Secure Multiparty Computation

2021年5月17日　　13:30

Two Millionaires Problem

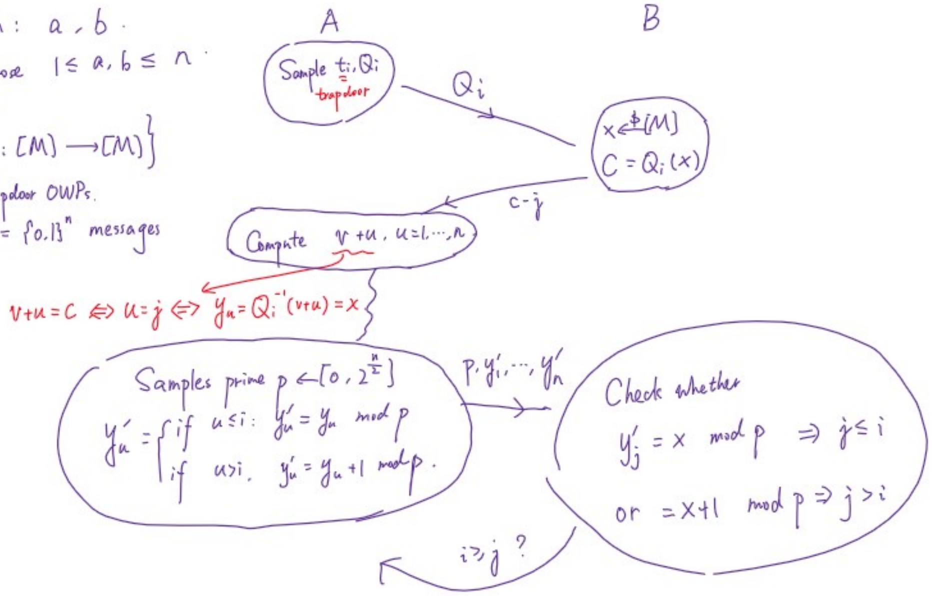
- Wealth: a, b.

  Suppose $1 \le a, b \le n$.

  $\{Q_i : [M] \longrightarrow [M]\}$

  Trapdoor OWPs.

  $M = \{0,1\}^n$ messages



Sample $\underset{\text{trapdoor}}{\underline{\underline{t_i}}}, Q_i$

$\xrightarrow{Q_i}$

$x \xleftarrow{\$} [M]$

$C = Q_i(x)$

$\xleftarrow{c-j}$

Compute $\underbrace{v}_{} + u,\ u = 1, \cdots, n$

$v + u = C \Leftrightarrow u = j \Leftrightarrow y_u = Q_i^{-1}(v+u) = x$

Samples prime $p \leftarrow [0, 2^{\frac{n}{2}}]$

$y_u' = \begin{cases} \text{if } u \le i: & y_u' = y_u \mod p \\ \text{if } u > i. & y_u' = y_u + 1 \mod p. \end{cases}$

$\xrightarrow{p, y_1', \cdots, y_n'}$

Check whether

$y_j' = x \mod p \Rightarrow j \le i$

or $= x+1 \mod p \Rightarrow j > i$

$i \ge j$?

Formalize:

$\text{Alice}: x \; \rightleftarrows \; \text{Bob}: y \qquad F: (X, Y) \to \{0,1\}^m$

as a public function to compute

View (A, B)

Security: if $\exists$ n.u.p.p.t. Sim_A Sim_B s.t. $\forall x, y$ — no additional knowledge learnt by A or B.

$$View_A(A,B) \approx_c Sim_A(x, F(x,y))$$

$$View_B(A,B) \approx_c Sim_B(y, F(x,y)).$$

$$View_A(A,B) = \{x, View(A,B), F(x,y)\}$$

Remark: Here A & B are honest by assumption.

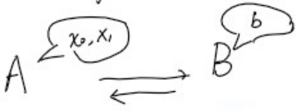
A trivial Construction from FHE

A　　　B

sk, pk　$\xrightarrow{FHE.Enc(a), pk}$

$\xleftarrow{FHE.Enc(F(a,b))}$.

Oblivious Transfer (OT).



A gets　B gets

$$F(x_0, x_1, b). = (\perp ; x_b)$$

A construction from Trapdoor OWP.

Alice (x_0, x_1) $\xrightarrow{f_i}$ Bob (b).

1. Sample f_i, t_i

2. Sample $u_b \xleftarrow{\$} \{0,1\}^n$.

Alice (x_0, x_1) $\xrightarrow{f_i}$ Bob (b).

1. Sample f_i, t_i

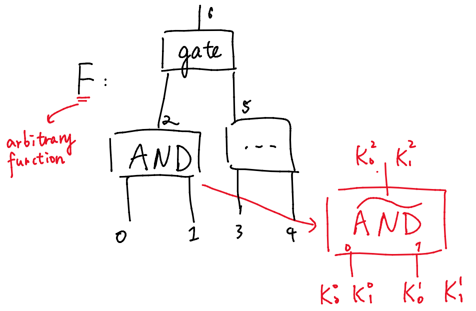
2. Sample $u_b \xleftarrow{\$} \{0,1\}^n$.
Compute $y_b = f_i(x_b)$
Sample $y_{1-b} \xleftarrow{\$} \{0,1\}^n$

$\xleftarrow{y_0, y_1}$

3. $z_b = f_i^{-1}(y)$.
h is hardcore bit of f_i $\xrightarrow{C_k = h(z_k) \oplus x_k}$ $k \in \{0,1\}$

4. Compute $h(u_b) \oplus C_b = x_b$

Yao's garbled circuit.



Example:

$$\widetilde{AND}(K_{\underline{0}}^0, K_{\underline{1}}^1) = K_{\underline{0}}^2$$

↓ Achieve by:

$$Enc_{K_0^0}(Enc_{K_0^1}(K_0^2)) = C_4$$
$$Enc_{K_0^0}(Enc_{K_1^1}(K_0^2)) = C_2$$
$$Enc_{K_1^0}(Enc_{K_0^1}(K_0^2)) = C_3$$
$$Enc_{K_{\underline{1}}^0}(Enc_{K_{\underline{1}}^1}(K_{\underline{1}}^2)) = C_1$$

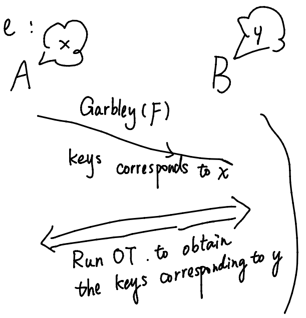
random permutated.

$\underline{K_x^0, K_y^1}$

decrypt C_i, if "looks correct", get $K_{AND(x,y)}^2$

wrong key detection:

$$\Pr[k \leftarrow Gen(1^n), k' \leftarrow Gen(1^n), \forall m \in M, Dec_{k'}(Enc_k(m)) = \perp] > 1 - negl(n)$$



get $F(x,y)$ by Running garble circuit.

Security Analysis

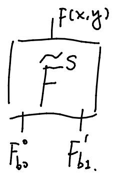
$Sim_A(x, F(x,y))$: View(A.B).

(1) Garbley(F). keys x (Trivial)

(2) OT. protocol. (Run simulator for OT)

(3) $F(x,y)$. Trivial

$Sim_B(y, F(x,y))$: View(A,B)



Only need one path correct:

$$Enc_{K_{b_0}^0}(Enc_{K_{b_1}^0}(F(x,y))) = C_i$$

Whenever asked for keys, gives $K_{b_0}^0$ and $K_{b_1}^1$.