Public key encryption from Diffie-Hellman

ElGamal Variants With Better Security

Review: ElGamal encryption

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 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.

Can we prove CCA security based on CDH $(g, g^a, g^b \not\rightarrow g^{ab})$?

- Option 1: use group G where CDH = IDH (a.k.a bilinear group)
- Option 2: change the ElGamal system

Variants: twin ElGamal [CKS'08]

KeyGen: $g \leftarrow \{\text{generators of } G\}$, $a1, a2 \leftarrow Z_n$

output $pk = (g, h_1=g^{a1}, h_2=g^{a2})$, $sk = (a1, a2)$

E(pk=(g,h_1,h_2), m) : $b \leftarrow Z_n$

$k \leftarrow H(g^b, h_1^b, h_2^b)$

$c \leftarrow E_s(k, m)$

output (g^b, c)

D(sk=(a1,a2), (u,c)) :

$k \leftarrow$ [redacted]

$m \leftarrow D_s(k, c)$

output m

Chosen ciphertext security

Security Theorem:

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

and **H:** $G^3 \longrightarrow K$ is a "random oracle"

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

Cost: one more exponentiation during enc/dec

– Is it worth it? No one knows …

ElGamal security w/o random oracles?

Can we prove CCA security without random oracles?

- Option 1: use Hash-DH assumption in "bilinear groups"
  - Special elliptic curve with more structure [CHK'04 + BB'04]

- Option 2: use Decision-DH assumption in any group [CS'98]

Further Reading

- The Decision Diffie-Hellman problem. D. Boneh, ANTS 3, 1998
- Universal hash proofs and a paradigm for chosen ciphertext secure public key encryption. R. Cramer and V. Shoup, Eurocrypt 2002
- Chosen-ciphertext security from Identity-Based Encryption.
  D. Boneh, R. Canetti, S. Halevi, and J. Katz, SICOMP 2007
- The Twin Diffie-Hellman problem and applications.
  D. Cash, E. Kiltz, V. Shoup, Eurocrypt 2008
- Efficient chosen-ciphertext security via extractable hash proofs.
  H. Wee, Crypto 2010