

# Cryptographic Protocols (Zoo)

Yu Zhang

Harbin Institute of Technology

Cryptography, Autumn, 2020

- 1** Protocols
- 2** SSL/TLS Handshaking
- 3** Three-Pass Protocol and Interlock Protocol
- 4** Pairing and Identity-Based Encryption
- 5** Blind/Group/Ring Signatures
- 6** Secret Sharing/Threshold Cryptography
- 7** Commitment Scheme
- 8** Zero Knowledge Proofs
- 9** Oblivious Transfer
- 10** Secure Multi-Party Computation and Homomorphic Enc.
- 11** Quantum Cryptography

- 1** Protocols
- 2 SSL/TLS Handshaking
- 3 Three-Pass Protocol and Interlock Protocol
- 4 Pairing and Identity-Based Encryption
- 5 Blind/Group/Ring Signatures
- 6 Secret Sharing/Threshold Cryptography
- 7 Commitment Scheme
- 8 Zero Knowledge Proofs
- 9 Oblivious Transfer
- 10 Secure Multi-Party Computation and Homomorphic Enc.
- 11 Quantum Cryptography

- **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
- It should not be possible to do more or learn more than what is specified in the protocol

- **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.
- **Self-enforcing protocols:** the best type of protocol. The protocol itself guarantees fairness.

# 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.

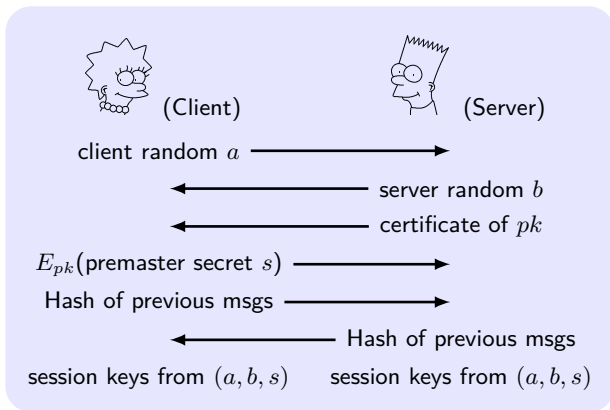
- **Passive cheaters:** follow the protocol, but try to obtain more information than the protocol intends them to.
- **Active cheaters:** disrupt the protocol in progress in an attempt to cheat.

- 1 Protocols
- 2 SSL/TLS Handshaking**
- 3 Three-Pass Protocol and Interlock Protocol
- 4 Pairing and Identity-Based Encryption
- 5 Blind/Group/Ring Signatures
- 6 Secret Sharing/Threshold Cryptography
- 7 Commitment Scheme
- 8 Zero Knowledge Proofs
- 9 Oblivious Transfer
- 10 Secure Multi-Party Computation and Homomorphic Enc.
- 11 Quantum Cryptography

# Simplified SSL/TLS Handshaking

**Purpose:** generate 4 secret keys with authenticated server

**Requirement:** the client has the public key of Trusted Third Party  
the server has the certificate of its own  $pk$  issued by TTP





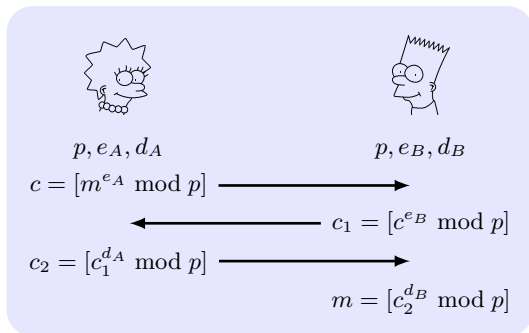
- 1 Protocols
- 2 SSL/TLS Handshaking
- 3 Three-Pass Protocol and Interlock Protocol**
- 4 Pairing and Identity-Based Encryption
- 5 Blind/Group/Ring Signatures
- 6 Secret Sharing/Threshold Cryptography
- 7 Commitment Scheme
- 8 Zero Knowledge Proofs
- 9 Oblivious Transfer
- 10 Secure Multi-Party Computation and Homomorphic Enc.
- 11 Quantum Cryptography

# Three-Pass Protocol

**Purpose:** communication without shared keys

**Requirement:**  $\text{Dec}_{k_1}(\text{Enc}_{k_2}(\text{Enc}_{k_1}(m))) = \text{Enc}_{k_2}(m)$

**Shamir Protocol:**  $p$  is a prime, find  $e, d$  with  $\gcd(e, p-1) = 1$  and  $ed \equiv 1 \pmod{p-1}$

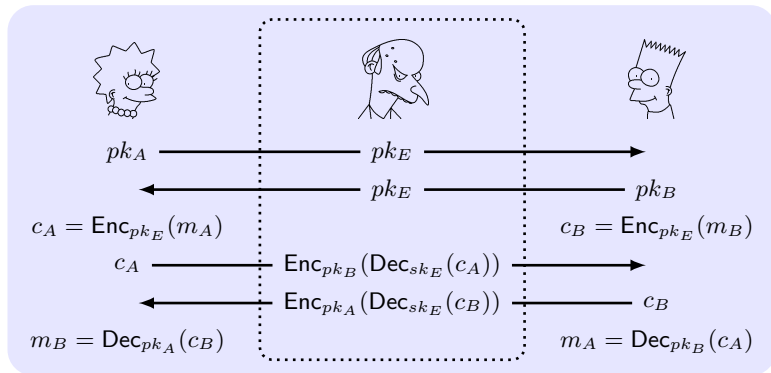


$$c_2^{d_B} = c_1^{d_A \cdot d_B} = c^{e_B \cdot d_A \cdot d_B} = m^{e_A \cdot e_B \cdot d_A \cdot d_B} = m^{e_A d_A \cdot e_B d_B} = m$$

**Weakness:** insecurity under the man-in-the-middle attack

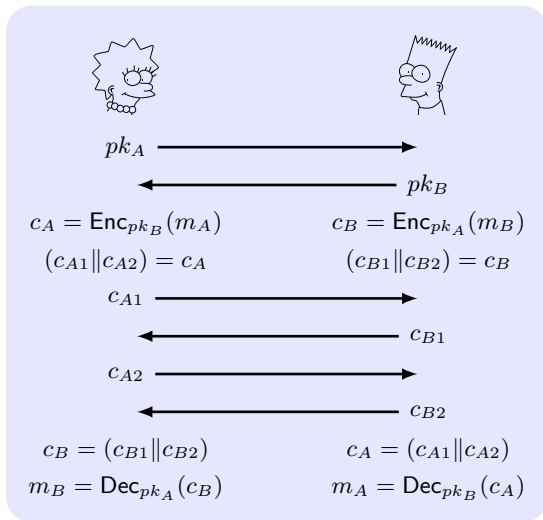
# The Man-In-The-Middle Attack

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



# Interlock Protocol

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



- 1 Protocols
- 2 SSL/TLS Handshaking
- 3 Three-Pass Protocol and Interlock Protocol
- 4 Pairing and Identity-Based Encryption**
- 5 Blind/Group/Ring Signatures
- 6 Secret Sharing/Threshold Cryptography
- 7 Commitment Scheme
- 8 Zero Knowledge Proofs
- 9 Oblivious Transfer
- 10 Secure Multi-Party Computation and Homomorphic Enc.
- 11 Quantum Cryptography

# Bilinear Maps

- Two cyclic groups:  $G_1$  with  $+$  and generator  $P$ ,  $G_2$  with  $\times$ .
- **Bilinear map**  $e : G_1 \times G_1 \rightarrow G_2$  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.
- Recall Joux'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, Joux's is secure.

# Identity-Based Encryption

- **IBE**: Anyone can directly use receiver's ID ( $A$ ) as the public key with help of a TTP, aka KGC (Key Generation Center). The receiver obtains its private key from KGC.
- **KGC** generates a global public key  $pk = sP$  and  $sk = s$ .
- **Enc**:  $\text{Enc}(sP, A, m) = \langle rP, m \oplus H_2(e(H_1(A), sP)^r) \rangle$ , where  $r$  is a random string,  $H_1$  and  $H_2$  are random oracles.
- **Dec**: The receiver obtains its private key  $d_A = sH_1(A)$  from KGC.  $\text{Dec}(d_A, u, v) = v \oplus H_2(e(d_A, u))$ .  
$$e(d_A, u) = e(sH_1(A), rP) = e(H_1(A), P)^{sr} = e(H_1(A), sP)^r.$$

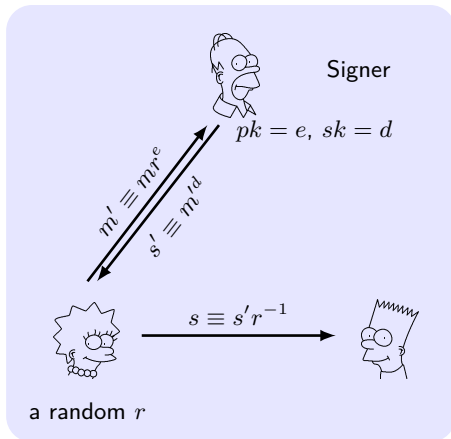
- 1 Protocols
- 2 SSL/TLS Handshaking
- 3 Three-Pass Protocol and Interlock Protocol
- 4 Pairing and Identity-Based Encryption
- 5 Blind/Group/Ring Signatures**
- 6 Secret Sharing/Threshold Cryptography
- 7 Commitment Scheme
- 8 Zero Knowledge Proofs
- 9 Oblivious Transfer
- 10 Secure Multi-Party Computation and Homomorphic Enc.
- 11 Quantum Cryptography



# Blind Signature

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

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 manager GM:**

- **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:** 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 by 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  $(\sigma_i), i = 1, \dots, n$  by  $U_k$ :

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

- **Verify:**

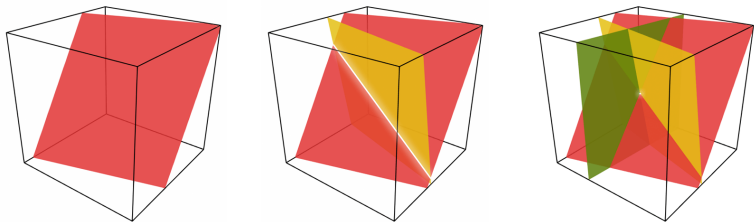
$$e(H(m), P) = \prod_i e(Y_i, \sigma_i)$$

- 1 Protocols
- 2 SSL/TLS Handshaking
- 3 Three-Pass Protocol and Interlock Protocol
- 4 Pairing and Identity-Based Encryption
- 5 Blind/Group/Ring Signatures
- 6 Secret Sharing/Threshold Cryptography**
- 7 Commitment Scheme
- 8 Zero Knowledge Proofs
- 9 Oblivious Transfer
- 10 Secure Multi-Party Computation and Homomorphic Enc.
- 11 Quantum Cryptography

# 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.

# 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  $s = \sum_i s_i \cdot \lambda_i$  with public info  $\lambda_i$  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  $\log_g h_i = \log_{c_1} d_i$

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

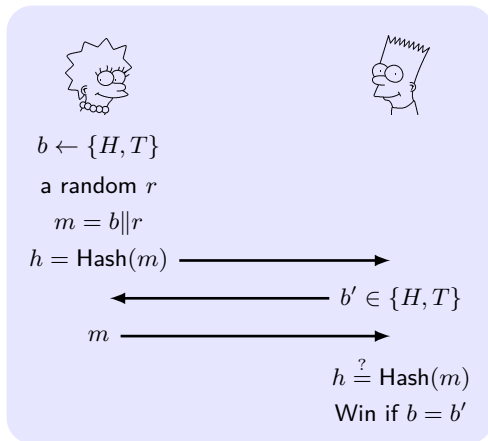
$$c_2 / \prod_i d_i^{\lambda_i} = c_2 / \prod_i c_1^{s_i \cdot \lambda_i} = c_2 / c_1^{\sum_i s_i \cdot \lambda_i} = c_2 / c_1^s = m$$

- 1 Protocols
- 2 SSL/TLS Handshaking
- 3 Three-Pass Protocol and Interlock Protocol
- 4 Pairing and Identity-Based Encryption
- 5 Blind/Group/Ring Signatures
- 6 Secret Sharing/Threshold Cryptography
- 7 Commitment Scheme**
- 8 Zero Knowledge Proofs
- 9 Oblivious Transfer
- 10 Secure Multi-Party Computation and Homomorphic Enc.
- 11 Quantum Cryptography

# Commitment Scheme

**Commitment scheme** allows one to commit to a value while keeping it hidden, with the ability to reveal the committed value

**Coin flipping over Internet:** Alice flips the coin, Bob guesses







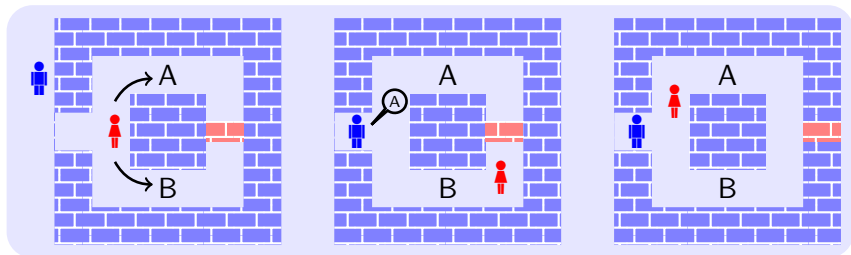
- 1 Protocols
- 2 SSL/TLS Handshaking
- 3 Three-Pass Protocol and Interlock Protocol
- 4 Pairing and Identity-Based Encryption
- 5 Blind/Group/Ring Signatures
- 6 Secret Sharing/Threshold Cryptography
- 7 Commitment Scheme
- 8 Zero Knowledge Proofs**
- 9 Oblivious Transfer
- 10 Secure Multi-Party Computation and Homomorphic Enc.
- 11 Quantum Cryptography

# Zero-Knowledge Proof

- **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

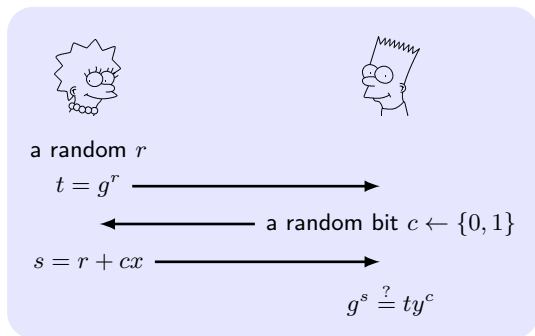
# A Toy Example of ZKP

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



# Schnorr Protocol

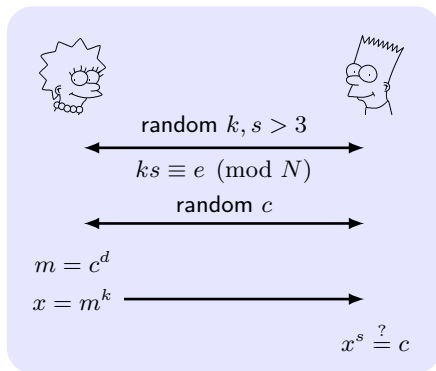
We have learned a ZKP as an identification scheme. Recall **Schnorr protocol**: Alice proves to Bob the knowledge of  $x = \log_g y$  in the discrete log problem.



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  $d$



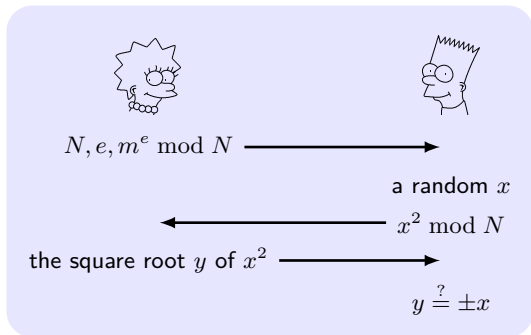
If Alice can manipulate  $c$ , Alice can cheat with  $c = m^e$ .

- 1 Protocols
- 2 SSL/TLS Handshaking
- 3 Three-Pass Protocol and Interlock Protocol
- 4 Pairing and Identity-Based Encryption
- 5 Blind/Group/Ring Signatures
- 6 Secret Sharing/Threshold Cryptography
- 7 Commitment Scheme
- 8 Zero Knowledge Proofs
- 9 Oblivious Transfer**
- 10 Secure Multi-Party Computation and Homomorphic Enc.
- 11 Quantum Cryptography

# Oblivious Transfer

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

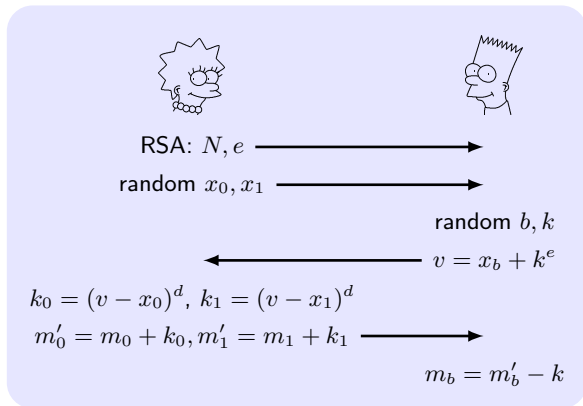
**Rabin's OT protocol:** RSA problem  $\langle N, e, d \rangle$



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.



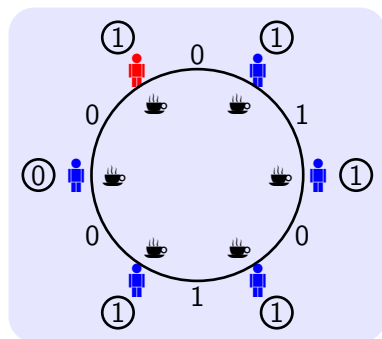





- 1 Protocols
- 2 SSL/TLS Handshaking
- 3 Three-Pass Protocol and Interlock Protocol
- 4 Pairing and Identity-Based Encryption
- 5 Blind/Group/Ring Signatures
- 6 Secret Sharing/Threshold Cryptography
- 7 Commitment Scheme
- 8 Zero Knowledge Proofs
- 9 Oblivious Transfer
- 10 Secure Multi-Party Computation and Homomorphic Enc.**
- 11 Quantum Cryptography

# 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



- 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  $\circ$ :  $\text{Dec}_{sk}(c_1 \circ c_2) = m_1 \circ m_2$ .
- 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  $+$ :  
 $\text{Enc}_N(m_1) \cdot \text{Enc}_N(m_2) = \text{Enc}_N([m_1 + m_2 \bmod N])$ .
- **Application**: voting without learning any individual votes.

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

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

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

- 1 Protocols
- 2 SSL/TLS Handshaking
- 3 Three-Pass Protocol and Interlock Protocol
- 4 Pairing and Identity-Based Encryption
- 5 Blind/Group/Ring Signatures
- 6 Secret Sharing/Threshold Cryptography
- 7 Commitment Scheme
- 8 Zero Knowledge Proofs
- 9 Oblivious Transfer
- 10 Secure Multi-Party Computation and Homomorphic Enc.
- 11 Quantum Cryptography**

# 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 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)

			Alice's random bits	01101001
			Alice's random sending basis	++x+xxx+
Basis	0	1	Photon polarization Alice sends	- \   \ / / -
+		-	Bob's random measuring basis	+xxx+x++
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

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