Universally Composable Security

Ran Canetti in FOCS '01

Presented by Glen Nuckolls
Goals and Claims

- Security definition guarantees security with arbitrary “composition”
- Unbounded number of protocol invocations by any application protocol
- Concurrent with same and other protocols
- Adaptive adversary can corrupt honest parties
A few Technicalities

- Parties are interactive Turing Machines (ITM): many read/write tapes, either active, waiting, or halted.

- Indistinguishability $\approx$ is negligible probability difference in security parameter of environment’s binary output

- Ideal functionality an ITM: “magic” modeled by restricting adversarial view of messages
UC Security

For all adversaries, no environment can tell between real protocol interacting with real adversary and ideal protocol in presence of “ideal” adversary.

∀A.∃S.∀Z \text{ REAL} _{\rho,A,Z} \approx \text{ IDEAL} _{F,S,Z}
The Real-life Model

\[ \text{REAL}_{\rho, A, Z} \]
The Ideal Model

\( \tilde{P_i} \) : "dummy" parties just relay i/o and msgs

\( \text{IDEAL}_{\mathcal{F},S,Z} \)
F-Hybrid Model

- A protocol $\pi$ has access to ideal functionality $F$
- Compare when $F$ replaced with secure, real $\rho$
- F-Hybrid adversary denoted $H$
F-Hybrid Model

HYBRID $F_{\pi, H, Z}$
Universal Composition Theorem

If $\rho$ realizes an ideal functionality $\mathcal{F}$, and $\pi$ is a protocol in the $\mathcal{F}$-hybrid model, then:

$$\forall A. \exists H. \forall Z \quad \text{REAL}_{\pi, A, Z} \approx \text{HYB}_{\pi, H, Z}$$

$\rho$ is indistinguishable from $\mathcal{F}$ in any protocol $\pi$
Corollary: Secure Composition

If $\rho$ securely realizes $\mathcal{F}$ and $\pi$ securely realizes $\mathcal{G}$ in the F-hybrid model, then

$$\forall A. \exists H, S. \forall Z \quad \text{REAL}_{\pi^\rho, A, Z} \approx \text{HYBRID}_F^{\pi, H, Z} \approx \text{IDEAL}_{G, S, Z}$$

If $\pi$, is secure using ideal functionality $\mathcal{F}$ and $\rho$ is secure, then the composition $\pi^\rho$ is secure.
Proof overview:

1. Formulate proof friendly definition of UC.

2. Define ideal adversary \( \mathcal{H} \)

3. Show that a good distinguisher environment \( \mathcal{Z} \) between \( \pi \) with \( \rho \) and \( \pi \) with ideal \( \mathcal{F} \), can be used to construct a good environment \( \mathcal{Z}_\rho \) distinguishing between \( \rho \) and \( \mathcal{F} \).

4. Existence of good \( \mathcal{Z} \) implies good \( \mathcal{Z}_\rho \)

5. Thus: no good \( \mathcal{Z}_\rho \) implies no good \( \mathcal{Z} \).
UC with Dummy Adversary

- Dummy adversary pushes adversarial role to environment, eliminates quantifying over all adversaries

- \( \tilde{A}_C \) takes input instructions from environment: report messages sent by parties, deliver message to party, corrupt some party

\[ \exists S. \forall Z \exists S. \forall Z \ \text{REAL}_{\pi, \tilde{A}_C, Z} \approx \text{IDEAL}_{\mathcal{F}, S, Z} \]
Define Hybrid Adversary

\( \mathcal{H} \) needs to handle requests from \( \mathcal{Z} \) with respect to parties \( \mathcal{P}_i \) and copies of \( \rho \).

\( \mathcal{Z} \) requests/messages relating to \( \mathcal{P}_i \) are relayed from \( \mathcal{P}_i \).

Requests/messages relating to \( \rho : \mathcal{H} \) mimics ideal \( S \) for request.
The Hybrid adversary

\[ \tilde{\mathcal{A}}_C \]
The (l-1) Hybrid model

Diagram:
The l-Hybrid model
Hybrid Argument

- Let m be a bound on invocations of \( \rho \) in \( \pi \)
- 0-hybrid is real model for \( \pi^\rho \)
- m-hybrid is hybrid model
- Environments that can tell between real and Hybrid can tell between \( l-1 \) and \( l \) hybrid for some \( l \).
- Reasoning: if all gaps small, then real vs hybrid gap is small
Reduction: real vs ideal to hybrid \( l-1 \) vs \( l \)
Real vs Ideal

\[ \rho, \tilde{A}_C, Z_\rho \]

\[ \tilde{\rho}, \tilde{A}_C, Z_\rho \]

\[ \rho, \tilde{\mathcal{F}}, S, Z_\rho \]

\[ \tilde{\rho}, \tilde{\mathcal{F}}, Z_\rho \]