IITB TRUST LAB

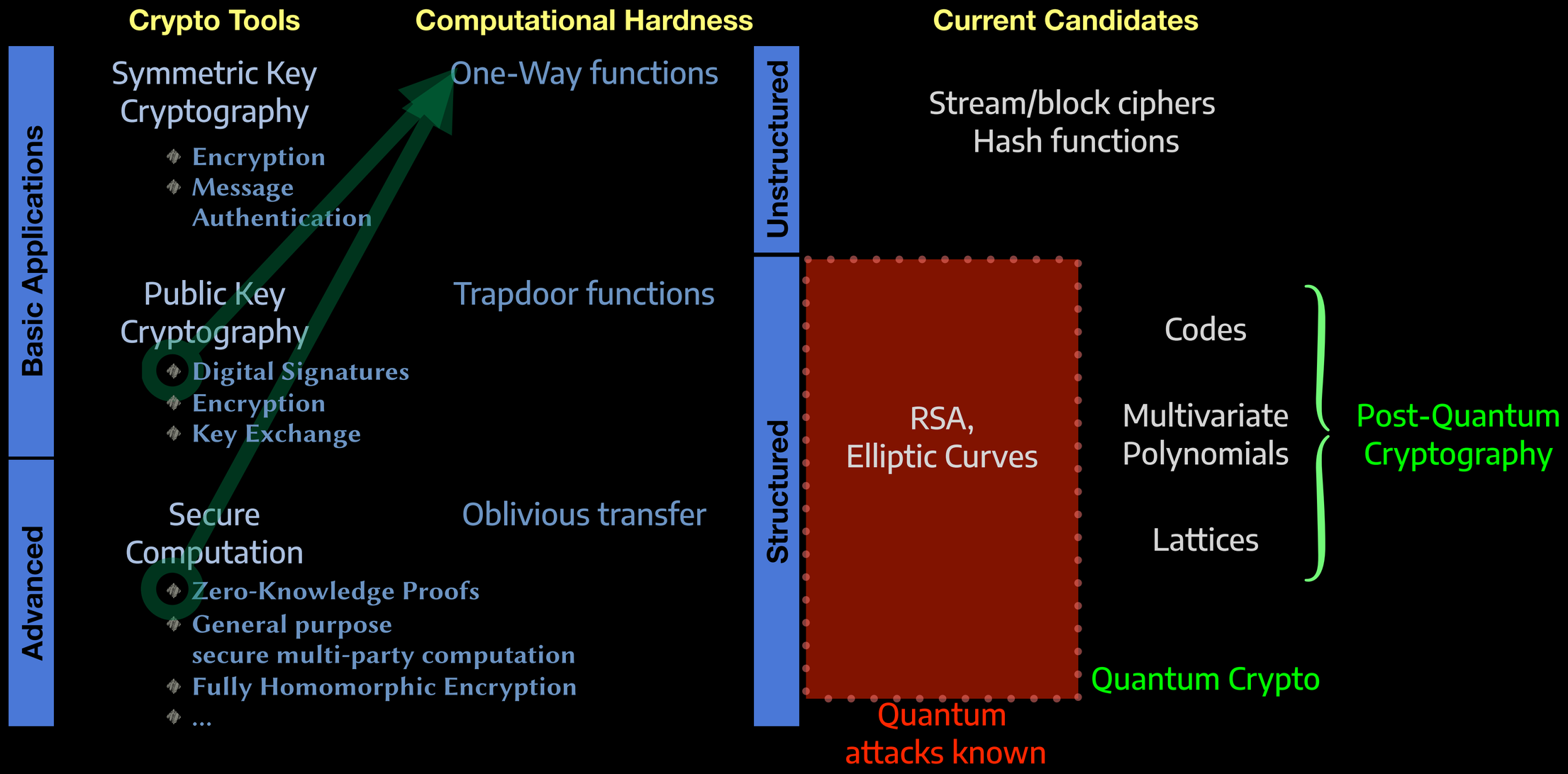
DIGITAL : SECURE : RESPONSIBLE

Post-Quantum & Quantum Cryptography

An Overview

Lecture 15

Cryptography Landscape



Quantum Attacks

- Quantum computation models: Manipulate and measure quantum mechanical states, to compute. Theory starting in 80's.
  - A large number of techniques for physically realising quantum computing
  - Already practical in small scales and/or for specialised tasks
- Polynomial time algorithms exist in this model for breaking mainstream public-key cryptography
  - Shor's algorithm for Integer Factorisation (1994)
    - Generalises to the (abelian) Hidden Subgroup Problem
    - "Breaks" RSA and Elliptic Curve Cryptography
- Also, algorithms that reduce the level of security for symmetric-key cryptography: Grover Search (1996), Brassard-Høyer-Tapp collision algorithm (1997), ...

Quantum Attacks

- Current physical realisations of quantum computers are far from posing a threat using quantum attacks
  - E.g., for integer factorisation, the current record using classical computers is to factorise an 829-bit challenge (in 2020)
    - Not considered a threat to 2048-bit RSA
  - Using Quantum computation:
    - Using only Shor's algorithm: 21 = 7 x 3 (in 2012)
    - Using Adiabatic Quantum Computing: < 20 bits (in 2017)
    - With "hybrid" computation models using "QAOA": < 50 bits (in 2022)
- But Shor's algorithm scales very differently from classical algorithms

Post-Quantum Cryptography

a.k.a. Quantum Resistant Cryptography

- We already have some “quantum resistant” candidates to replace RSA and ECC
  - Main candidates employ **Lattice-based cryptography**
  - Other candidates: Code-based, Multivariate polynomials-based
  - **Recent shock:** Isogeny-based cryptography, a leading approach studied for over a decade, was completely (and classically) broken a few months back!
    - **Caution:** PQC candidates may turn out to be less secure than current schemes. They should be used in conjunction with current schemes rather than instead of them.
- Big picture for users of secure communication: PQC is for the future
  - When necessary, high-level standards like TLS will incorporate standardised PQC algorithms
  - For long-term secrecy, may use current PQC candidates now, but only in combination with current standards (using longer keys, when possible)

Of great independent interest in cryptography

Quantum Cryptography

- Cryptography using basic elements of quantum computing
  - Main(stream) application: Quantum Key Distribution [Bennett-Brassard'84,...]
  - Commercially available. Needs a quantum communication channel.
- Original motivation: Secrecy against a computationally unbounded adversary
  - Or, security without relying on computational hardness assumptions
  - Important caveat: Still needs an authenticated (classical) channel
- Yields a post-quantum cryptography candidate

Using Qubits for QKD

- Involves Alice send “qubits” to Bob over a quantum channel, encoded as, e.g., polarised photons
- **Basic principle: Measuring alters the system**
- A metaphor:
  - Qubits are “cards” that can be read using “card readers.” Cards come in two colors (red and blue), and have a value 0/1 on them. Cannot tell the colour or the value of a card w/o “reading” it
  - If a card is inserted into a reader of the same colour, it reports the value on the card correctly.
  - But if it is inserted into a reader of the other colour, then the card gets transformed into the reader’s colour with a random value! And the reader will report that value

Not exploiting all possibilities here. But enough for BB84.

BB84

Alice

Bob

Prepare several cards, with random colors and values
Send the cards to Bob (via Eve)

Read all cards using red or blue readers randomly.

Tell Alice which colour reader was used for each card

Now tell Bob which colour each card originally was

Discard all cards which were read using the wrong color

Among the undiscarded cards, Alice and Bob check for consistency:

Send values obtained for a random subset of the cards

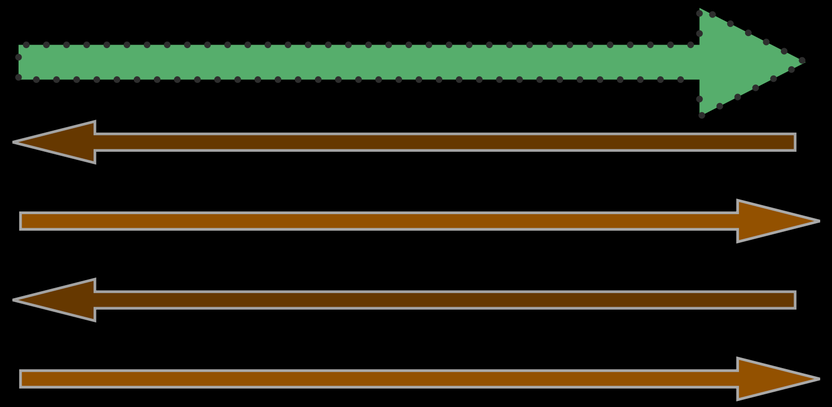
If any value wrong, abort

If consistency check OK, Alice and Bob “almost agree on” the values on the remaining cards and it is “mostly hidden” from Eve: **Raw keys**

BB84

Alice

Bob



If consistency check OK, Alice and Bob “almost agree on” the values on the remaining cards and it is “mostly hidden” from Eve: **Raw keys**

- Raw keys are refined into proper keys, so that both parties exactly agree on the key, and it is fully hidden from Eve (except for a negligible error)
- Two steps: Reconciliation (leading to further leakage) and Privacy Amplification
- Privacy Amplification simply uses a strong randomness extractor (recall)

Quantum Cryptography

QKD History

- BB84 implemented at IBM Research in 1989: 32cm free air quantum channel
- Geneva, 2002: 23 km optical fiber cable quantum channel
  - 421 km in 2018
- DARPA network, Boston (since 2003): Between Boston University, Harvard and BBN Technologies
  - With wireless links too
- Tokyo QKD Network, 2011: 90 km optical fiber
- Earth-Space QKD (2017) using a Chinese satellite

Quantum Cryptography

QKD Caveats

- Important caveat: Needs an authenticated (classical) channel
  - Can be implemented using a short shared-key (no computational hardness)
  - But if we have a shared-key, do we need QKD?

Using digital signatures based on symmetric-key crypto

Need to generate very long keys

	No pre-shared key			With a pre-shared key		
Adversary / Crypto power	Non-Quantum	Future Quantum	Quantum	Non-Quantum	Future Quantum	Quantum
PQ Crypto	C	C	C	C	C	C
PQ-Symmetric Crypto & Non-PQ Crypto	C	Q	Q	C	C	C
Non-PQ Crypto	C	Q	X	C	Q	Q
No Crypto	X	X	X	Q	Q	Q

Quantum Cryptography

QKD Caveats

- Important caveat: Needs an authenticated (classical) channel
  - Can be implemented using a short shared-key (no computational hardness)
  - QKD relevant in only certain situations
- No standards yet (even for quantum communication)
  - Implementation-specific attacks possible
  - Not tested in the wild (cf. many breaks/fixes for protocols like SSL and TLS)
- Side-channels are not well-understood
- Bottom line: Need more research (e.g., on side-channels), development (protocol standardisation, tested software), and industrial standards (e.g., designed for which situation) before serious deployment