Cryptographic Protocols (Zoo)

Yu Zhang

Harbin Institute of Technology

Cryptography, Autumn, 2020

Outline

Content

Protocols

- **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

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.
- **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.

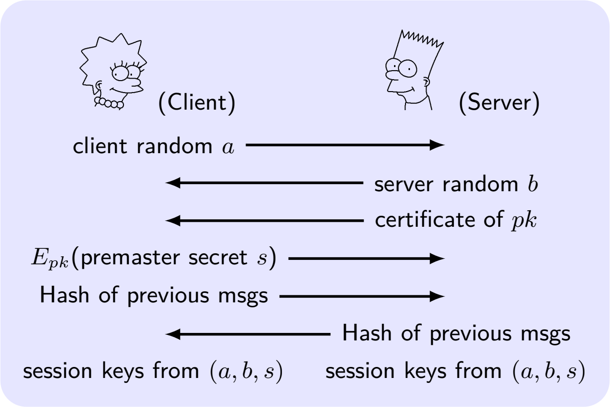
Cheater: the attacker could be one of the parties involved in the protocol.

- **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.

Content

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



(Client) (Server)

client random a →

← server random b

← certificate of pk

E_{pk}(premaster secret s) →

Hash of previous msgs →

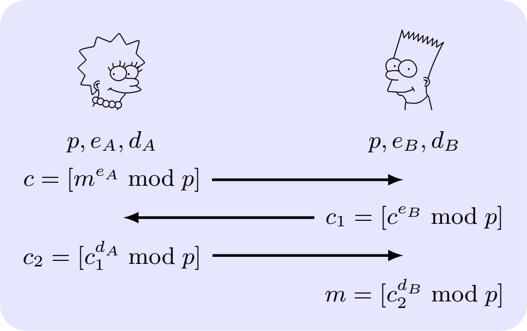
← Hash of previous msgs

session keys from (a, b, s) session keys from (a, b, s)

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 $ed \equiv 1 \pmod{p-1}$



p, e_A, d_A $\qquad\qquad$ p, e_B, d_B

$c = [m^{e_A} \bmod p] \longrightarrow$

$\longleftarrow c_1 = [c^{e_B} \bmod p]$

$c_2 = [c_1^{d_A} \bmod p] \longrightarrow$

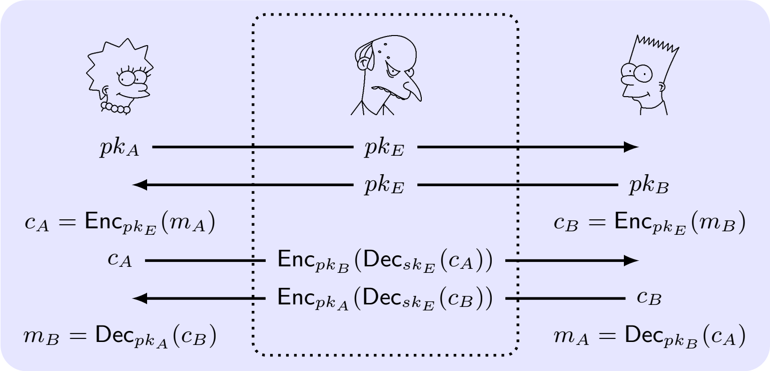
$m = [c_2^{d_B} \bmod p]$

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

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



pk_A ⟶ pk_E ⟶

⟵ pk_E ⟵ pk_B

$c_A = \mathsf{Enc}_{pk_E}(m_A)$ $\quad$ $c_B = \mathsf{Enc}_{pk_E}(m_B)$

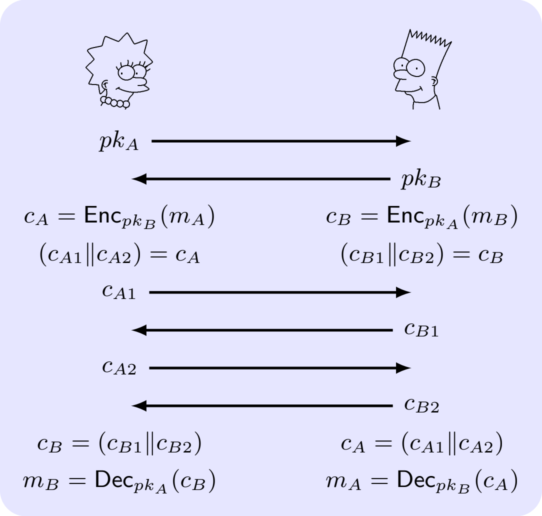
c_A ⟶ $\mathsf{Enc}_{pk_B}(\mathsf{Dec}_{sk_E}(c_A))$ ⟶

⟵ $\mathsf{Enc}_{pk_A}(\mathsf{Dec}_{sk_E}(c_B))$ ⟵ c_B

$m_B = \mathsf{Dec}_{pk_A}(c_B)$ $\quad$ $m_A = \mathsf{Dec}_{pk_B}(c_A)$

Interlock Protocol

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



$pk_A \longrightarrow$

$\longleftarrow pk_B$

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

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

$c_{A1} \longrightarrow$

$\longleftarrow c_{B1}$

$c_{A2} \longrightarrow$

$\longleftarrow c_{B2}$

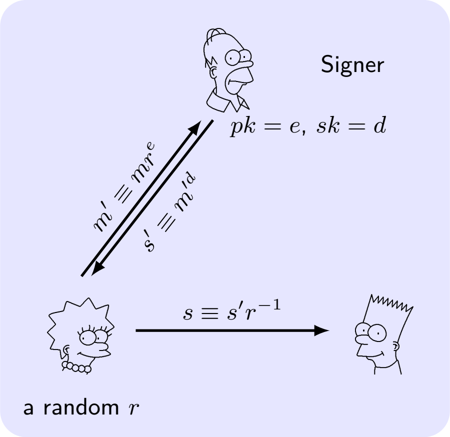
$c_B = (c_{B1} \| c_{B2})$ $\qquad$ $c_A = (c_{A1} \| c_{A2})$

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

Content

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:

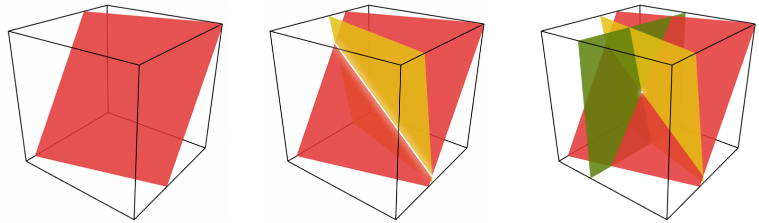
- **KeyGen**: GM generates a secret key list for each member and publishes all of public keys
- **Sign**: sign with an unused secret key
- **Verify**: try all of public keys

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.

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 $\log_g h_i = \log_{c_1} d_i$

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

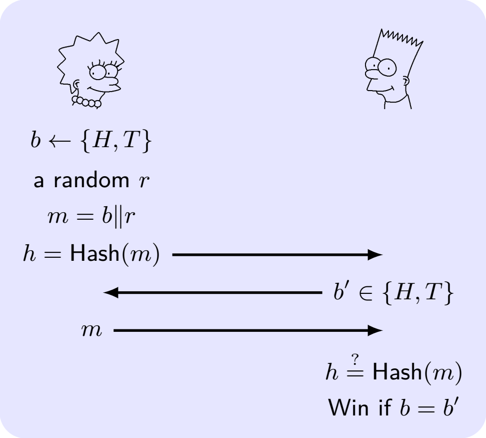
$$c_2 / \Pi_i d_i^{\lambda_i} = c_2 / \Pi_i c_1^{s_i \cdot \lambda_i} = c_2 / c_1^{\Sigma_i s_i \cdot \lambda_i} = c_2 / c_1^s = m$$

Content

Commitment Scheme

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

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



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

a random r

$m = b \| r$

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

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

$m \longrightarrow$

$h \overset{?}{=} \text{Hash}(m)$

Win if $b = b'$

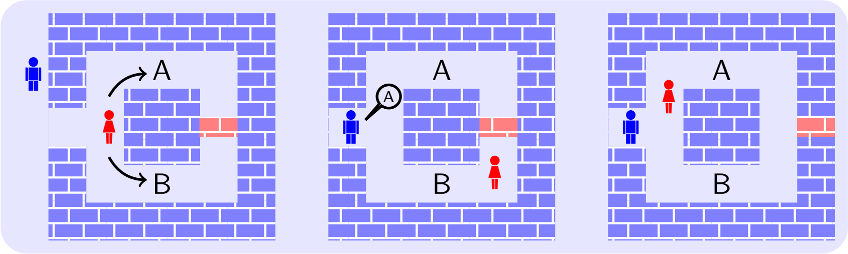
Content

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

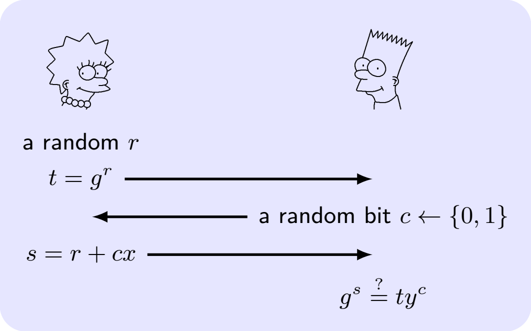
A Toy Example of ZKP

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



Schnorr Protocol

Schnorr protocol: Alice proves to Bob the knowledge of $x = \log_g y$ in the discrete log problem



a random r

$t = g^r \longrightarrow$

$\longleftarrow$ a random bit $c \leftarrow \{0, 1\}$

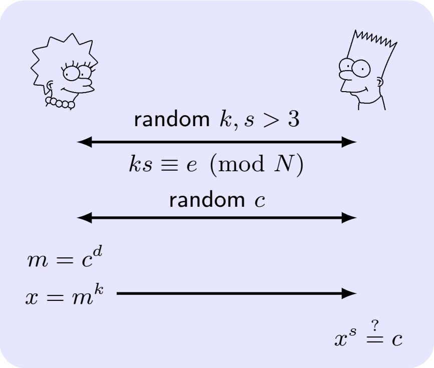
$s = r + cx \longrightarrow$

$g^s \overset{?}{=} ty^c$

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



random $k, s > 3$

$ks \equiv e \pmod{N}$

random c

$m = c^d$

$x = m^k$

$x^s \overset{?}{=} c$

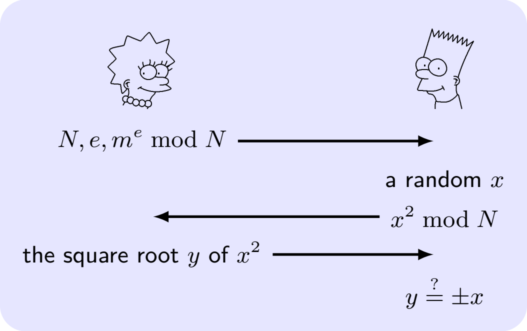
If Alice can manipulate c, Alice can cheat with $c = m^e$.

Content

Oblivious Transfer

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

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



$N, e, m^e \bmod N$ →

a random x

← $x^2 \bmod N$

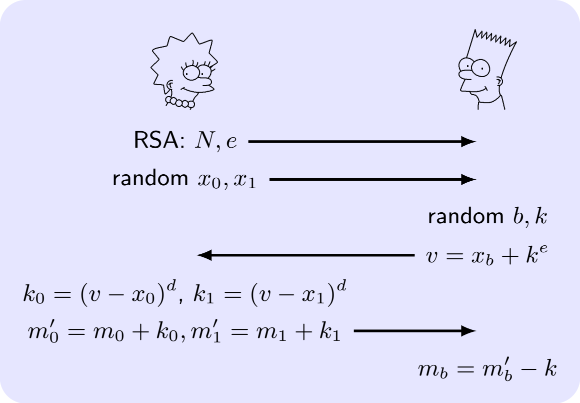
the square root y of x^2 →

$y \overset{?}{=} \pm x$

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.



RSA: N, e →

random x_0, x_1 →

random b, k

← $v = x_b + k^e$

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

$m'_0 = m_0 + k_0, m'_1 = m_1 + k_1$ →

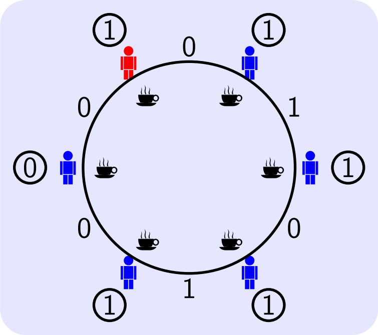
$m_b = m'_b - k$

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



- 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

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 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)

<table>
<tr><td>Basis</td><td>0</td><td>1</td></tr>
<tr><td>+</td><td>|</td><td>–</td></tr>
<tr><td>x</td><td>/</td><td>\</td></tr>
</table>

<table>
<tr><td>Alice's random bits</td><td>01101001</td></tr>
<tr><td>Alice's random sending basis</td><td>++x+xxx+</td></tr>
<tr><td>Photon polarization Alice sends</td><td>|-\|\//-</td></tr>
<tr><td>Bob's random measuring basis</td><td>+xxx+x++</td></tr>
<tr><td>Photon polarization Bob measures</td><td>|/\/-/--</td></tr>
<tr><td>Shared secret key</td><td>0 1   0 1</td></tr>
</table>

- 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

- SSL/TLS handshaking
- Shamir three-pass protocol
- interlock protocol, man-in-the-middle attack
- blind/group/ring signature
- secret sharing, threshold cryptography
- commitment scheme
- zero knowledge proofs, Schnorr protocol
- Rabin's/1-out-of-2 oblivious transfer
- multi-party computation, dining cryptographers problem
- quantum cryptography, BB84