A Quick Tour of Cryptographic Protocols Zoo

Yu Zhang

Harbin Institute of Technology

Cryptography, Autumn, 2022

What's in the zoo?

https://www.eliottbulpett.com/zoo-map

Outline

Content

Protocols (Animals)

- **Communications protocol** is a formal description of digital message formats and the rules for exchanging those messages for a specific purpose.
  - Protocols are to communications what algorithms are to computations
  - Everyone must know it and agree to follow it
- **Unambiguous**: each step must be well defined and there must be no chance of a misunderstanding
- **Complete**: there must be a specified action for every possible situation
- **Cryptographic protocol**: Additionally, it should not be possible to do more or learn more than what is specified in the protocol

Protocol Types

- **Arbitrated protocols**: An arbitrator is a disinterested third party trusted to complete a protocol.
- **Adjudicated protocols**: An adjudicator is also a disinterested and trusted third party. Unlike an arbitrator, he is not directly involved in every protocol unless .
- **Self-enforcing protocols**: the best type of protocol. The protocol itself guarantees fairness.

How to split a cake equally between two kids?

Attacks against Protocols

- **Passive attacks**: the attacker does not affect the protocol.
- **Active attacks**: the attacker alters the protocol to his own advantage.

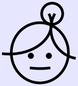
Cheater: the attacker could be one of the parties involved in the protocol.

- **Passive cheaters**: follow the protocol, but try to obtain more information than the protocol intends them to.
- **Active cheaters**: disrupt the protocol in progress in an attempt to cheat.

Content

Three-Pass Protocol

Purpose: communication without shared keys
Requirement: $\mathsf{Dec}_{k_1}(\mathsf{Enc}_{k_2}(\mathsf{Enc}_{k_1}(m))) = \mathsf{Enc}_{k_2}(m)$
Shamir Protocol: p is a prime, find e, d with $\gcd(e, p-1) = 1$ and $ed \equiv 1 \pmod{p-1}$

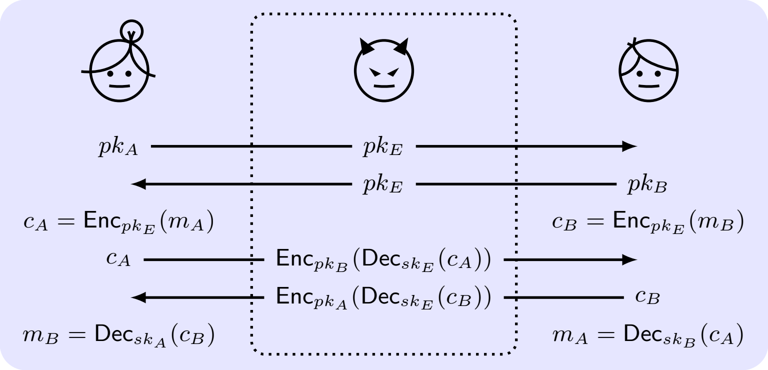


Alice		Bob
p, e_A, d_A		p, e_B, d_B
$c = [m^{e_A} \bmod p]$	$\longrightarrow$	
	$\longleftarrow$	$c_1 = [c^{e_B} \bmod p]$
$c_2 = [c_1^{d_A} \bmod p]$	$\longrightarrow$	
		$m = [c_2^{d_B} \bmod p]$

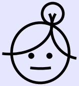
$c_2^{d_B} = c_1^{d_A \cdot d_B} = c^{e_B \cdot d_A \cdot d_B} = m^{e_A \cdot e_B \cdot d_A \cdot d_B} = m^{e_A d_A \cdot e_B d_B} = m$
Weakness: insecurity under the man-in-the-middle attack

The Man-In-The-Middle Attack

Also called **bucket-brigade attack**: A form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other



Purpose: foil the man-in-the-middle attack.



$$pk_A \longrightarrow$$

$$\longleftarrow pk_B$$

$$c_A = \mathsf{Enc}_{pk_B}(m_A) \qquad c_B = \mathsf{Enc}_{pk_A}(m_B)$$

$$(c_{A1} \| c_{A2}) = c_A \qquad (c_{B1} \| c_{B2}) = c_B$$

$$c_{A1} \longrightarrow$$

$$\longleftarrow c_{B1}$$

$$c_{A2} \longrightarrow$$

$$\longleftarrow c_{B2}$$

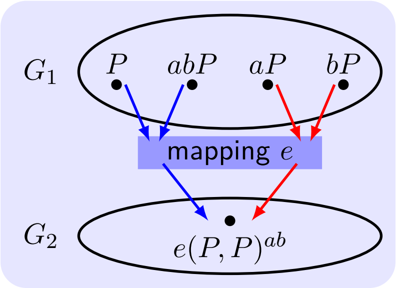
$$c_B = (c_{B1} \| c_{B2}) \qquad c_A = (c_{A1} \| c_{A2})$$

$$m_B = \mathsf{Dec}_{sk_A}(c_B) \qquad m_A = \mathsf{Dec}_{sk_B}(c_A)$$

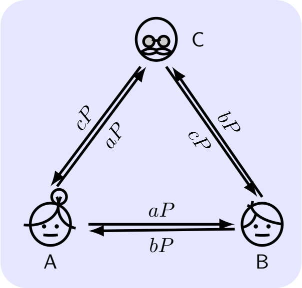
Content

Bilinear Maps

- Two cyclic groups: G_1 with $+$ and generator P, G_2 with $\times$.
- **Bilinear map** $e : G_1 \times G_1 \to G_2$ with $e(aP, bP) = e(P, P)^{ab}$.
- **Theorem**: When e is efficient, the Decisional Diffie-Helman is easy in G_1, as $e(aP, bP) = e(P, P)^{ab} = e(P, abP)$.
- The Weil and Tate pairings are bilinear maps. G_1 is an elliptic-curve group and G_2 is a finite field.



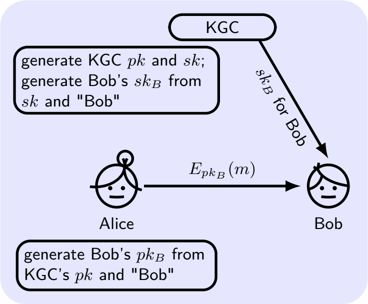
Jounx's Key Agreement Protocol



- Recall Jounx's one-round, 3-party key agreement protocol, where Alice computes the key $e(bP, cP)^a = e(P, P)^{abc}$.
- **Bilinear Diffie-Helman (BDH) Assumption**: computing $e(P, P)^{abc}$ is hard given $\langle P, aP, bP, cP \rangle$.
- **Theorem**: Given BDH assumption, Jounx's is secure.

Identity-Based Encryption

- **IBE**: Anyone can directly use receiver's ID (A) as the pubic key with help of a TTP, aka KGC (Key Generation Center). The receiver obtains its private key from KGC.
- **Strength**: TTP could be removed for a finite number of users, no need for PKI.
- **Weakness**: Single-point-of-failure, implicit key escrow.



Boneh-Franklin's IBE Scheme

Boneh-Franklin's IBE Scheme (2001):

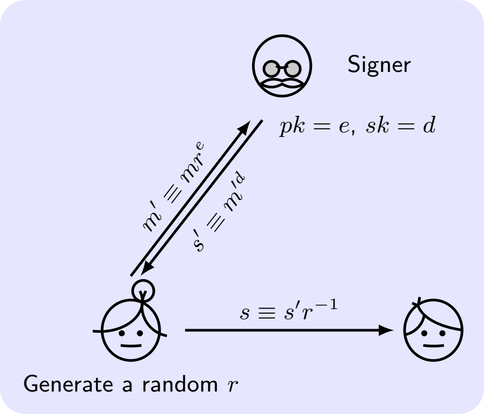
- **KGC** generates a global public key $pk = sP$ and $sk = s$.
- **Encryption**: $\mathsf{Enc}(sP, A, m) = \langle rP, m \oplus H_2(e(H_1(A), sP)^r)\rangle$, where r is a random string, H_1 and H_2 are random oracles.
- **Decryption**: The receiver obtains its private key $d_A = sH_1(A)$ from KGC. $\mathsf{Dec}(d_A, u, v) = v \oplus H_2(e(d_A, u))$.
- **Correctness**: $e(d_A, u) = e(sH_1(A), rP) = e(H_1(A), P)^{sr} = e(H_1(A), sP)^r$.

Content

Blind Signature

Blind signature is a form of digital signature in which the message is blinded before it is signed.

Chaum's blind signature: Alice asks for Signer to sign m blindly and then sends to Bob



$$s \equiv s'r^{-1} \equiv m'^d r^{-1} \equiv (mr^e)^d r^{-1} \equiv m^d.$$

Group Signature

Group Signature: allowing a member of a group to anonymously sign a message on behalf of the group (with a group manager)

- **Soundness**: valid sigs by members verify correctly
- **Unforaeable**: only members can create valid sigs
- **Anonymity**: signer can be determined only by manager
- **Traceability**: manager can trace which member signed
- **Unlinkability**: cannot tell if two sigs were from same signer
- **Exculpability**: cannot forge a sig for other/non members

A trivial group signature with trusted GM [Chaum (1991)]:

- **KeyGen**: GM generates a secret key list for each member and publishes all of public keys
- **Sign**: sign with an unused secret key
- **Verify**: try all of public keys

Ring Signature

Ring Signature: Group signature without group manager, and:

- cannot revoke the anonymity of an individual signature
- any group of users can be a group without additional setup

A ring signature based on bilinear map [Boneh et al. (2003)]:

- **KeyGen**: for member U_i: $sk = x_i \leftarrow Z_q, pk = Y_i = x_i P$.
- **Sign**: message m with $(\sigma_i), i = 1, \cdots, n$ by U_k:

$$\text{for } i \neq k, a_i \leftarrow Z_q, \sigma_i = a_i P; \quad \sigma_k = \frac{1}{x_k}(H(m) - \Sigma_{j \neq k} a_j Y_j)$$

- **Verify**:

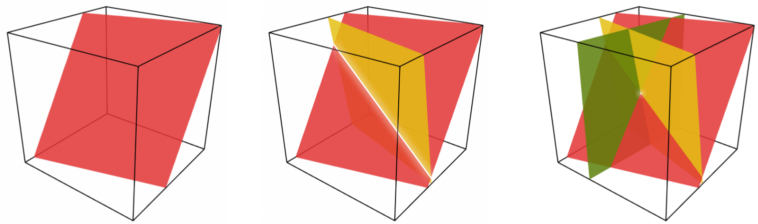
$$e(H(m), P) = \Pi_i e(Y_i, \sigma_i)$$

Content

Secret Sharing

Purpose: distribute a secret amongst a group of n participants, each of whom is allocated a share of the secret. The secret can be reconstructed only when a sufficient number of shares t are combined together. It is called (t, n)-**threshold scheme**.

Blakley's scheme: any n nonparallel n-dimensional hyperplanes intersect at a specific point.



Chinese remainder theorem: the shares of secret are generated by reduction modulo some relatively prime integers, and the secret is recovered by solving the system of congruences using the CRT.

Shamir's Secret Sharing

Adi Shamir "How to share a secret", Comm. of ACM, 1979.
t points define a polynomial of degree $t-1$,
$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$, where a_0 is the secret S, and a_i for $i \neq 0$ is chosen randomly. Choose n points $(x_i, f(x_i))$ for $i = 1, \ldots, n$ and send one point to each party.

An example of Shamir's secret sharing with $(t = 3, n = 6)$

$f(x) = 1234 + 166x + 94x^2 \mod 1613$, where $S = 1234$.
6 points: $(1, 1494), (2, 329), (3, 965), (4, 176), (5, 1188), (6, 755)$.
Attacker has 2 points $(1, 1494)$ and $(2, 329)$ and try to learn S.
$1419 = S + a_1 + a_2 - 1613m_1$, $329 = S + 2a_1 + 4a_2 - 1613m_2$,
$448 = a_1 + 3a_2 + 1613(m_1 - m_2)$, $(m_1 - m_2)$ could be any integer.
There are infinite possible values of a_1 and a_2, so that S is secured.

Strength: information theoretic security, extensible for n
Weakness: Issue with the verification of correctness of the retrieved shares (verifiable secret sharing).

Threshold Cryptography

(t, n)-**threshold scheme**: at least t of parties can efficiently decrypt/sign the ciphertext, while less than t have no useful information

Threshold Elgamal Cryptosystem:

- **Key sharing**: $sk = s, pk = h = g^s$. Party i obtains a share s_i with Shamir's scheme ((t, n)-threshold secret sharing) such that $s = \Sigma_i s_i \cdot \lambda_i$ with public info λ_i and publishes $h_i = g^{s_i}$
- **Enc**: $y \leftarrow \mathbb{Z}_q$, $\langle c_1, c_2 \rangle = \langle g^y, h^y \cdot m \rangle$
- **Dec**: Party i outputs $d_i = c_1^{s_i}$ and ZKP of $\log_g h_i = \log_{c_1} d_i$

$$m = c_2 / \Pi_i d_i^{\lambda_i}$$

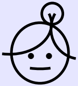
$$c_2 / \Pi_i d_i^{\lambda_i} = c_2 / \Pi_i c_1^{s_i \cdot \lambda_i} = c_2 / c_1^{\Sigma_i s_i \cdot \lambda_i} = c_2 / c_1^s = m$$

Content

Commitment Scheme

Commitment scheme allows one to commit to a value (which can not be changed later, **binding**) while keeping it hidden (**hiding**), with the ability to reveal the committed value

Coin flipping over telephone [Manuel Blum]:



$b \leftarrow \{H, T\}$

$m = b \| r$, r is random

$h = \mathsf{Hash}(m) \longrightarrow$

$\longleftarrow b' \in \{H, T\}$

$m \longrightarrow h \stackrel{?}{=} \mathsf{Hash}(m)$

Win if $b = b'$

Q1: Is Hash as CRHF enough for hiding?

Q2: Is it possible to achieve info.-theoretically binding and info.-theoretically hiding at the same time?

Content

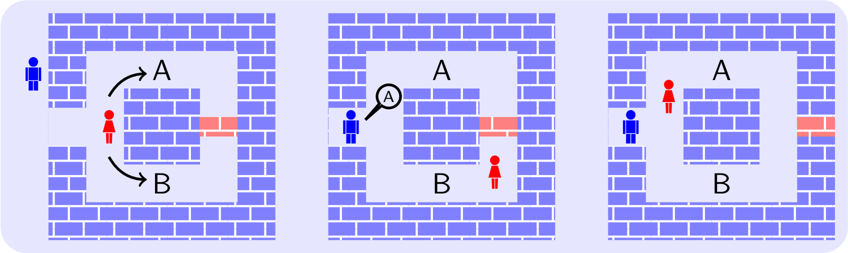
Zero-Knowledge Proof

O. Goldreich, S. Micali, A. Wigderson, "How to Play ANY Mental Game," ACM Conference on Theory of Computing, 1987

- **Interactive proof system** is an abstract machine that models computation as the exchange of messages between two parties: verifier and prover
- **Proof of knowledge**: an interactive proof in which **prover** succeeds convincing **verifier** that it knows something
- **Zero-knowledge proof (ZKP)**: an interactive proof *without revealing anything other than the veracity of the statement*
  - **Completeness**: if the statement is true, the honest "verifier" will be convinced by an honest prover
  - **Soundness**: if the statement is false, no cheating prover can convince the honest verifier
  - **Existence**: If OWF exists, ZKP exists for any NP-set
- Σ-**protocol**: ZKP in 3 rounds: announcement (commitment), challenge, and response

A Toy Example of ZKP

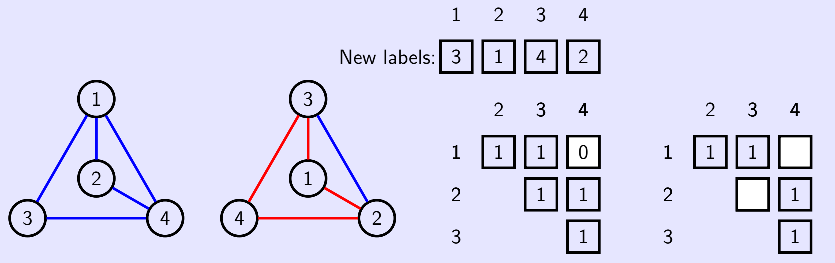
Alice proves to Bob that she knows the secret word used to open a magic door in a circular cave.



Q: If Alice does not know the secret word, what kind of magic could she master to cheat Bob?

ZKP on Hanmilton Cycle

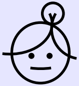
ZKP for a solution of Hanmilton Cycle (NPC). [Blum (1986)]
Prover relabels the graph (1) randomly, encrypts the randomly relabeld graph (2) with $N + N * (N-1)/2$ boxes (3), and sends them to verifier.
Verifier asks only one question: either (a) show the relabelled graph is valid by openning all boxes (3); or (b) show one Hanmilton cycle by openning the boxes on the cycle (4).



(1) The Graph (2) A Relabeled Graph (3) Commited Boxes (4) Opened Boxes

ZKP and Commitment

The simulation paradigm: by seeing Y , a party learns no more than X if Y can be efficiently generated given only X.
A simple example: without commitment, the verifier learns the message given a ciphertext. With commitment, the prover can check whether the verifier already knows the message.



Prover knows sk | a random m

$m' = \mathsf{Dec}_{sk}(c) \xleftarrow{c} c \leftarrow \mathsf{Enc}_{pk}(m)$

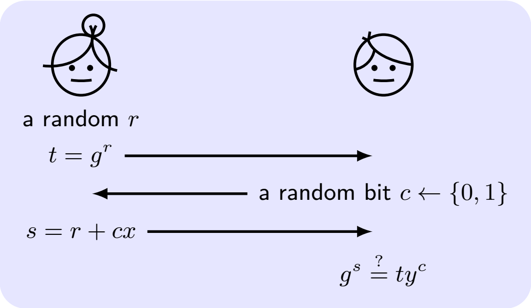
$h = \mathsf{commit}(m') \xrightarrow{h}$

$m \stackrel{?}{=} m' \xleftarrow{m}$

If No, stop;

$\xrightarrow{m'}$ Accept if $m = m'$

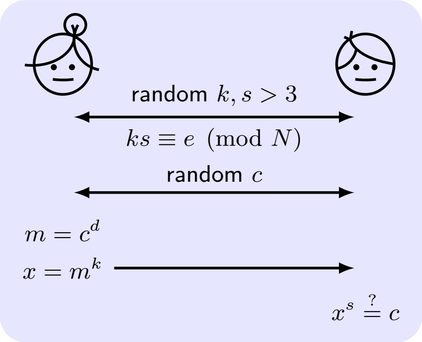
We have learned a ZKP as an identification scheme. Recall **Schnorr protocol**: Alice proves to Bob the knowledge of $x = \log_g y$ in the discrete log problem.



If Alice can foresee c, Alice can cheat with $t = g^s / y$ when $c = 1$.

ZKP of the Ability to Break RSA

Purpose: Alice convinces Bob that she knows Charlie's private key d for RSA problem $\langle N, e, d\rangle$, but she doesn't want to tell Bob d



If Alice can manipulate c, Alice can cheat with $c = m^e$.

Content

Oblivious Transfer

Oblivious transfer (OT) protocol: a sender remains oblivious as to whether or which info has been transferred.

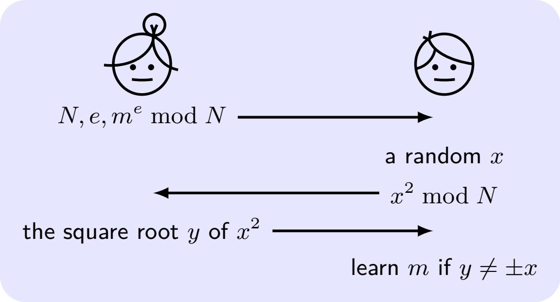
A toy example of **Socialist Millionaires Problem**: Alice ($3M) and Bob ($2M) wonder whether they makes the same money, while keeping their salaries secret. [source link]

1. Bob prepares 4 lockable suggestion boxes marked w/ salaries.
2. Bob destroys the keys except for the box marked w/ his salary.
3. Alice puts a paper "YES" into the box marked w/ her salary, "NO" for the others.
4. Bob open the box and may (or may not) share the paper with Alice.

Alice sends 4 papers to Bob, but is oblivious to which paper Bob gets.

Rabin's OT Protocol

Rabin's OT protocol: Alice is not sure about whether Bob receives the message. RSA problem $\langle N, e, d \rangle$.



If $y \neq \pm x$, then Bob can factorize N with $\gcd(y - x, N)$ and find d. Since every quadratic residue modulo N has four square roots, Bob can learn m with probability $\frac{1}{2}$.

1-out-of-2 Oblivious Transfer

1-out-of-2 OT: the sender has two messages m_0 and m_1, and the receiver wishes to receive m_b, without the sender learning b, while the sender ensures that the receiver receive only one message.

Privacy: What is retrieved by the receiver is protected, while the sender only reveals one of two messages.

RSA: N, e $\longrightarrow$

random x_0, x_1 $\longrightarrow$

pick b, random k

$\longleftarrow$ $v = x_b + k^e$

$k_0 = (v - x_0)^d$, $k_1 = (v - x_1)^d$

$m_0' = m_0 + k_0, m_1' = m_1 + k_1$ $\longrightarrow$

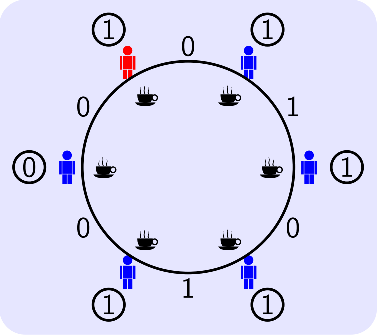
$m_b = m_b' - k$

Content

Secure Multi-Party Computation

Secure multi-party computation (MPC): enable parties to jointly compute a function over their inputs, while at the same time keeping these inputs private

Dining Cryptographers Problem: how to perform a secure MPC of the boolean-OR function [David Chaum (1988)]



- at most one  (1), other  (0)
- every two adjacent people establish a shared one-bit secret
- everyone shouts the XOR of two shared secrets and its own bit
- output the XOR of all of what everyone shouts. If 1, there is a , otherwise there is none

Homomorphic Encryption

- **Homomorphic Encryption** with $\circ$: $\mathsf{Dec}_{sk}(c_1 \circ c_2) = m_1 \circ m_2$.
- Elgamal encryption is homomorphic with $\times$: $\langle g^{y_1}, h^{y_1} \cdot m_1 \rangle \cdot \langle g^{y_2}, h^{y_2} \cdot m_2 \rangle = \langle g^{y_1+y_2}, h^{y_1+y_2} \cdot m_1 m_2 \rangle$
- Paillier scheme is homomorphic with $+$: $\mathsf{Enc}_N(m_1) \cdot \mathsf{Enc}_N(m_2) = \mathsf{Enc}_N([m_1 + m_2 \bmod N])$.
- **Application**: voting without learning any individual votes.

$$c_i := [(1+N)^{v_i} \cdot r^N \bmod N^2], v_i \in \{0,1\}$$

$$c^* := [\Pi_i c_i \bmod N^2], v^* = \Sigma_i v_i$$

- First **Fully** homomorphic with $\times$ and $+$ by Craig Gentry (2009).

Content

End-to-End Voting System

End-to-End Voting System:

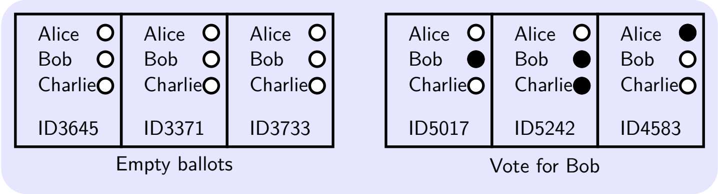
1. **Cast**: Voter casts ballot at Voting Machine (VM)
2. **Post**: Ballots are posted on Public Bulletin Board (PBB)
3. **Count**: Tally is computed by election officials (EO) from PBB

Security goals:

- **End-to-End Verifiability**: any voter gets assurance that **cast as intended**, **post as cast**, and **counted as posted**;
- **Privacy**: no one knows what the voter cast; even the voter can not convince others what she cast; privacy also means **coercion-resistance**;

ThreeBallot [Rivest (2006)] w/o Crypto

Philosophy: "vote by rows, cast by columns"



- Each voter casts three plaintext ballots.
- Each row has 1 or 2 marks. Not 0, not 3.
- Each ballot should have a unique ID.
- All three cast ballots go on PBB.
- Voter takes home copy of arbitrarily-chosen one as receipt.
- Receipt serves as integrity check on PBB.
- Does threeballot achieve e2e verifiability and privacy?

Content

Why Quantum Cryptography?

Quantum cryptography taps the natural uncertainty of the quantum world

- **Superposition**: object doesn't have definite properties (location, speed) but has probabilities over them
- **Interference**: probabilities can be negative
- **Entanglement**: properties of many particles can be correlated
- **Measurement**: object's properties collapse to definite value when measured, collapsing also properties of other entangled objects

State-of-the-Art of Quantum Cryptography

- (Unsurprisingly) there is **no proof** that quantum computers are more powerful than classical computers/Boolean circuits/Turing machines
- There are **polynomial** algorithms (e.g., Shor's algorithm) for quantum computers solving problems unknown to be solvable classically in poly-time: factoring and discrete logs
- There are **hard** problem with no quantum poly-time algorithm: NPC, inverting many candidate OWF, private key encryption and signature schemes

Quantum Key Distribution

Purpose: Using photon polarization states to transmit the information in a public channel against eavesdroppers

BB84 protocol: C. H. Bennett and G. Brassard (1984)

Basis	0	1
+	|	–
x	/	\

Alice's random bits	01101001
Alice's random sending basis	++x+xxx+
Photon polarization Alice sends	|–\\|\//–
Bob's random measuring basis	+xxx+x++
Photon polarization Bob measures	|/\/–/––
Shared secret key	0 1 0 1

- Two bases are public
- Eavesdropping would change the photon polarization states
- Check for the presence of eavesdropping by comparing a subset of shared bit string

Summary

One of Clarke's three laws: *Any sufficiently advanced technology is indistinguishable from magic.*