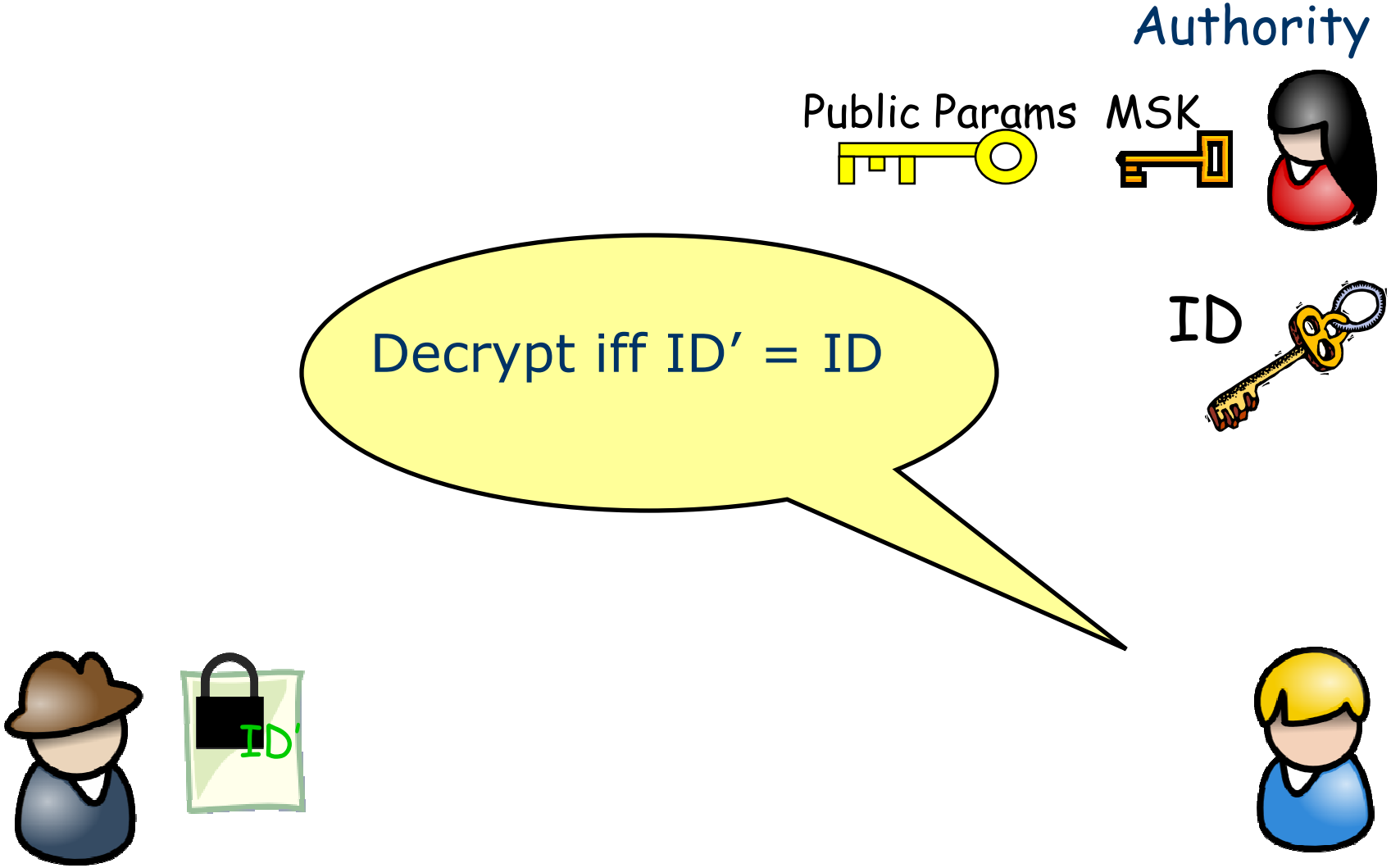
Dual System Encryption:

Realizing IBE and HIBE from Simple Assumptions

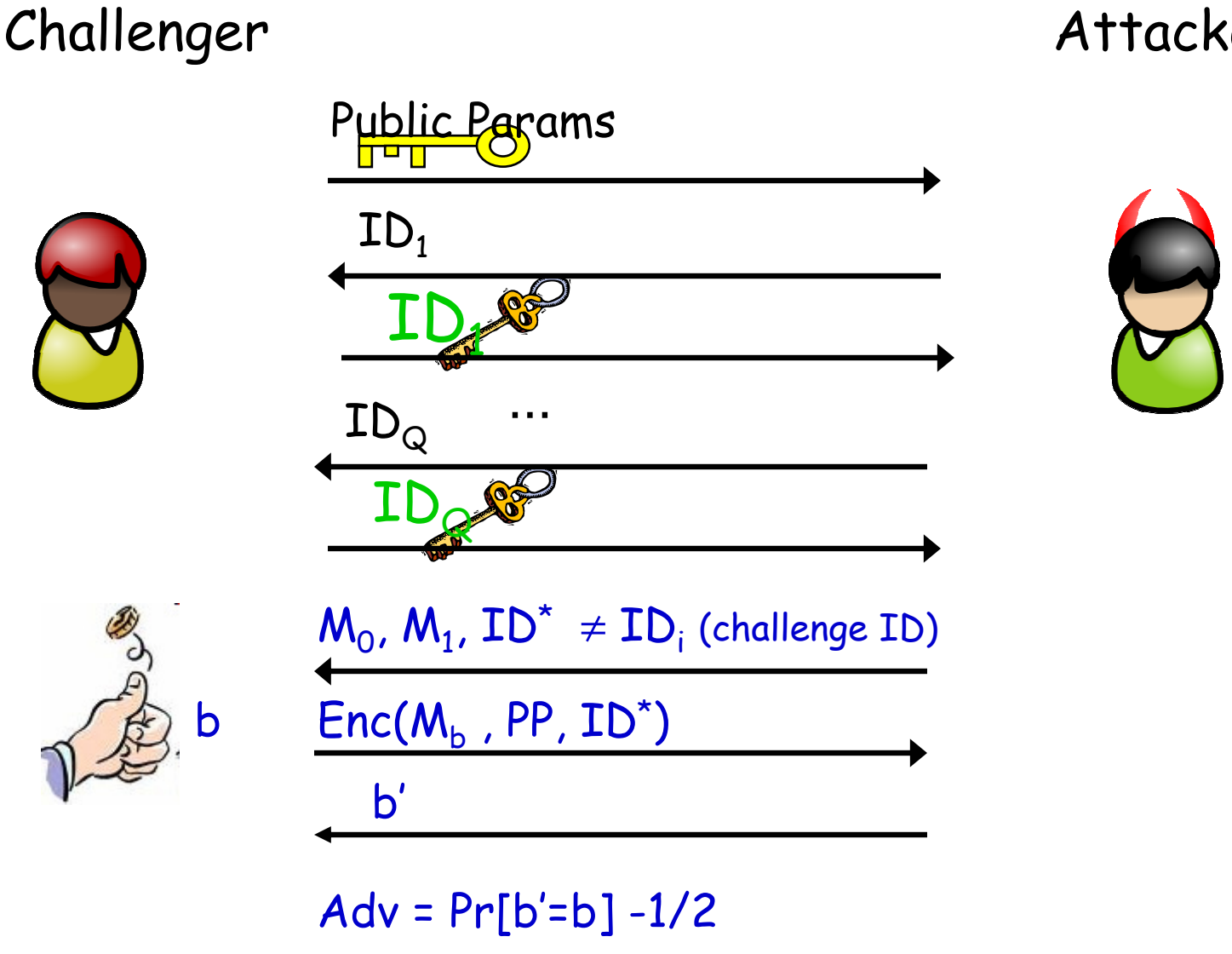
Brent Waters

THE UNIVERSITY OF
TEXAS
AT AUSTIN™

Identity-Based Encryption [S84,BF01,C01]

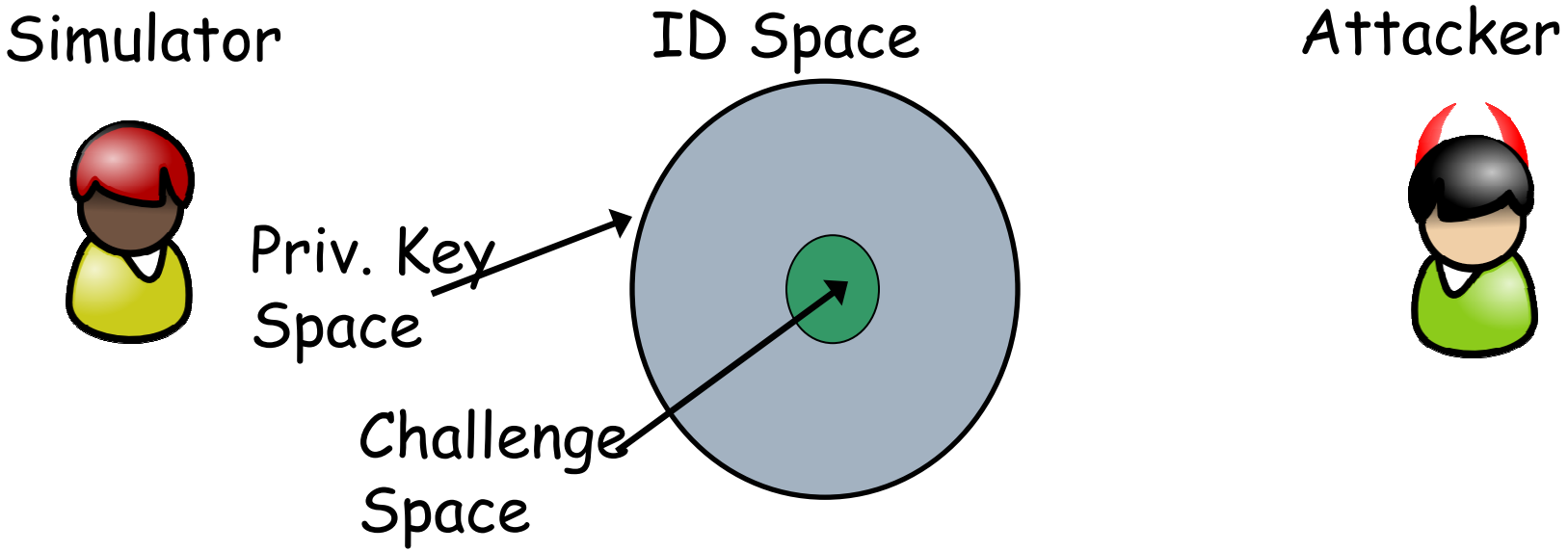


IBE Security [BF01]

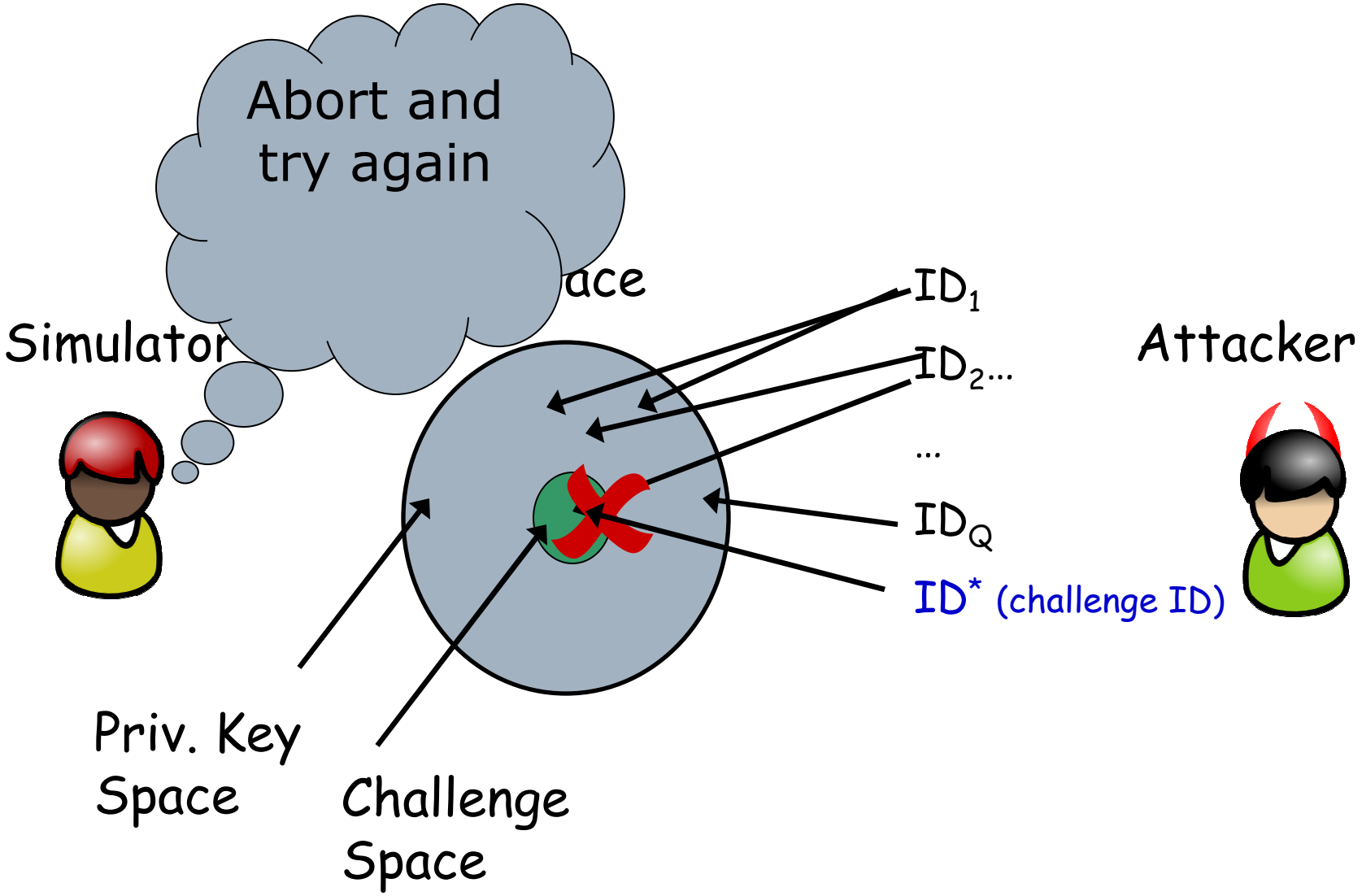


IBE Security Proofs

- 2 Goals:
  - Answer Attacker Queries
  - Use Attacker Response
- "Partitioning" [BF01, C01, CHK03, BB04, W05]

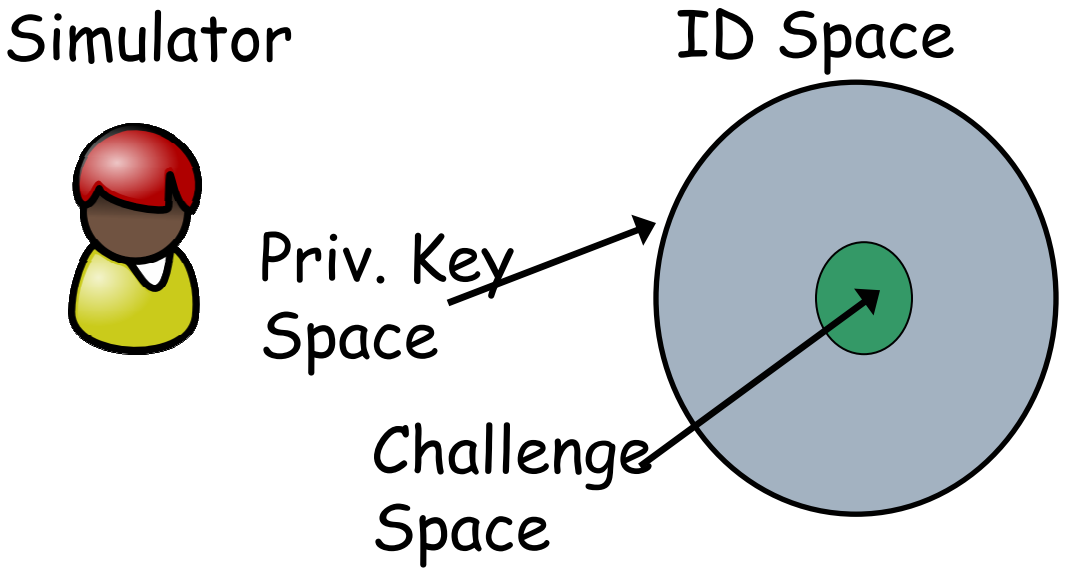


Partitioning and Aborts



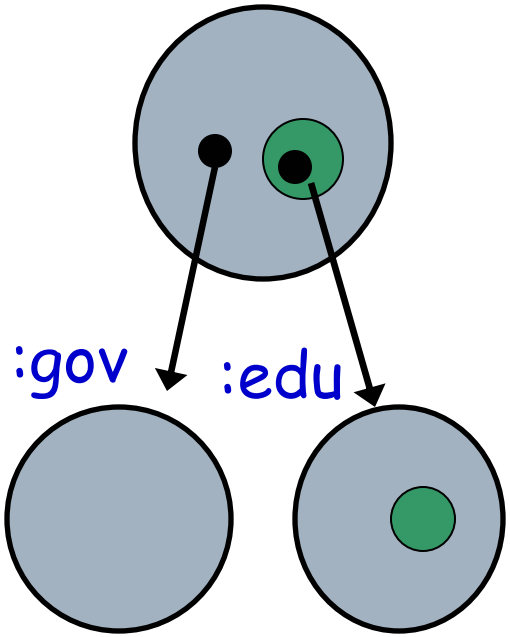
Finding a Balance

- Aborts effect security loss
- Challenge Space -> "right size"
- C.S. = 1/Q (for Q queries) => 1/Q no abort



Structure gives problems!

- Hierarchical IBE
- Q queries per HIBE level => $(1/Q)^{depth}$ loss
- Attribute-Based Encryption similar



The Gentry Approach [G06,GH09]

- Ready for both
- Shove degree Q poly into Short params =>

  Complex Assumption

$g, g^a, g^{a^2}, \ldots, g^{a^n}, , g^{a^{n+2}}, \ldots, g^{a^{2n}}, h$ Decide $e(g,h)^{a^{n+1}}$

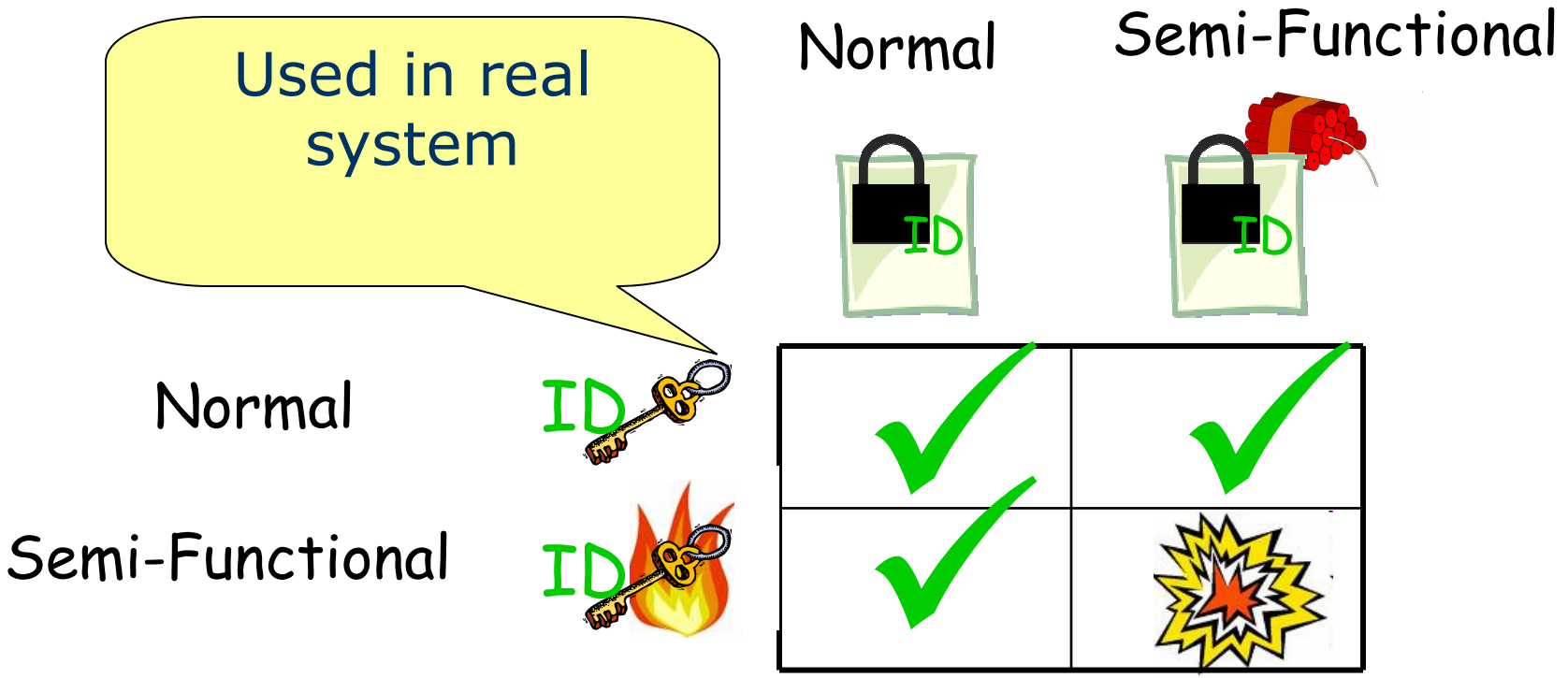
Our Results

- IBE (w/ short parameters)
- HIBE
- Broadcast Encryption
- Full Security
- Simple Assumption: Decision Linear

Given: g, u, v, g^a, u^b, Dist: v^{a+b} from R

Dual System Encryption

- 2 types of Keys & CTs



- Types are indist. (with a caveat)

Principles

- No aborts

- Change things slowly
  - Hybrid over keys form
  - Goal: Everything Semi Functional

Proof Overview – 3 Steps

1) Challenge CT → Semi Func.
2) Keys → Semi. Func. (one at a time!!)
3) Argue Security

Simulator

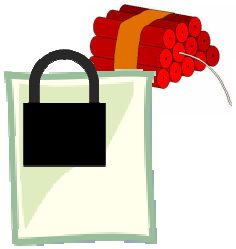
Problem: Simulator can test keys!

- Create S.F. CT for "Bob" and unknown key for "Bob"
- Decryption works iff key is normal

Simulator

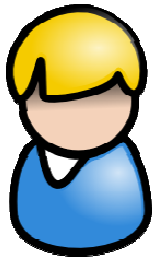
"Bob"

"Bob"



Resolution: Tweak Semantics

- Add "tags" t_c , t_k to C.T. and Key
- Decrypt iff $ID_c = ID_k$ AND $t_c \neq t_k$
- Negl. correctness error (can patch)
- SW08 revocation



ID_c , t_c

ID_K , t_K

Problem: Simulator can test keys!

- Sim. Picks $A, B \in Z_p$: $F(ID) = A \cdot ID + B$
- Challenge CT and unknown key tags → F(ID)

Simulator

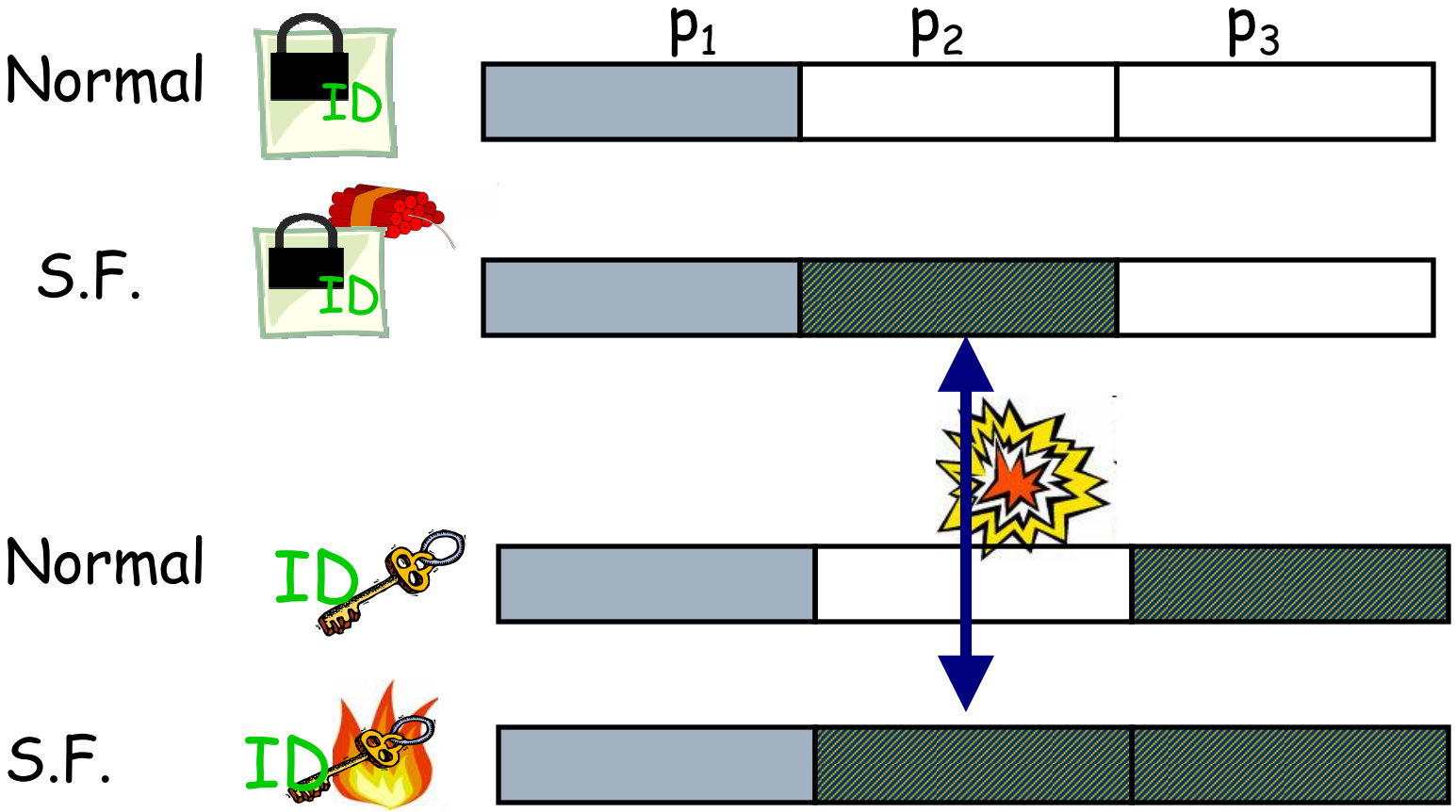
"Bob" , $t_c = x$

"Bob" , $t_k = x$

- Dec. Fails regardless of Semi Functionality!
- 2 different IDs look independent
- Hybrid → simple assumption

How it is built

- Subgroup version N= p_1 p_2 p_3



Glimpse of Subgroup Construction

Setup:

$$g, u, h, w, \in G_{p_1}, \ \ e(g,g)^{\alpha}$$

KeyGen(ID):

$$D_0 = g^{\alpha}(u^{ID}h)^{r}R_{p_4}, \ \ D_A = g^{r}, \ \ D_B = (u^{ID}hw^{tag_k})^{r}$$

Encrypt(ID,M):

$$C' = M \cdot e(g,g)^{\alpha s}, \ \ C_1 = g^{s}, \ \ C_2 = (u^{ID}hw^{tag_c})^{s}$$

- Similarities to Boneh-Boyen04
- D. Linear same concepts, more messy

Conclusions and Speculation

- Dual Encryption: Change Forms First!
  - One by one → Small Assumptions
  - HIBE, B.E. became easier
- Prediction: ABE + Functional Enc.
  - Need new techniques
- Prediction: Simple Assumptions & Full Security

Dual Interpretation

Interpretation 1:

Selective Security + Assumptions were bad

- Not ultimately necessary

Alternative:

They lead us in the right directions

- Full secure schemes "look like" selective
- Gentry06 beyond partitioning

Thank you

The Gentry Approach [G06,GH09]

- Ready for both
- Simulator 1-key per identity – always looks good
- Shove degree Q poly into Short params =>

  Complex Assumption

$g, g^a, g^{a^2}, \ldots, g^{a^n}, , g^{a^{n+2}}, \ldots, g^{a^{2n}}, h$ Decide $e(g,h)^{a^{n+1}}$