

Provably Secure Substitution of Cryptographic Tools

Lea Kissner
leak@cs.cmu.edu

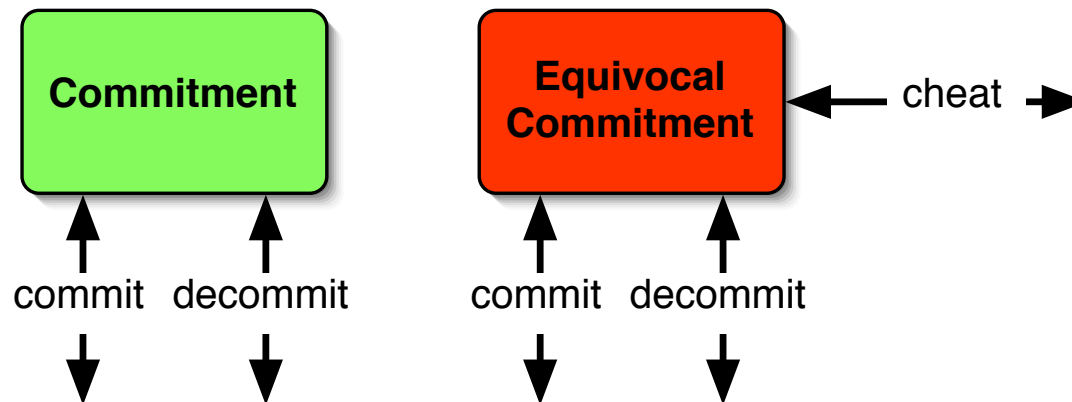
David Molnar
dmolnar@eecs.berkeley.edu

Motivation

- Protocols secure against malicious parties are expensive
- **Why?** Simulation proofs often require **expensive tools**
 - Special types of commitments (equivocal, chameleon, ...)
 - Encrypted data with unknown key
 - Many more

Main Idea

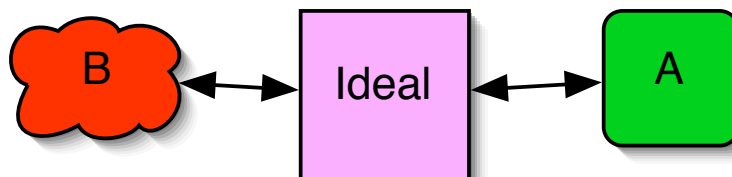
- Many expensive tools used in these protocols have corresponding efficient tools
- Hash commitment vs. equivocal bit string commitment



- We prove that in non-pathological protocols, corresponding tools can be substituted

Definitions

- Tool A is a **workalike** of tool B if
 - B is secure with respect to some ideal
 - A is *indifferentiable* from ideal



- A **handle** is any data whose domain or distribution varies between A and B
- A **replacement-friendly protocol** is one in which no player must compute a function of any handle (except through the designated tool), and handles can be ID'd

Prelim. Results

- In *any replacement-friendly protocol* secure against malicious players:
 - If B is used as a *black-box subroutine*
 - If A is a *workalike* of B
 - Then tool A can be **securely substituted** for tool B

Bounty

- Do you have a tool or protocol where this can be applied?

- **We will buy
you a drink!**

Bounty

- Do you have a tool or protocol where this can be applied?

- We will buy
you a drink!

Lea Kissner	David Molnar
leak@cs.cmu.edu	dmolnar@eecs.berkeley.edu