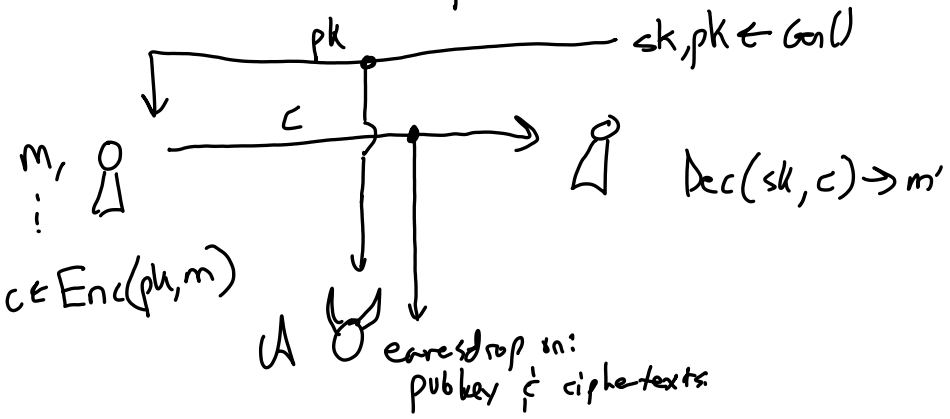
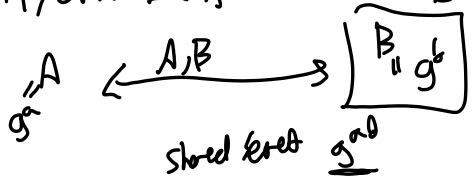
Public Key Encryption

Friday, October 29, 2021 3:57 PM

Public Key Encryption



- Hybrid Encryption ← overall publickey



- DDH ⇒ g^{ab} is effectively random, even after seeing g^a, g^b.

↓ Use g^{ab} as a seed for a PRF used in symmetric encryption.

even simpler... one time pad, fresh diffie hellman each time.

- Also ElGamal encryption called —

Gen():
$b \xleftarrow{\$} \mathbb{Z}_p$
$pk, sk = g^b, b$ — $m \in G$

Enc(pk = B, m):
$a \xleftarrow{\$} \mathbb{Z}_p$ $A := g^a$
sess = B^a
* Symenc(sess, m) → c
more specifically, OTP in group,

$c = (A, m \cdot B^a)$

A: Alices' part of DH exchange.
$m \cdot B^a$: one time pad w/ shared secret.

$Dec(sk=b, (A, c'))$:

return c' / A^b ✓

- Homomorphic Encryption.
  - $Enc(m_1) \times Enc(m_2)$

  ≈ $Enc(m_1 \cdot m_2)$

Can there be sym enc homomorphic?

Consider m_1, m_2 ↔

$c_1 = (m_1 \cdot B^{a_1}, g^{a_1})$

$c_2 = (m_2 \cdot B^{a_2}, g^{a_2})$

$c_1 \times c_2 = (m_1 m_2 B^{a_1+a_2}, g^{a_1+a_2})$

Dec: $(g^{a_1+a_2})^{b^{-1}} \cdot m_1 m_2 B^{(a_1+a_2)}$

$= g^{(a_1+a_2)b^{-1}} \cdot m_1 m_2 g^{b(a_1+a_2)}$

$= m_1 m_2$ $\quad m_1 m_2 \cdots m_n$

Why is this secure?

Main step:

- A's view in real world:

$(g^b, g^a, g^{ab} \cdot M)$

g^b: pk; g^a: first part of c; $g^{ab} \cdot M$: second

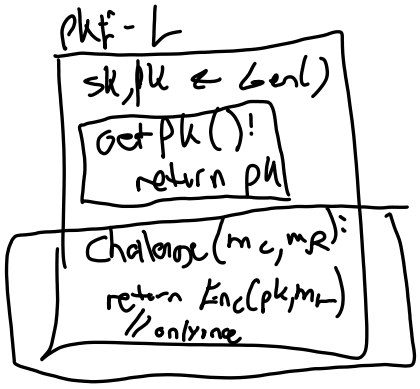
- Replace $(g^b, g^a, g^r \cdot M)$ for $r \xleftarrow{\$} \mathbb{Z}_p$ by DDH

$\approx (g^b, g^a, g^r)$ regardless of m, $g^{ab} \cdot m$ is a uniform sampled group element

---

One time security $\Rightarrow$ IND-CPA

Pub key Game:

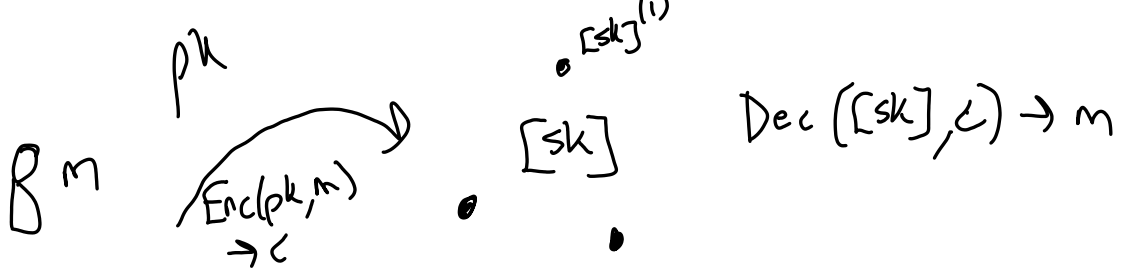


$\approx_s$ PKE-R

Why this def'n doesn't change if A can ask for more encryptions?

A can run Enc(pk, ·) directly.

Threshold Enc and E-voting



Ex. 3-of-3.

Choose $b_1, b_2, b_3 \xleftarrow{\$} \mathbb{Z}_p$

$B_1 = g^{b_1}$

$B_2 = g^{b_2}$ $B_3 = g^{b_3}$

$b = b_1 + b_2 + b_3$

$pk = B = g^{b_1+b_2+b_3} = B_1 \cdot B_2 \cdot B_3$

$Dec((A, c'), b_i)$:

A^{b_i} ⟶ partial decryption.

$finalDec(A_1, A_2, A_3, c') \rightarrow$

$c' / A^{b_1+b_2+b_3}$ $\quad c'/(A_1 A_2 A_3)$

$A^{b_1} \cdot A^{b_2} \cdot A^{b_3}$

E-Voting.

$m_1 \in \{g^0, g^1\}$ $\quad c_1$

m_2 $\quad c_2$

m_3 $\quad c_3$

Tally Servers

[SK]

(c_1, c_2, c_3)

Bulletin

- c_1
- c_2
- c_3

Dec $c_1 \cdot c_2 \cdot c_3$

- Tally servers run

$Dec([SK], c_1 * c_2 \cdot c_3) \rightarrow$ output $\in \{g^0, \ldots g^3\}$

Check which one to recover exponent.

- IF ANY of the Servers are honest, we only learn Total sum of votes.

$C = m \cdot g^{(b_1+b_2+b_3)a}, g^a$