CMSC 858K — Introduction to Secure Computation November 8, 2013

Lecture 27

Lecturer: Jonathon Katz *Scribe(s): Xiao Wang*

1 Covert Security[1]

An attacker can cheat(successfully) with non-negligible probability, but to do so, they risk getting caught.

In real world protocol, it allows parties to output $corrupted(j)$

2 Three definitions

2.1 Failed-Simulation Formulation

Protocol Π is covertly-secure with ε-deterrent if for all PPT $\mathcal{A}$, there exists Sim, s.t. for any PPT distinguisher D

$$Pr\{correuption\,is\,detected\,in\,Real\} \geq \varepsilon|Pr\{D(Ideal_{Sim}(x)) = 1\} - Pr\{D(Real_{\Pi}(x)) = 1\}|$$

Issues:

- It does not rule out attempt cheating based on honest input.
- It has difficulties with composition.

2.2 Explicit Cheat Formulation

Idea world:

- Both parties send input to the ideal functionality
- The adversary can also send a special signal *cheat*.
- if the adversary does not sent *cheat*, run as usually; if adversary does send *cheat*, he will get the input of the honest party. Then:
  - with probability ε, the trusted party will send $corrupted(j)$ to the honest party
  - with probability $1 - \varepsilon$, the attack is allowed to arbitrary specify the output for the honest party.

2.3 Strong Explicit Cheat Formulation

Idea world:

- Both parties send input to the ideal functionality
- The adversary can also send a special signal *cheat*.
- if the adversary does not sent *cheat*, run as usually; if adversary does send *cheat*, then:
  - with probability ε, the trusted party will send $corrupted(j)$ to the honest party
  - with probability $1-\varepsilon$, the attack is allowed to arbitrary specify the output for the honest party. He will also get the input of the honest party.

Strong explicit cheat formulation with $\varepsilon = 1 - negligible$ is the same as malicious security

3 More details

composition Under strong explicit cheat forumulation, if Π is an ε-covert secure in the $\{(f_i, \varepsilon_i)\}$ hybrid-model, then instantiating $\{f_i\}$ using ε_i-covert protocol gives an ε-covert protocol.

Using Cut-And-Choose to construct A cut and choose protocol where the circuit generator send l Garbled Circuits, and circuit evaluator checks $l-1$ of these is $(1-\frac{1}{l})$-covert secure.

Covert security with public verifiability[2] Idea: Even cheating is detected, we cannot prove it to the third party: Covert security with public verifiability:

- Strong explicit cheat security.
- If an honest party output *corrupted* it also output a valid certificate of cheating.
- The certificate does not leak information on parties' input
- Defamation free

References

[1] Aumann, Yonatan, and Yehuda Lindell. "Security against covert adversaries: Efficient protocols for realistic adversaries." In *Theory of Cryptography*, pp. 137-156. Springer Berlin Heidelberg, 2007.

[2] Gilad Asharov and Claudio Orlandi. Calling Out Cheaters: Covert Security with Public Verifiability *ASIACRYPT* 2012, Springer-Verlag (LNCS 7658), pages 681-698, 2012.