Improvements to Garbled Circuits

Tuesday, October 10, 2017 12:15 PM

(see slides)

- Permute and Point

What do we need to prove?

- Correctness:

$\forall a,b, \quad Out_{A,B}\left[\underline{A}(a) \longleftrightarrow \underline{B}(b)\right] \approx \{f(a,b), f(a,b)\}$

- Simulatability

$Sim_B \approx View_B\left[A(a) \leftrightarrow B(b)\right]$

$View_B = \{b, o^{=f(a,b)}, \{e^{g_i}_{j \in \{0,1,2,3\}}\}, \{K^{a_i}\}, \{K^{b_i}\}, \{C^{o_i}_{b \in \{0,1\}}\}, \gamma_{OT,B}\}$

$color_{w_i} \xleftarrow{\$} \{0,1\} \quad K^{w_i}_0 \xleftarrow{\$} \{0,1\}^\lambda + color_{w_i}$

$K^{w_i}_1 \xleftarrow{\$} \{0,1\}^\lambda + \neg color_{w_i}$

Malicious Security

Malicious Correctness

$\forall A, \exists D, \forall b, Out_B\left[\underline{\underline{A}}(1^\lambda) \longleftrightarrow \underline{\underline{B}}(b)\right] \approx \{\hat{a} \leftarrow D : f(\hat{a}, b)\}$

Cut-and-choose

1. Alice generate λ instances of garbled circuits

$\{e^{g_i}_{j,m}\}_{m \in [1 \ldots \lambda]}, \{K^{w_i}_{\{a_i\},m}\}_m, \{C^{o_i}_{b,m}\}_m$

C_m = Commit Scheme $M_{i,m} : \{K^{w_i}_{b,m}\} \rightarrow \{0,1\}$

$\{e\}, C_-$

2. Alice → [OT] ← b_i Run OT for every garbled circuit.

3. Bob chooses $\frac{\lambda}{2}$ circuits to open, $\Theta \subset [1 \ldots \lambda]$

4. Alice sends all the wirelabels $\{K^{w_i}_{\{0,1\},m}\}_{m \in \Theta}$
   Opens C_m for $m \in \Theta$

5. Bob checks mapping for his inputs.

6. Alice sends inputs for $\neg\Theta$

7. Evaluate all remaining $\neg\Theta$
   Check that all outputs are consistent.