Lossy Trapdoor Functions

Chris Peikert Brent Waters

SRI International

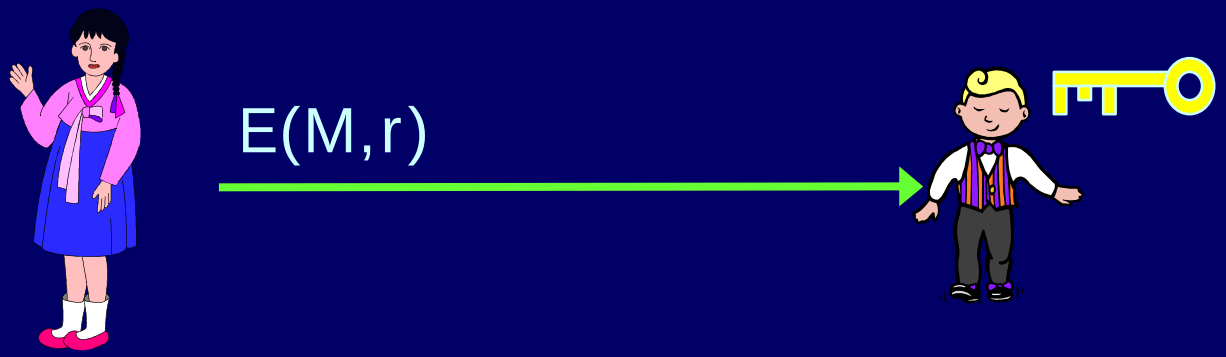
Results

- Trapdoor Functions
  - Discrete Log & Lattice Constructions
  - First since RSA
- CCA-Secure Encryption from Lattice Assumptions

Trapdoor Functions

- Recover all function's input

P.K. Encryption

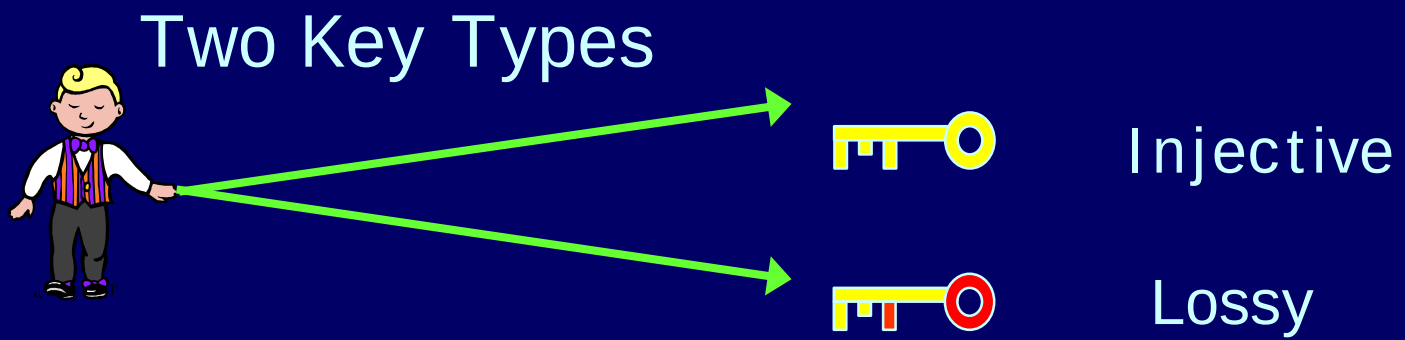


Can't Build TDF from PK Enc. [GMR01]

E.g. E(x,x) no reduction possible

Lossy Trapdoor Functions

Main Idea: Simulation over Public Key



1. Injective Key Recovers: f(x) + trapdoor -> x
2. Lossy Key: Input Info lost
3. Can't distinguish type

Summary

Realizations: DDH, Lattices (LWE [R05])

- CCA Constructions
- Recover randomness (not Zero Knowledge!)

	TDF	CCA-Enc
DDH	✓	[CS98]
Lattices	✓	✓

Thank You