Tutorial X

11 December 2020 14:25

TWO PARTY CRYPTOGRAPHY

(Alice and Bob do not trust each other, there is no external adversary)

- → Bit commitment
- → Oblivious transfer
- → Zero knowledge proofs (graph isomorphism)

Bit commitment

Generally this can be taken from a larger set

1.) Commitment Alice commits to a bit $b \in \{0,1\}$

2.) reveal phase Alice reveals b to Bob

1.) Alice writes b on a piece of paper, locks the paper into a box and sends the box to Bob.

2.) Alice sends the key to Bob, who can learn b.

Binding - Alice can't change the value of b after the commitment.

Hiding - Bob cannot learn b before the reveal phase.

Slides: Protocol I

→ based on QR mod n

Elements: $n = p \cdot q$ (p and q are large primes)

$m \in QNR(\mathbb{Z}_n)$

Calculating $\sqrt{x}$ mod n is computationally hard (without knowledge p, q)

Deciding whether $X \in QR(\mathbb{Z}_n)$ is computationally hard (without knowledge of p,q)

1.) Commitment: Alice chooses a random number $x \in \mathbb{Z}_n$ and sends $c = m^b x^2 \bmod n$ to Bob.

2.) Reveal: Alice sends b and x to Bob. Bob verifies $c = m^b x^2 \bmod n$.

Hiding: Can Bob after receiving c decide whether Alice commited to 0 or 1?
is computational

if $b = 0$ then $c = x^2$ mod n and $c \in QR(\mathbb{Z}_n)$

if $b = 1$ then $c = m \cdot x^2 \bmod n$ $c \in QNR(\mathbb{Z}_n)$

deciding whether $c \in QNR$ is computationally hard

Binding: How can Alice cheat? She needs to find three numbers (c, x, y) s.t. c can be "opened" by sending either $(0, x)$ or $(1, y)$ in the reveal phase
is information theoretical (IT)

$$\underbrace{m^0 x^2}_{\in QR} = c = \underbrace{m^1 \cdot y^2}_{\in QNR} \mod n$$

$\Downarrow$

No such a triple

It is impossible to have IT security for both hiding and binding. The best you can do is to have one property IT secure and the other computational.

Scheme 2.

based on discrete logarithm

Elements: p - large prime

All public:

q a large prime dividing $(p-1)$

$g \in \mathbb{Z}_p^*$ of order q $\quad (g^q = 1)$ (use mod q algebra in the exponent)

$h = g^k \bmod p$ $\quad$ ($0 < k < q$ is a random integer not known to any party)

1.) Commitment: $\quad c = g^r h^b \bmod p \qquad (A \to B)$

r is a random number $0 \leq r < q$ and b is the commited bit

2.) reveal: Alice sends b, r to Bob. Bob checks whether

$$c = g^r h^b \bmod p$$

Hiding (IT security):

$$c = g^r g^{kb} = g^r \bmod p \text{ in case of } b = 0$$
$$= g^{r+k} \bmod p \text{ in case of } b = 1$$

Can Bob decide? g^r and g^{r+k} are distributed equally

$$r \in_R \{0, 1, \dots, q-1\}$$
$$r+k \in_R \{1, \dots, q-1\}$$

Binding: Alice cheats if she can find $r, r' \in \mathbb{Z}_q^*$ such that

is computational.

$$g^r h^b = c = g^{r'} h^{(1-b)} \bmod p$$

$$g^r \cdot g^{kx} = g^{r'} \cdot g^{k(1-x)} \bmod p$$

$$g^{r+kx} = g^{r' + k(1-x)} \mod p$$

$$r + kx = r' + k(1-x) \mod q$$

$$k(2x-1) = (r'-r) \mod q$$

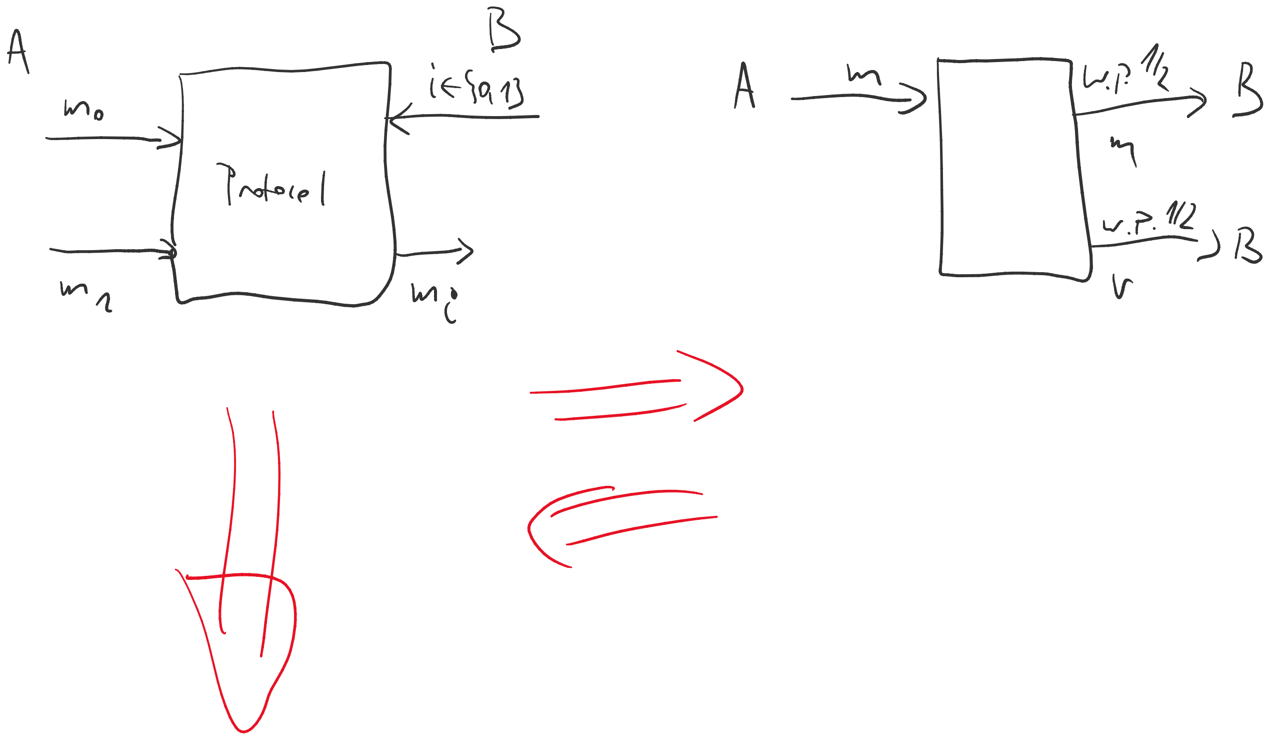
$$k = (r'-r)\cdot(2x-1)^{-1} \mod q$$

$$k = \log_g h \mod p \; !$$ ← hard computationally (discrete logarithm problem)

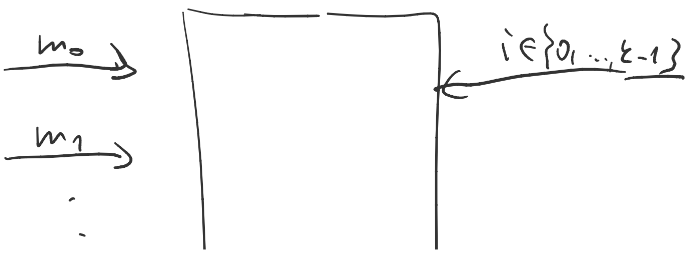
Oblivious transfer

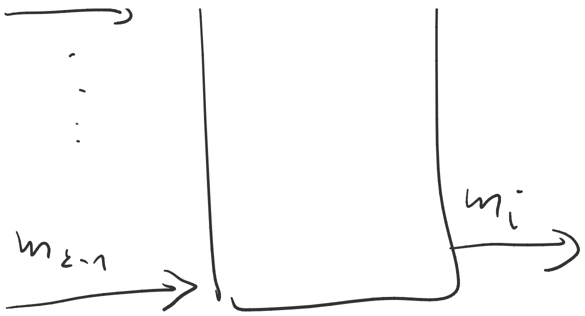
1 out of 2 OT

Rabin - OT



1-out of-k





1-out-of-2 protocol

can be used to build protocols for

SMC = secure multiparty computation

SFE = secure function evaluation

$\Rightarrow$ n users each have inputs (i^{th} user has x_i)

and they want to calculate $f(x_1, \dots, x_n)$

in such a way that do not reveal x_i

VOTING: $\rightsquigarrow$ function that outputs the input with the largest "population"

Security properties of OT (1-out-of-2)

1.) Alice doesn't learn Bob's choice i.

2.) Bob learns only m_i and knows nothing about $m_{i \oplus 1}$

Protocol using PKE

1.) Alice generates two pairs of PKE keys $\overset{\text{Secret}}{(S_0}, \overset{\text{Public}}{P_0)}$ (S_1, P_1) and sends P_0, P_1 to Bob

2.) Bob encrypts a random string ξ with a key of his choice (P_0 if he wants to learn m_0, P_1 if m_1) and sends $B = e_{P_b}(\xi)$ to Alice

3.) Alice after recieves B and calculates $A_0 = d_{S_0}(B)$ and $A_1 = d_{S_1}(B)$, then she sends $\underline{M_0 = m_0 \oplus A_0}$ and $\underline{M_1 = m_1 \oplus A_1}$ to Bob

4.) Bob decrypts M_i of his choice, the other message is not available

Security

Can Alice find Bob's choice? B is either $e_{P_0}(\xi)$ $e_{P_1}(\xi)$ and ξ is random
these are statistically indistinguishable $\Rightarrow$ IT

Can Bob find both messages? Bob needs to calculate S_0 and S_1
this possible but computationally hard
$\Rightarrow$ computational

Zero-knowledge proofs

Graph isomorphism

$G_1 = (V, E) \qquad |V| = n$

$G_2 = (V, E)$

If two graphs G_1 and G_2 are isomorphic there exists a permutation σ s.t. $G_1 = \sigma G_2$

permutation σ changes the labels $\sigma = (2, 3)$

$G_1 = [g_{ij}]_{ij=1}^{n} \qquad G_2 = [g_{ij}]_{ij=1}^{n}$

$$\begin{array}{cc} & \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \end{array} & \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \end{array} \qquad \begin{array}{cc} & \begin{array}{ccc} 1 & & 3 \end{array} \\ \begin{array}{c} 1 \\ \\ 3 \end{array} & \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \end{array} \overset{\sigma}{\sim} \begin{array}{cc} & \begin{array}{ccc} 1 & 3 & 2 \end{array} \\ \begin{array}{c} 1 \\ 3 \\ 2 \end{array} & \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \end{array} \sim \begin{array}{cc} & \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \end{array} & \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \end{array}$$

$$\sigma = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = (a\, c\, b)$$

$$G_2 = \sigma G_1 \sigma^{-1} \iff G_2 = \sigma G_1$$

ZK-proof of isomorphism between G_1 and G_2

→ Alice knows σ, st $G_1 = \sigma G_2$

→ Alice wants to convince Bob G_1 and G_2 are isomorphic without revealing anything about σ.

1.) Alice chooses a random permutation ρ and calculates $H = \rho G_1$ and sends it to Bob

2.) Bob sends a challenge $j \in \{1, 2\}$

3.) Alice sends isomorphism between G_j and H

if $j=1$ she sends ρ ↗ $H \to G_1$

if $j=2$ she sends $\rho \circ \sigma^{-1}$ ↘ $H \to G_2$

ρ

4.) Bob can check whether H is isomorphic to G_j according to Alice's response.

TRANSCRIPTS

$(H, j, \rho) \to$ valid if $H = \rho \cdot G_j$

$$\rho_2 G_2 = H = \rho_1 G_1$$

it is difficult to find $\left.\begin{matrix}(H, 1, \rho_1) \\ (H, 2, \rho_2)\end{matrix}\right\} \sigma = \rho_1 \cdot \rho_2^{-1}$