Topics in Cryptography

Mohammad Mahmoody

26 Jan 2014

Homomorphic Enc. (~~2~~ 3)

Last time

- Diffie Hellman Key Exchange
- DDH assumption
- ElGamal: Public key based on DDH
- ElGamal is multiplicatively homomorphic

Today

- Formal Def of fully homomorphic enc
- FHE vs CCA security
- FHE: from private-key to public-key
- Intro to “learning with error” problem

Formal def. of FHE

- $KeyGen(1^n) \rightarrow (ek, dk)$
- $Dec_{dk}(Enc_{ek}(m)) = m$
- Single message Eval: for any "given function" f it holds that:

$$Dec_{dk}(Eval_{ek}(f, Enc_{ek}(m)) = f(m)$$

- Semantic security: for any poly-time adversary Adv and any two messages m_0, m_1 it holds that:

$$\Pr[Adv(ek, Enc_{ek}(m_0)) = 1] - \Pr[Adv(ek, Enc_{ek}(m_1)) = 1] \leq neg(n)$$

$m \in \mathcal{M}$

$\leq \frac{1}{poly(n)}$

any poly(n)

Multi-message Eval: $f: \mathcal{M}^k \rightarrow \mathcal{M}$

- For any "given function" f and $c_1, \ldots, c_k$ where $c_i = Enc_{ek}(m_i)$:

$$Dec_{dk}(Eval_{ek}(f, c_1, \ldots, c_k) = f(\underbrace{c_1}_{m_1}, \ldots, \underbrace{c_k}_{m_k})$$

- ~~Multi~~ Two-message Eval implies single message Eval:

Let $f: \mathcal{M} \rightarrow \mathcal{M}$ be a given function.

→ let $f': \mathcal{M} \times \mathcal{M} \rightarrow \mathcal{M}$ be that $f'(x, x') = f(x)$

then computing $Enc(f(x))$ is the same as computing $Enc(f(x, x'))$ for any arbitrary x'.

Trivial FHE?

$Dec(Eval(f, Enc(x))) = Dec(Enc(f(x))) = f(x)$

Stat. Versions $(pk, Eval(f, Enc(x))) \equiv (pk, Enc(f(x)))$

- How about $Eval(c, f) = (c, f)$ and change decryption as:

$$Dec(c, f_1, f_2, \dots, f_k) = f_k(\dots f_1(Dec(c)) \dots)$$

- Compactness requirement:

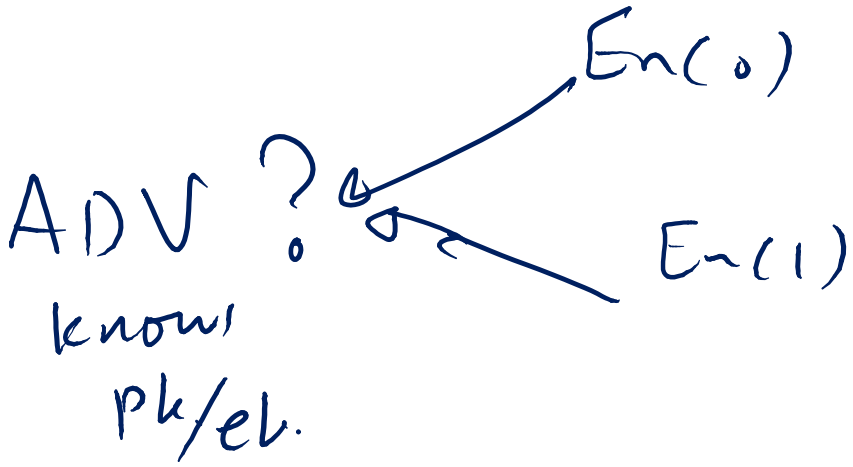
$|Eval(\dots)| \leq poly(n)$ (Eval(·))

Final definition

- $KeyGen(1^n) \rightarrow (ek, dk)$
- $Dec_{dk}(Enc_{ek}(m) = m$
- For any "given function" f and $c_1, \ldots, c_k$ where $c_i = Enc_{ek}(m_i)$:
  $$Dec_{dk}(Eval_{ek}(f, c_1, \ldots, c_k) = f(c_1, \ldots, c_k)$$
- Compactness: $|Eval_{ek}(f, c_1, \ldots, c_k)| \leq poly(n)$ indep. of k
- Semantic security: for any poly-time adversary Adv and any two messages m_0, m_1 it holds that:
  $\Pr[Adv(ek, Enc_{ek}(m_0) = 1] - \Pr[Adv(ek, Enc_{ek}(m_0) = 1] \leq neg(n)$

No CCA security

Recall: CPA or Semantic Sec:



Why is FHE NOT CCA secure?

ADV asks Dec of $y = Enc(x \oplus 1)$ using Eval(...)

Same game.

+

ADV can ask anything other than y to be decrypted

From **private-key** to public key homomorphic encryption.

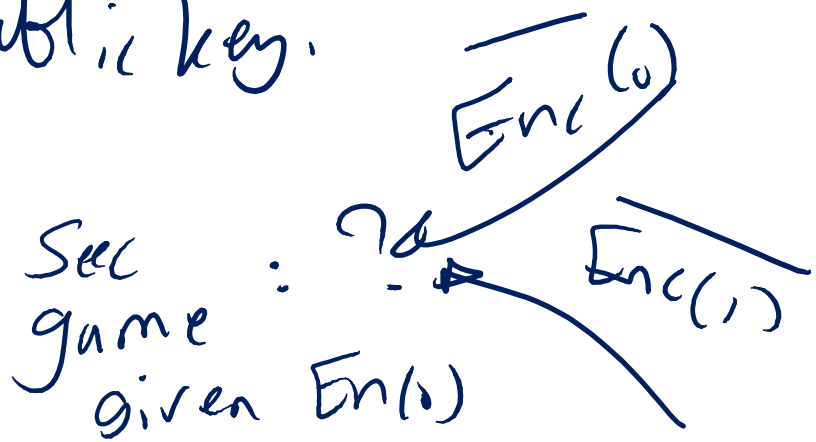
2013 Ron Rothblum.

Given $(Enc, Dec, Eval)$ which is private key

Want $(\overline{Enc}, \overline{Dec}, \overline{Eval}, \overline{KeyGen})$ in public key setting.

1st Try: Publish $\overline{Enc(\alpha)}$ as public key.

$\overline{Enc(b)} := Eval(f_{b+x}, \alpha)$



Theorem [Rom Roth] : assuming CPA-secure private-key Enc.

$\Rightarrow$ the following is CPA-secure public key Enc.

CPA: ADV can request Enc(·) of his choice to dist. between Enc(0) / Enc(1)

public key: $\text{Enc}(\$), \text{Enc}(\$) \cdots \text{Enc}(\$), r, s(b_1 - b_n)$

(b_1, b_2, b_n)

given b: choose $S \in_R \{0,1\}^k$ so that $\langle S, r \rangle = \bigoplus_{S_i=1} b_i$

use Eval and get enc of XOR of $\{b_i\}_{S_i=1}$

THM: if only m bits of S is revealed

left-over hash lemma:

if we are given $r (= b_1 \cdots b_n)$ chosen at random

and given only m bits of $\inf$ about $s = (s_1 \cdots s_k)$ which is also rand.

the dist of $\langle s, r \rangle$ remains a random bit.