# Foundations of Garbled Circuits

by Mihir Bellare, Viet Tung Hoang and Phillip Rogaway

Sebastian Verschoor

CS 858: Computing on Encrypted Data
September 23rd, 2016

UNIVERSITY OF WATERLOO

## Outline

Paper overview

Definitions
- Garbling scheme
- Circuit
- Security

Security relations
- priv.sim $\Rightarrow$ priv.ind
- priv.ind $\wedge$ eff.inv $\Rightarrow$ priv.sim

Rest of the paper

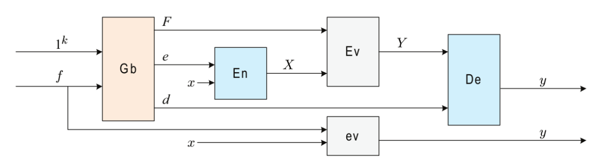


## Garbled Circuits

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



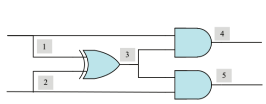
## Garbling scheme

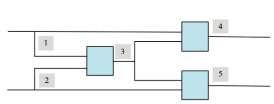



- $\mathcal{G} = (\mathrm{Gb}, \mathrm{En}, \mathrm{De}, \mathrm{Ev}, \mathrm{ev})$
- Compute $F(X) = Y \sim f(x) = y$
- Gb: Garbler
- En, De: encrypter/decrypter
- Ev, ev: "interpreters"



## Circuit



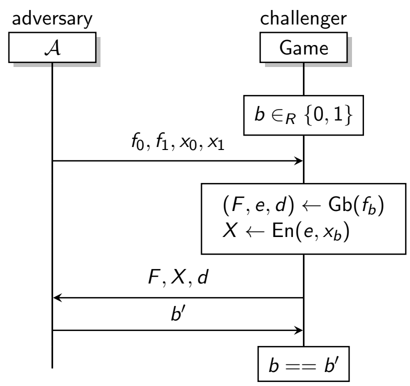

- $f = (n, m, q, A, B, G)$
- $f$ is both an *encoding* of a function and the function itself
  - $\mathrm{ev}(f, x) = f(x)$



## Security

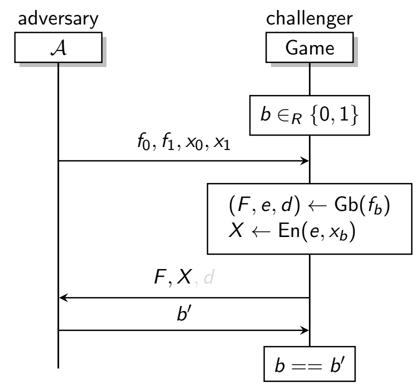
- $\Phi(f)$: side-information on f
  - $\Phi_{size}(f) = (n, m, q)$
  - $\Phi_{topo}(f) = (n, m, q, A, B)$
  - $\Phi_{circ}(f) = (n, m, q, A, B, G) = f$
- Privacy
  - (F,X,d) reveals nothing beyond $\Phi(f)$ and $y$
- Obliviousness
  - (F,X) reveals nothing beyond $\Phi(f)$
- Authenticity
  - Given $F,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

## Indistinguishability (privacy)



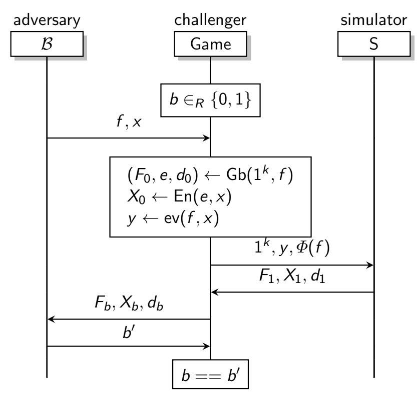



## Indistinguishability (obliviousness)



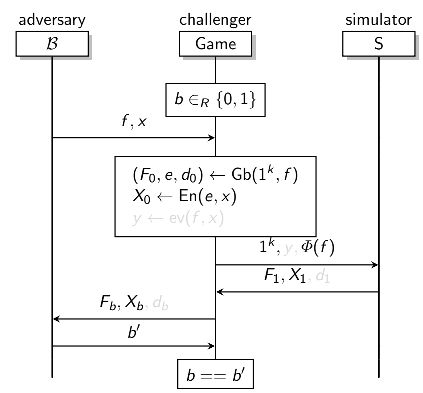



## Simulation (privacy)



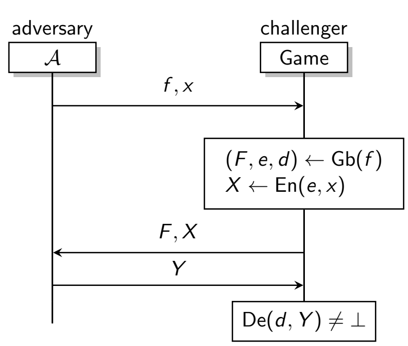



## Simulation (obliviousness)



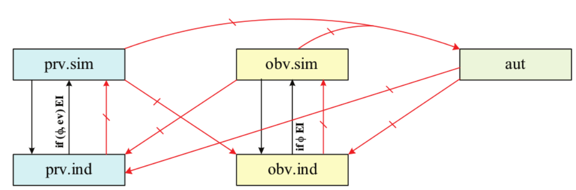



## Authenticity



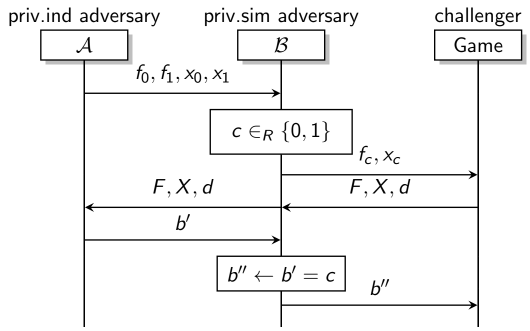



## Security relations




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

# priv.sim $\Rightarrow$ priv.ind



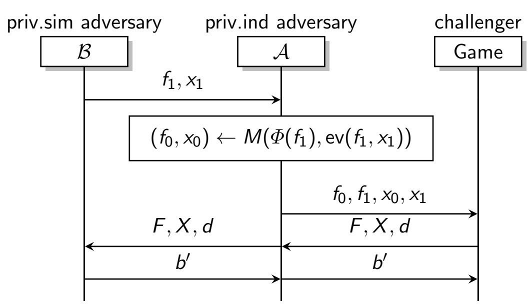



# Efficient invertibility

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



# priv.ind $\wedge$ eff.inv $\Rightarrow$ priv.sim






# 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 $\Phi_{topo}(\Rightarrow \mathit{priv.sim})$
    - obv.ind over $\Phi_{topo}(\Rightarrow \mathit{obv.sim})$
    - aut
- Casting existing schemes to the GS framework
  - Secure function evaluation (SFE)
  - Private function evaluation (PFE)



# Thank you

Any questions?