Homomorphic encryption $\longleftrightarrow$ Isomorphic encryption

m_1, m_2 – messages; $Enc(PrK, m) = c$

$Enc(PrK, m_1) = c_1$
$Enc(PrK, m_2) = c_2$

$Enc(PrK, m_1 * m_2) = c_1 * c_2$ — multiplicative homom. encr.

$Enc(PrK, m_1 + m_2) = c_1 * c_2$ — additively-mult. homom. encr.

Paillier Encryption-Decryption

$N = p \cdot q$; $N^2 = p^2 \cdot q^2$; E.g. $p = 3$; $q = 5$; $N = 15$.

$\mathcal{I}_N = \{0, 1, 2, \ldots, N-1\}$; $+ \bmod N$; $* \bmod N$ $\quad \mathcal{I}_N^* = \{z \mid \gcd(z, N) = 1\}$; $* \bmod N$

$\mathcal{I}_{N^2}^* = \{w \mid \gcd(w, N^2) = 1\}$; $\circledast \bmod N^2$

$f : \mathcal{I}_N \times \mathcal{I}_N^* \longrightarrow \mathcal{I}_{N^2}^*$;

$\mathcal{I}_{15} = \{0, 1, 2, \ldots, 14\}$; $+ \bmod 15$; $* \bmod 15$ $\quad \mathcal{I}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$;

The number of elements in $\mathcal{I}_N^*$ defines Euler Totient function $\phi(N)$

$|\mathcal{I}_{15}^*| = 8$; $\phi(15) = \phi(3 \cdot 5) = (3-1) \cdot (5-1) = 2 \cdot 4 = 8 = \phi$

$\phi(N) = \phi(p \cdot q) = (p-1) \cdot (q-1) = \phi$ ⟹ to find $PrK = \phi$ one must find p, q.

To find p, q one must factorize $N = p \cdot q$.

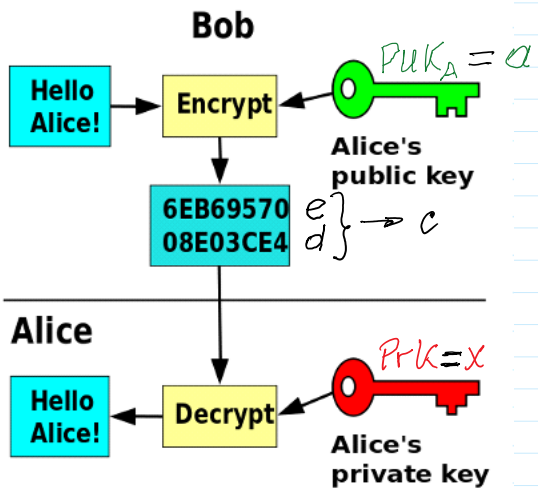
$m \in \mathcal{I}_N = \{0, 1, 2, \ldots, N-1\}$; $\mathcal{I}_N = \{0, 1, 2, \ldots, N-1\}$

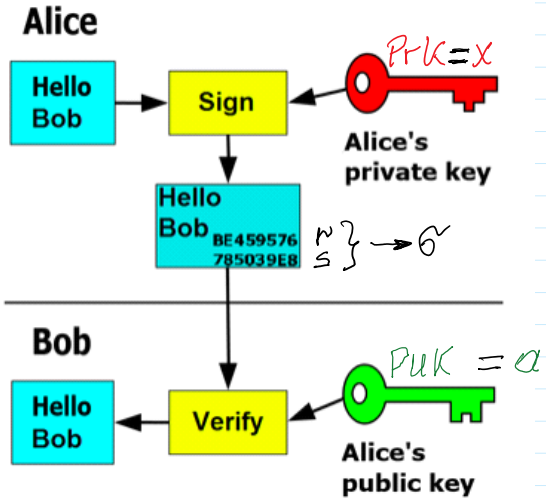
$r \in \mathcal{I}_N^* = \{z ; \gcd(z, N) = 1\}$; $\mathcal{I}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$

>> $\gcd(4, 15) = 1$

>> $\gcd(9, 15) = 3 \neq 1$.

>> $\gcd(7, 15) = 1$





Paillier Encryption-Decryption $PrK = \phi$; $PuK = N$.

To encrypt message m (probabilistically) the random number r must be generated: (m, r)

$Enc(N, r, m) = c$

$(m, r) \in \mathbb{Z}_N \times \mathbb{Z}_N^*$;

$c \in \mathbb{Z}_{N^2}^* = \{z ;\ gcd(z, N^2) = 1\}$;

$Dec(\phi, c) = m \in \mathbb{Z}_N$.

$f : \mathbb{Z}_N \times \mathbb{Z}_N^* \leftrightarrow \mathbb{Z}_{N^2}^*$; $f(m, r) = c \in \mathbb{Z}_{N^2}^*$; $Enc(PuK, m, r) = c$

$f^{-1} : \mathbb{Z}_{N^2}^* \leftrightarrow \mathbb{Z}_N \times \mathbb{Z}_N^*$; $f^{-1}(c) = (m, r)$; $Dec(PrK, c) = m$

$\phi(N) = \phi(p \cdot q) = \phi(p) \cdot \phi(q) = (p-1) \cdot (q-1) = \phi = PrK_A$

$\phi(N^2) = p \cdot (p-1) \cdot q \cdot (q-1) = p \cdot q \cdot (p-1) \cdot (q-1)$

$= |\mathbb{Z}_N| \cdot |\mathbb{Z}_N^*| = |\mathbb{Z}_N \times \mathbb{Z}_N^*| = |\mathbb{Z}_{N^2}^*|$.

PuK = N --> **PrK = fy =** $\phi = (p-1) \cdot (q-1)$ $N = P \cdot q$; When $N \sim 2^{2048} \Rightarrow$ to find P, q is infeasible → RSA problem.

Security:

When $PuK = N$ it is infeasible to find $\phi = (p-1)\cdot(q-1) \Rightarrow$

$\Rightarrow$ RSA problem is infeasible $\Leftrightarrow$ factorization problem.

>> factor(15) $\rightarrow$ ans 3, 5

Factorization problem is infeasible if N is sufficiently large.

$N \sim 2^{2048} \rightarrow |N| = 2048$ bits.

$f(m, r) = c \in \mathcal{I}_{N^2}^*$ Encryption

$f^{-1}(c) = (m, r) \in \mathcal{I}_N \times \mathcal{I}_N^*$ Decryption

CONSTRUCTION 11.32

Let **GenModulus** be a polynomial-time algorithm that, on input 1^n, outputs (N, p, q) where $N = pq$ and p and q are n-bit primes (except with probability negligible in n). Define a public-key encryption scheme as follows:

- **Gen:** on input 1^n run **GenModulus**(1^n) to obtain (N, p, q). The public key is N and the private key is $\langle N, \phi(N)\rangle = \langle N, \phi\rangle$.
- **Enc:** on input a public key N and a message $m \in \mathbb{Z}_N$, choose a random $r \leftarrow \mathbb{Z}_N^*$ and output the ciphertext

$$c := [(1+N)^m \cdot r^N \bmod N^2].$$

- **Dec:** on input a private key $\langle N, \phi(N)\rangle$ and a ciphertext c, compute

$$m := \left[\frac{[c^{\phi(N)} \bmod N^2] - 1}{N} \cdot \phi(N)^{-1} \bmod N\right].$$

The Paillier encryption scheme.

A: $PrK_A = x = \phi$. $PuK_A = a = N$. B: $PuK_A = a = N$; m – message to be encrypted in dec. form: $m < N = pq$.

$Dec(\phi, c) = m$

$r \leftarrow randi(\mathcal{I}_N^*)$

$\leftarrow c$ $Enc(N, r, m) = c$

Probabilistic encryption:

Let B is encrypting message m (plaintext) 2 times,

1) $r_1 \leftarrow rand(\mathcal{I}_N^*)$; $c_1 = (1+N)^m r_1^N \bmod N^2$

2) $r_2 \leftarrow rand(\mathcal{I}_N^*)$; $c_2 = (1+N)^m r_2^N \bmod N^2$

$c_1 \neq c_2$ since $r_1 \neq r_2$.

Homomorphic property:

Paillier encryption is additively-multiplicative homomorphism.

Let m_1, m_2 – messages to be encrypted by $\mathcal{B}$.

r_1, r_2 – random numbers for encryption.

$$\left.\begin{aligned} Enc(N, r_1, m_1) &= c_1 \\ Enc(N, r_2, m_2) &= c_2 \end{aligned}\right\} \quad Enc(N, \underset{\text{mod } N}{r_1 \cdot r_2}, \underset{\text{mod } N}{m_1 + m_2}) = c = \underset{\text{mod } N^2}{c_1 \cdot c_2}$$

$$\left.\begin{aligned} c_1 &= (1+N)^{m_1} \cdot r_1^N \bmod N^2 \\ c_2 &= (1+N)^{m_2} \cdot r_2^N \bmod N^2 \end{aligned}\right\} \quad c = c_1 \cdot c_2 \bmod N^2$$

$$c_1 \cdot c_2 \bmod N^2 = (1+N)^{m_1} \cdot r_1^N \cdot (1+N)^{m_2} \cdot r_2^N \bmod N^2 =$$

$$= (1+N)^{m_1+m_2} \cdot (r_1 \cdot r_2)^N \bmod N^2 =$$

$$= Enc(N, \underbrace{r_1 \cdot r_2}_{r}, m_1 + m_2) = c$$

$$Dec(\phi, c) = m_1 + m_2$$

Shortcoming: Paillier encryption requires computations with large numbers taken mod N^2: $|N^2| = 4096$ bits.

We use toy example $|N^2| = 28 \rightarrow |N| = 14 \rightarrow |p| = |q| = 7$ bits

eVoting: Can1 := m_1 ; Can2 := m_2 ; Can3 := m_3

Voters: PuK = N.

Election Commetee – EC

PuK = N; PrK = ϕ.

V1: $v_1 \in \{m_1, m_2, m_3\}$

$Enc(N, r_1, v_1) = c_1$ ——c_1——→

V2: $v_2 \in \{m_1, m_2, m_3\}$

$Enc(N, r_2, v_2) = c_2$ ——c_2——→

– – – – – – –

Vk: $v_k \in \{m_1, m_2, m_3\}$

$Enc(N, r_k, v_k) = c_k$ ——c_k——→ Votes Registration Authority

$c_1 \cdot c_2 \cdot \ldots \cdot c_k = c \bmod N^2$

$c = Enc(N, r, v)$

$r = r_1 \cdot r_2 \cdot \ldots \cdot r_k \bmod N$

$$v = (v_1 + v_2 + \ldots + v_k) \bmod N$$

EC: $Dec(\phi, c) = v = (v_1 + v_2 + \ldots + \quad) \bmod N$

since $v_1 + v_2 + \ldots + v_k < N$: $12 \bmod 15 = 12$ & $27 \bmod 15 = 12$.

$$v = v_1 + v_2 + \ldots + v_k$$

Example. $N = 15$; $v = 12$ & $m_1 = 2$; $m_2 = 3$; $m_3 = 4$.

$12 = 2 \cdot 2 \cdot 3$ (can1, can2, can3)

$12 = 3 \cdot 4$ (can2, can3)

Super increasing set: $\{e_1, e_2, e_3, e_4, \ldots\}$ Eg. $= \{1, 2, 2^2, 2^3, 2^4, \ldots\}$

$e_1 < e_2$ & $e_1 + e_2 < e_3$ & $e_1 + e_2 + e_3 < e_4$ & ...

$1 < 2$ & $1 + 2 < 4$ & $1 + 2 + 4 < 8$ & ...