New Proof Methods for Attribute-Based Encryption: Achieving Full Security through Selective Techniques

Allison Lewko

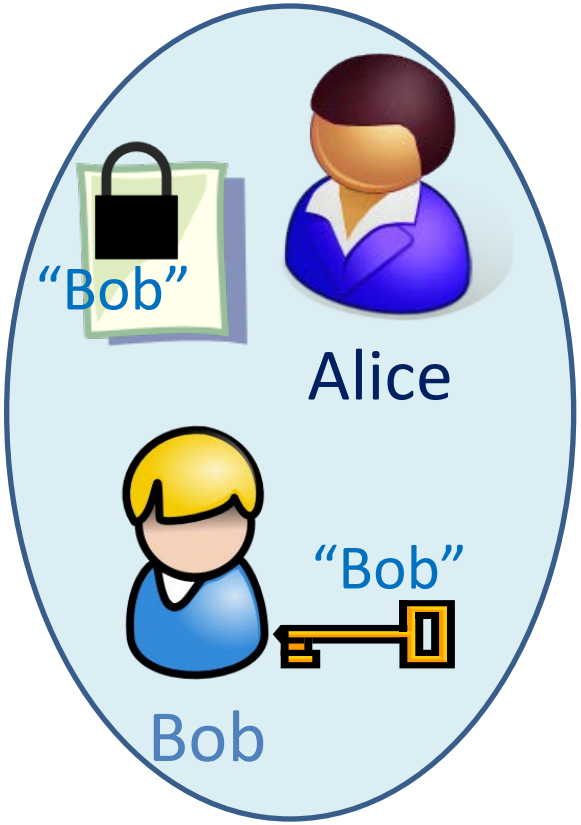
Microsoft Research

Brent Waters

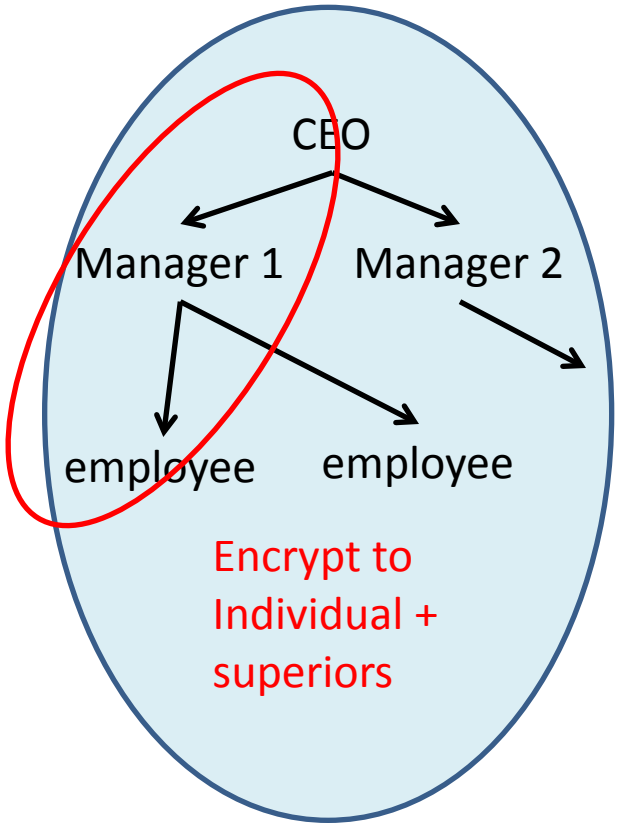
THE UNIVERSITY OF TEXAS AT AUSTIN™

Roots of Attribute-Based Encryption

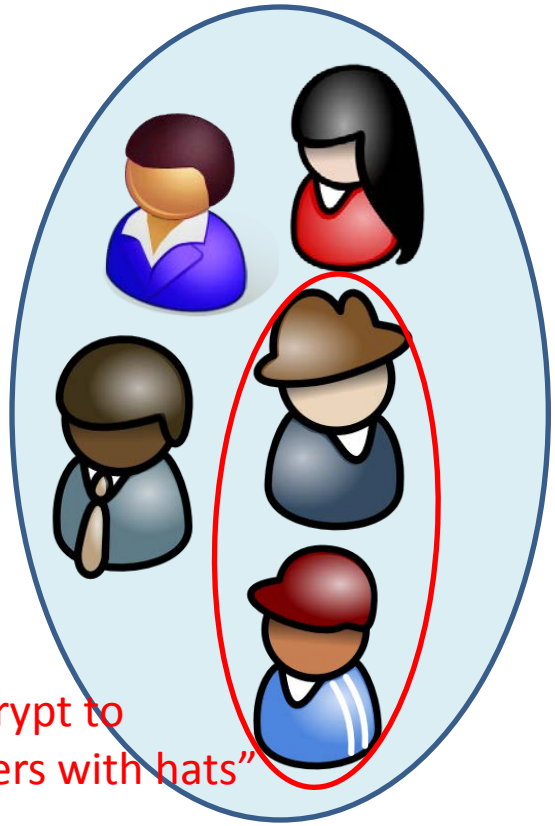
Moving beyond Public Key Encryption:



Identity-based Encryption [S84,BF01,C01]



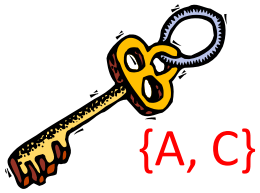
Hierarchical Identity-based Encryption [HL02,GS02]



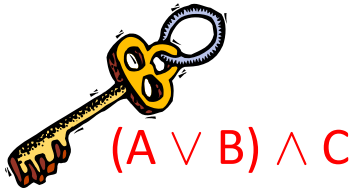
Attribute-based Encryption [SW05]

Two Kinds of ABE

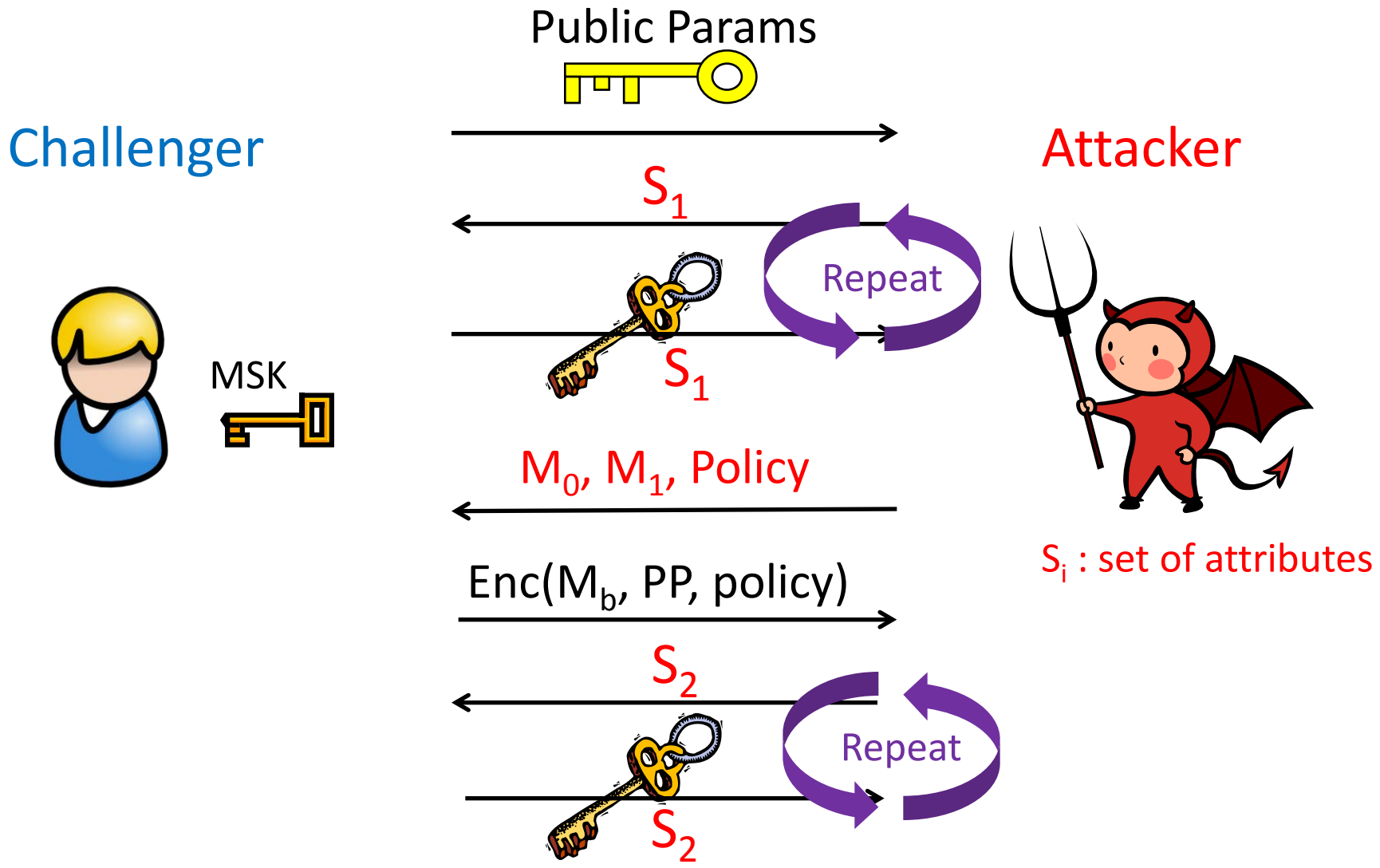
Ciphertext Policy ABE:



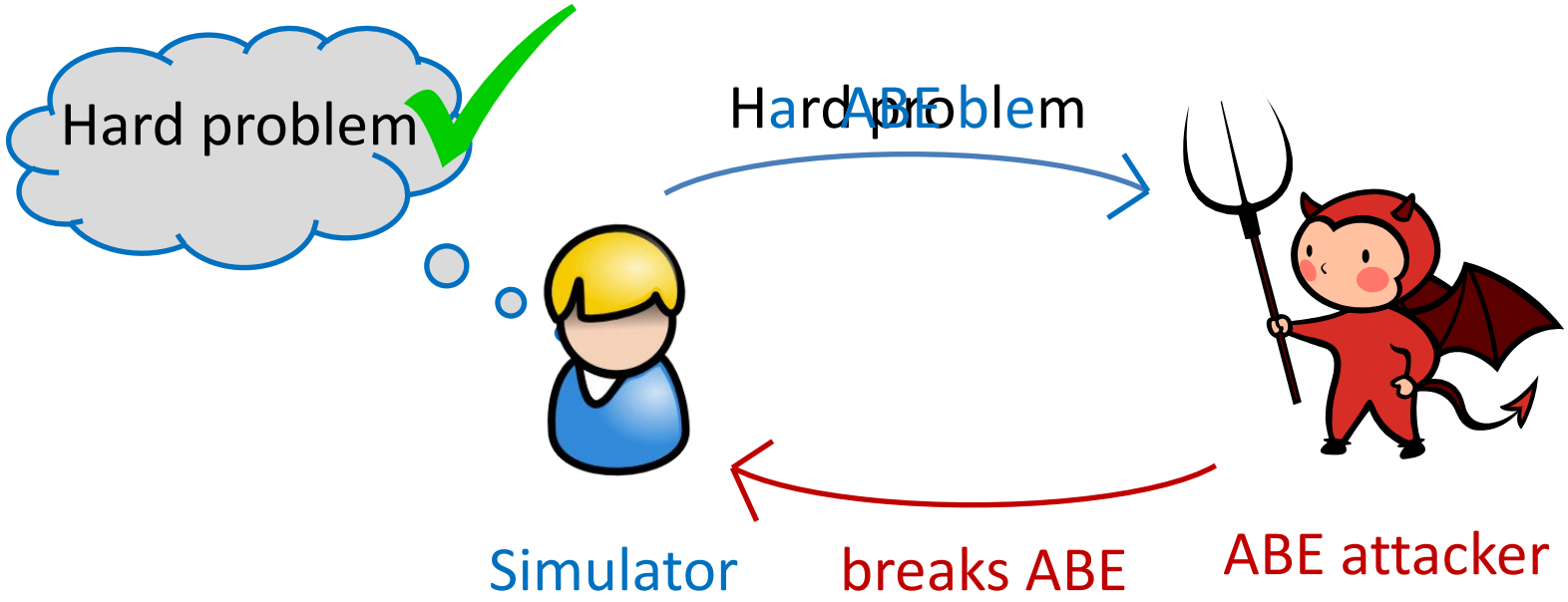
Key Policy ABE:



Security Goal for ABE



Proof Challenges

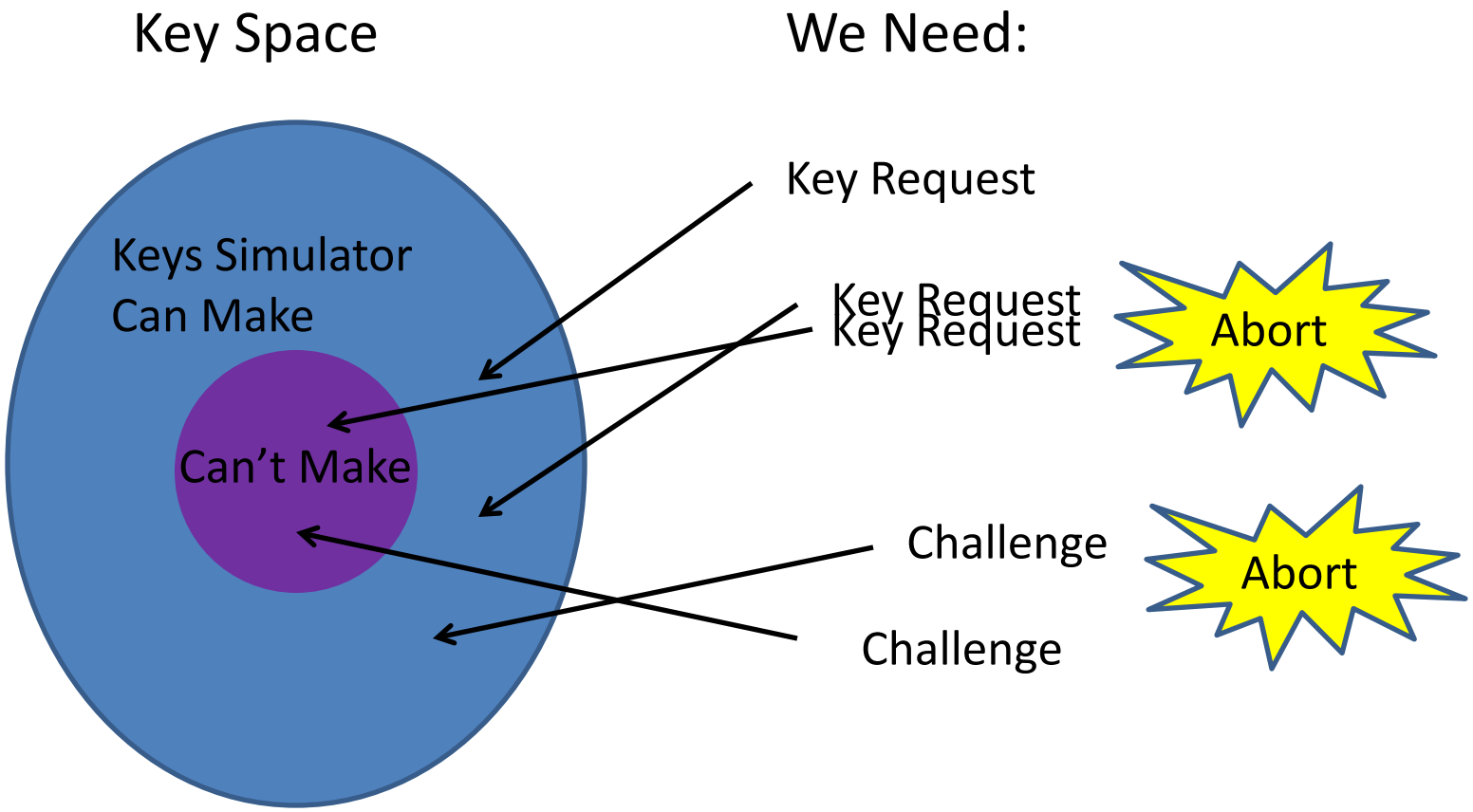


Challenge: simulator must:

- respond to key requests
- leverage attacker's success on challenge

Partitioning Proofs

Previous approach – Partitioning [BF01, BB04, W05, GPSW06]



Problem: Why Should Attacker Respect the Partition?

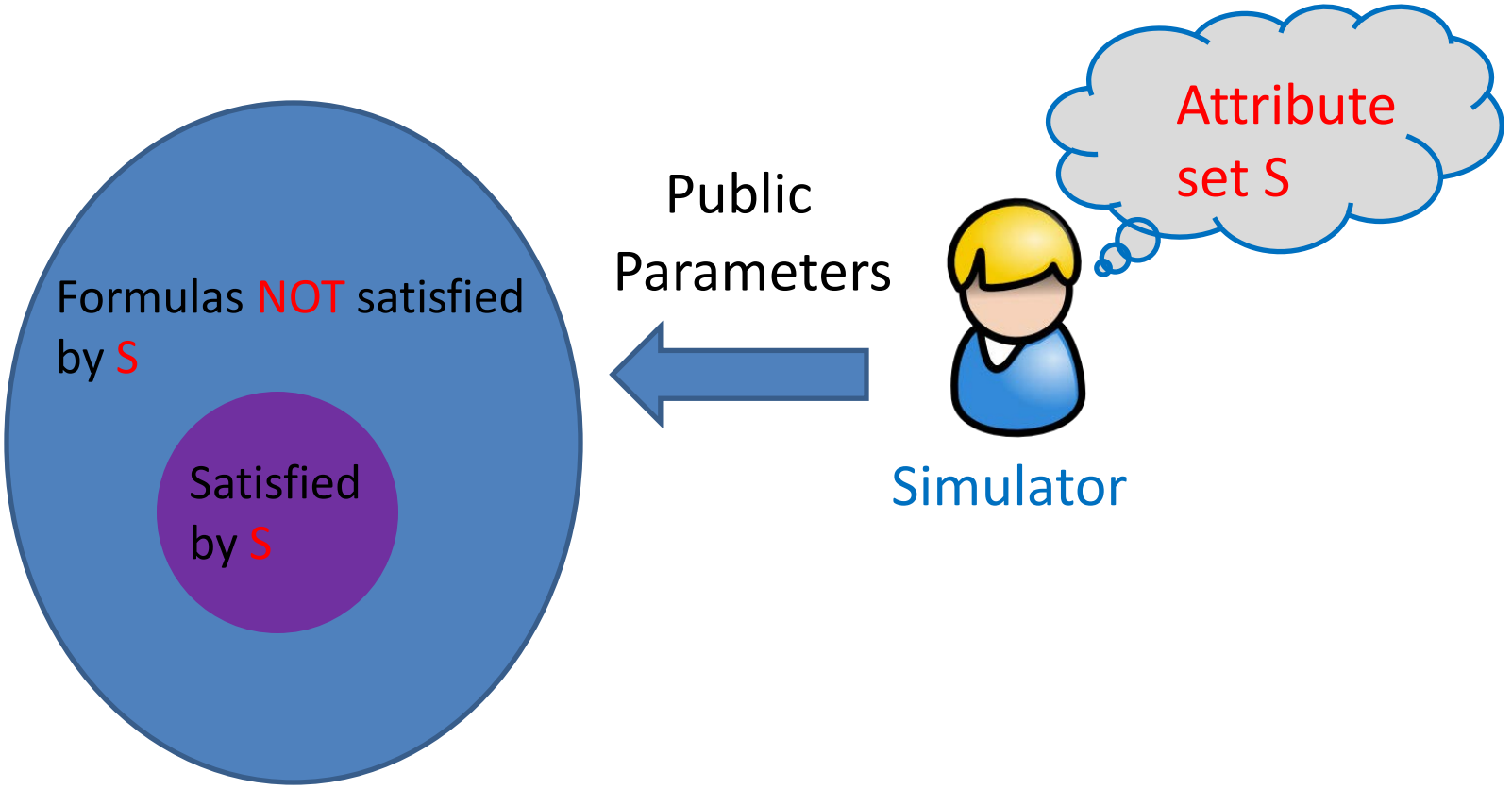
Two Approaches:

1. *Make Attacker Commit (weaker) selective security*

2. *Guess and quit when wrong*

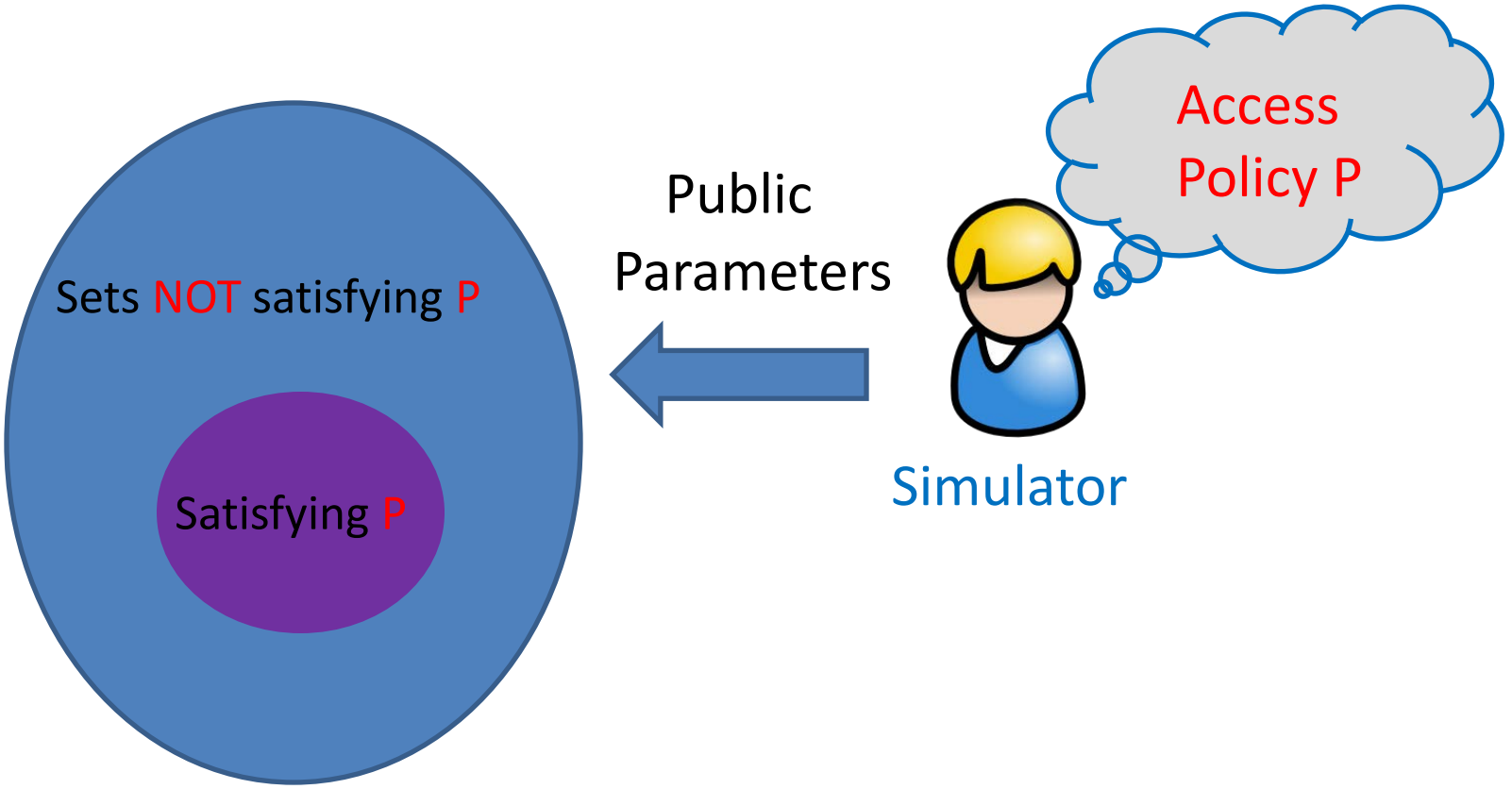
Selectively Secure ABE [GPSW06, W11]

Selectively Secure KP-ABE [GPSW06]:



Selectively Secure ABE [GPSW06, W11]

Selectively Secure CP-ABE [W11]:

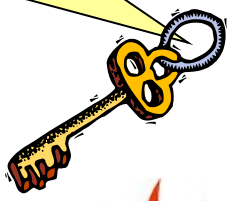


Dual System Encryption [W09]

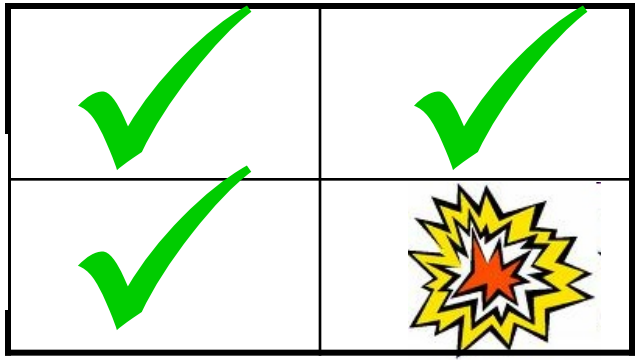
Used in real system

Normal

Semi-Functional



Normal

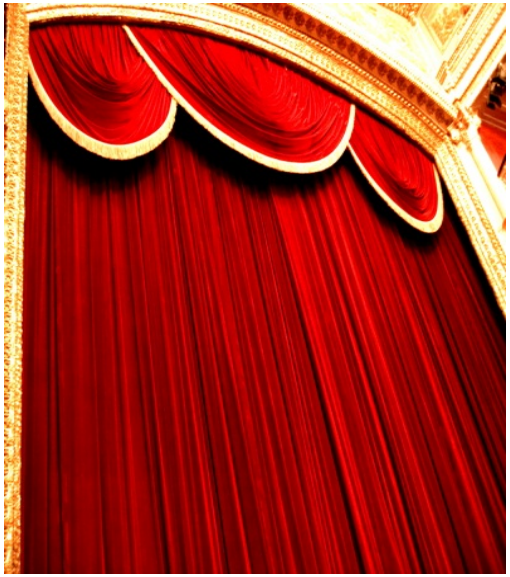


A Dual System Encryption Proof

Real Security Game:

Hybrid Argument:

Hardest step previously done
With info-theoretic argument
- Efficiency drawbacks

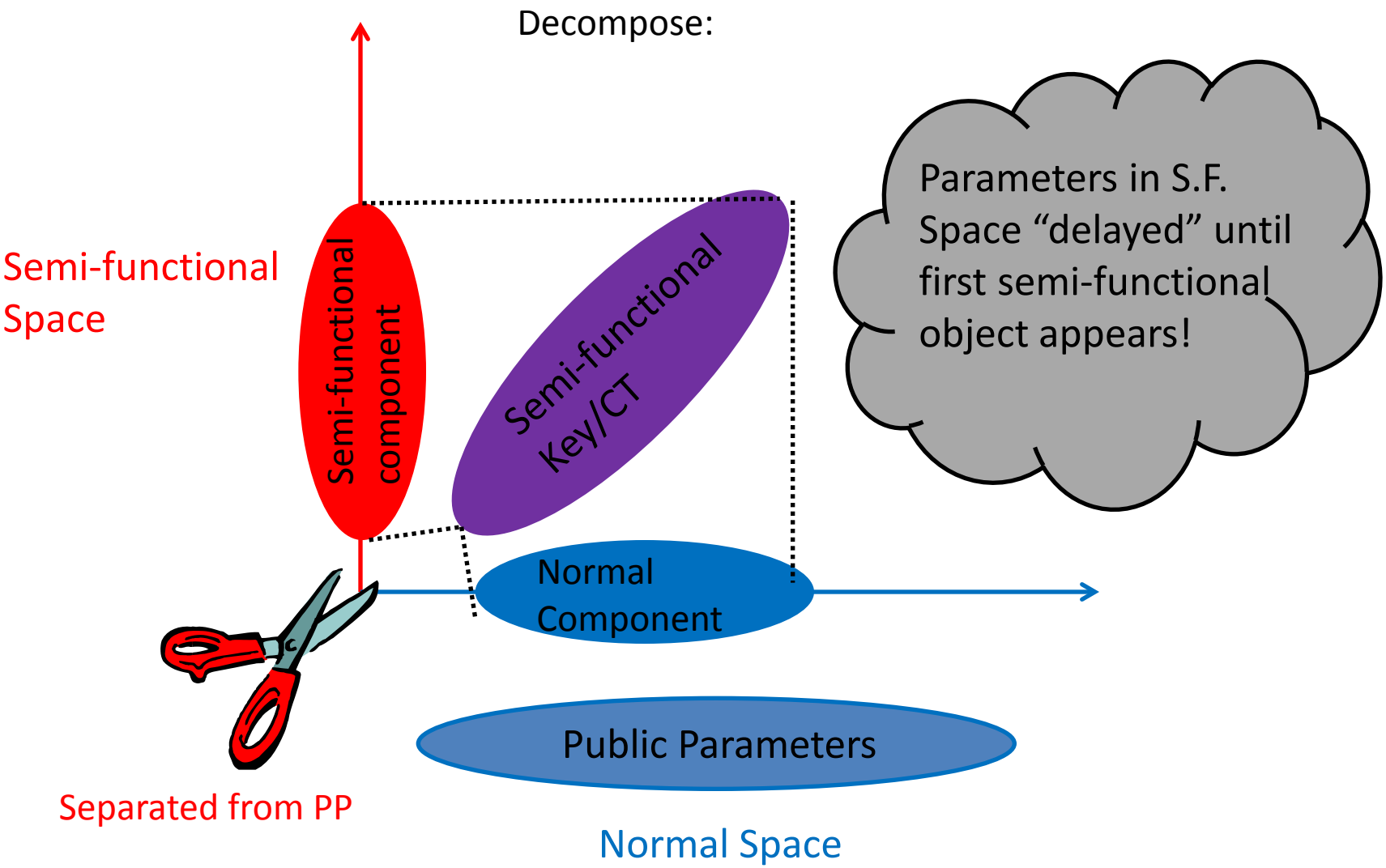


Regardless of
Compability!

Incompatiblity of key/CT ⟶ High probability decryption failure

Decryption failure ⟶ Message independent CT

Dual System Encryption Reimagined



The Security Game in S.F. Space

Challenger

Public Params

S_1

Repeat

$M_0, M_1,$ policy

Enc(M_b, PP, policy)

S_i

Repeat

Attacker

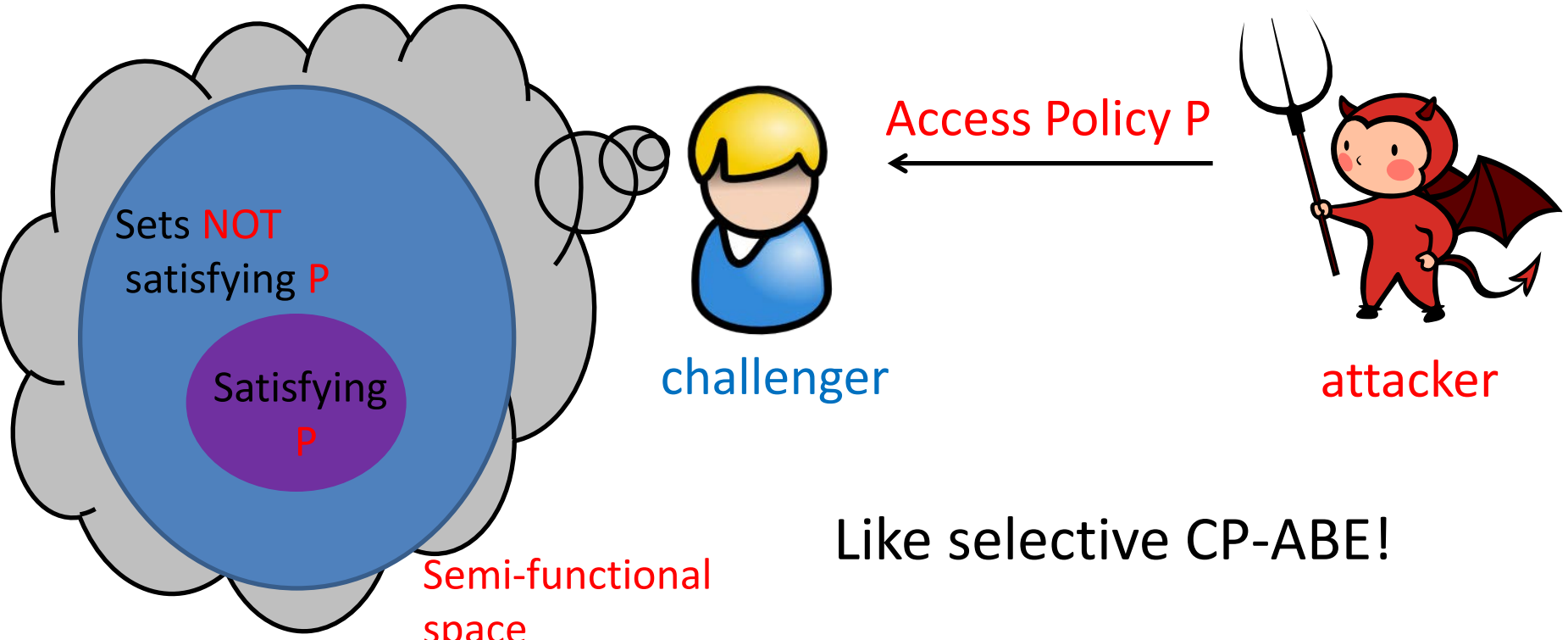
S_i : sets of attributes

Dividing the Proof: Two Cases

Thought experiment: consider attacker requesting one key

(generalize to many keys via hybrid argument)

Case 1: CT request comes before key

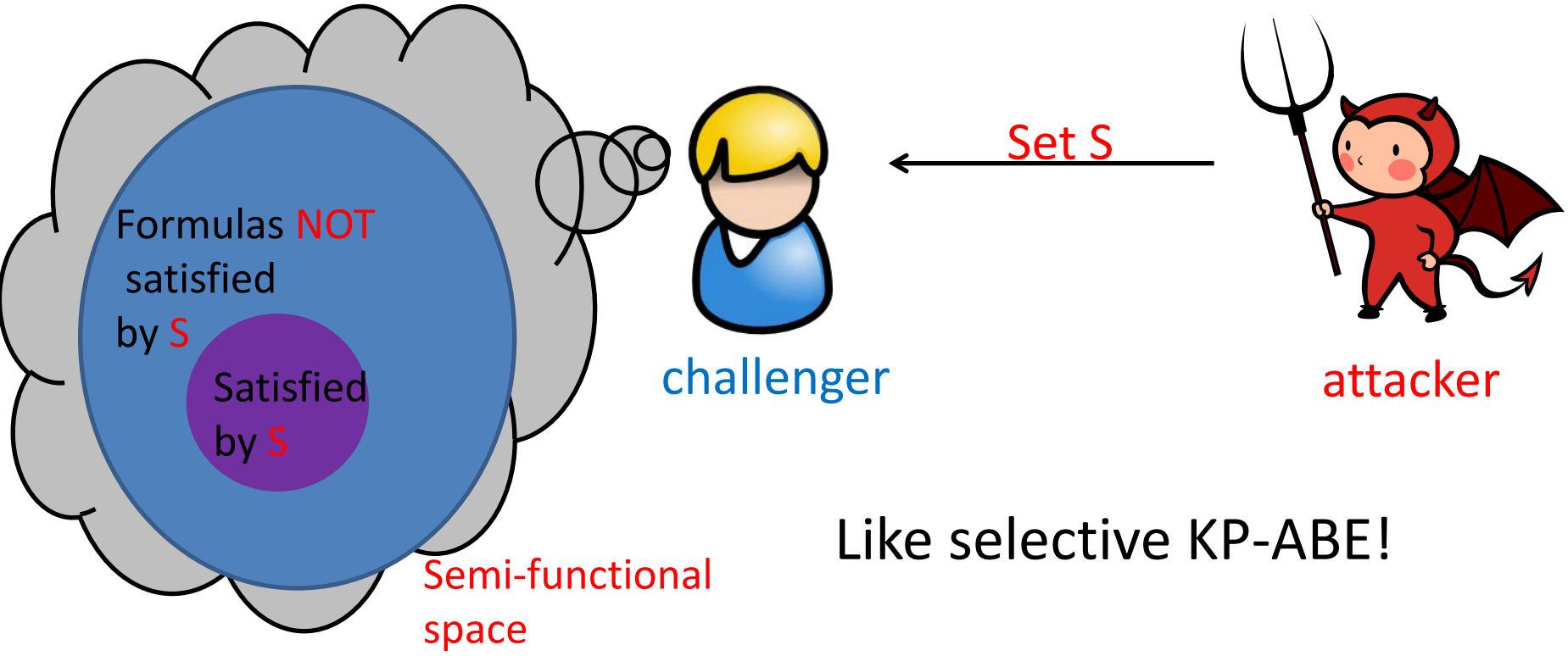


Like selective CP-ABE!

Dividing the Proof: Two Cases

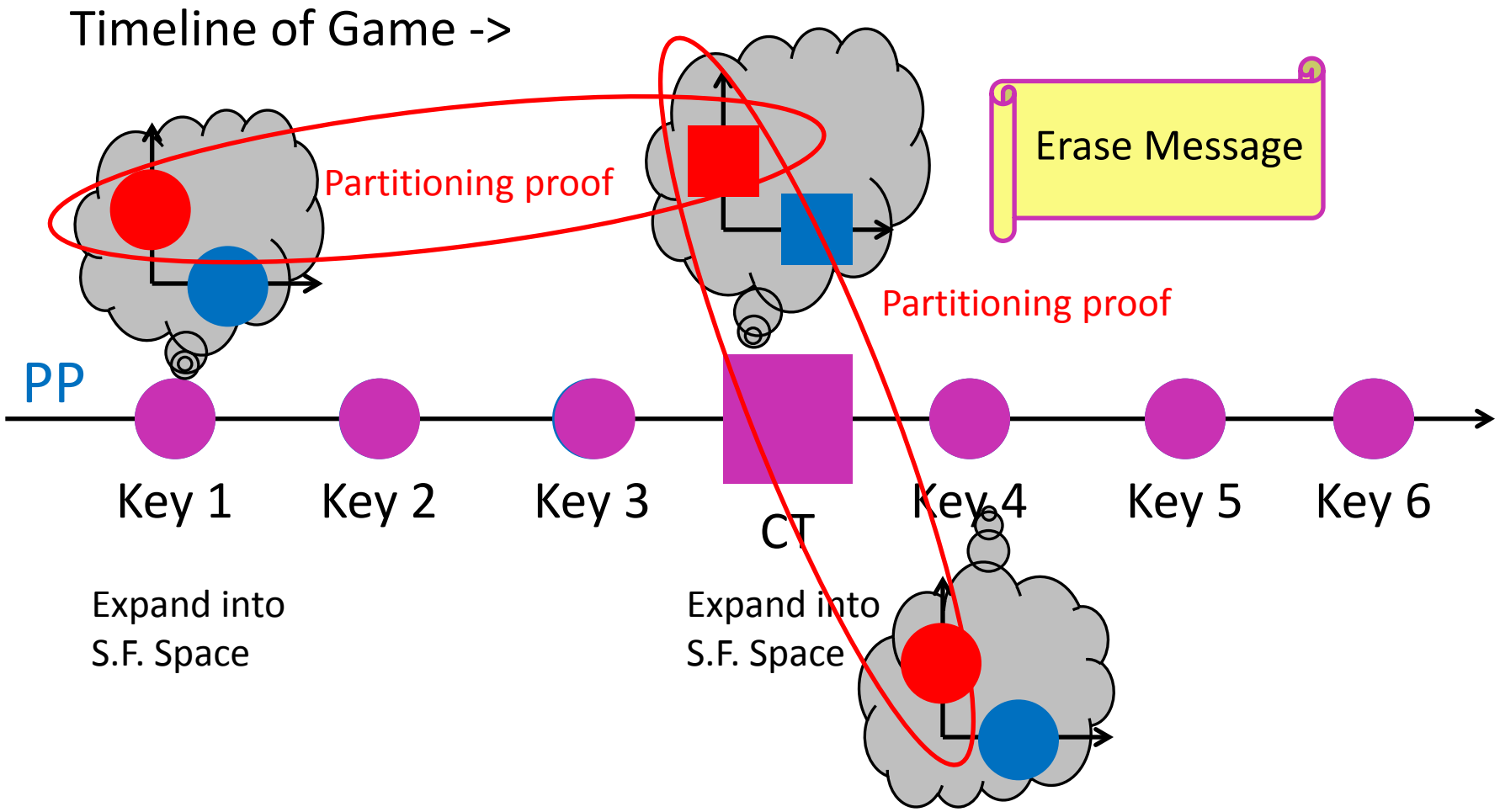
Thought experiment: consider attacker requesting one key
(generalize to many keys via hybrid argument)

Case 2: key request comes before CT

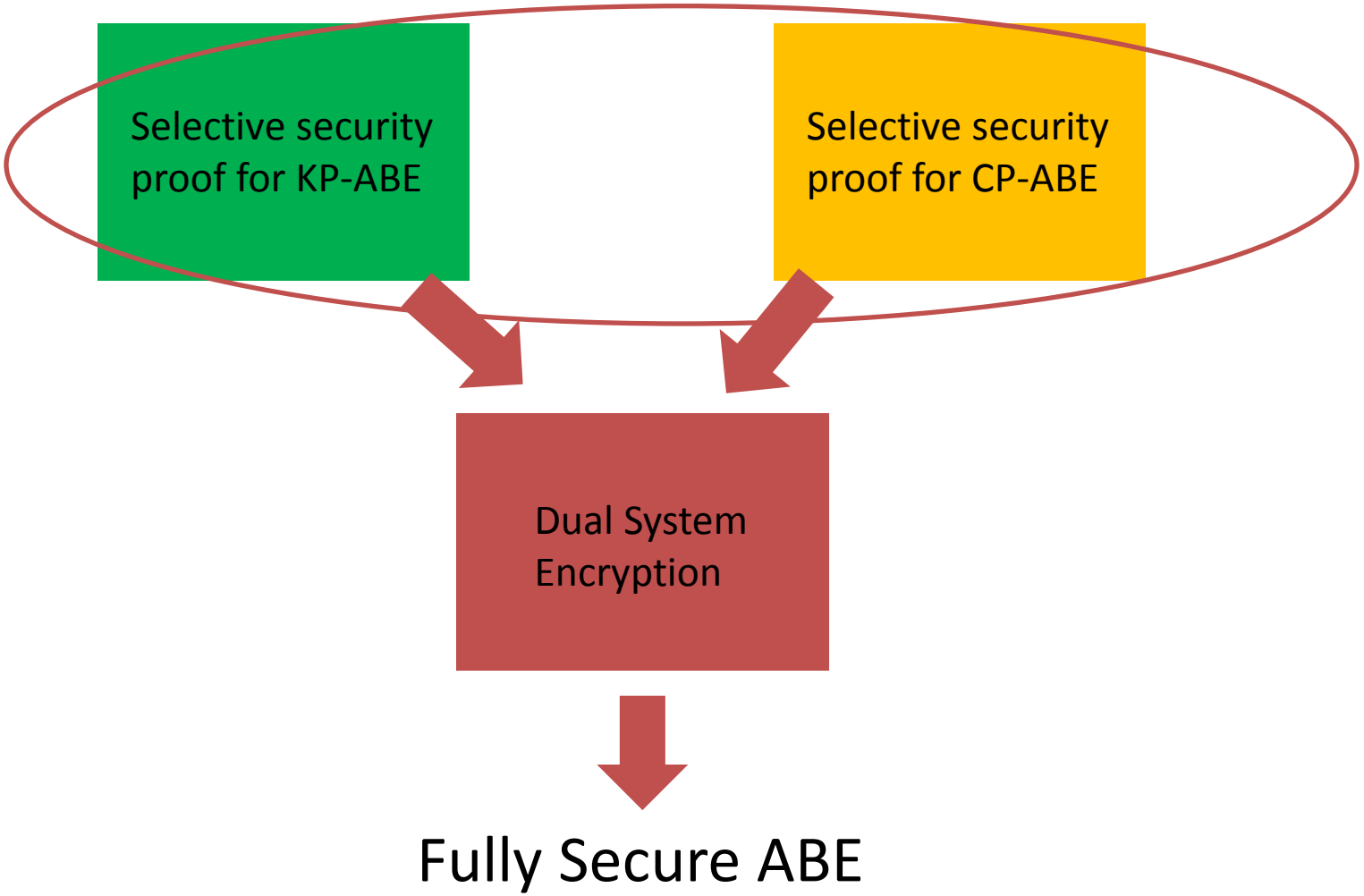


Like selective KP-ABE!

Proof Schematic



Summary of Techniques



Open Problems

- Selectively secure CP-ABE from a non-“q-type” assumption
- ABE for more general policies (ideally, circuits)
  - Progress to be reported later in this session

Thanks for your attention!

Questions?