Tutorial 10 ENG

24 November 2021 14:00

TWO PARTY CRYPTOGRAPHY

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

- Bit commitment
- Zero-knowledge proofs
- Oblivious transfer -> next time

Bit commitment

1.) commitment. Alice commits to a bit $b \in \{0,1\}$. (Generally this can be taken from a larger set)

2.) reveal phase. Alice reveals her choice 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.

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

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

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

Calculating $\sqrt{x} \bmod n$, is computationally hard without the knowledge of p, q

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

Whether $C = m^b x^2 \bmod n$

Hiding: Can Bob after receiving C decide whether Alice commited to 0 or 1?

is computationally secure

if $b=0$ then $C = x^2 \bmod n$ $\quad C \in QR(\mathbb{Z}_n)$

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

Deciding whether $C \in QNR$ is computationally hard

Binding: How can Alice cheat? She needs to find numbers (C, t, y) information S.t. C can be opened as either $(0, x)$ or $(1, y)$

theoretical (IT) secure

$$m^0 x^2 = C = m \cdot y^2 \bmod n$$

x^2: QR, y^2: QNR

⇓

No such 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 computationally secure.

Scheme 2:

based on discrete logarithm

Elements: p - large prime

Public ←

- q a large prime dividing $(p-1)$
- $g \in \mathbb{Z}_p^*$ of order q $(g^q = 1 \bmod p)$ (use modular algebra in the exponent)
- $h = g^k \bmod p$ (k is a random number not known to either party) $0 \le k < q$

1.) Commitment: $C = g^r h^b \bmod p$

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

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

$$C = g^r h^b \mod p$$

Hiding: IT secure

$$C = g^r g^{kb} = g^r \mod p \quad \text{in case of } b=0$$

$$= g^{r+k} \mod p \quad \text{in case of } b=1$$

r is random from $\{0, \dots, q-1\}$

$(r+k) \bmod q$ is also a random number from $\{0, \dots, q-1\}$

Binding: is computational

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

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

$$g^r \cdot g^{kb} = g^{r'} \cdot g^{k \cdot (1-b)} \mod p$$

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

$$r + kb = r' + k(1-b) \mod q$$

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

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

$$k = \log_g h \mod p$$

this could be used for an efficient algorithm for discrete log problem.

Zero-Knowledge proofs

Zero-Knowledge proofs

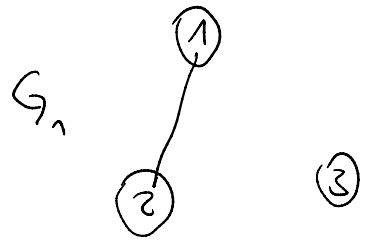
Zero-knowledge proofs

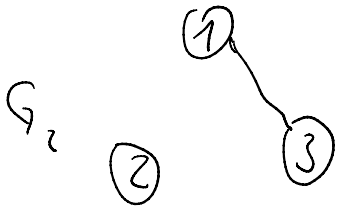
Graph isomorphism

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

$G_2 = (V, E)$

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 $\sigma = (2, 3)$

1 2 3 4 5

(1 2 3)(4 5)

3 1 2 5 4

$G_1 = \{g_{ij}\}_{ij=1}^{n}$

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

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

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

G_1 is isomorphic to G_2

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

Zero-knowledge proof of isomorphism between G_1 and G_2

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

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

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

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

3.) Alice sends isomorphism between G_j and H to Bob

if $j=1$ she sends P $\quad G_1 \to H$

if $j=2$ she sends $\boxed{P \cdot \sigma^{-1}}$ $\quad G_2 \to PG_1 \to H$

4.) Bob checks whether the received permutation is valid.

TRANSCRIPTS

(H, j, P) → valid if $H = P \circ G_j$

it is difficult to find $(H,1,P_1)$ $\quad P_2 \cdot G_2 = H = P_1 G_1$

$(H,2,P_2)$

$\Downarrow$

$G_2 = \underbrace{P_2^{-1} \cdot P_1}_{\sigma^{-1}} \cdot G_1$