Tutorial X group 2

21 November 2019 16:05

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 Alice reveals b to Bob (Later in time)

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

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

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

Hiding - Bob can't find b before the reveal phase.

Slides: Protocol I

→ based on QR mod n

→ 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 knowing p, q)

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

1.) Commitment: Alice chooses a random number $x \in \mathbb{Z}_n$ and sends $c = m^b x^2$ mod n to Bob (this is her commitment to bit b)

2.) Reveal phase: Alice sends b and x. Bob verifies

$$c = m^b x^2 \mod n$$

Hiding is computational

Can Bob decide whether Alice commited to 0 or 1?

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

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

deciding whether $c \in QNR$ is hard

Binding is information theoretical (IT)

How can Alice cheat. She needs to find 3 numbers c, x, y, s.t. c can opened with both $(0, x)$ and $(1, y)$

$$m^0 x^2 = c = m . y^2 \mod n$$

$\Uparrow$ QR $\qquad\qquad$ $\Uparrow$ QNR

$\Downarrow$

there's no such triple

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

PEDERSEN SCHEME

p – large prime $\quad \mathbb{Z}_p^*$

exponent algebra is mod q (q is a prime)

q – is a large prime dividing $p-1$

$g \in \mathbb{Z}_p^*$ and has order q $\quad (g^q \equiv 1 \mod p)$

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

1.) Commitment $\quad$ commit(b,r)

b – commited bit

r – is a random integer $0 < r < q$

$$\text{commit}(b,r) = (A, B)$$

$$A = g^r \mod p$$

$$B = h^{(r+b)} \mod p$$

2.) Reveal $\quad$ Alice sends b and r. Bob can verify

$$A = g^r \mod p$$

$$B = \underline{\underline{h}}^{(r+b)} \bmod p$$

HIDING is computational

How can Bob calculate b from A and B?

$$r = \log_g A \mod p$$

$$r+b = \log_h B \mod p$$

$$b = \log_g A - \log_h B \mod p$$

This is hard

BINDING is IT

In order to cheat Alice needs to find $C \overset{=(A,B)}{,} x, y$, such that $C \overset{=(A,B)}{}$ can be calculated from $(0,x)$ and $(1,y)$

$$A = g^x = g^y \mod p \Rightarrow x = y$$

$$B = h^x = h^{x+1} \mod p \Rightarrow \text{not possible}$$

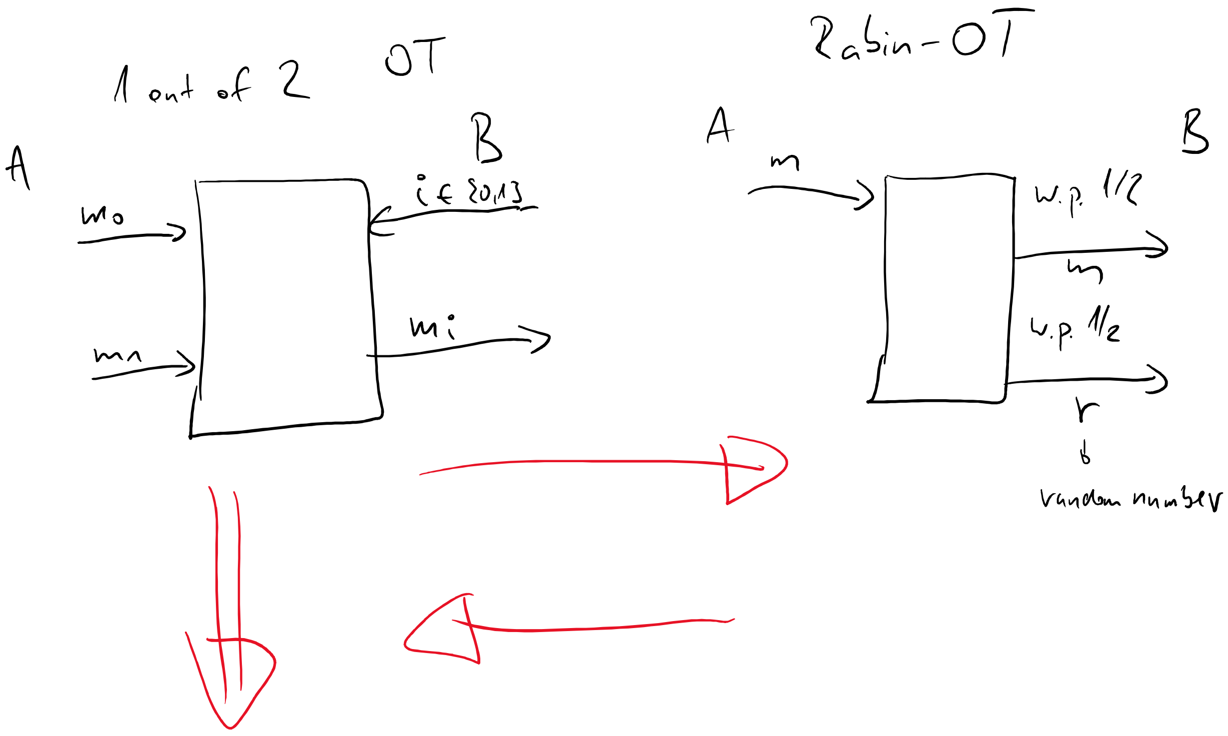
Why is bit commitment important / interesting?

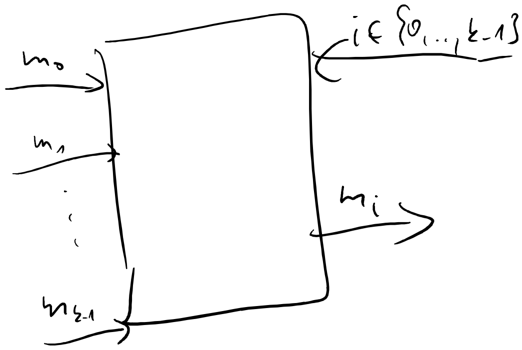
- this is a cryptographic primitive
- it can be used to build more interesting protocols
- Coin tossing (Slide 19)

$\boxed{\text{Oblivious transfer}}$

1-out-of-2 OT

Rabin-OT





the simplest protocols have
$m_0, m_1 \in \{0,1\}$
$\Downarrow$
bit oblivious protocols can be used to build protocols with larger messages.

---

1 out of k protocol with large m_i

$\Downarrow$

SMC ~ secure multiparty computation
SFE ~ secure function evaluation

n users each have inputs (ith user has x_i) and they want to calculate $f(x_1, \dots, x_n)$, and they want to calculate $f(x_1, \dots, x_n)$, in such a way that they do not reveal x_i.

VOTING ⇝ function that outputs the input with the largest "population".

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

1.) After the protocol Alice doesn't know i.

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

Protocol using Public Key Encryption (PKE)

1.) Alice generates two PKE keys (she keeps $\overbrace{s_0 \text{ and } s_1}^{\text{secret keys}}$) and sends public keys (p_0 and p_1) to Bob

2.) Bob encrypts a randomly chosen string k with a key of his choice (p_0 if he wants to learn m_0) and p_1 if he wants to learn m_1. The result of this encryption is $B \to$ Alice

3.) Alice calculates $A_0 = d_{s_0}(B)$ and $A_1 = d_{s_1}(B)$ then she sends $m_0 \oplus A_0$ and $m_1 \oplus A_1$ to Bob

4.) Bob decrypt m of his choice, the other message is not available

Security

Can Alice find Bob's choice?

B is either $e_{p_0}(\xi)$ of $e_{p_1}(\xi)$ and ξ is random. these are statistically indistinguishable $\Rightarrow$ IT

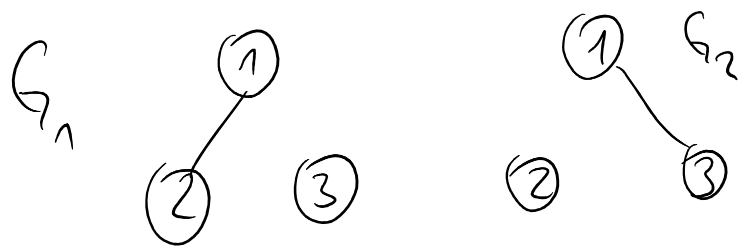
Can Bob find both messages? Assume Bob calculates s_0 and s_1 (which is possible but hard). Then he can calculate both A_0 and A_1 thus he can recover both m_0 and m_1

COMPUTATIONAL

Zero-knowledge proofs

Graph isomorphism

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 labels. we need $\sigma = (2\,3)$

$$G_1 = [a_{ij}]_{ij=1}^{n}$$

$$G_1 = \begin{array}{c|ccc} & 1 & 2 & 3 \\ \hline 1 & 0 & 1 & 0 \\ 2 & 1 & 0 & 0 \\ 3 & 0 & 0 & 0 \end{array} \rightsquigarrow \begin{array}{c|ccc} & 1 & 3 & 2 \\ \hline 1 & 0 & 1 & 0 \\ 3 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 \end{array}$$

$$\begin{array}{c|ccc} & 1 & 2 & 3 \\ \hline 1 & & & \\ 2 & & & \\ 3 & & & \end{array}\quad \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} = G_2$$

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

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

$$G_2 = \sigma G_1$$

ZK-proof of isomorphism of G_1 and G_2

Alice knows σ, s.t. $G_1 = \sigma G_2$.

She 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 $j \in \{1, 2\}$

— isomorphism $H \to G_1$

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

3.) if $j = 1$ Alice sends ρ → isomorphism $H \to G_1$

if $j = 2$ Alice sends $\rho \circ \sigma^{-1}$ → isomorph $H \to G_2$

4.) Bob can check whether H is isomorphic to G_j according to Alices response.

TRANSCRIPTS

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

it is difficult to find $(H, 1, \rho_1)$, $(H, 2, \rho_2)$ → $\rho_1^{-1} \circ \rho_2 = \sigma$