+u_0) - \sigma(t_0+u_0) + \sigma(t_0+u_0+u) = \sigma(t+t_0+u_0) - \sigma(t_0) + \sigma(t_0+u))$$

Equating the two we get $\sigma(0)-\sigma(t)+\sigma(t+u)-\sigma(u) = 0$, or equivalently, $\sigma(t+u) = \sigma(t)-\sigma(0)+\sigma(u)$. □

Lemma 6 follows from Lemma 18 and Lemma 19.

Lemma 7 (Restated)**.** *If A is a domain, then $RI_{\mathrm{W}}(\mathrm{OLE}_A^n) = \log|A|$.*

Proof: Recall that if A is a ring, OLE_A^n is of the form BA_σ where $\sigma : A^{n+1} \to A$ given by $\sigma(\boldsymbol{a}, b) = \boldsymbol{a}b$, is bi-linear w.r.t. $(A^n \times \{0\}, \{\mathbf{0}\} \times A)$. Since A is a domain, σ is non-defective: we have $\boldsymbol{a}b \neq 0$ unless $\boldsymbol{a} = \mathbf{0}$ or $b = 0$. Now, applying Lemma 19 and Lemma 6, we obtain that $RI_{\mathrm{W}}(\mathrm{OLE}_A^n) = \log|A|$ whenever A is a domain. □

D Proofs of Results in Section 5

D.1 Computing from Biased Correlations

Lemma 8 (Restated)**.** $\mathsf{Comp}_{\sigma|\mathrm{U}}$ *and* $\mathsf{Comp}_{\sigma|\mathrm{TU}}$ *(Figure 3) UC-securely realize the functionalities* $\mathcal{F}_{\sigma|\mathrm{U}}$ *and* $\mathcal{F}_{\sigma|\mathrm{TU}}$*, respectively in the* $\widetilde{\mathcal{F}}_\sigma$ *hybrid.*

Proof: To prove security, first we check correctness of the output when both parties are honest.

Correctness. We verify that if Alice and Bob are honest, then Alice's output a and Bob's output b are such that $a \oplus b = \sigma(t + u)$. Since Alice's and Bob's outputs are:

$$a := \sigma(t + \Delta_u) \oplus -\sigma(t) \oplus \tilde{a}$$
$$b := \tilde{b} \oplus -\sigma(\tilde{u}) \oplus \sigma(\Delta_t + \tilde{u})$$

Then, we have

$$\begin{aligned} a \oplus b &= [\sigma(t + \Delta_u) \oplus -\sigma(t)] \oplus [\tilde{a} \oplus \tilde{b}] \oplus [-\sigma(\tilde{u}) \oplus \sigma(\Delta_t + \tilde{u})] \\ &= [\sigma(t + \Delta_u) \oplus -\sigma(t)] \oplus [\sigma(\tilde{t} + \tilde{u})] \oplus [-\sigma(\tilde{u}) \oplus \sigma(\Delta_t + \tilde{u})] \\ &= [\sigma(t + \Delta_u) \oplus -\sigma(t)] \oplus [\sigma((\tilde{t} + u) +_u (\Delta_t + \tilde{u})] \\ &= \sigma((t + \Delta_u) +_t (t + \tilde{u})) \\ &= \sigma(t + u) \end{aligned}$$

where, we use the properties of σ (refer Definition 7) and the fact that $\tilde{a} \oplus \tilde{b} = \sigma(\tilde{t} + \tilde{u})$.

Proof of Security. We argue security for each of the following corruption scenarios, by constructing a simulator Sim in each case.

- No corruption: In this case, the adversary Adv may choose a correlation $\big((\tilde{t}, \tilde{a}), (\tilde{u}, \tilde{b})\big) \in \mathsf{BA}_\sigma$ for $\widetilde{\mathcal{F}}_\sigma$, but receives no other information during the protocol. The simulator Sim receives no information from the functionalities, nor sends any information to Adv. By the correctness guarantee above, the real and ideal executions are identical from the point of view of the environment.
- Simulation against corrupt Alice:
  - Alice sends $(\tilde{t}, \tilde{a})$ to Sim which then samples $(\tilde{u}, \tilde{b}) \leftarrow \{(u', b') \mid \big((\tilde{t}, \tilde{a}), (u', b')\big) \in \mathsf{BA}_\sigma\}$
  - Sim samples u^* and sends $\Delta_{u^*} = u^* + -\tilde{u}$ to Alice.
  - Alice sends Δ_t to Sim. Sim extracts Alice's input $t := \tilde{t} + \Delta_t$. Sim feeds t as Alice's input to the functionality $\mathcal{F}_{\sigma|\mathrm{TU}}$ (resp. $\mathcal{F}_{\sigma|\mathrm{U}}$) and gets a as the output. In $\mathsf{Comp}_{\sigma|\mathrm{U}}$, Alice's input is exactly $\tilde{t}$.

– Sim sends a to Alice (as the output of the functionality).

In the protocol as well as in the simulation, $\tilde{u}$ is distributed uniformly conditioned on the adversary and environment's view before any messages are exchanged; hence Δ_u in the protocol and Δ_{u^*} in the simulation are both distributed uniformly. Moreover, every choice of message Δ_t by the adversary corresponds to a valid input t. Thus, this is a perfect simulation.

- Simulation against corrupt Bob:
  - Bob sends $(\tilde{u}, \tilde{b})$ to Sim which then samples $(\tilde{t}, \tilde{a}) \leftarrow \{(t', a') \mid \big((t', a'), (\tilde{u}, \tilde{b})\big) \in \mathsf{BA}_\sigma\}$
  - On receiving Δ_u from Bob, Sim extracts Bob's input $u := \Delta_u + \tilde{u}$. Sim feeds u as Bob's input to the functionality $\mathcal{F}_{\sigma|\text{TU}}$ (resp. $\mathcal{F}_{\sigma|\text{U}}$) and gets b as the output.
  - Sim samples t^* and sends $\Delta_{t^*} = -\tilde{t} + t^*$ to Bob. In $\mathsf{Comp}_{\sigma|\text{U}}$, this step is skipped.

  In the protocol as well as in the simulation, $\tilde{t}$ is distributed uniformly conditioned on the adversary and environment's view before any messages are exchanged; hence Δ_t in the protocol and Δ_{t^*} in the simulation are both distributed uniformly. Moreover, every choice of message Δ_u by the adversary corresponds to a valid input u. Thus, this is a perfect simulation.

□

Lemma 9 (Restated)**.** $\mathsf{Comp}_{\sigma|\text{TAU}}$ *(Figure 3) UC-securely realizes the functionality* $\mathcal{F}_{\sigma|\text{TAU}}$ *in the* $\widetilde{\mathcal{F}}_\sigma$ *hybrid.*

Proof: We first prove that Π_σ is a UC-secure realization of $\mathcal{F}_{\sigma|\text{TAU}}$ in the $\mathcal{F}_{\sigma|\text{TU}}$ hybrid model. We then, replace $\mathcal{F}_{\sigma|\text{TU}}$ with the protocol $\mathsf{Comp}_{\sigma|\text{TU}}$ (which from Lemma 8 is a secure realization) to get a secure protocol in the $\widetilde{\mathcal{F}}_\sigma$ hybrid model.

To prove the security of Π_σ, first we check correctness of the output when both parties are honest.

Proof of Security. We argue security for each of the following corruption scenarios, by constructing a simulator Sim in each case.

- No corruption: In this case, the Adv neither receives nor sends any messages, and the environment's view consists only of the inputs and outputs of the honest parties. We verify that, if Alice and Bob are honest, then Bob's output is the unique value b such that $a \oplus b = \sigma(t + u)$ (as it would be in the ideal execution of $\mathcal{F}_{\sigma|\text{TAU}}$):

$$\begin{aligned} b =& \Delta_a \oplus \tilde{b} \\ a \oplus b =& a \oplus \Delta_a \oplus \tilde{b} \\ =& a \oplus -a \oplus \tilde{a} \oplus \tilde{b} = \tilde{a} \oplus \tilde{b} \\ =& \sigma(t + u) \end{aligned}$$

- Simulation against corrupt Alice:
  - Alice sends t to Sim (as input to $\mathcal{F}_{\sigma|\text{TU}}$), which then samples $(\tilde{a}, u, \tilde{b}) \leftarrow \{(a', u, b') \mid \big((t, a'), (u, b')\big) \in \mathsf{BA}_\sigma\}$ and sends $\tilde{a}$ to Alice (as output of $\mathcal{F}_{\sigma|\text{TU}}$).
  - Alice sends Δ_a to Sim (as message to Bob). Sim extracts Alice's input $a := \tilde{a} \oplus -\Delta_a$. Sim feeds (t, a) as Alice's input to the functionality $\mathcal{F}_{\sigma|\text{TAU}}$.

In the protocol as well as in the simulation, adversary receives no messages. Moreover, every choice of message Δ_a by the adversary corresponds to a valid input a. Thus, this is a perfect simulation.

- Simulation against corrupt Bob:
  - Bob sends u to Sim (as input to $\mathcal{F}_{\sigma|\text{TU}}$), which then samples $(t, \tilde{a}, \tilde{b}) \leftarrow \{(t, a', b') \mid \big((t, a'), (u, b')\big) \in \mathsf{BA}_\sigma\}$ and sends $\tilde{b}$ to Bob (as output of $\mathcal{F}_{\sigma|\text{TU}}$).
  - Sim feeds u as Bob's input to the functionality $\mathcal{F}_{\sigma|\text{TAU}}$ and obtains b as output.
  - Sim sets $\Delta_a = b \oplus -\tilde{b}$, and sends to Bob (as message from Alice).

  In the protocol as well as in the simulation, adversary sends no messages. Moreover, the message it receives Δ_a is fixed given the output $\tilde{b}$ from the oracle call to $\mathcal{F}_{\sigma|\text{TU}}$ and output b from the functionality $\mathcal{F}_{\sigma|\text{TAU}}$. Thus, this is a perfect simulation.

□

D.2 Inner-Product Bi-Affine Correlations from Bi-Affine Correlations

Lemma 10 (Restated)**.** *The protocol in Figure 4 is a non-interactive UC-secure secure protocol for reducing* $\mathsf{BA}_{\sigma^{\langle \ell, m\rangle}}$ *to* $\ell + m$ *instances of* BA_σ*.*

Proof: The ideal functionality samples a uniformly random correlation from the support of $\mathsf{BA}_{\sigma^{\langle \ell, m\rangle}}$ and sends corresponding shares to Alice and Bob.

- **Security against corrupt Alice:** When Adv makes a request to $\mathcal{F}_\sigma$, Sim makes a request to the ideal functionality and obtains $(t_1, \ldots, t_\ell, u'_1, \ldots, u'_m, h_1)$. The simulator sets $r_i = t_i$ and $s'_j = -u'_j$. It then samples $\{x_i\}_{i\in[\ell]}$ and $\{y'_i\}_{i\in[m-1]}$ uniformly at random and sets

$$y'_m = h_1 \oplus \sum_{k=1}^{\ell} -x_k \oplus \sum_{k=1}^{m-1} -y'_k \tag{9}$$

  and sends $(r_1, \ldots, r_\ell, x_1, \ldots, x_\ell, s'_1, \ldots, s'_m, y'_1, \ldots, y'_m)$ to Adv. r_i's and s_i's can be obtained directly from the output. In the simulation h_1 is uniformly random, hence the distribution of $(x_1, \ldots, x_\ell, y'_1, \ldots, y'_m)$ is uniformly random conditioned on (9). This is identical to the distribution in the protocol. Thus, this is a perfect simulation.
- **Security against corrupt Bob:** Proof is analogous to the previous case.

In both scenarios, Sim sends abort to the ideal functionality whenever the adversary issues abort. □

D.3 Bi-Affine Correlations from String OT

Lemma 11 (Restated)**.** $\mathsf{Comp}_{\sigma|\text{TAU}}$ *(Figure 5) is a semi-honest secure protocol realising* $\mathcal{F}_{\sigma|\text{TAU}}$*.*

Proof: **Correctness:** For correctness, when both parties are honest, Bob must compute $b = -a \oplus \sigma(t + u)$. The adversary specifies Alice's input (t, a) and Bob's input u. At the end of the protocol, Bob computes

$$b = \sum_{i=1}^{k-1} (-r_i \oplus \sigma(t + M_U(i, c_i)) \oplus -\sigma(t) \oplus r_{i+1}) \oplus -r_k \oplus \sigma(t + M_U(k, c_k))$$

$$= - a \oplus \sigma(t + \sum_{i=1}^{k} M_U(i, c_i))$$
$$= - a \oplus \sigma(t + u)$$

Security: We now argue for security in each of the following corruption scenarios:

- Security against corrupt Alice: Since Alice is passively corrupt, she follows the protocol as instructed and receives no messages during the protocol. Alice's view consists of her inputs (t, a) and the messages she prepares for $\binom{m}{1}$-OT^{ℓ}. Neither of which, reveals any information that was not already available.
- Security against corrupt Bob: The messages Bob receives $\{m_i\}_{i\in[k]}$ are uniformly random conditioned on $b = \sum_{i=1}^{k} m_i$. Since b is something that Bob can extract from the output, he does not learn any extra information.

□

D.4 Biasable Correlations from Tamperable Correlations

Lemma 13 (Restated)**.** TRSamp_{σ} *(Figure 6) securely realizes the functionality* $\widetilde{\mathcal{F}}_{\sigma}$ *against passive corruption, with statistical security.*

Proof: We show correctness and security as follows.

Correctness. Suppose both parties are honest. Let the errors in the correlation pairs provided by the adversary Adv to the functionality $\widehat{\mathcal{F}}_{\sigma}$ be such that the error is:

$$\forall i \in [n], e_i = a_i \oplus b_i \oplus -\sigma(t_i + u_i)$$

If Alice and Bob are to not abort the protocol, it must be the case that (1) $e_i = 0_H$ for all $1 \le i \le \frac{n}{2}$, and (2) $e_i = x_i \oplus e_{i-1} \oplus -x_i$ for all $\frac{n}{2} < i \le n$. (the latter condition follows from the error-preservation guarantee of $\mathsf{Comp}_{\sigma|\text{TAU}}$.) However, unless $e_i = 0_H$ for all $i \in [n]$, the probability of this happening over the random choice of the permutation is at most $1/\binom{n}{n/2}$ (this probability is achieved when there are exactly $\lfloor \frac{n}{2} \rfloor$ $i \in [n]$ such that $e_i = 0_H$, and all the others have the same non-zero value).

On the other hand, if $e_i = 0_H$ for all $i \in [n]$, then all the correlation pairs are valid. In this case, Alice and Bob would never abort, and would output one of those valid pairs.

Security. We argue security for each of the following corruption scenarios.

- No corruption: If both parties Alice and Bob are honest, then adversary feeds the correlation pairs to be sent by the functionality $\widehat{\mathcal{F}}_{\sigma}$. In this case, we construct a simulator Sim that works as follows: Sim accepts $\{((t^i, a^i), (u^i, b^i))\}_{i\in[n]}$ from Adv. It checks if the pairs are valid. If it is valid, it outputs $\perp$ to Adv, and forwards a pair $((t^i, a^i), (u^i, b^i))$ for a random $i \leftarrow [n]$, to $\widetilde{\mathcal{F}}_{\sigma}$. If at least one pair is invalid, then Sim sends an abort command to the functionality $\widetilde{\mathcal{F}}_{\sigma}$ (thus aborting the parties). This will be indistinguishable from the view of Adv in the real execution of the protocol, provided the honest parties abort if any correlation $((t^i, a^i), (u^i, b^i)) \notin C$, in the real execution as well. From the above, this is indeed the case, except with a negligible probability $1/\binom{n}{\lfloor n/2 \rfloor}$.

- Security against corrupt Alice or Bob: If either Alice or Bob is (passively) corrupt, then $\widehat{\mathcal{F}}_\sigma$ is uncorrupted, and behaves as $\mathcal{F}_\sigma$. In this case, we shall show that the protocol is a perfectly secure protocol for $\mathcal{F}_\sigma$ in the $\mathcal{F}_\sigma$-hybrid, against passive corruption.
  Firstly, note that the protocol never aborts. Thus, the cut-and-choose step can be ignored in the analysis. Further, we can view the $n/2$ sequential invocations of $\mathsf{Comp}_{\sigma|\text{TAU}}$ as follows:
  A single sample $((t_j, a_j), (u_j, b_j)) \leftarrow C$, where $j = \lfloor \frac{n}{2} \rfloor$, is obtained from $\mathcal{F}_\sigma$; then, for $i > j$, Alice locally samples $(t_i, a_i) \leftarrow T \times H$ and Bob samples $u_i \leftarrow U$, and they invoke $\mathsf{Comp}_{\sigma|\text{TAU}}^{(t_{i-1},a_{i-i}),(u_{i-1},b_{i-1})}$ for Bob to compute $b_i = -a_i \oplus \sigma(t_i + u_i)$. (Note that here we relied on the passive corruption model to be able to ignore the availability of b_i from the original correlations, as they will be equal to the b_i computed in the above protocol.)
  We can now rewrite our original protocol (ignoring the cut-and-choose steps) as an invocation of $\Pi^{\Pi^{\cdots^{\Pi^{\mathcal{F}_\sigma}}}}$, where the protocol $\Pi^{\mathcal{F}}$ invokes $\mathsf{Comp}_{\sigma|\text{TAU}}^{\mathcal{F}}$, with Alice and Bob inputting locally sampled $(t, a) \leftarrow T \times H$ and $u \leftarrow U$, respectively. By the security of $\mathsf{Comp}_{\sigma|\text{TAU}}$, $\Pi^{\mathcal{F}_\sigma}$ can be seen to be a passive-secure protocol for $\mathcal{F}_\sigma$ (because an invocation of $\mathsf{Comp}_{\sigma|\text{TAU}}^{\mathcal{F}_\sigma}$ can be replaced by an invocation of $\mathcal{F}_{\sigma|\text{TAU}}$). Hence, the protocol above collapses to a perfectly secure protocol for $\mathcal{F}_\sigma$.

□

Lemma 14 (Restated)**.** $\mathsf{altTRSamp}_\sigma$ *(Figure 8) passive-securely realizes the functionality* $\widetilde{\mathcal{F}}_\sigma$*, in the* $\widehat{\mathcal{F}}_\sigma$*,* $\mathcal{E}_\sigma$ *hybrid model*

Proof: Firstly, we relate the output of the protocol to the following error quantities:

$$e_0 = -\sigma(t_0 + u_0) \oplus a_0 \oplus b_0$$
$$e_1 = -\sigma(t_1 + u_1) \oplus a_1 \oplus b_1$$

Here e_0 is the error for the correlation pair provided by the adversary Adv to the functionality $\widehat{\mathcal{F}}_\sigma$, and e_1 is an error term for the first sample provided by $\mathcal{E}_\sigma$. Now, by the error preservation property of $\mathsf{Comp}_{\sigma|\text{TAU}}$, we have that

$$\begin{aligned} b^* = b_1 &\Leftrightarrow e_1 = [-\sigma(t_1 + u_0) \oplus \sigma(t_0 + u_0)] \oplus e_0 \oplus -[-\sigma(t_1 + u_0) \oplus \sigma(t_0 + u_0)] \\ &\Leftrightarrow \sigma(t_0 + u_0) \oplus e_0 \oplus -\sigma(t_0 + u_0) = \sigma(t_1 + u_0) \oplus e_1 \oplus -\sigma(t_1 + u_0) \end{aligned}$$

Note that e_0, t_0, u_0 are adversarially determined prior to the invocation of $\mathcal{E}_\sigma$. Thus, writing $z_0 = \sigma(t_0 + u_0) \oplus e_0 \oplus -\sigma(t_0 + u_0)$ (which is determined before $\mathcal{E}_\sigma$ is invoked), the outcome of the protocol can be described as follows: If $z_0 = \sigma(t_1 + u_0) \oplus e_1 \oplus -\sigma(t_1 + u_0)$, then it outputs the pair $\big((t_2, a_2), (u_2, b_2)\big)$, and otherwise it aborts.

Security. We argue security for each of the following corruption scenarios:

- No corruption: If both parties Alice and Bob are honest, then adversary sets the correlation pairs to be sent by the functionality $\widehat{\mathcal{F}}_\sigma$ and $\mathcal{E}_\sigma$. In this case, the simulation is as follows: Sim accepts $\big((t_0, a_0), (u_0, b_0)\big)$, $\big((\tilde{t}, \tilde{a}), (\tilde{u}, \tilde{b})\big)$ and $\mathcal{D}$ from Adv. It checks if $\mathcal{D}$ passes the min-entropy check. If it does, then Sim sends abort to the functionality $\widetilde{\mathcal{F}}_\sigma$ (thus aborting the parties). This will be indistinguishable from the view of Adv in the protocol, because, the honest parties abort in the real execution of the protocol with overwhelming probability $\Pr[E_{u_0} \neq z_0] \geq 1 - 2^{\mathrm{H}_\infty(E_{u_0})} \geq$

$1 - 2^{\ell}$, if the min-entropy check passes. If $\mathcal{D}$ does not satisfy the min-entropy condition, then $\big((t_2, a_2), (u_2, b_2)\big)$ is guaranteed to be in BA_σ. In this case, Sim can carry out a perfect simulation by sending $\big((t_2, a_2), (u_2, b_2)\big)$ to $\widetilde{\mathcal{F}}_\sigma$ with probability $\Pr[E_{u_0} = z_0]$, and abort otherwise.

- Security against corrupt Alice: If either Alice or Bob is (passively) corrupt, then $\widehat{\mathcal{F}}_\sigma$ behaves like $\widetilde{\mathcal{F}}_\sigma$, while $\mathcal{E}_\sigma$ allows the corrupt party to specify the "corrupt side" of the pairs $\big((t_1, a_1), (u_1, b_1)\big)$, $\big((t_2, a_2), (u_2, b_2)\big)$ along with the function ξ.

  Suppose Alice is corrupt. Then Sim accepts (t_0, a_0) from Alice (as its message to $\widehat{\mathcal{F}}_\sigma$), (t_1, a_1), (t_2, a_2) and ξ (as its messages for $\mathcal{E}_\sigma$). Sim simply returns (t_1, a_1) and (t_2, a_2) as outputs from ξ to Alice. Then Sim sends $\Delta_u \leftarrow U$ as the message in $\mathsf{Comp}_{\sigma|\text{TAU}}$ from Bob to Alice. Finally, Sim sends (t_2, a_2) to $\widetilde{\mathcal{F}}_\sigma$.

  To see that this is a valid simulation, note that irrespective of ξ and (t_1, a_1), such that firstly, conditioned on Alice's view, the pair (u_2, b_2) that $\mathcal{E}_\sigma$ outputs to Bob is distributed uniformly in the set $\{(u, b) \mid ((t_2, a_2), (u, b)) \in \mathsf{BA}_\sigma\}$, as would be the output Bob receives from $\widetilde{\mathcal{F}}_\sigma$ in the ideal execution.

  The pair (u_1, b_1) that Bob receives from $\mathcal{E}_\sigma$ can be arbitrarily correlated with (u_2, b_2), but note that the only information about this pair that is revealed to Alice and the environment is whether Bob aborted the protocol or not, and the message from Bob in $\mathsf{Comp}_{\sigma|\text{TAU}}$. Since it is guaranteed by $\mathcal{E}_\sigma$ that $\big((t_1, a_1), (u_1, b_1)\big) \in \mathsf{BA}_\sigma$ (and since $((t_0, a_0), (u_0, b_0)) \in \mathsf{BA}_\sigma$, and Alice is only passively corrupt), Bob does not abort the protocol. The message from Bob in $\mathsf{Comp}_{\sigma|\text{TAU}}$ protocol is $\Delta_u = u_1 - u_0$. However, since u_0 is uniformly random over U (given t_0, a_0), Δ_u simulated by Sim correctly distributed conditioned on the rest of the view of Alice and the environment.

  Thus in this case, the simulation is perfect.
- Security against corrupt Bob: The simulation and the argument of its correctness in this case is analogous to the above case. Here, Sim needs to additionally simulate the last message from Alice to Bob in the execution of $\mathsf{Comp}_{\sigma|\text{TAU}}$. The property that $\big((t_1, a_1), (u_1, b_1)\big) \in \mathsf{BA}_\sigma$ translates to the fact that this message is uniquely determined so that the output b^* from $\mathsf{Comp}_{\sigma|\text{TAU}}$ equals b_1. Again, this results in a perfect simulation.

□

Lemma 15 (Restated)**.** *The protocols in (Figure 9) passive-securely realize the functionality $\mathcal{E}_\sigma$, in the $\widehat{\mathcal{F}}_\sigma$ hybrid model, provided the stated security conditions are satisfied.*

Proof:

We argue the security of the three protocols for the three kinds of biaffine operators considered in Figure 9. In each case, we consider the three corruption scenarios corresponding to both parties being honest (but the adversary controlling $\widehat{\mathcal{F}}_\sigma$) and exactly one party being honest.

Modules:

- No corruption: If both parties Alice and Bob are honest, then the adversary sends the pair $\big((t, a), (u, b)\big)$ for $\widehat{\mathcal{F}}_\sigma$ to output to the two parties. On receiving this, the simulator Sim sends $\big(\mathcal{D}, ((\tilde{t}, \tilde{a}), (\tilde{u}, \tilde{b}))\big)$ to $\mathcal{E}_\sigma$, where $\mathcal{D}$ is the uniform distribution over the set $\{\big((t \cdot r, a \cdot r), (u, b \cdot r)\big) \mid r \in \text{units}(R)\}$, and $((\tilde{t}, \tilde{a}), (\tilde{u}, \tilde{b})) = \big((t, a), (u, b)\big)$.

  To see that this is a perfect simulation, firstly note that in the real protocol execution Alice and Bob's outputs are such that $((t_1, a_1), (u_1, b_1)) \leftarrow \mathcal{D}$ and $((t_2, a_2), (u_2, b_2)) = ((\tilde{t}, \tilde{a}), (\tilde{u}, \tilde{b}))$. In

the ideal execution too, we claim that the outputs are distributed in the same way, because the condition

$$\big((\tilde{t},\tilde{a}),(\tilde{u},\tilde{b})\big) \in \mathsf{BA}_\sigma \text{ or } \forall r_0 \in R, \mathrm{H}_\infty(E_{r_0}) \geq \ell$$

holds. To see this, note that for $((t,a),(u,b))$ in the support of $\mathcal{D}$, the error term $e := -\sigma(t+u) \oplus a \oplus b = \tilde{e} \cdot r$, where $\tilde{e} = -\sigma(\tilde{t}+\tilde{u}) \oplus \tilde{a} \oplus \tilde{b}$, and $r \in \mathrm{units}(R)$. Then, if $\big((\tilde{t},\tilde{a}),(\tilde{u},\tilde{b})\big) \notin \mathsf{BA}_\sigma$, then $\tilde{e} \neq 0_H$, and hence $\{\tilde{e} \cdot r | r \in \mathrm{units}(R)\}$ is of size for any $r_0 \in R$, the distribution E_{r_0}, which is uniform over $\{-x \oplus e \oplus x | x := \sigma((\tilde{t} \cdot r) + r_0)\}$. checks if it is in BA_σ. If so, it picks a random $r \in \mathrm{units}(R)\}$, and sends $\big((t \cdot r, a \cdot r),(u, b \cdot r)\big)$ to $\mathcal{E}_\sigma$; From correctness, this is a valid pair in BA_σ. Otherwise, it specifies the distribution $\mathcal{D}$ as uniform over the set $\{\big((t \cdot r, a \cdot r),(u, b \cdot r)\big) \mid r \in \mathrm{units}(R)\}$. Note that this is indeed the distribution of the outputs in the protocol execution. To complete the proof, we argue below that $\mathcal{D}$ satisfies the min-entropy condition checked by $\mathcal{E}_\sigma$, so that this is the output distribution in the ideal world as well.

Since a module is an abelian group, we have $x + e - x = e$ for any x, and hence for all u', $E_{u'}$ is the distribution $\{-(t' \cdot u') \oplus a' \oplus b'\}_{\big((t',a'),(u',b')\big) \leftarrow \mathcal{D}}$. This equals a fixed distribution E given $\{e \cdot r\}_{r \leftarrow \mathrm{units}(R)}$, where $e = -(t \cdot u) \oplus a \oplus b$. Note that if $e \neq 0$, then the support of E is at least $\mathrm{minimg}_R(H)$. Further, E is uniform over its support. To see this, let $S_d = \{r \in \mathrm{units}(R) | e \cdot r = d\}$. Then, for a d in the support of E, say, $d = e \cdot v$, $S_d = \{uv \mid u \in S_e\}$, because $d = e \cdot r \Leftrightarrow e \cdot rv^{-1} = e \Leftrightarrow r = uv, u \in S_e$, and hence $|S_d| = |S_e|$ for all d in the support of E.

Thus, the min-entropy of $E \geq \log \mathrm{minimg}_R(H) = \omega(\log \lambda)$.

- Security against corrupt Alice: If Alice is passively corrupt $\widehat{\mathcal{F}}_\sigma$ behaves like $\mathcal{F}_\sigma$. From correctness it can be seen that Alice and Bob will output a valid pair at the end of the protocol. Further, conditioned on r and Alice's output $(t', a') = (t \cdot r, a \cdot r)$, the Bob's output has a uniformly random u', and $b' = t' \cdot u' - a'$. Hence, the following is a perfect simulation: Sim samples $(t, a) \leftarrow H \times H$ to Alice, and also $r \leftarrow \mathrm{units}(R)$, which it sends to Alice; then it sends $(t \cdot r, a \cdot r)$ to $\mathcal{E}_\sigma$.
- Security against corrupt Bob: Here, we additionally rely on the fact that $r \leftarrow \mathrm{units}(R)$. Conditioned on Bob's view of r and (u', b'), we still have $t' = t \cdot r$ uniformly random over H, since t itself is uniformly random, and scalar multiplication by $r \in \mathrm{units}(R)$ is an invertible operation $((t \cdot r) \cdot r^{-1} = t \cdot 1_R = t)$.

Semi-abelian Bi-Affine Correlations:

- No corruption: If both parties Alice and Bob are honest, then the adversary specifies the pair $\big((t,a),(u,b)\big)$ produced during the the invocation of functionality $\widehat{\mathcal{F}}_\sigma$. Sim then specifies the distribution $\mathcal{D}$ as uniform over the set

$$\{\big((kt, ka),(u, kb \oplus -(k-1)\sigma(u))\big) \mid k \in \mathbb{Z}_{\mathrm{minord}(H)}\}$$

Note that this is indeed the distribution of the output $\big((t_1,a_1)(u_1,b_1)\big)$ in the protocol execution. Sim also specifies $\big((\tilde{t},\tilde{a})(\tilde{u},\tilde{b})\big) = \big((t,a)(u,b)\big)$. To complete the proof, we argue below that the output distributions in the real and ideal world are indistinguishable.

Since a semi-abelian bi-affine correlation is abelian in the group H, hence for all $t_0 \in T$, E_{t_0} is the distribution $\{e' \mid e' = -\sigma(t'+u') \oplus a' \oplus b',\ \big((t',a'),(u',b')\big) \in \mathcal{D}\}$. Note that $ka \oplus kb \oplus -\sigma(kt + u) \oplus -(k-1)\sigma(u) = k(a \oplus b \oplus -\sigma(t+u))$ from the property of bi-affine homomorphisms. This implies that E_{t_0} is a uniform distribution over the set $\{ke \mid k \leftarrow \mathbb{Z}_{\mathrm{minord}(H)}\}$ where $e = -\sigma(t + u) \oplus a \oplus b$.

If $e \neq 0$, the min-entropy of $\mathcal{D}$ is $\mathrm{H}_\infty(E_{t_0}) = \log \mathrm{minord}(H) = \omega(\log \lambda)$ and the check passes, hence the output $\big((t_2, a_2), (u_2, b_2)\big) = \big((\tilde{t}, \tilde{a})(\tilde{u}, \tilde{b})\big)$ is indistinguishable from that in the real world. If $e = 0$, then the min-entropy check fails since the $\mathrm{H}_\infty(E_{t_0}) = 0$. However, this means that $\big((\tilde{t}, \tilde{a})(\tilde{u}, \tilde{b})\big) \in \mathsf{BA}_\sigma$ and thus $\big((t_2, a_2), (u_2, b_2)\big) = \big((\tilde{t}, \tilde{a})(\tilde{u}, \tilde{b})\big)$. Again, the output is indistinguishable from that in the real world

- Security against corrupt Alice: If Alice is passively corrupt $\widehat{\mathcal{F}}_\sigma$ behaves like $\widetilde{\mathcal{F}}_\sigma$. Alice sends her side of the correlation (t, a) and $k \leftarrow \mathbb{Z}_{\mathrm{minord}(H)}$ to Sim. Sim then sends $(t_1, a_1) = (kt, ka)$ and $(t_2, a_2) = (t, a)$ along with the function $\xi(u, b) = (u, kb \oplus -(k-1)\sigma(u))\big)$ to the $\mathcal{E}_\sigma$ functionality.
- Security against corrupt Bob: If Bob is passively corrupt $\widehat{\mathcal{F}}_\sigma$ behaves like $\widetilde{\mathcal{F}}_\sigma$. Bob sends his side of the correlation (u, b). Sim samples $k \leftarrow \mathbb{Z}_{\mathrm{minord}(H)}$ and sends it to Bob. Sim also sets $(u_1, b_1) = (u, kb \oplus -(k-1)\sigma(u))$, $(u_2, b_2) = (u, b)$ and specifies $\xi(t, a) = (kt, ka)$ to the functionality $\mathcal{E}_\sigma$.

Surjective Bi-Affine Correlation:

- No corruption: If both parties Alice and Bob are honest, then the adversary specifies the pair $\big((\tilde{t}, \tilde{a}), (\tilde{u}, \tilde{b})\big)$ produced during the the invocation of functionality $\widehat{\mathcal{F}}_\sigma$. Sim then specifies the distribution $\mathcal{D}$ as uniform over the set

$$\{\big((\tilde{t}, \sigma(\tilde{t} + \Delta u) \oplus -\sigma(\tilde{t}) \oplus \tilde{a}), (\Delta u + \tilde{u}, \tilde{b})\big) \mid \Delta u \leftarrow U\}$$

  Note that this is indeed the distribution of the output $\big((t_1, a_1)(u_1, b_1)\big)$ in the protocol execution. Sim also sends $\big((\tilde{t}, \tilde{a})(\tilde{u}, \tilde{b})\big)$. To complete the proof, we argue below that the output distributions in the real and ideal world are indistinguishable. Firstly, note that the error preservation property of $\mathsf{Comp}_{\sigma|_{\mathrm{TAU}}}$ implies that $\sigma(\tilde{t} + 0_U) \oplus -\sigma(\tilde{t} + \Delta u) \oplus e_1 \oplus \sigma(\tilde{t} + \Delta u) \oplus -\sigma(\tilde{t}) = \tilde{e}$ where $a_1 \oplus b_1 = e_1 \oplus \sigma(t_1 + u_1)$ and $\tilde{a} \oplus \tilde{b} = \tilde{e} \oplus \sigma(\tilde{t} + \tilde{u})$.
  We now show that when σ is surjective and Δ_u is sampled uniformly at random from U, then $\sigma(\tilde{t} + \Delta u) \oplus -\sigma(\tilde{t})$ is uniform over H. Define the set $U_0 = \{u_0 \mid \sigma(\tilde{t} + u_0) = \sigma(\tilde{t} + 0_U)$. Since σ is surjective, this set is non-empty. For every $u_0 \in U_0$ $\exists\, u_r$ such that $\sigma(\tilde{t} + u_r) = r$. A bijective map from the solutions of $\sigma(\tilde{t} + u_0) = \sigma(\tilde{t} + 0_U)$ is $u_0 \to u_0 + u_1$, where u_1 is some solution of $\sigma(\tilde{t} + u_r) = r$. $u_0 + u_1$ is a valid solution since $\sigma(\tilde{t} + u_0 + u_1) = \sigma(\tilde{t} + u_0) - \sigma(\tilde{t} + 0_U) + \sigma(\tilde{t} + u_1) = \sigma(\tilde{t} + u_1) = r$. The map is bijective since $u_0 + u_1 = u_0' + u_1 \Rightarrow u_0 = u_0'$. Thus, if Δu is sampled uniformly at random from U, then $\sigma(\tilde{t} + \Delta u)$ is uniformly random over H and hence $\sigma(\tilde{t} + \Delta u) \oplus -\sigma(\tilde{t})$ is uniform over H.
  E_{t_0} is the distribution $\{-\sigma(t_0 + u') \oplus e' \oplus \sigma(t_0 + u') \mid e' = a' \oplus b' \oplus -\sigma(t' + u'),\ \big((t', a'), (u', b')\big) \in \mathcal{D}\}$. This can now be rewritten as $\{r \oplus e \oplus -r \mid r \leftarrow H\}$, where $e = a \oplus b \oplus -\sigma(t + u)$.
  - If $e \neq 0$, the min-entropy of $\mathcal{D}$ is $\mathrm{H}_\infty(E_{t_0}) = \log \mathrm{minorbit}(H) = \omega(\log \lambda)$ and the check passes, hence the output $\big((t_2, a_2), (u_2, b_2)\big) = \big((\tilde{t}, \tilde{a})(\tilde{u}, \tilde{b})\big)$ is indistinguishable from that in the real world.
  - If $e = 0$, then the min-entropy check fails since the $\mathrm{H}_\infty(E_{t_0}) = 0$. However, this means that $\big((\tilde{t}, \tilde{a})(\tilde{u}, \tilde{b})\big) \in \mathsf{BA}_\sigma$ and thus $\big((t_2, a_2), (u_2, b_2)\big) = \big((\tilde{t}, \tilde{a})(\tilde{u}, \tilde{b})\big)$. Again, the output is indistinguishable from that in the real world.
- Security against corrupt Alice: If Alice is passively corrupt $\widehat{\mathcal{F}}_\sigma$ behaves like $\widetilde{\mathcal{F}}_\sigma$. Alice specifies her side of the correlation $(\tilde{t}, \tilde{a})$ to Sim. Now, Sim samples $\Delta u \leftarrow U$ and sends it to Alice in the half-$\mathsf{Comp}_{\sigma|_{\mathrm{TAU}}}$ protocol. Sim also sets $(t_1, a_1) = (\tilde{t}, \sigma(\tilde{t} + \Delta u) \oplus -\sigma(\tilde{t}) \oplus a)$ and $(t_2, a_2) = (\tilde{t}, \tilde{a})$ and specifies the function $\xi(u_2, b_2) = (\Delta u + u_2, b_2)$.

- Security against corrupt Bob: If Bob is passively corrupt $\widehat{\mathcal{F}}_\sigma$ behaves like $\widetilde{\mathcal{F}}_\sigma$. Bob specifies his side of the correlation $(\tilde{u}, \tilde{b})$ along with $\Delta u \leftarrow U$. Sim now sets $(u_1, b_1) = (\Delta u + \tilde{u}, \tilde{b})$, $(u_2, b_2) = (\tilde{u}, \tilde{b})$ and specifies the function $\xi(t_2, a_2) = (t_2, \sigma(t_2 + \Delta u) \oplus -\sigma(t_2) \oplus a_2))$.

□

E Details Omitted from Section 6

Theorem 2 (Restated). *The protocol in Figure 10 is a UC-secure protocol for the Alternate Summation functionality $\mathcal{F}_{D,n}^{\text{altsum}}$ over a non-abelian group D, in the $\mathcal{F}_{\sigma_D^{\text{ZAS}}|\text{TAU}}$ hybrid model.*

Correctness: Bob computes the output of the flattened sum function $f(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n)$ as $\sum_{i\in[n-1]}(x'_i - y'_i) + x'_n + y_n = \sum_{i\in[n-1]}(-r_i + x_i + s_i - s_i + y_i + r_{i+1}) + x'_n + y_n = -r_1 + (\sum_{i\in[n-1]}(x_i + y_i)) + r_n + (-r_n + x_n + s_n + y_n) = \sum_{i\in[n]}(x_i + y_i)$ (since $r_1 = s_n = 0$). Hence, correctness holds.

Security: The protocol in Figure 10 is in fact a perfectly UC-secure protocol for the $\mathcal{F}_{D,n}^{\text{altsum}}$ functionality.

- Simulation against corrupt Alice: On receiving $\{x'_i\}_{i\in[n]}$ and $\{(-s_i, r_{i+1})\}_{i\in[n-1]}$ from Alice, the simulator sets $r_1 = s_n = 0$, and extracts $x_i := r_i + x'_i - s_i$, for $i \in [n]$, and sends it to the functionality as Alice's input.
- Simulation against corrupt Bob: First the simulator samples random $x'_i \leftarrow D$ for each $i \in [n]$. Then, on receiving each y_i from Bob (as his input to a simulated invocation of $\mathcal{F}_{\sigma_D^{\text{ZAS}}|\text{TAU}}$), the simulator responds with a random value y'_i, except for the last one, say y_k. (Since the instances are invoked in parallel, Bob can invoke them in any order he wishes.) At this point, having received y_i for all $i \in [n]$, the simulator inputs them to $\mathcal{F}_{D,n}^{\text{altsum}}$ and obtains an output a. It then sets y'_k such that $a = (\sum_{i\in[n-1]}(x'_i - y'_i)) + x'_n + y_n$. Now, in the real execution too, until the last instance of $\mathcal{F}_{\sigma_D^{\text{ZAS}}|\text{TAU}}$ is invoked, each y'_i received is uniformly randomly distributed, independent of Alice's inputs and Bob's view thus far.
  This can be seen by considering Bob's view and Alice's input together as consisting of a graph on the nodes $\{r_i, s_i\}_{i\in[n]}$, with all the edges of the form (r_i, s_i) (corresponding to x_i and x'_i being fixed) and edges of the form (s_i, r_{i+1}) for those i for which $\mathcal{F}_{\sigma_D^{\text{ZAS}}|\text{TAU}}$ has been invoked (corresponding to y_i and y'_i being fixed). Note that this graph consists of connected components which are in the form of paths $(r_i, s_i, r_{i+1}, \cdots, s_j)$. Now, when the k^{th} instance of $\mathcal{F}_{\sigma_D^{\text{ZAS}}|\text{TAU}}$ is being invoked, if this is not the last invocation, then it must be the case that the corresponding edge (s_k, r_{k+1}) would lie in a connected component of the form $(r_i, \cdots, s_j)$ where either $i \neq 1$ or $j \neq n$ (because otherwise all $n-1$ invocations would have been made). Say, e.g., $i \neq 1$. Then for each choice of value for r_i there is a different value of y'_k that can be uniquely solved to be consistent with the view so far (and a choice of s_j, if $j \neq n$).
  Further, by correctness, the last y'_i received, conditioned on the previous values, is fully determined by the condition $\sum_{i\in[n]}(x_i + y_i) = (\sum_{i\in[n-1]}(x'_i - y'_i)) + x'_n + y_n$, in both cases.

F 2PC in the Pre-Processing model

Recently, Boyle et. al. [5] showed that given a function secret sharing scheme for *offset* gates, it is possible to perform secure two party computation. The authors give explicit constructions for a

variety of gates including bi-linear gates over abelian groups. Here we give a scheme where a dealer provides circuit dependent correlations using which parties can evaluate bi-affine gates. While this scheme does not provide any significant advantages over the protocol using random correlations, it is still instructive to show how our framework can be used in different settings.

In Figure 13 we give a passive secure protocol for $\mathcal{G}_{\sigma|\text{TAU}}$, when Alice and Bob do not collude with each other. To help with securely computing this functionality even if Carol is actively corrupt, we allow Alice, Bob and Carol to access the following 3-party functionality $\tilde{\mathcal{G}}_\sigma$. It lets Carol specify (t, u), and outputs a correlation $\big((t_1, u_1, a), (t_2, u_2, b)\big)$ to Alice and Bob conditioned on $t_1 + t_2 = t, u_1 + u_2 = u$ and $\sigma(t_1 + t_2 + u_1 + u_2) = a \oplus b$. (Security against actively corrupt Carol is not important for our specific application, but we use the functionality $\tilde{\mathcal{G}}_\sigma$ to highlight the fact that Alice and Bob receive a sample satisfying required constraints.)

Biasable Sampling Functionality $\tilde{\mathcal{G}}_\sigma$
(where $\sigma : Q \to H$ and $T, U \leqslant Q$)

Inputs: Carol has input $(t, u) \in T \times U$.
Output: (t_1, u_1, a) to Alice, (t_2, u_2, b) to Bob and $\perp$ to Carol, where $((t_1, u_1, a), (t_2, u_2, b)) \leftarrow \{(t'_1, u'_1, a'), (t'_2, u'_2, b') \mid t'_1 + t'_2 = t, u'_1 + u'_2 = u, a' \oplus b' = \sigma(t + u)\}$.

Lemma 20. $\mathsf{xComp}_{\sigma|\text{TAU}}$ *(Figure 13) securely realizes the functionality $\mathcal{G}_{\sigma|\text{TAU}}$ in an adversary model where Alice and Bob do not collude with each other and can only be passively corrupt, but Carol can be actively corrupt.*

Proof: **Correctness.** We verify that if Charlie, Alice, Bob are honest, then Alice, Bob's output s are such that $s \oplus 0 = \sigma(t_1 + t_2 + u_1 + u_2)$. We have:

$$\begin{aligned}
s &= s_1 \oplus s_2 \oplus s_3 \oplus s_4 \oplus s_5 \oplus s_6 \oplus s_7 \oplus s_8 \\
&= [\sigma(t_1 + u_1) \oplus -\sigma(u_1) \oplus \sigma(t'_1 + u_1)] \\
&\oplus [-\sigma(u_1) \oplus \sigma(t'_2 + u_1) \oplus -\sigma(t'_2) \oplus \sigma(0)] \\
&\oplus [-\sigma(t'_1) \oplus \sigma(0) \oplus -\sigma(t_1) \oplus \sigma(t_1 + u'_1)] \\
&\oplus [-\sigma(t_1) \oplus \sigma(t_1 + u'_2) \oplus -\sigma(u'_2) \oplus \sigma(0)] \\
&\oplus [-\sigma(u'_1) \oplus a']\big) \oplus [b'] \oplus [a''] \oplus [b''] \\
&= \sigma(t_1 + t'_1 + t'_2 + u_1 + u'_1 + u'_2) \oplus a \\
&= \sigma(t_1 + t_2 + u_1 + u_2) \oplus a
\end{aligned}$$

where, we used the properties of bi-affine homomorphisms and the fact that $a' \oplus b' = \sigma(t'_1 + t'_2 + u'_1 + u'_2)$.

Proof of Security. Security against Charlie is trivial as he does not receive any messages during the protocol. The view of Alice and Bob during the protocol consists of their shares which are uniformly random elements and their final output s. Hence, they do not learn any more information in the real world as compared to the the ideal world.

□

Protocol $\times\mathsf{Comp}_{\sigma|\text{TAU}}$ in the $\tilde{\mathcal{G}}_\sigma$, $\mathcal{F}_{H,4}^{\text{altsum}}$ hybrid model

- **Inputs:** Alice, Bob receive (t_1, u_1) and Carol receives (t_2, u_2, a_2).
- **Invocation of $\tilde{\mathcal{G}}_\sigma$:** Carol feeds $(t_2, u_2, \sigma(t_2 + u_2))$. Alice gets (t_1', u_1', a') and Bob gets (t_2', u_2', b') where, $t_1' + t_2' = t_2$, $u_1' + u_2' = u_2$ and $a' \oplus b' = \sigma(t_1' + t_2' + u_1' + u_2') = \sigma(t_2 + u_2)$.
- **Carol:** Carol sends a'' to Alice and b'' to Bob such that $a'' + b'' = -a_2$.
- **Alice:** Alice computes (s_1, s_3, s_5, s_7) as:

$$s_1 = \sigma(t_1 + u_1) \oplus -\sigma(u_1) \oplus \sigma(t_1' + u_1) \qquad s_3 = -\sigma(t_1') \oplus \sigma(0) \oplus -\sigma(t_1) \oplus \sigma(t_1 + u_1')$$
$$s_5 = -\sigma(u_1') \oplus a' \qquad s_7 = a''$$

- **Bob:** Bob computes (s_2, s_4, s_6, s_8) as:

$$s_2 = -\sigma(u_1) \oplus \sigma(t_2' + u_1) \oplus -\sigma(t_2') \oplus \sigma(0) \qquad s_4 = -\sigma(t_1) \oplus \sigma(t_1 + u_2') \oplus -\sigma(u_2') \oplus \sigma(0)$$
$$s_6 = b' \qquad s_8 = b''$$

- **Invocation of $\mathcal{F}_{H,4}^{\text{altsum}}$** Alice and Bob invoke $\mathcal{F}_{H,4}^{\text{altsum}}$ with inputs (s_1, s_3, s_5, s_7) and (s_2, s_4, s_6, s_8). Bob receives s as output and sends this to Alice.
- **Output:** Alice, Bob output s.

Figure 13: Passively-secure protocol for $\mathcal{G}_{\sigma|\text{TAU}}$ in the $\tilde{\mathcal{G}}_\sigma$, $\mathcal{F}_{H,4}^{\text{altsum}}$ hybrid model.