Linearly Homomorphic Encryption from DDH

Guilhem Castagnos

Institut de Mathématiques de Bordeaux

Lfant Seminar Bordeaux — mardi 10 mars 2015

Joint work with Fabien Laguillaumie

Linearly Homomorphic Encryption ?

- Public key encryption scheme with the following properties:
- Suppose that the set of plaintexts $\mathscr{M}$ is a ring
- $c \leftarrow \mathsf{Encrypt}(pk, m)$, $c' \leftarrow \mathsf{Encrypt}(pk, m')$
- $c_1 \leftarrow \mathsf{EvalSum}(pk, c, c')$ s.t.

$$\mathsf{Decrypt}(sk, c_1) = m + m'$$

- For $\alpha \in \mathscr{M}$, $c_2 \leftarrow \mathsf{EvalScal}(pk, c, \alpha)$ s.t.

$$\mathsf{Decrypt}(sk, c_2) = \alpha m$$

Example: Goldwasser Micali (84)

- $\mathscr{M} = \mathbf{Z}/2\mathbf{Z}$,
- $pk = (N, g)$ with $N = pq$ an RSA integer and $g \in (\mathbf{Z}/N\mathbf{Z})^\times$, s.t.

$$\left(\frac{g}{p}\right) = \left(\frac{g}{q}\right) = -1.$$

- $c \equiv g^m r^2 \pmod{N}$ where $r \xleftarrow{\$} (\mathbf{Z}/N\mathbf{Z})^\times$
- $sk = p$
- $\left(\frac{c}{p}\right) = (-1)^m$.
- $\mathsf{EvalSum} : cc'r''^2 \equiv g^{m+m'}(rr'r'')^2$
- $\mathsf{EvalScal} : c^\alpha r''^2 \equiv g^{m\alpha}(r^\alpha r'')^2$

Example: Paillier (99)

- $\mathscr{M} = \mathbf{Z}/N\mathbf{Z}$,
- $pk = N$ with $N = pq$ an RSA integer
- $c \equiv (1+N)^m r^N \equiv (1+mN)r^N \pmod{N^2}$ where $r \xleftarrow{\$} (\mathbf{Z}/N\mathbf{Z})^\times$
- $sk = \varphi(N)$
- $c^{\varphi(N)} \equiv (1+N)^{m\varphi(N)} r^{N\varphi(N)} \equiv 1 + m\varphi(N)N \pmod{N^2}$
- $\mathsf{EvalSum} : cc'r''^N \equiv (1+N)^{m+m'}(rr'r'')^N$
- $\mathsf{EvalScal} : c^\alpha r''^N \equiv (1+N)^{m\alpha}(r^\alpha r'')^N$

Security

- CPA security: Oscar can encrypt plaintexts of his choice (Chosen Plaintext Attack)
- No CCA (Chosen Ciphertext Attack) security for homomorphic schemes:
  - Oscar is given a challenge ciphertext c
  - He computes $c' \leftarrow \mathsf{Encrypt}(pk, 0)$ and $c_1 \leftarrow \mathsf{EvalSum}(pk, c, c')$
  - A decryption oracle queried with c_1 gives m
- Total Break (TB – CPA): find sk
  - Goldwasser Micali and Paillier: factorisation of N

Security

- Attack against Semantic Security ($\mathsf{IND-CPA}$): find a bit of information on m given c.
- For a linearly homomorphic scheme, equivalent to distinguish encryptions of $m \xleftarrow{\$} \mathrm{M}$ and encryptions of 0.
- Golwasser Micali is $\mathsf{IND-CPA}$ if it is hard to distinguish squares from non-squares in the set of elements of $(\mathbf{Z}/\mathrm{N}\mathbf{Z})^\times$ whose Jacobi symbol is 1 (Quadratic Residuosity assumption).
- Paillier is $\mathsf{IND-CPA}$ if it is hard to distinguish x^N from random elements of $(\mathbf{Z}/\mathrm{N}^2\mathbf{Z})^\times$ (Composite Residuosity assumption).

One Application: An Electronic Voting Scheme

- Yes/No choice: vote 1 or 0

$$\left.\begin{array}{ccccc} \text{Alice} & : & 0 & \to & \mathsf{Encrypt}(pk, 0) \\ \text{Bob} & : & 1 & \to & \mathsf{Encrypt}(pk, 1) \\ \vdots & & \vdots & \vdots & \vdots \\ \text{Zack} & : & 1 & \to & \mathsf{Encrypt}(pk, 1) \end{array}\right\} \rightsquigarrow \begin{array}{c} c \text{ s.t.} \\ \mathsf{Decrypt(sk, c)} \\ = \\ \sum \text{votes.} \end{array}$$

- Paillier: $\mathscr{M} = \mathbf{Z}/N\mathbf{Z}$ with $N > 2^{1023}$.

DDH ?

- ElGamal encryption scheme (85), $(G, \times) = \langle g \rangle$ of order n

Alice		Bob
h	$\xleftarrow{h = g^x \text{ public key}}$	$\boxed{x \xleftarrow{\$} \mathbf{Z}/n\mathbf{Z} \text{ secret key}}$
$\boxed{r \xleftarrow{\$} \mathbf{Z}/n\mathbf{Z}}$	$\xrightarrow{c_1 = g^r}$	c_1
$Z = h^r \ (= g^{xr})$		$Z = c_1^x \ (= g^{xr})$
$\boxed{m \in G}$	$\xrightarrow{c_2 = mZ}$	$c_2/Z \rightsquigarrow m$

- Ciphertext of m is $(g^r, h^r m) = (c_1, c_2)$. Decryption: c_2/c_1^x

ElGamal

- Security:
  - $\mathsf{TB}-\mathsf{CPA}$: Given $h = g^x$ find x:

    Discrete Logarithm problem in G (DL)
  - $\mathsf{IND}-\mathsf{CPA}$: Distinguish triplets (g^x, g^r, g^{xr}) in G^3:

    Decisional Diffie Hellman Assumption in G (DDH)
- Homomorphic properties:
  - $(c_1, c_2) = (g^r, h^r m) \leftarrow \mathsf{Encrypt}(pk, m)$,
  - $(c_1', c_2') = (g^{r'}, h^{r'} m') \leftarrow \mathsf{Encrypt}(pk, m')$,

$$(c_1 c_1', c_2 c_2') = (g^{r+r'}, h^{r+r'} mm')$$

$$(c_1^\alpha, c_2^\alpha) = (g^{r\alpha}, h^{r\alpha} m^\alpha)$$

- Encoding problem: if $M \in \mathbf{N}$, need to map M to $m \in G$

ElGamal "in the exponent"

- Folklore solution : $\mathrm{M} \in \mathbf{N} \mapsto g^{\mathrm{M}}$
- $(c_1, c_2) = (g^r, h^r g^{\mathrm{M}}) \leftarrow \mathsf{Encrypt}(pk, \mathrm{M})$
- $\mathsf{Decrypt}(pk, c) : c_2 / c_1^x = g^{\mathrm{M}} \rightsquigarrow \mathrm{M}$
- M must be small. Can only do a bounded number of homomorphic operations:
  - $(c_1, c_2) = (g^r, h^r g^{\mathrm{M}}) \leftarrow \mathsf{Encrypt}(pk, \mathrm{M})$,
  - $(c_1', c_2') = (g^{r'}, h^{r'} g^{\mathrm{M}'}) \leftarrow \mathsf{Encrypt}(pk, \mathrm{M}')$,

$$(c_1 c_1', c_2 c_2') = (g^{r+r'}, h^{r+r'} g^{\mathrm{M}+\mathrm{M}'})$$

$$(c_1^{\alpha}, c_2^{\alpha}) = (g^{r\alpha}, h^{r\alpha} g^{\mathrm{M}\alpha})$$

DDH group with an easy DL subgroup

- $(\mathrm{G}, \times) = \langle g \rangle$ a cyclic group of order n
- $n = ps$, $\gcd(p, s) = 1$
- $\langle f \rangle = \mathrm{F} \subset \mathrm{G}$ subgroup of G of order p
- The DL problem is easy in F: There exists, Solve, a deterministic polynomial time algorithm s.t.

$$\mathsf{Solve}(p, f, f^x) \rightsquigarrow x$$

- The DDH problem is hard in G even with access to the Solve algorithm

A Generic Linearly Homomorphic Encryption Scheme

- $\mathscr{M} = \mathbf{Z}/p\mathbf{Z}$
- $pk : h = g^x, sk : x$
- Encrypt : $c = (c_1, c_2) = (g^r, f^m h^r)$
- Decrypt : $\mathrm{A} \leftarrow c_2/c_1^x$, Solve$(p, f, \mathrm{A}) \rightsquigarrow m$
- EvalSum :

$$(c_1 c_1' g^{r''}, c_2 c_2' h^{r''}) = (g^{r+r'+r''}, h^{r+r'+r''} f^{m+m'})$$

- EvalScal :

$$(c_1^{\alpha} g^{r''}, c_2^{\alpha} h^{r''}) = (g^{r\alpha+r''}, h^{r\alpha+r''} f^{m\alpha})$$

An Unsecure Instantiation

- p a prime and $\mathrm{G} = \langle g \rangle = (\mathbf{Z}/p^2\mathbf{Z})^\times$
- $f = 1 + p \in \mathrm{G}$, $\mathrm{F} = \langle f \rangle = \{1 + kp, k \in \mathrm{Z}/p\mathrm{Z}\}$
- $f^m = 1 + mp$.
- There exist a unique $(\alpha, r) \in (\mathbf{Z}/p\mathbf{Z}, (\mathbf{Z}/p\mathbf{Z})^\times)$ such that $g = f^\alpha r^p$

$$g^{p-1} = f^{\alpha(p-1)} = f^{-\alpha}$$

- Public key : $h = g^x$,

$$h^{p-1} = f^{-\alpha x} \rightsquigarrow x \mod p$$

- $(c_1, c_2) = (g^r, h^r f^m)$

$$c_1^{p-1} = f^{-\alpha r} \rightsquigarrow r \mod p$$

$$c_2^{p-1} = f^{-\alpha x r - m} \rightsquigarrow m \mod p$$

Partial Discrete Logarithm Problem

- $(G, \times) = \langle g \rangle$ a cyclic group of order n
- $n = ps$, $\gcd(p, s) = 1$
- $\langle f \rangle = F \subset G$ subgroup of G of order p
- Partial Discrete Logarithm (PDL) Problem:

$$\text{Given } X = g^x \text{ compute } x \mod p.$$

- The knowledge of s makes the PDL problem easy.
- Let $\pi : G \to G/F$ be the canonical surjection.
  Lift Diffie-Hellman (LDH) Problem:

$$\text{Given } X = g^x, Y = g^r \text{ and } \pi(g^{xr}) \text{ compute } g^{xr}$$

- The LDH and PDL are equivalent. The Linearly Homomorphic Encryption Scheme is One-Way if those problems are hard.

A Secure Instantiation

- Bresson, Catalano, Pointcheval (03)
- Let N be an RSA integer, $G = \langle g \rangle = (\mathbf{Z}/N^2\mathbf{Z})^\times$
- $\mathrm{Card}(G) = N\varphi(N) = n$, $s = \varphi(N)$, $p = N$
- $f = 1 + N \in G$, $F = \langle f \rangle = \{1 + kN, k \in Z/NZ\}$, of order N
- Public key : $h = g^x$, x secret key
- $(c_1, c_2) = (g^r, h^r f^m)$
- Based on DDH in $(\mathbf{Z}/N^2\mathbf{Z})^\times$ and the Factorisation problem.
- The factorisation of N acts as a second trapdoor.

Imaginary Quadratic Orders

Imaginary Quadratic Fields

- $K = \mathbf{Q}(\sqrt{\Delta_K})$, $\Delta_K < 0$
- Fundamental Discriminant:
  - $\Delta_K \equiv 1 \pmod 4$ square-free
  - $\Delta_K \equiv 0 \pmod 4$ and $\Delta_K/4 \equiv 2, 3 \pmod 4$ square-free

Imaginary Quadratic Orders

- $\mathscr{O}$ is a subring of K containing 1 and $\mathscr{O}$ is a free $\mathbf{Z}$-module of rank 2

Imaginary Quadratic Orders

Characterisation of Orders

- $\mathcal{O}_{\Delta_K}$: ring of integers of K is the maximal order,

$$\mathcal{O}_{\Delta_K} = \mathbf{Z} + \frac{\Delta_K + \sqrt{\Delta_K}}{2}\mathbf{Z}$$

- $\mathcal{O} \subset \mathcal{O}_{\Delta_K}, \ell := [\mathcal{O}_{\Delta_K} : \mathcal{O}]$ is the conductor,

$$\mathcal{O} = \mathbf{Z} + \frac{\Delta_\ell + \sqrt{\Delta_\ell}}{2}\mathbf{Z}$$

$\Delta_\ell = \ell^2 \Delta_K$ is the non fundamental discriminant of $\mathcal{O}_{\Delta_\ell} := \mathcal{O}$

Class Group

Class Group of discriminant Δ

$$\mathrm{C}(\mathcal{O}_\Delta) := \mathrm{I}(\mathcal{O}_\Delta)/\mathrm{P}(\mathcal{O}_\Delta)$$

its finite cardinal is the class number denoted $h(\mathcal{O}_\Delta)$

- $\mathrm{I}(\mathcal{O}_\Delta)$: group of Invertible Fractional Ideals of $\mathcal{O}_\Delta$
- $\mathrm{P}(\mathcal{O}_\Delta)$: subgroup of Principal Ideals
- Class Number: $h(\mathcal{O}_\Delta) \approx \sqrt{|\Delta|}$

ElGamal in Class Group of Maximal Order

- Buchmann and Williams (88): Diffie-Hellman key exchange and ElGamal
- Düllmann, Hamdy, Möller, Pohst, Schielzeth, Vollmer (90-07): Implementation
  - Construct Δ_K a fundamental negative discriminant, in order to maximize the odd-part of $C(\mathcal{O}_{\Delta_K})$; *e.g.*, $\Delta_k = -q$, $q \equiv 3 \pmod 4$, q prime : $h(\mathcal{O}_{\Delta_K})$ is odd
  - choose g a random class of $C(\mathcal{O}_{\Delta_K})$ of odd order $\rightsquigarrow$ order of g will be close to $h(\mathcal{O}_{\Delta_K}) \approx \sqrt{|\Delta_K|}$
  - secret key: $x \xleftarrow{\$} \{0, \dots, \lfloor \sqrt{|\Delta_K|} \rfloor\}$, public key: $h = g^x$.
- Encoding of message in $G = \langle g \rangle$ can be problematic

Class Number and Discrete Logarithm computations

- Size of Δ_K? Index calculus algorithm to compute $h(\mathcal{O}_{\Delta_K})$ and Discrete Logarithm in $C(\mathcal{O}_{\Delta_K})$
- Security Estimates from Biasse, Jacobson and Silvester (10):
  - Complexity conjectured $L_{|\Delta_K|}(1/2, o(1))$
  - Δ_k : 1348 bits as hard as factoring a 2048 bits RSA integer
  - Δ_k : 1828 bits as hard as factoring a 3072 bits RSA integer

Class Groups of Non Maximal Orders

Order of discriminant $\Delta_\ell := \ell^2 \Delta_K$

$\mathcal{O}_{\Delta_\ell}$

$\mathcal{O}_{\Delta_K}$

Order of discriminant Δ_K

Class Groups of Non Maximal Orders

$$\begin{tikzcd} \mathcal{O}_{\Delta_\ell} & \mathfrak{a} \arrow[d, "\varphi_\ell"] & \text{ideal prime to } \ell \\ \mathcal{O}_{\Delta_K} & \mathfrak{a}\mathcal{O}_{\Delta_K} & \text{ideal of same norm} \end{tikzcd}$$

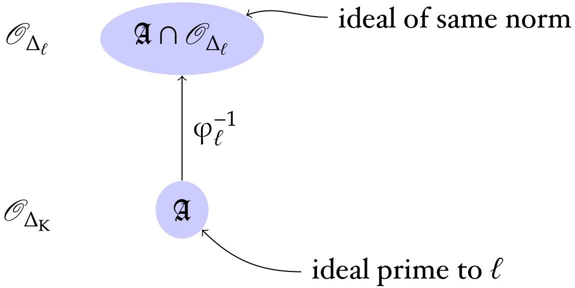
Class Groups of Non Maximal Orders

$$
\begin{tikzcd}
\mathcal{O}_{\Delta_\ell} & \mathfrak{A} \cap \mathcal{O}_{\Delta_\ell} \\
\mathcal{O}_{\Delta_K} & \mathfrak{A} \arrow[u, "\varphi_\ell^{-1}"']
\end{tikzcd}
$$

ideal of same norm

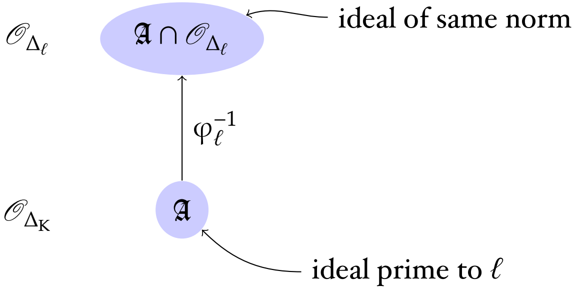
ideal prime to ℓ

Class Groups of Non Maximal Orders



- φ_ℓ et φ_ℓ^{-1} are effective isomorphisms, computable if ℓ is known

Class Groups of Non Maximal Orders



For Class Groups:

- φ_ℓ gives a surjection :

$$\bar{\varphi}_\ell \; : \; C(\mathcal{O}_{\Delta_\ell}) \longrightarrow\!\!\!\!\rightarrow C(\mathcal{O}_{\Delta_K})$$

Class Groups of Non Maximal Orders

$$\begin{tikzcd}
\mathscr{O}_{\Delta_\ell} & \mathfrak{A} \cap \mathscr{O}_{\Delta_\ell} \\
\mathscr{O}_{\Delta_K} & \mathfrak{A} \arrow[u, "\varphi_\ell^{-1}"']
\end{tikzcd}$$

ideal of same norm

ideal prime to ℓ

For Class Groups:

- If $\Delta_K < 0$, $\Delta_K \neq -3, -4$,

$$h(\mathscr{O}_{\Delta_\ell}) = h(\mathscr{O}_{\Delta_K}) \times \ell \prod_{p \mid \ell} \left(1 - \left(\frac{\Delta_K}{p}\right) \frac{1}{p}\right)$$

Cryptography in Class Groups of Non Maximal Orders

- NICE cryptosystem (New Ideal Coset Encryption), Paulus and Takagi (00)
- $\Delta_K = -q$, $\Delta_p = -qp^2$, p, q primes and $q \equiv 3 \pmod 4$

$$h(\mathcal{O}_{\Delta_p}) = h(\mathcal{O}_{\Delta_K}) \times \left(p - \left(\frac{\Delta_K}{p}\right)\right)$$

- Public key: Δ_p and $h \in \ker \bar{\varphi}_p$, with $\bar{\varphi}_p : C(\mathcal{O}_{\Delta_p}) \to C(\mathcal{O}_{\Delta_K})$
- Secret key: p
- C., Laguillaumie (09) :

In each non trivial class of $\ker \bar{\varphi}_p$, there exists an ideal of norm p^2

A Subgroup with an Easy DL Problem

- $\Delta_K = -pq$, $\Delta_p = -qp^3$, p, q primes and $pq \equiv 3 \pmod 4$

$$h(\mathcal{O}_{\Delta_p}) = p \times h(\mathcal{O}_{\Delta_K})$$

- There exists an effective isomorphism

$$\psi_p\colon \left(\mathcal{O}_{\Delta_K}/p\mathcal{O}_{\Delta_K}\right)^\times / \left(\mathbf{Z}/p\mathbf{Z}\right)^\times \xrightarrow{\sim} \ker \bar{\varphi}_p$$

Evaluation of ψ_p :

As $p \mid \Delta_K$,

$$\left(\mathcal{O}_{\Delta_K}/p\mathcal{O}_{\Delta_K}\right)^\times \simeq \left(\mathbf{F}_p[X]/(X^2)\right)^\times$$

A Subgroup with an Easy DL Problem

- $\Delta_K = -pq$, $\Delta_p = -qp^3$, p, q primes and $pq \equiv 3 \pmod 4$

$$h(\mathcal{O}_{\Delta_p}) = p \times h(\mathcal{O}_{\Delta_K})$$

- There exists an effective isomorphism

$$\psi_p\colon \ \left(\mathcal{O}_{\Delta_K}/p\mathcal{O}_{\Delta_K}\right)^{\times} / \left(\mathbf{Z}/p\mathbf{Z}\right)^{\times} \xrightarrow{\ \sim\ } \ker \bar{\varphi}_p$$

Evaluation of ψ_p :

Elements of $\left(\mathcal{O}_{\Delta_K}/p\mathcal{O}_{\Delta_K}\right)^{\times} / \left(\mathbf{Z}/p\mathbf{Z}\right)^{\times}$: $[1]$ and $[a + \sqrt{\Delta_K}]$ where a is an element of $(\mathbf{Z}/p\mathbf{Z})^{\times}$

A Subgroup with an Easy DL Problem

- $\Delta_K = -pq$, $\Delta_p = -qp^3$, p, q primes and $pq \equiv 3 \pmod 4$

$$h(\mathcal{O}_{\Delta_p}) = p \times h(\mathcal{O}_{\Delta_K})$$

- There exists an effective isomorphism

$$\psi_p\colon \left(\mathcal{O}_{\Delta_K}/p\mathcal{O}_{\Delta_K}\right)^\times / \left(\mathbf{Z}/p\mathbf{Z}\right)^\times \xrightarrow{\sim} \ker \bar{\varphi}_p$$

Evaluation of ψ_p :

Let $A = [1 + \sqrt{\Delta_K}]$, one has $A^m = [1 + m\sqrt{\Delta_K}] = [m^{-1} + \sqrt{\Delta_K}]$ for all $m \in \{1, \dots, p-1\}$ and $A^p = [1]$.

A Subgroup with an Easy DL Problem

- $\Delta_K = -pq$, $\Delta_p = -qp^3$, p, q primes and $pq \equiv 3 \pmod 4$

$$h(\mathcal{O}_{\Delta_p}) = p \times h(\mathcal{O}_{\Delta_K})$$

- There exists an effective isomorphism

$$\psi_p\colon \left(\mathcal{O}_{\Delta_K}/p\mathcal{O}_{\Delta_K}\right)^\times / \left(\mathbf{Z}/p\mathbf{Z}\right)^\times \xrightarrow{\ \sim\ } \ker \bar{\varphi}_p$$

Evaluation of ψ_p :

- Let $\alpha_m = \frac{L(m)+\sqrt{\Delta_K}}{2} \in \mathcal{O}_{\Delta_K}$, a representative of the class A^m, where $L(m)$ is the odd integer in $[-p, p]$ such that $L(m) \equiv 1/m \pmod p$
- The element A^m maps to the class $\psi_p(A^m) = [\varphi_p^{-1}(\alpha_m \mathcal{O}_{\Delta_K})]$ of the kernel of $\bar{\varphi}_p$

A Subgroup with an Easy DL Problem

- $\Delta_K = -pq$, $\Delta_p = -qp^3$, p, q primes and $pq \equiv 3 \pmod 4$

$$h(\mathcal{O}_{\Delta_p}) = p \times h(\mathcal{O}_{\Delta_K})$$

- There exists an effective isomorphism

$$\psi_p\colon \left(\mathcal{O}_{\Delta_K}/p\mathcal{O}_{\Delta_K}\right)^\times / \left(\mathbf{Z}/p\mathbf{Z}\right)^\times \xrightarrow{\sim} \ker \bar{\varphi}_p$$

Evaluation of ψ_p :

A tedious computation yields

$$\psi_p(\mathrm{A}^m) = \left[p^2\mathbf{Z} + \frac{-\mathrm{L}(m)p + \sqrt{\Delta_p}}{2}\mathbf{Z}\right]$$

A Subgroup with an Easy DL Problem

- Let $f = \psi_p(\mathrm{A}) = \left[p^2\mathbf{Z} + \frac{-p+\sqrt{\Delta_p}}{2}\mathbf{Z}\right] \in \mathrm{C}(\mathscr{O}_{\Delta_p})$
- $\mathrm{F} = \langle f \rangle$ is of order p, and

$$f^m = \psi_p(\mathrm{A}^m) = \left[p^2\mathbf{Z} + \frac{-\mathrm{L}(m)p + \sqrt{\Delta_p}}{2}\mathbf{Z}\right]$$

- Moreover if $q > 4p$, then $p^2 < \sqrt{|\Delta_p|}/2$. As a result, the ideals of norm p^2 are reduced (there are the canonical representatives)

A New Linearly Homomorphic Encryption Scheme

- $\Delta_K = -pq$, $\Delta_p = -qp^3$, p, q primes and $pq \equiv 3 \pmod 4$ and $(p/q) = -1$, $q > 4p$
- Let g be an element of $C(\mathcal{O}_{\Delta_p})$, $h = g^x$ where x secret key
- $(c_1, c_2) = (g^r, h^r f^m)$
- Based on DDH in $C(\mathcal{O}_{\Delta_p})$ (and the Class number problem).
- Linearly homomorphic over $\mathbf{Z}/p\mathbf{Z}$ where p can be chosen (almost) independently from the security parameter

Removing the Condition on the Relative Size of p and q

- We impose that $q > 4p$, in order that the reduced elements of $\langle f \rangle$ are the ideals of norm p^2.
- As a consequence $|\Delta_K| = pq > 4p^2$
- If we want a large message space, *e.g.,* p of 2048 bits, Δ_K has 4098 bits (only 1348 needed for security).

Work with $\Delta_K = -p$, and $\Delta_p = p^2\Delta_K = -p^3$.

Removing the Condition on the Relative Size of p and q

- $\Delta_K = -p$, and $\Delta_p = p^2\Delta_K = -p^3$.
- Let $f = \left[p^2\mathbf{Z} + \frac{-p+\sqrt{\Delta_p}}{2}\mathbf{Z}\right] \in C(\mathscr{O}_{\Delta_p})$, f^m still contains the non reduced ideal
$$p^2\mathbf{Z} + \frac{-L(m)p + \sqrt{\Delta_p}}{2}\mathbf{Z}$$
- We lift f and f^m in the class group of discriminant $\Delta_{p^2} = p^4\Delta_K$ where the ideals of norm p^2 are reduced. This is done with the map
$$[\varphi_p^{-1}(\cdot)]^p$$
- One can show that $[\varphi_p^{-1}(F)]^p$ is a subgroup of order p generated by the class of the reduced ideal $[p^2\mathbf{Z} + \frac{-p+\sqrt{\Delta_{p^2}}}{2}\mathbf{Z}]$ and Discrete Logarithms are easy to compute in this subgroup

A Faster Variant

- Original Scheme :
  - $\Delta_K = -p$, and $\Delta_p = p^2\Delta_K = -p^3$.
  - $g \in C(\mathcal{O}_{\Delta_p})$, $h = g^x$
  - f generates the subgroup of order p of $C(\mathcal{O}_{\Delta_p})$
  - $\mathsf{Encrypt}(pk, m) = (g^r, h^r f^m)$

- A faster variant :
  - Choose $g' \in C(\mathcal{O}_{\Delta_K})$ and $h' = g^{x'}$
  - Denote $\psi_p : C(\mathcal{O}_{\Delta_K}) \to C(\mathcal{O}_{\Delta_p})$ the map $[\varphi_p^{-1}(\cdot)]^p$
  - Define $\mathsf{Encrypt}(pk, m) = (c_1, c_2) = (g'^r, \psi(h'^r) f^m)$
  - Decryption: Compute $c_1' = \psi(c_1^{x'})$ and $f^m = c_2/c_1'$.
  - Smaller ciphertext: c_1 is in $C(\mathcal{O}_{\Delta_K})$ instead of $C(\mathcal{O}_{\Delta_p})$
  - Faster computation: exponentiations in $C(\mathcal{O}_{\Delta_K})$ instead of $C(\mathcal{O}_{\Delta_p})$
  - However, the semantic security is now based on a non standard problem.

Performance comparison

Cryptosystem	Parameter	Message Space	Encryption (ms)	Decryption (ms)
Paillier	2048 bits modulus	2048 bits	**28**	**28**
BCP03	2048 bits modulus	2048 bits	107	54
New Proposal	1348 bits Δ_K	80 bits	93	49
Fast Variant	1348 bits Δ_K	80 bits	82	45
Fast Variant	1348 bits Δ_K	256 bits	105	68
Paillier	3072 bits modulus	3072 bits	**109**	109
BCP03	3072 bits modulus	3072 bits	427	214
New Proposal	1828 bits Δ_K	80 bits	179	91
Fast Variant	1828 bits Δ_K	80 bits	145	**78**
Fast Variant	1828 bits Δ_K	512 bits	226	159
Fast Variant	1828 bits Δ_K	912 bits	340	271

Timings performed with Sage and PARI/GP.

Others Variants and Further developments

- More general message spaces:
  - $\mathbf{Z}/N\mathbf{Z}$ with $N = \prod_{i=1}^{n} p_i$, with a discriminant of the form $\Delta_K = -Nq$
  - $\mathbf{Z}/p^t\mathbf{Z}$ for $t > 1$, with discriminants of the form $\Delta_{p^t} = p^{2t}\Delta_K$, and $\Delta_K = -pq$
- An adaptation may also be possible in the infrastructure of real quadratic fields