Topics in Cryptography

Mohammad Mahmoody

21 Jan 2014

Homomorphic Enc. (2)

Last Time

Computation

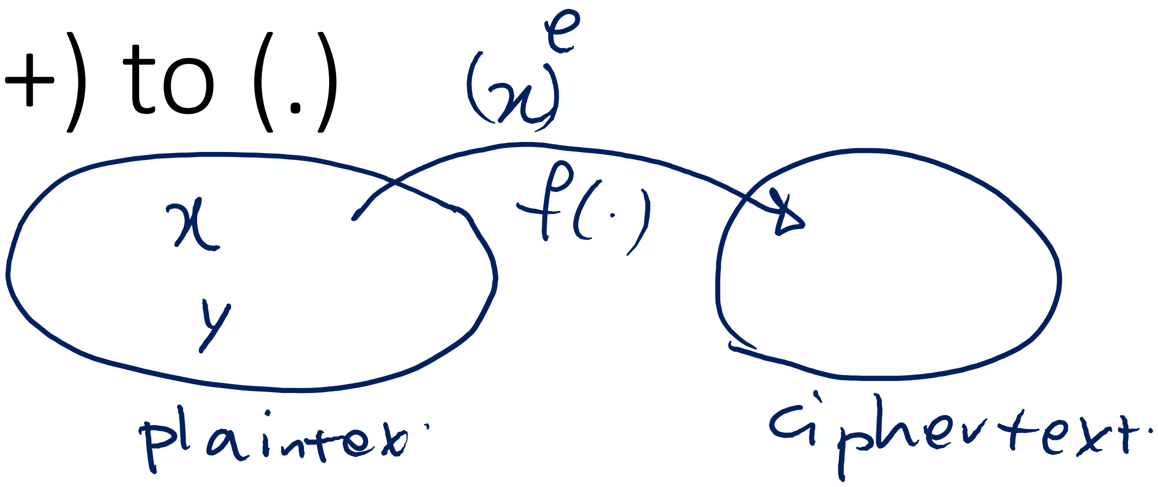
- Homomorphic Enc : ~~encryption~~ over (publically encrypted) data
- Some basic applications
- Why called Homomorphic (term coming from group theory)
- A construction based on code obfuscation + any public-key encryption
- (Basic deterministic) RSA encryption is already (weakly) homomorphic

Today

- Another (weakly) homomorphic encryption:
- It is based on “hardness” of “discrete logarithm”
- It is also a secure encryption (without homomorphism)

Exponentiation:
Homomorphism from (+) to (.)

How RSA is homomorphic:



$f(x.y) = f(x).f(y)$

also multiplication.

homomorphic eval.

---

how about $f(x) = g^x$

$f(x+y) = f(x).f(y)$

g^{x+y} $\quad$ $g^x . g^y$

get enc. from it?

Hom. enc from it?

Diffie and Hellman's Breakthrough

first "secure" key Agreement protocol:

public channel

Alice $\rightleftarrows$ Bob

a Eve b

key   key

hidden in eyes of Eve.

1st Try: A   B.b

$x \xrightarrow{f(x)} $ y

$\xleftarrow{f(y)}$

hom. $f(x), f(y) \to \underbrace{f(x \circ y)}_{\text{key.}}$

2nd Try: given $x, f(y) \xrightarrow{\text{efficiency}} f(x \cdot y)$ given x, g^y

$f(x) := g^x$ $\longrightarrow g^{x \cdot y} := (g^y)^x$

Z_p^*: The group to implement DH:

prime number

set: $\{1, 2 \ldots, p-1\} = X$ $\quad x \odot y = (x \cdot y) \bmod p$

integer mult.

$\forall x.\ \exists y.\ \ x \cdot y = 1$

use Euclid's Al's.

proof: Lemma: $\forall a, b\ \exists\ \alpha, \beta\ \ \ \alpha \cdot a + \beta \cdot b = \gcd(a, b)$

$\forall x, p\ \exists\ x', p'$ such th. $x \cdot x' + p \cdot p' = 1 \rightarrow x x' = 1$

x' (mod p)

$\Rightarrow (X, \odot)$ form Z_p^*

Security of DH :
the hardness assumption behind DH

ideal: prove if any ADV breaks DH $\Longrightarrow$ we can solve discrete log. in poly(n) time

real: ADV gets to see: (g^x, g^y)
wants to know $g^{x \cdot y}$

these two rand. var. indistinguishable

$(g^x, g^y, g^{x \cdot y})$

$(g^x, g^x, \cancel{g^z})$ g^z

if g is a "generator" for G

→ DDH assump. no poly-Time ADV can diff. between above two.

ElGamal: Public-Key Encryption from DDH

Alice $\xrightarrow{\text{public key:}}$ Bob

$= (G, g, \underbrace{g^x}_{=h})$

to encrypt m: 1st Try. (g^m) Alice can send $g^{x \cdot m}$ securely...

2nd Try: $\begin{pmatrix} g^y \\ , \\ g^{x \cdot y} \cdot m \end{pmatrix}$ $g^{x \cdot y}$ → "private key"

Dec. $(\underbrace{g^y}_{h'}, \underbrace{g^{x \cdot y} \cdot m}_{\ell})$

$h' \to (h')^x = g^{x \cdot y}$

Compute $(g^{x \cdot y})^{-1} \xrightarrow{\text{mult. } \ell} m$

ElGamal is (weakly) Homomorphic

Public key: $(\mathbb{G}, g, g^x)$ ← fixed

Enc(m) : $\left(g^r, \left(g^{r \cdot x}\right) \cdot m\right)$

$\underbrace{\left(\text{Enc}(m_1) \quad \text{Enc}(m_2)\right)}_{\text{given,}} \xrightarrow[?]{\text{Eval.}} \text{Enc}(m_1 \times m_2)$

$(g^{r_1}, g^{r_1 \cdot x} \cdot m_1)$

$(g^{r_2}, g^{r_2 \cdot x} \cdot m_2)$

$\left(g^{r_2 \cdot x} \cdot g^{r_1 \cdot x} \cdot m_1 m_2\right) \longrightarrow \left(g^{r'}, g^{r' \cdot x} \cdot m_1 m_2\right)$

$g^{(r_1+r_2)x} = g^{r_1 \cdot x} \times g^{r_2 x}$

Next Time:

- Gentry and friends' ideas to get **fully** homomorphic enc.

$\boxed{2009}$