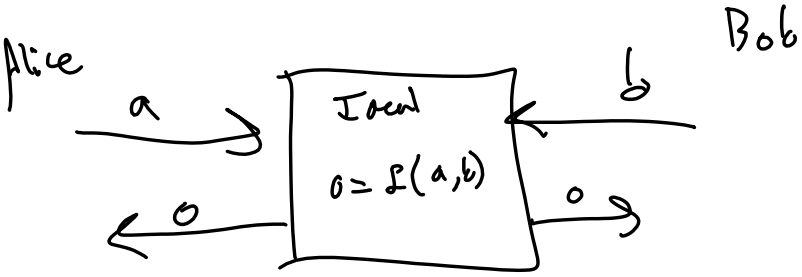
Garbled Circuits

Thursday, September 28, 2017 1:13 PM



"honest-but-curious"

Def'n: 2 party secure computation is a pair of ITMs (A, B)

"generator" "evaluator"

Such that

- Correctness $\forall a,b \quad out_{A,B}\left[A(a) \leftrightarrow B(b)\right] \approx \{f(a,b), f(a,b)\}$

- Simulatable $S_A \approx$ view

$$\exists S_A \; \forall a,b, \; \{View_A[A(a) \leftrightarrow B(b)]\} \approx \{S_A(a, f(a,b))\}$$

same for S_B

Yao's Protocol (wiki under Yao!)

f: circuit ⟨m wires, n gates⟩

$A(f, a)$ $\quad B(f, b)$

Round 1

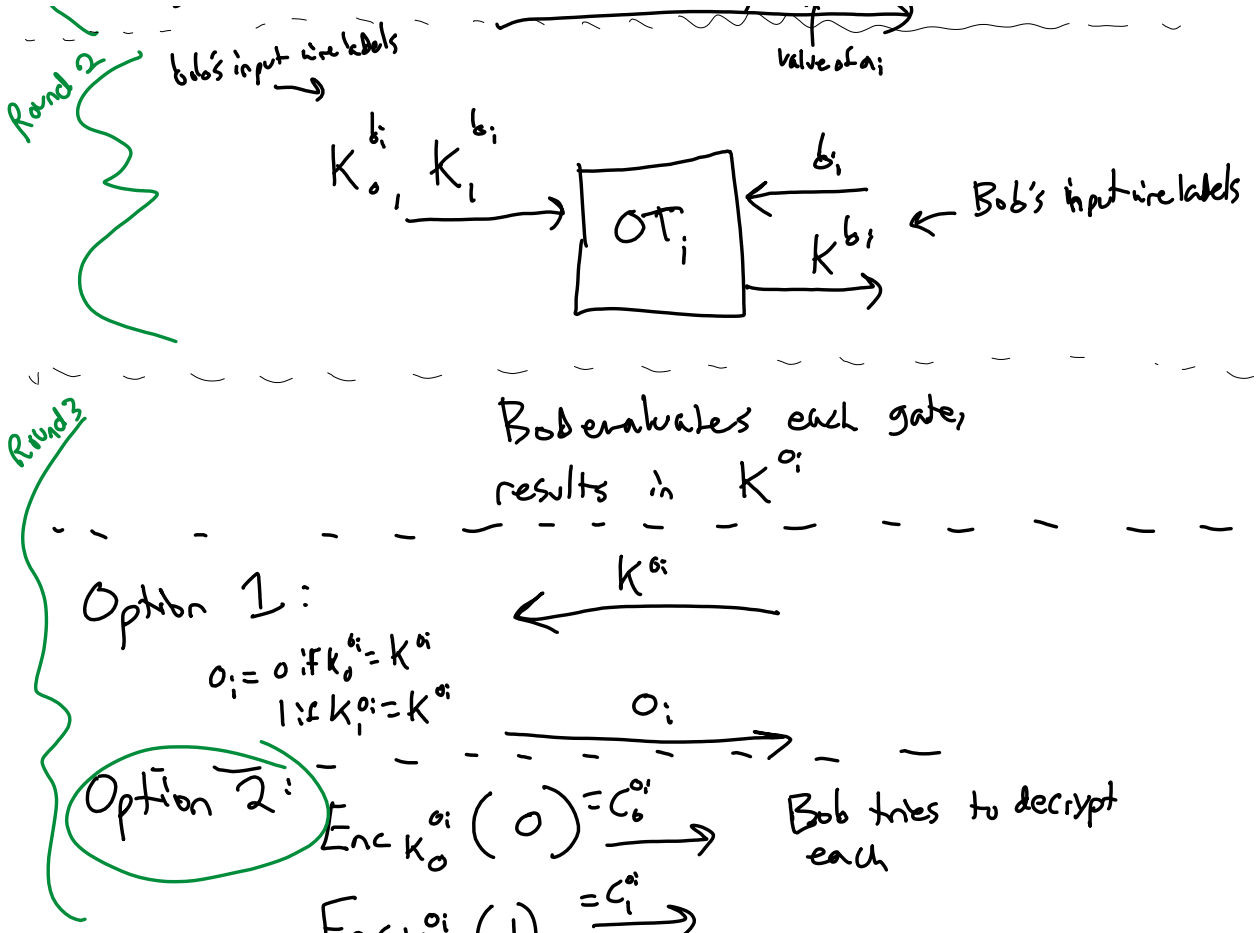
$A(f, a)_{\text{wire IDs}}$

$\forall_{b \in \{0,1\}, i \le m} K_b^{w_i} \xleftarrow{\$} \{0,1\}^{\lambda}$

garble tables

$e_0^{g_i} \leftarrow Enc$
$e_1^{g_i} \leftarrow \ldots$
$e_2^{g_i} \leftarrow \ldots$
$e_3^{g_i} \leftarrow \ldots$

$\{e_i^{g_i}\}_{i \le n}, \{K_{a_i}^{a_i}\}$ (name of alice's input bits)



How to build the simulator proof (Sim_A, Sim_B)

View of Alice

$$View_A[A \leftrightarrow B] = \left(a, f(a,b), \{K_b^{w_i}\}, \{e_j^{g_i}\}, \gamma_{OT}\right)$$

($K_b^{w_i}$: all wires, $b = 0,1$; $e_j^{g_i}$: all gates, all 4 rows; γ_{OT}: OT transcripts)

$Sim_A(f, a, o)$:

Everything ordinary

Generate $\{K_b^{w_i}\}$, encrypt $\{e_j^{g_i}\}$,

$\gamma_{OT} \leftarrow Sim_{OT,A}(K_0^{b_i}, K_1^{b_i})$

$View_B[A \leftrightarrow B]$ $\quad (b, f(a,b), \{e_j^{g_i}\}, \{K^{a_i}\}, \{K^{b_i}\}, \{C_b^{o_i}\}, \gamma_{OT})$

$Sim_B(f, b, o)$:

Only the input wire labels

Generate wire keys ordinarily $\{K_b^{w,\$} \leftarrow \{0,1\}^\lambda\}$

For e, remap the circuit to always output o.

One way to do it:

$$e_0^{g_{0,i}} = Enc.Enc.(K_{0,i}^{0,i})$$

$$e_1^{g_{0,i}} = Enc\ Enc\ (K_{e,i}^{e,i})$$

$$e_2^{g_{0,i}} = Enc\ Enc\ (K_{0,i}^{0,i})$$

$$e_3^{g_{0,i}} = (K_{0,i}^{g,i})$$

Arbitrary choices for remaining gates $e_j^{g,i} = Enc(K_0^{g,i})$

Output $(b, o, \{e_j^{g,i}\}, \{K^{a,i}\}, \{K^{b,i}\}, \{C_b^{o,i}\})$

How to prove indistinguishable: $\{Sim_B\} \approx \{Ideal_B\}$

Hybrid games and reduction to multi-message security.