Advanced Tools from Modern Cryptography

Lecture 2

First Tool: Secret-Sharing

Secret-Sharing

- Dealer encodes a message into n shares for n parties
  - Privileged subsets of parties should be able to reconstruct the secret
  - View of an unprivileged subset should be independent of the secret
- Very useful
  - Direct applications (distributed storage of data or keys)
  - Important component in other cryptographic constructions
    - Secure multi-party computation
    - Attribute-Based Encryption
    - Leakage resilience ...

Threshold Secret-Sharing

- (n,t)-secret-sharing
  - Divide a message m into n shares $s_1,\ldots,s_n$, such that
    - any t shares are enough to reconstruct the secret
    - up to t-1 shares should have no information about the secret
- Recall last time: (2,2) secret-sharing

e.g., $(s_1,\ldots,s_{t-1})$ has the same distribution for every m in the message space

Threshold Secret-Sharing

Additive Secret-Sharing

- Construction: (n,n) secret-sharing
  - Message-space = share-space = G, a finite group
    - e.g. $G = \mathbb{Z}_2$ (group of bits, with xor as the group operation)
    - or, $G = \mathbb{Z}_2{}^d$ (group of d-bit strings)
    - or, $G = \mathbb{Z}_p$ (group of integers mod p)
  - Share(M):
    - Pick $s_1,\ldots,s_{n-1}$ uniformly at random from G
    - Let $s_n = -(s_1 + \ldots + s_{n-1}) + M$
  - Reconstruct($s_1,\ldots,s_n$): $M = s_1 + \ldots + s_n$
  - Claim: This is an (n,n) secret-sharing scheme [Why?]

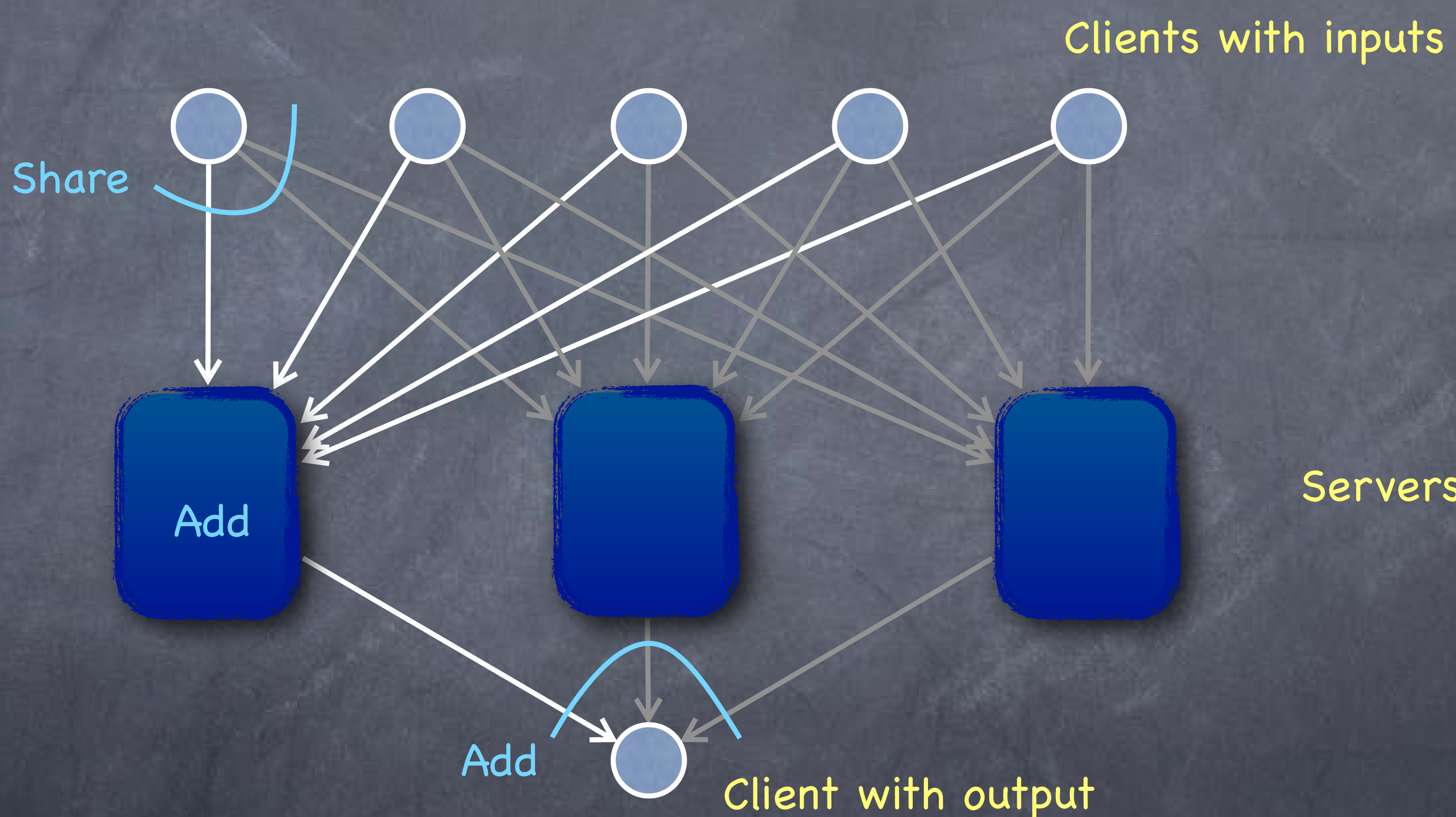
PROOF

Additive Secret-Sharing: Proof

- Share(M):
  - Pick $s_1,\ldots,s_{n-1}$ uniformly at random from G
  - Let $s_n = M - (s_1 + \ldots + s_{n-1})$
- Reconstruct($s_1,\ldots,s_n$): $M = s_1 + \ldots + s_n$
- Claim: Upto n-1 shares give no information about M
- Proof: Let $T \subseteq \{1,\ldots,n\}$, $|T| = n-1$. We shall show that $\{ s_i \}_{i\in T}$ is distributed the same way (in fact, uniformly) irrespective of what M is.
  - For concreteness consider $T = \{2,\ldots,n\}$. Fix any (n-1)-tuple of elements in G, $(g_1,\ldots,g_{n-1}) \in G^{n-1}$. To prove $\Pr[\ (s_2,\ldots,s_n)=(g_1,\ldots,g_{n-1})\ ]$ is same for all M.
  - Fix any M.
  - $(s_2,\ldots,s_n) = (g_1,\ldots,g_{n-1}) \Leftrightarrow (s_2,\ldots,s_{n-1}) = (g_1,\ldots,g_{n-2})$ and $s_1 = M-(g_1+\ldots+g_{n-1})$.
  - So $\Pr[\ (s_2,\ldots,s_n)=(g_1,\ldots,g_{n-1})\ ] = \Pr[\ (s_1,\ldots,s_{n-1})=(a,g_1,\ldots,g_{n-2})\ ]$, $a:=(M-(g_1+\ldots+g_{n-1})$
  - But $\Pr[(s_1,\ldots,s_{n-1})=(a,g_1,\ldots,g_{n-2})] = 1/|G|^{n-1}$, since $(s_1,\ldots,s_{n-1})$ are picked uniformly at random from G
  - Hence $\Pr[\ (s_2,\ldots,s_n)=(g_1,\ldots,g_{n-1})\ ] = 1/|G|^{n-1}$, irrespective of M. □

An Application

- Gives a "private summation" protocol (for commutative groups)



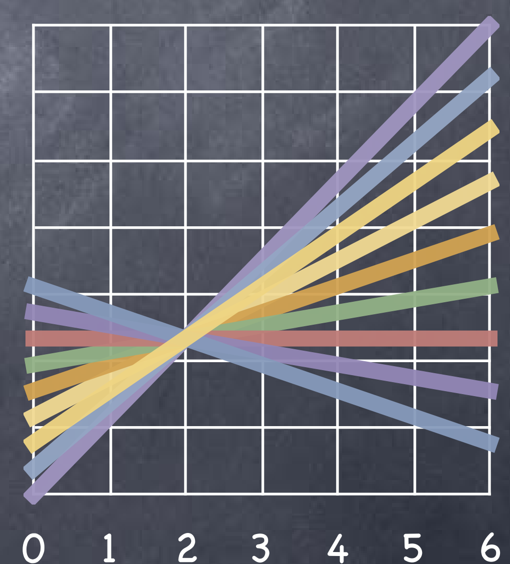
- "Secure against passive corruption" (i.e., no colluding set of servers/clients learn more than what they must) if at least one server stays out of the collusion

Threshold Secret-Sharing

- Construction: (n,2) secret-sharing
- Message-space = share-space = F, a finite field (e.g. integers mod prime)
  - Share(M): pick random r. Let $s_i = r \cdot a_i + M$ (for $i=1,\ldots,n < |F|$)

    a_i are n distinct, non-zero field elements
  - Reconstruct(s_i, s_j): $r = (s_i-s_j)/(a_i-a_j)$; $M = s_i - r \cdot a_i$
  - Each s_i by itself is uniformly distributed, irrespective of M [Why?]

    Since a_i^{-1} exists, exactly one solution for $r \cdot a_i+M=d$, for every value of d
  - "Geometric" interpretation
    - Sharing picks a random "line" $y = f(x)$, such that $f(0)=M$. Shares $s_i = f(a_i)$.
    - s_i is independent of M: exactly one line passing through (a_i,s_i) and $(0,M')$ for any secret M'
    - But can reconstruct the line from two points!



PROOF

(n,2) Secret-Sharing: Proof

- Share(M): pick random $r \leftarrow F$. Let $s_i = r \cdot a_i + M$ (for $i=1,\dots,n < |F|$)
- Reconstruct(s_i, s_j): $r = (s_i-s_j)/(a_i-a_j)$; $M = s_i - r \cdot a_i$

- Claim: Any one share gives no information about M
- Proof: For any $i \in \{1,..,n\}$ we shall show that s_i is distributed the same way (in fact, uniformly) irrespective of what M is.
- Consider any $g \in F$. We shall show that $\Pr[\ s_i=g\ ]$ is independent of M.
- Fix any M.
- For any $g \in F$, $s_i = g \Leftrightarrow r \cdot i + M = g \Leftrightarrow r = (g-M) \cdot a_i^{-1}$ (since $a_i \neq 0$)
- So, $\Pr[\ s_i=g\ ] = \Pr[\ r=(g-M) \cdot a_i^{-1}\ ] = 1/|F|$, since r is chosen uniformly at random □

Threshold Secret-Sharing

Shamir Secret-Sharing

- (n,t) secret-sharing in a (large enough) field F
- Generalizing the geometric/algebraic view: instead of lines, use polynomials
  - Share(m): Pick a random degree t-1 polynomial $f(X)$, such that $f(0)=M$. Shares are $s_i = f(a_i)$.
    - Random polynomial with $f(0)=M$: $c_0 + c_1X + c_2X^2 + \ldots + c_{t-1}X^{t-1}$ by picking $c_0=M$ and $c_1,\ldots,c_{t-1}$ at random.
  - Reconstruct($s_1,\ldots,s_t$): Lagrange interpolation to find $M=c_0$
    - Need t points to reconstruct the polynomial. Given t-1 points, out of $|F|^{t-1}$ polynomials passing through $(0,M')$ (for any M') there is exactly one that passes through the t-1 points

Lagrange Interpolation

- Given t distinct points on a degree t–1 polynomial (univariate, over some field of more than t elements), reconstruct the entire polynomial (i.e., find all t coefficients)
  - t variables: $c_0,\ldots,c_{t-1}$. t equations: $1.c_0 + a_i.c_1 + a_i^2.c_2 + \ldots a_i^{t-1}.c_{t-1} = s_i$
  - A linear system: $W\mathbf{c}=\mathbf{s}$, where W is a txt matrix with i^{th} row, $W_i= (1\ a_i\ a_i^2 \ldots a_i^{t-1})$
  - W (called the Vandermonde matrix) is invertible
    - $\mathbf{c} = W^{-1}\mathbf{s}$

Linear Secret-Sharing

- Share(M): For some fixed n×t matrix W, let $\overline{s} = W \cdot \overline{c}$, where $c_0 = M$ and other t-1 coordinates are random
  - The shares are subsets of coordinates of $\overline{s}$

Shamir Secret-Sharing is of this form

- Reconstruction: pool together all the available coordinates of $\overline{s}$; can reconstruct if there are enough equations to solve for c_0
  - Claim: If not reconstructible, shares independent of secret
- May not correspond to a threshold access structure
- Reconstruction too is a linear combination of available shares (coefficients depending on which subset of shares available)

Linear Secret-Sharing

- Claim: If not reconstructible, shares independent of secret
- Suppose $T \subseteq [n]$ s.t. c_0 not reconstructible from s_T
  - i.e., solution space for $W_T \cdot \overline{c} = s_T$ is an affine subspace of some dimension $d \geq 1$, and contains at least two points with distinct values α and β for c_0
  - Then, $\forall \gamma \in F$, the solution space has a point with $c_0 = \gamma$ (e.g., linearly combine the above points with factors $(\gamma-\beta)/(\alpha-\beta)$ and $(\alpha-\gamma)/(\alpha-\beta)$)
  - Therefore, for any $\gamma \in F$, can add equation $c_0 = \gamma$ and get a solution space of dimension $d-1$
    - i.e., with $x_0 = \gamma$, exactly $|F|^{d-1}$ choices of randomness that give s_T
  - i.e., for all s_T and γ, $\Pr[\text{view}=s_T \mid M=\gamma] = |F|^{d-1}/|F|^{t-1}$

Today

- Secret-sharing schemes
  - (n,t) Threshold secret-sharing
    - Additive sharing for (n,n)
    - Shamir secret-sharing for all (n,t)
      - Optimal (ideal) when |message-space| is a prime-power, larger than n
  - Linear secret-sharing