Garbled Circuits

- Garbling as a goal, not a technique
- Garbling scheme
- Fit existing literature in the framework
- Examples: Garble1/Garble2
- Goal:
  - More efficient construction
  - More rigorous analyses
  - More modular design

Circuit

- $f = (n, m, q, A, B, G)$
- $f$ is both an encoding of a function and the function itself
  - $ev(f, x) = f(x)$

Security

- $\Phi(f)$: side-information on $f$
- $\Phi_{\text{size}}(f) = (n, m, q)$
- $\Phi_{\text{topo}}(f) = (n, m, q, A, B)$
- $\Phi_{\text{circ}}(f) = (n, m, q, A, B, G) = f$
- Privacy
  - $(F, X, d)$ reveals nothing beyond $\Phi(f)$ and $y$
- Obliviousness
  - $(F, X)$ reveals nothing beyond $\Phi(f)$
- Authenticity
  - Given $F, X$, adversary is unable to produce $Y^*$, s.t.
    $d(Y^*) \neq \bot$
Indistinguishability (privacy)

\[ b \in \{0, 1\} \]

\[ (f_0, f_1, x_0, x_1) \]

\[ (F, e, d) \leftarrow \text{Gb}(f_b) \]

\[ X \leftarrow \text{En}(e, x_b) \]

\[ F, X, d \]

\[ b = b' \]

Indistinguishability (obliviousness)

\[ b \in \{0, 1\} \]

\[ (f_0, f_1, x_0, x_1) \]

\[ (F, e, d) \leftarrow \text{Gb}(f_b) \]

\[ X \leftarrow \text{En}(e, x_b) \]

\[ F, X \]

\[ b = b' \]

Simulation (privacy)

\[ b \in \{0, 1\} \]

\[ (f_0, e, d_0) \leftarrow \text{Gb}(1^k, f) \]

\[ X_0 \leftarrow \text{En}(e, x) \]

\[ y \leftarrow \text{ev}(f, x) \]

\[ F_0, X_0, d_0 \]

\[ b = b' \]

Simulation (obliviousness)

\[ b \in \{0, 1\} \]

\[ (f_0, e, d_0) \leftarrow \text{Gb}(1^k, f) \]

\[ X_0 \leftarrow \text{En}(e, x) \]

\[ y \leftarrow \text{ev}(f, x) \]

\[ F_0, X_0 \]

\[ b = b' \]

Authenticity

\[ f, x \]

\[ (F, e, d) \leftarrow \text{Gb}(f) \]

\[ X \leftarrow \text{En}(e, x) \]

\[ F, X, Y \]

\[ \text{De}(d, Y) \neq \bot \]

Security relations

- GS(\text{priv.sim}, \Phi) is the set of all garbling schemes that are privacy simulation secure over \Phi.
- similar for \text{priv.ind}, \text{obv.sim}, \text{obv.ind}
- similar for aut, but without \Phi.

\[ \Phi \]
Efficient invertibility

- \( M \) is a \( \Phi \)-inverter if
  - \( M(\phi) \) returns \( f \) s.t. \( \Phi(f) = \phi \)
- \( M \) is a \((\Phi, \text{ev})\)-inverter if
  - \( M(\phi, y) \) returns \((f, x)\) s.t. \( \Phi(f) = \phi \) and \( \text{ev}(f, x) = y \)
- Efficient inverters do it in polynomial time

Rest of the paper

- Proofs for the other drawn security relations
- Garble1
  - Definition
  - Dual-key ciphers
  - Proof of security (priv.ind over \( \Phi_{\topo} \))
- Garble2
  - Definition
  - Proof of security
    - priv.ind over \( \Phi_{\topo} \Rightarrow \text{priv.sim} \)
    - obv.ind over \( \Phi_{\topo} \Rightarrow \text{obv.sim} \)
  - aut
- Casting existing schemes to the GS framework
  - Secure function evaluation (SFe)
  - Private function evaluation (PFE)

Thank you

Any questions?