A universally composable cryptographic library

Long Ngo

April 28, 2008
Outline

Background

Problem statement

Our library

Application

Conclusion
Outline

Background

Problem statement

Our library

Application

Conclusion
Simulatable security

(Borrowed from Canetti’s slide)

- Standard simulatability: $\forall A \forall Z \exists S \ldots$
- Universal simulatability: $\forall A \exists S \forall Z \ldots$
Universal composability

- G securely realizes ρ
- If G UC-securely realizes ρ, then Polynomial many copies of G
Outline

Background

Problem statement

Our library

Application

Conclusion
A gap in security protocol analysis

- Formal or symbolic methods
  \((K1, Enc(K1, secret)) \Rightarrow (K1, Enc(K1, secret)) \Rightarrow secret\)
  - Can automatic
  - Can not guarantee security, but can find potential attacks

- Computation method: If the output distribution almost coincides the distribution in the ideal setting
  - complete
  - done manually
  - error-prone
Backes’s universally composable library

- Try to bridge the gap
- Define a Dolev-Yao style library: abstract terms
- Define a secure realization one: Bitstring
- We can use the abstract library in formal methods
- Current version: Signature, CCA2 public key encryption
Our motivation

- Another library with threshold homomorphic encryption
- But it may be "Conditional universally composable" because homomorphic encryption is not CCA2
Ideal library

\[ S_H \]

\[ \text{in}_u! \quad \text{out}_u? \]

\[ \text{net}_{id_{u,v,x}} \quad \text{for} \quad (u, v, x) \in \text{ch}_{\text{honest}} \]

\[ A \]
Real library
Security of the cryptographic library

Theorem

Given an encryption scheme $\mathcal{E}_{\text{thres}}$, a functionality FNIZK as a non-interactive zero-knowledge proof system for plaintext validity, a functionality $\text{FKEY}^{\mathcal{E}_{\text{thres}}}$ as a distributed key generation system for $\mathcal{E}_{\text{thres}}$ for all $n \in \mathbb{N}$, all correct parameters $L'$ and all $\mathcal{H} \subseteq \{1, \ldots, n\}$, there exist a simulator $\text{Sim}_H$ that satisfies the following property: For all polynomial-time honest users $H$ and adversary $A$, the view of $H$ while interacting with a real machine $M_{u,\mathcal{H}}$ for all $u \in \mathcal{H}$ and $A$ are polynomial indistinguishable from the view of $H$ while interacting with $\text{TH}_\mathcal{H}$ and $\text{Sim}_\mathcal{H}(A)$ with a parameter $L := \text{R2Ipar}(\mathcal{E}_{\text{thres}}, \text{FNIZK}, \text{FKEY}^{\mathcal{E}_{\text{thres}}}, L')$ under the following condition

- **Condition:** For each key generation of $\mathcal{E}_{\text{thres}}$, the indistinguishability holds only before the second time of decryption.
Outline

Background

Problem statement

Our library

Application

Conclusion
Application

- Automatic tool for analyzing security of protocol that contain homomorphic encryption
- For example: E-voting
There is a gap in security protocol analysis methods ⇒
Difficult to have complete automated tool
We can bridge the gap by a Dolev-Yao style library which is securely realized
We are trying to make such a library, which has a threshold homomorphic encryption, under some working condition.
Thank you!

ANY QUESTION?