Paillier's cryptosystem

Addtive homomorphic encryption

Tanja Lange

Eindhoven University of Technology

2MMC10 – Cryptology

System setup

KeyGen:

1. Pick primes $p, q; p \neq q$.
2. Compute $n = p \cdot q$, $\varphi(n) = (p-1)(q-1)$, and $\mu \equiv \varphi(n)^{-1} \bmod n$.
3. Put $g = n + 1$ and
4. Output public key (n, g), private key $(n, \varphi(n), \mu)$.

System setup

KeyGen:

1. Pick primes $p, q; p \neq q$.
2. Compute $n = p \cdot q$, $\varphi(n) = (p-1)(q-1)$, and $\mu \equiv \varphi(n)^{-1} \bmod n$.
3. Put $g = n + 1$ and
4. Output public key (n, g), private key $(n, \varphi(n), \mu)$.

Enc message $0 \leq m < n, \gcd(m, n) = 1$:

1. Pick a random $1 \leq r < n$ with $\gcd(r, n) = 1$.
2. Compute and output $c \equiv g^m \cdot r^n \bmod n^2$.

   Note the computation is done modulo n^2, not modulo n.

System setup

KeyGen:

1. Pick primes $p, q; p \neq q$.
2. Compute $n = p \cdot q$, $\varphi(n) = (p-1)(q-1)$, and $\mu \equiv \varphi(n)^{-1} \bmod n$.
3. Put $g = n + 1$ and
4. Output public key (n, g), private key $(n, \varphi(n), \mu)$.

Enc message $0 \leq m < n, \gcd(m, n) = 1$:

1. Pick a random $1 \leq r < n$ with $\gcd(r, n) = 1$.
2. Compute and output $c \equiv g^m \cdot r^n \bmod n^2$.

   Note the computation is done modulo n^2, not modulo n.

Dec ciphertext $0 \leq c < n^2$:

1. Compute $d \equiv c^{\varphi(n)} \bmod n^2$.
2. Consider d as an integer.

   Note that $d - 1$ is a multiple of n (see below).
3. Compute $e = (d-1)/n$.
4. Compute and output $m' \equiv e\mu \bmod n$.

Enc is additively homomorphic

Enc message $0 \leq m < n, \gcd(m, n) = 1$:

1. Pick a random $1 \leq r < n$ with $\gcd(r, n) = 1$.
2. Compute and output $c \equiv g^m \cdot r^n \bmod n^2$.

   Note the computation is done modulo n^2, not modulo n.

Let $c_1 \equiv g^{m_1} \cdot {r_1}^n \bmod n^2$, $c_2 \equiv g^{m_2} \cdot {r_2}^n \bmod n^2$.

Enc is additively homomorphic

Enc message $0 \leq m < n, \gcd(m, n) = 1$:

1. Pick a random $1 \leq r < n$ with $\gcd(r, n) = 1$.
2. Compute and output $c \equiv g^m \cdot r^n \bmod n^2$.

   Note the computation is done modulo n^2, not modulo n.

Let $c_1 \equiv g^{m_1} \cdot {r_1}^n \bmod n^2$, $c_2 \equiv g^{m_2} \cdot {r_2}^n \bmod n^2$.

Then

$$c_1 \cdot c_2 \equiv g^{m_1} \cdot g^{m_2} \cdot {r_1}^n \cdot {r_2}^n$$

Enc is additively homomorphic

Enc message $0 \leq m < n, \gcd(m, n) = 1$:

1. Pick a random $1 \leq r < n$ with $\gcd(r, n) = 1$.
2. Compute and output $c \equiv g^m \cdot r^n \bmod n^2$.

   Note the computation is done modulo n^2, not modulo n.

Let $c_1 \equiv g^{m_1} \cdot {r_1}^n \bmod n^2$, $c_2 \equiv g^{m_2} \cdot {r_2}^n \bmod n^2$.

Then

$$c_1 \cdot c_2 \equiv g^{m_1} \cdot g^{m_2} \cdot {r_1}^n \cdot {r_2}^n \equiv g^{m_1+m_2} \cdot (r_1 r_2)^n \bmod n^2$$

is the encryption of $m_1 + m_2$ under randomness $r = r_1 r_2$.

Decryption recovers m from $c \equiv g^m \cdot r^n \bmod n^2$

Dec ciphertext $0 \leq c < n^2$:

1. Compute $d \equiv c^{\varphi(n)} \bmod n^2$.
2. Consider d as an integer.
3. Compute $e = (d-1)/n$.
4. Compute and output $m' \equiv e\mu \bmod n$.

Decryption recovers m from $c \equiv g^m \cdot r^n \bmod n^2$

Dec ciphertext $0 \leq c < n^2$:

1. Compute $d \equiv c^{\varphi(n)} \bmod n^2$.
2. Consider d as an integer.
3. Compute $e = (d-1)/n$.
4. Compute and output $m' \equiv e\mu \bmod n$.

Note first that $\varphi(n^2) = pq(p-1)(q-1) = n\varphi(n)$
and $g \in \mathbf{Z}^*/n^2$ has order n:

Decryption recovers m from $c \equiv g^m \cdot r^n \bmod n^2$

Dec ciphertext $0 \leq c < n^2$:

1. Compute $d \equiv c^{\varphi(n)} \bmod n^2$.
2. Consider d as an integer.
3. Compute $e = (d-1)/n$.
4. Compute and output $m' \equiv e\mu \bmod n$.

Note first that $\varphi(n^2) = pq(p-1)(q-1) = n\varphi(n)$
and $g \in \mathbf{Z}^*/n^2$ has order n:
$g^n = (n+1)^n = 1 + n \cdot n + \cdots \equiv 1 \bmod n^2$ while
$g^p = (n+1)^p = 1 + pn + \binom{p}{2} n^2 + \cdots \equiv 1 + pn \neq 1 \bmod n^2$

Decryption recovers m from $c \equiv g^m \cdot r^n \bmod n^2$

Dec ciphertext $0 \leq c < n^2$:

1. Compute $d \equiv c^{\varphi(n)} \bmod n^2$.
2. Consider d as an integer.
3. Compute $e = (d-1)/n$.
4. Compute and output $m' \equiv e\mu \bmod n$.

Note first that $\varphi(n^2) = pq(p-1)(q-1) = n\varphi(n)$
and $g \in \mathbf{Z}^*/n^2$ has order n:
$g^n = (n+1)^n = 1 + n \cdot n + \cdots \equiv 1 \bmod n^2$ while
$g^p = (n+1)^p = 1 + pn + \binom{p}{2} n^2 + \cdots \equiv 1 + pn \neq 1 \bmod n^2$

$d \equiv c^{\varphi(n)} \equiv (g^m \cdot r^n)^{\varphi(n)} \equiv g^{m\varphi(n)} \cdot r^{n\varphi(n)} \equiv (n+1)^{m\varphi(n)} \equiv$
$1 + m\varphi(n)n + \ldots n^2 + \cdots \equiv 1 + m\varphi(n)n \bmod n^2$.

Decryption recovers m from $c \equiv g^m \cdot r^n \bmod n^2$

Dec ciphertext $0 \leq c < n^2$:

1. Compute $d \equiv c^{\varphi(n)} \bmod n^2$.
2. Consider d as an integer.
3. Compute $e = (d-1)/n$.
4. Compute and output $m' \equiv e\mu \bmod n$.

Note first that $\varphi(n^2) = pq(p-1)(q-1) = n\varphi(n)$
and $g \in \mathbf{Z}^*/n^2$ has order n:
$g^n = (n+1)^n = 1 + n \cdot n + \cdots \equiv 1 \bmod n^2$ while
$g^p = (n+1)^p = 1 + pn + \binom{p}{2} n^2 + \cdots \equiv 1 + pn \neq 1 \bmod n^2$

$d \equiv c^{\varphi(n)} \equiv (g^m \cdot r^n)^{\varphi(n)} \equiv g^{m\varphi(n)} \cdot r^{n\varphi(n)} \equiv (n+1)^{m\varphi(n)} \equiv$
$1 + m\varphi(n)n + \ldots n^2 + \cdots \equiv 1 + m\varphi(n)n \bmod n^2$.

So $d-1$ is indeed a multiple of n, so $e = (d-1)/n$ is an integer satisfying $e \equiv m\varphi(n) \bmod n$. Remember $\mu \equiv \varphi(n)^{-1} \bmod n$.

Then $m' \equiv e\mu \equiv m\varphi(n)\varphi(n)^{-1} \equiv m \bmod n$