Public key encryption from Diffie-Hellman

ElGamal Security

Computational Diffie-Hellman Assumption

G: finite cyclic group of order n

Comp. DH (CDH) assumption holds in G if: $g,\ g^a,\ g^b \not\Rightarrow g^{ab}$

for all efficient algs. A:

$$\Pr\left[\ A(g, g^a, g^b) = g^{ab}\ \right] < \text{negligible}$$

where $g \leftarrow \{\text{generators of } G\}$, $a, b \leftarrow Z_n$

Hash Diffie-Hellman Assumption

G: finite cyclic group of order n , $H: G^2 \longrightarrow K$ a hash function

Def: Hash-DH (HDH) assumption holds for (G, H) if:

$$\left(g,\ g^a,\ g^b,\ H(g^b, g^{ab})\right) \approx_p \left(g,\ g^a,\ g^b,\ R\right)$$

where $g \leftarrow \{\text{generators of } G\}$, $a, b \leftarrow Z_n$, $R \leftarrow K$

H acts as an extractor: strange distribution on G^2 $\Rightarrow$ uniform on K

Suppose $K = \{0,1\}^{128}$ and

$H: G^2 \longrightarrow K$ only outputs strings in K that begin with 0

(i.e. for all x,y: msb(H(x,y))=0)

Can Hash-DH hold for (G, H) ?

- Yes, for some groups G
- No, Hash-DH is easy to break in this case
- Yes, Hash-DH is always true for such H

ElGamal is sem. secure under Hash-DH

KeyGen: $g \longleftarrow \{\text{generators of } G\}$, $a \longleftarrow Z_n$

output $pk = (g, h=g^a)$, $sk = a$

E(pk=(g,h), m) : $b \longleftarrow Z_n$

$k \longleftarrow H(g^b, h^b)$, $c \longleftarrow E_s(k, m)$

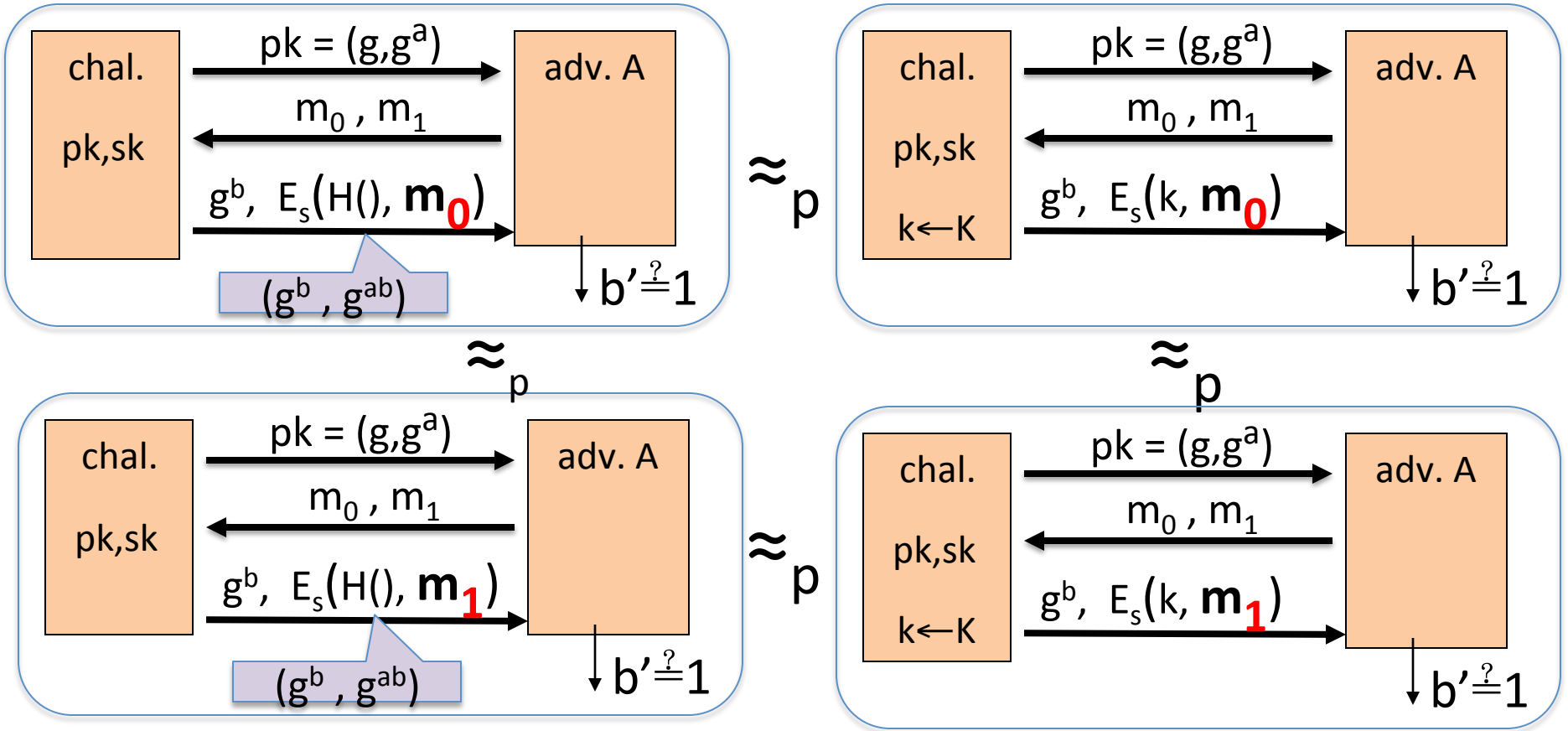
output (g^b, c)

D(sk=a, (u,c)) :

$k \longleftarrow H(u, u^a)$, $m \longleftarrow D_s(k, c)$

output m

ElGamal is sem. secure under Hash-DH

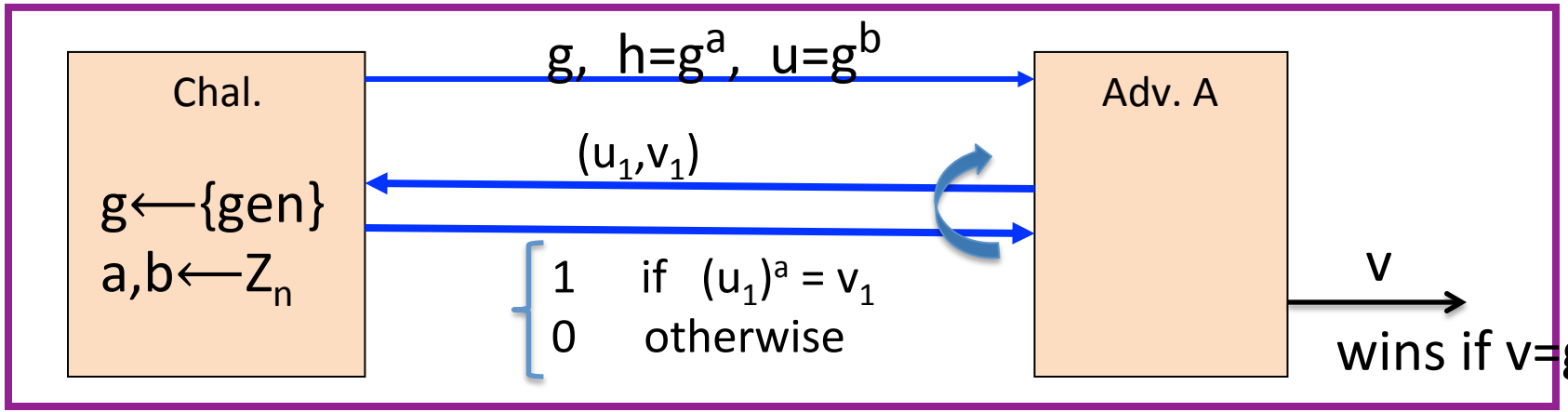


Dan Boneh

ElGamal chosen ciphertext security?

To prove chosen ciphertext security need stronger assumption

Interactive Diffie-Hellman (IDH) in group G:



IDH holds in G if: **$\forall$ efficient A: Pr[A outputs g^{ab}] < negligible**

ElGamal chosen ciphertext security?

Security Theorem:

If **IDH** holds in the group G, **(E_s, D_s)** provides auth. enc.

and **H:** $G^2 \longrightarrow K$ is a "random oracle"

then **ElGamal** is CCA^{ro} secure.

Questions: (1) can we prove CCA security based on CDH?

(2) can we prove CCA security without random oracles?

End of Segment