CL 0000 Threshold CL 00000000

Threshold Cryptography based on Class Groups of Imaginary Quadratic Fields

Guilhem Castagnos





Class Groups



Threshold CL 00000000

Outline

Threshold Linear Homomorphic Encryption

Class Groups

CL

Threshold CL

Class Groups

CL 0000 Threshold CL 00000000

- Bob : $(pk, sk) \leftarrow \text{KeyGen}(1^k)$
- Publish *pk*

Class Groups

CL 0000 Threshold CL 00000000

- Bob : $(pk, sk) \leftarrow \text{KeyGen}(1^k)$
- Publish *pk*





Class Groups

CL 0000 Threshold CL 00000000

- Bob : $(pk, sk) \leftarrow \text{KeyGen}(1^k)$
- Publish *pk*





Class Groups 00000000 CL 0000 Threshold CL 00000000

- Bob : $(pk, sk) \leftarrow \text{KeyGen}(1^k)$
- Publish *pk*



Class Groups 00000000 CL 0000 Threshold CL 00000000

- Bob : $(pk, sk) \leftarrow \text{KeyGen}(1^k)$
- Publish *pk*



Class Groups

CL 0000 Threshold CL 00000000

Traditional PKE

- Bob : $(pk, sk) \leftarrow \text{KeyGen}(1^k)$
- Publish *pk*



• Linearly Homomorphic Encryption (LHE):

$$\mathsf{Encrypt}_{pk}(m_1) \otimes \mathsf{Encrypt}_{pk}(m_2) \rightsquigarrow \mathsf{Encrypt}_{pk}(m_1 + m_2)$$

 $\mathsf{Encrypt}_{pk}(m)^{\otimes a} \rightsquigarrow \mathsf{Encrypt}_{pk}(a \cdot m)$

Class Groups



Threshold CL 00000000

Threshold LHE

• *n* Bobs collaborate to decrypt a ciphertext





Class Groups



Threshold CL 00000000

- *n* Bobs collaborate to decrypt a ciphertext
- Distributed Key Generation (DKG)







Class Groups

CL 0000 Threshold CL 00000000

- *n* Bobs collaborate to decrypt a ciphertext
- Distributed Key Generation (DKG)



Class Groups

CL 0000 Threshold CL 00000000

- *n* Bobs collaborate to decrypt a ciphertext
- Distributed Key Generation (DKG)



Class Groups

CL 0000 Threshold CL 00000000

- *n* Bobs collaborate to decrypt a ciphertext
- Distributed Key Generation (DKG)



Class Groups

CL

Threshold CL 00000000

- *n* Bobs collaborate to decrypt a ciphertext
- Distributed Key Generation (DKG) $\rightsquigarrow pk$



$$\operatorname{Bob}_2$$
 sk_2

$$\operatorname{Bob}_n sk_n$$

Class Groups

CL 0000 Threshold CL 00000000

Threshold LHE

• *n* Bobs collaborate to decrypt a ciphertext





$$\operatorname{Bob}_2$$
 sk_2

$$\operatorname{Bob}_n sk_n$$

Class Groups

CL 0000 Threshold CL 00000000

Threshold LHE

• *n* Bobs collaborate to decrypt a ciphertext



4/30

Class Groups

CL 0000 Threshold CL 00000000

- *n* Bobs collaborate to decrypt a ciphertext
- Distributed Decryption



$$\operatorname{Bob}_n sk_n c$$

Class Groups

CL 0000 Threshold CL 00000000

- *n* Bobs collaborate to decrypt a ciphertext
- Distributed Decryption



Class Groups



Threshold CL 00000000

- *n* Bobs collaborate to decrypt a ciphertext
- Distributed Decryption



Class Groups

CL 0000 Threshold CL 00000000

Threshold LHE

- *n* Bobs collaborate to decrypt a ciphertext
- Distributed Decryption



4/30

Class Groups

CL 0000 Threshold CL 00000000

Threshold LHE

- *n* Bobs collaborate to decrypt a ciphertext
- Distributed Decryption



4/30

Class Groups



- *n* Bobs collaborate to decrypt a ciphertext
- Threshold:
 - t < n Bobs $\rightsquigarrow \emptyset$ info on m
 - t + 1 Bobs $\rightsquigarrow m$
 - Assume t < n/2 to get guaranteed output delivery







CL 0000

NIST Call

Computer Security RESOURCE CENTER

PUBLICATIONS

NIST IR 8214C (2nd Public Draft)

NIST First Call for Multi-Party Threshold Schemes

f 🗙 in 🖾

Date Published: March 27, 2025 Comments Due: April 30, 2025 Email Comments to: <u>nistir-8214C-comments@nist.gov</u>

Author(s) Luís T. A. N. Brandão (NIST, Strativia), Rene Peralta (NIST)

Announcement

This is a second public draft. Threshold schemes should NOT be submitted until the final version of this report is published. However, the present draft can be used as a baseline to prepare for future submissions.

The scope of the call is erganized into categories related to signing (Sign), public low encryption (RKE).

DOCUMENTATION

Publication: C.https://doi.org/10.6028/NIST.IR.8214C.2pd Download URL

Supplemental Material: None available

Document History: 01/25/23: <u>IR 8214C (Draft)</u> 03/27/25: IR 8214C (Draft)

CL 0000 Threshold CL 00000000

Applications of TLHE

$$\begin{array}{cccc} \text{Alice}_{1} : & 0 & \rightarrow & c_{1} \coloneqq \text{Encrypt}_{pk}(0) \\ \text{Alice}_{2} : & 1 & \rightarrow & c_{2} \coloneqq \text{Encrypt}_{pk}(1) \\ \vdots & \vdots & \vdots & \vdots \\ \text{Alice}_{\ell} : & 1 & \rightarrow & c_{\ell} \coloneqq \text{Encrypt}_{pk}(1) \end{array} \right\} \rightsquigarrow c \coloneqq \otimes_{i=1}^{\ell} c_{i} \\ \end{array}$$

Class Groups

CL 0000 Threshold CL 00000000

Applications of TLHE



$$\begin{array}{rcl} \operatorname{Alice}_{1}:&0&\rightarrow&c_{1}:=\operatorname{Encrypt}_{pk}(0)\\ \operatorname{Alice}_{2}:&1&\rightarrow&c_{2}:=\operatorname{Encrypt}_{pk}(1)\\ \vdots&\vdots&\vdots&\vdots\\ \operatorname{Alice}_{\ell}:&1&\rightarrow&c_{\ell}:=\operatorname{Encrypt}_{pk}(1) \end{array}\right\} \rightsquigarrow c:=\otimes_{i=1}^{\ell}c_{i}$$

Class Groups

CL 0000 Threshold CL 00000000

Applications of TLHE



Class Groups

CL 0000

Bob

Threshold CL 00000000

Applications of TLHE

$$\begin{array}{cccc} \text{Alice}_{1} & 0 & \rightarrow & c_{1} \coloneqq \text{Encrypt}_{pk}(0) \\ \text{Alice}_{2} & 1 & \rightarrow & c_{2} \coloneqq \text{Encrypt}_{pk}(1) \\ \vdots & \vdots & \vdots & \vdots \\ \text{Alice}_{\ell} & 1 & \rightarrow & c_{\ell} \coloneqq \text{Encrypt}_{pk}(1) \end{array} \right\} \rightsquigarrow c \coloneqq \bigotimes_{i=1}^{\ell} c_{i} \qquad \qquad \begin{array}{c} & \overset{SK}{m} \leftarrow \text{Dec}_{sk}(c) \\ & & \downarrow \\ & m = \sum \text{votes.} \end{array}$$

Class Groups

CL 0000 Threshold CL 00000000

Applications of TLHE



$$\begin{array}{cccc} \operatorname{Alice}_{1} : & 0 & \to & c_{1} \coloneqq \operatorname{Encrypt}_{pk}(0) \\ \operatorname{Alice}_{2} : & 1 & \to & c_{2} \coloneqq \operatorname{Encrypt}_{pk}(1) \\ \vdots & \vdots & \vdots & \vdots \\ \operatorname{Alice}_{\ell} : & 1 & \to & c_{\ell} \coloneqq \operatorname{Encrypt}_{pk}(1) \end{array} \right\} \rightsquigarrow c \coloneqq \otimes_{i=1}^{\ell} c_{i} \\ \end{array}$$

Class Groups

CL 0000 Threshold CL 00000000

Applications of TLHE





$$\operatorname{Bob}_n sk_n$$

CL 0000 Threshold CL 00000000

Applications of TLHE

Multi-Party Computation: Cramer, Damgård, Nielsen, EC'or

computation of an arithmetic function over a ring $\mathcal R$

- Parties share a decryption key for a TLHE over ${\mathcal R}$
- Encrypt their secret input and broadcast $\text{Encrypt}_{vk}(x_i)$
- Without interaction: Addition of secret values, multiplication by a public value $\operatorname{Encrypt}_{pk}(x) \otimes \operatorname{Encrypt}_{pk}(y)$; $\operatorname{Encrypt}_{pk}(x)^{\otimes a}$
- Multi-Party subprotocol to compute

 $\text{Encrypt}_{pk}(xy)$ from $\text{Encrypt}_{pk}(x)$ and $\text{Encrypt}_{pk}(y)$

• Final threshold decryption to compute the result

Applications of TLHE

Multi-Party Computation

- CDN less efficient than MPC with pre-processing (SPDZ)
- YOSO! Gentry, Halevi, Krawczyk, Magri, Nielsen, Rabin, Yakoubov, C'21
- Large universe of M servers
- Computation done by a committee of $N\ll M$ servers
- Goal: Hide the committee to the adversary
- You Only Speak Once: committee sends only one round of messages
- Instantiation from CDN

CL 0000 Threshold CL 00000000

Examples of TLHE

ElGamal in the Exponent (C'84)

- sk = x $pk = g^x$ $c = (g^r, g^m pk^r)$
- Discrete Log. computation during decryption
- Limited homomorphism (few $c \otimes c'$, no $c^{\otimes a}$ for large *a*)
- Sufficient for voting (Helios, Benelios)

Paillier (EC'99)

- sk = p, q pk = N $c = (1 + N)^m r^N \pmod{N^2}$
- Easy Discrete Log. computation during decryption
- Linear homomorphism without restriction
- Requires a trusted setup for Keygen, or costly MPC, $\mathcal{R} = \mathbf{Z}/\mathbf{NZ}$

CL 0000 Threshold CL 00000000

Examples of TLHE

ElGamal in the Exponent (C'84)

- sk = x $pk = g^x$ $c = (g^r, g^m pk^r)$
- Discrete Log. computation during decryption
- Limited homomorphism (few $c \otimes c'$, no $c^{\otimes a}$ for large *a*)
- Sufficient for voting (Helios, Benelios)

Paillier (EC'99)

- sk = p,q pk = N $c = (1 + N)^m r^N \pmod{N^2}$
- Easy Discrete Log. computation during decryption
- Linear homomorphism without restriction
- Requires a trusted setup for Keygen, or costly MPC, $\mathcal{R} = \mathbf{Z}/N\mathbf{Z}$

What about CL ?



Threshold CL 00000000

What can I help with?





Can you explain CL encryption ?

Sure! **CL encryption** usually refers to **Camenisch-Lysyanskaya encryption**, a cryptographic scheme developed by Jan Camenisch and Anna Lysyanskaya. It's mainly known for being used in **privacy-preserving credentials**—especially in **anonymous credential systems** like Idemix.



Can you explain the Castagnos Laguillaumie encryption scheme?

The **Castagnos-Laguillaumie encryption scheme** is a public-key encryption system that is based on the hardness of certain problems in **ideal lattices**. Specifically, it is one of the cryptographic schemes that uses **lattice-based cryptography**, which is a field that aims to provide security based on mathematical structures like lattices rather than traditional number-theoretic problems (e.g., factoring large integers or the discrete logarithm problem).

Lattice-based cryptography has become particularly attractive because, unlike traditional cryptographic systems (RSA, ECC), it is believed to be resistant to attacks by quantum computers. As such, it is considered a potential candidate for **post-quantum cryptography**.

CL 0000

Conclusion

Jean-Charles Castagnos and Éric Laguillaumie have made significant contributions to **lattice-based cryptography**, particularly in the context of **class group encryption schemes**. The Castagnos-Laguillaumie encryption scheme, based on the **class group problem** of quadratic number fields, is one of the promising **post-quantum cryptography** solutions that offer security against quantum adversaries. Their work has helped shape the development of cryptographic systems that will remain secure even in the age of quantum computing.

If you'd like more detailed information on their specific publications or other works, feel free to ask!

Class Groups



Threshold CL 00000000

Outline

Threshold Linear Homomorphic Encryption

Class Groups

CL

Threshold CL

Defining Class Groups in two slides (1/2)

Imaginary Quadratic Fields

• $K = \mathbf{Q}(\sqrt{\Delta_K}), \Delta_K < 0$

Orders of K

• $\mathscr{O}_{\Delta_{\mathrm{K}}}$: ring of integers of K, the maximal order, Δ_{K} square free,

$$\mathscr{O}_{\Delta_{\mathrm{K}}} = \mathbf{Z} + \frac{\Delta_{\mathrm{K}} + \sqrt{\Delta_{\mathrm{K}}}}{2} \mathbf{Z}$$

•
$$\mathscr{O}_{\Delta_{\ell}} \subset \mathscr{O}_{\Delta_{\mathrm{K}}}, \Delta_{\ell} = \ell^2 \Delta_{\mathrm{K}},$$

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

CL 0000 Threshold CL 00000000

Class groups in two slides (2/2)

Definition

- $I(\mathscr{O}_{\Delta_{\ell}})$: (Invertible Fractional) Ideals of $\mathscr{O}_{\Delta_{\ell}}$
- $P(\mathscr{O}_{\Delta_{\ell}})$: Subgroup of Principal Ideals
- Class group of $\mathscr{O}_{\Delta_{\ell}}$

$$\mathbf{C}(\mathscr{O}_{\Delta_{\ell}}) := \mathbf{I}(\mathscr{O}_{\Delta_{\ell}})/\mathbf{P}(\mathscr{O}_{\Delta_{\ell}})$$

Properties

- Equivalence relation: $a \sim b \iff \exists \alpha \in K^*, b = \alpha a$
- Short representations, efficient computation of the group law
- Class Number: $h(\mathcal{O}_{\Delta_{\ell}}) \approx \sqrt{|\Delta_{\ell}|}$

Class Groups

CL 0000 Threshold CL 00000000

A tiny class group

- $\Delta_{\rm K} = -131$
- $\mathscr{C}(\mathscr{O}_{\Delta_{\mathrm{K}}})$ has 5 classes. Reduced elements:

$$\begin{bmatrix} 3\mathbf{Z} + \frac{-1+\sqrt{\Delta_{\mathrm{K}}}}{2}\mathbf{Z} \end{bmatrix} \begin{bmatrix} 5\mathbf{Z} + \frac{3+\sqrt{\Delta_{\mathrm{K}}}}{2}\mathbf{Z} \end{bmatrix} \begin{bmatrix} 5\mathbf{Z} + \frac{-3+\sqrt{\Delta_{\mathrm{K}}}}{2}\mathbf{Z} \end{bmatrix} \begin{bmatrix} 3\mathbf{Z} + \frac{1+\sqrt{\Delta_{\mathrm{K}}}}{2}\mathbf{Z} \end{bmatrix}$$
$$\begin{bmatrix} \mathbf{Z} + \frac{\Delta_{\mathrm{K}}+\sqrt{\Delta_{\mathrm{K}}}}{2}\mathbf{Z} \end{bmatrix}$$

- A multiplication : $\left(3\mathbf{Z} + \frac{-1+\sqrt{\Delta_{\mathrm{K}}}}{2}\mathbf{Z}\right)\left(5\mathbf{Z} + \frac{3+\sqrt{\Delta_{\mathrm{K}}}}{2}\mathbf{Z}\right) = \left(15\mathbf{Z} + \frac{23+\sqrt{\Delta_{\mathrm{K}}}}{2}\mathbf{Z}\right)$
- Reduction : $3\mathbf{Z} + \frac{1+\sqrt{\Delta_{K}}}{2}\mathbf{Z}$ (by multiplication by $\frac{-7-\sqrt{\Delta_{K}}}{30}$)

CL 0000 Threshold CL 00000000

Hard Problems in Class Goups

- Computation of $h(\mathscr{O}_{\Delta_{\mathsf{K}}})$, the structure of $C(\mathscr{O}_{\Delta_{\mathsf{K}}})$ and DL
- Sub exponential algorithm Hafner and McCurley, JoAMS'89
- Heuristic Complexity $L_{|\Delta_K|}[1/2, 1 + o(1)]$
- Smaller parameters than factoring

1827 bits Δ_K vs 3072 bits N



Threshold CL 00000000

Vintage Crypto in $C(\mathscr{O}_{\Delta_{K}})$

- Diffie-Hellman key exchange and ElGamal Buchmann and Williams, JoC'88
- DSA and GQ signatures adaptations : Biehl, Buchmann, Hamdy, Meyer (01-02)

• Public coin setup:

- $\Delta_k := -q, q \equiv 3 \pmod{4}, q \text{ prime} : h(\mathscr{O}_{\Delta_K}) \text{ is odd}$
- Choose g a random class of $C(\mathscr{O}_{\Delta_{K}})$ \rightsquigarrow order of g will be close to $h(\mathscr{O}_{\Delta_{K}}) \approx \sqrt{|\Delta_{K}|}$
- Work in the cyclic group $G = \langle g \rangle \subset C(\mathscr{O}_{\Delta_{K}})$
- The order of *g* is unknown!



Threshold CL 00000000

Paradox of Unknown Order 😕

- DL in a cyclic group $G = \langle g \rangle \subset C(\mathscr{O}_{\Delta_K})$ of unknown order s
- *s* is divisible by small primes with non negligible probability!
- But *s* not smooth for cryptographic sizes
- Uniform sampling in G possible with an upper bound on $h(\mathscr{O}_{\Delta_{K}}) \ge s$
- Can not decide if an element of $C(\mathscr{O}_{\Delta_{K}})$ is in G
- Many technicalities with ZK proofs

• ...



Threshold CL 00000000

Paradox of Unknown Order 😎

Public coin setup to generate a group of unknown order!

- Cryptographic accumulators Lipmaa, ACNS'12
- Verifiable delay functions Wesolowski, EC'19
- Transparent SNARKS Bünz, Fisch, Szepieniec, EC'20
- Range Proofs Couteau, Klooß, Lin, Reichle, EC'21

- RSA based construction: someone knows $\phi(N)$! Needs some trusted setup.
- With class groups, $h(\mathscr{O}_{\Delta_{\mathbf{K}}})$ is really unknown to anyone!
- Another application: LHE modulo a prime \rightsquigarrow the CL cryptosystem

Class Groups



Threshold CL 00000000

Outline

Threshold Linear Homomorphic Encryption

Class Groups

CL

Threshold CL

Class Groups

CL o●oo Threshold CL 00000000

A Subgroup with an Easy DL

- C. Laguillaumie CT-RSA'15
- $\Delta_{\mathrm{K}} = -pq, \Delta_q = -pq^3, p, q \text{ primes and } pq \equiv 3 \pmod{4}$

$$h(\mathcal{O}_{\Delta_q}) = q \times h(\mathcal{O}_{\Delta_{\mathrm{K}}})$$

• Let
$$f := \left[q^2 \mathbf{Z} + \frac{-q + \sqrt{\Delta_q}}{2} \mathbf{Z}\right] \in \mathcal{C}(\mathscr{O}_{\Delta_q})$$

• $F = \langle f \rangle$ is of order q, and

$$f^{m} = \left[q^{2}\mathbf{Z} + \frac{-\mathcal{L}(m)q + \sqrt{\Delta_{q}}}{2}\mathbf{Z}\right] \text{ where } \mathcal{L}(m) \equiv 1/m \pmod{q}$$



CL Framework

Group with an easy DL subgroup

- q a prime
- $G = \langle g \rangle$ cyclic group of order $q \cdot s$ such that gcd(q, s) = 1
- $\mathbf{F} = \langle f \rangle$ subgroup of G of order q
- $G^q = \langle h \rangle = \{x^q, x \in G\}$ subgroup of G of order *s*,

 $G \simeq F \times G^q$

• DL is easy in F:

Given $u \in F$, find $m \in \mathbb{Z}/q\mathbb{Z}$ such that $u = f^m$

CL 0000 Threshold CL 00000000

CL Framework

Group with an easy DL subgroup

- q a prime
- $G = \langle g \rangle$ cyclic group of order $q \cdot s$ such that gcd(q, s) = 1
- $\mathbf{F} = \langle f \rangle$ subgroup of G of order q
- $G^q = \langle h \rangle = \{x^q, x \in G\}$ subgroup of G of order *s*,

 $G \simeq F \times G^q$

• Hard to distinguish elements of G^q:

 $\{Z \hookleftarrow G\} \approx_c \{Z \hookleftarrow G^q\}$

Hard Subgroup Membership Assumption (HSM)



CL Framework

Group with an easy DL subgroup

- q a prime
- $G = \langle g \rangle$ cyclic group of order $q \cdot s$ such that gcd(q, s) = 1
- $\mathbf{F} = \langle f \rangle$ subgroup of G of order q
- $G^q = \langle h \rangle = \{x^q, x \in G\}$ subgroup of G of order *s*,

 $G \simeq F \times G^q$

• Inspired by Camenisch, Shoup C'03 / Bresson, Catalano, Pointcheval AC'03 (03) : constructions over Paillier $(1 + N) \subset (\mathbf{Z}/N^2\mathbf{Z})^{\times}$

Class Groups

CL 0000 Threshold CL 00000000

CL(-HSM) LHE

- $\mathcal{M} = \mathbf{Z}/q\mathbf{Z}$
- KeyGen: $sk = x \stackrel{\$}{\leftarrow} \{1, \dots, B\}$ $pk \leftarrow h^x$
- Encrypt:

$$r \stackrel{\$}{\leftarrow} \{1, \dots, B\}$$

$$c = (c_1, c_2) \leftarrow (h^r, f^m p k^r)$$

Decrypt:

$$\mathsf{DL}_f(c_2/c_1^x) \rightsquigarrow m$$

•
$$c \otimes c' := (c_1 c'_1, c_2 c'_2) = (h^{r+r'}, f^{m+m'} p k^{r+r'})$$

•
$$c^{\otimes \alpha} := (c_1^{\alpha}, c_2^{\alpha}) = (h^{r\alpha}, f^{m\alpha} p k^{r\alpha})$$

C., Laguillaumie, Tucker AC'18, IND-CPA under HSM

Class Groups

CL 0000 Threshold CL •0000000

Outline

Threshold Linear Homomorphic Encryption

Class Groups

CL

Threshold CL

Works on Threshold CL and Applications

- First construction by Braun, Damgård, Orlandi, C'23
 - Pedersen-style Distributed Key Generation
 - Feldman's Verifiable Secret Sharing over Z
 - Introduced Rough Order Assumption for ZKP
 - Application to YOSO
- Application to YOSO further developed by Cascudo and David, EC'24
- Improvement by Braun, C., Damgård, Laguillaumie, Melissaris, Orlandi, Tucker, SCN'24
 - Remove a costly PoK
 - Provide an implementation

CL 0000 Threshold CL 0000000

Distributed Key Generation

CL Keygen:
$$sk = x \xleftarrow{\$} \{1, \dots, B\}$$
 $pk \leftarrow h^x$

DKG for Elgamal Pedersen EC'91

- Party *i*:
 - samples α_i
 - publishes h^{α_i}
 - acts as a Dealer for a verifiable additive secret sharing: $\alpha_i \rightsquigarrow (\alpha_{i,1}, ..., \alpha_{i,n})$
- Party *i* sums the shares received from the qualified parties: γ_i := Σ_{j∈∞} α_{j,i}
 → secret sharing of implicit sk := Σ_{i∈∞} α_i
- Set $pk := \prod_{i \in \mathscr{Q}} h^{\alpha_i}$
- Computations modulo the known order of \boldsymbol{h}

CL 0000 Threshold CL 0000000

Distributed Key Generation

CL Keygen:
$$sk = x \xleftarrow{\$} \{1, \dots, B\}$$
 $pk \leftarrow h^x$

Moving to CL

- Unknown order: computations over Z
- Use Shamir's secret sharing over **Z**: $\alpha_{i,j} := f_i(j)$
- Feldman's verification of the received shares (evaluation of f_i in the exponent)
- Weak Feldman reconstruction: Sharing α only assures to reconstruct $\bar{\alpha} \in \mathbb{Z}$ s.t. $h^{\bar{\alpha}} = h^{(n!)^2 \cdot \alpha}$

$$\rightsquigarrow$$
 implicit $sk = (n!)^2 \cdot \sum_{i \in \mathscr{Q}} \alpha_i$

- Pedersen DKG allows the adversary to bias the key: CL still IND-CPA
- Efficient ZKP using the Rough Order Assumption

CL 0000



Distributed Decryption

CL Decryption: $DL_f(c_2/c_1^{sk}) \rightsquigarrow m$

Distributed computation of c_1^x

- Qualified Party *i* computes and publishes $c_1^{(n!)^2 \cdot \gamma_i}$ (+ZKP)
- Combination of the results using Lagrange coefficient allows to get $W = c_1^{(n!)^2 \cdot sk}$
- Compute

$$\mathrm{DL}_f(c_2^{(n!)^2}/\mathrm{W}) \rightsquigarrow (n!)^2 \cdot m$$

• Defined modulo the known prime *q*

We can recover *m* !







- BICYCL Implements CryptographY in CLass groups
- C++ library C., Bouvier, Imbert, Laguillaumie, JoC'23
- Efficient implementation of exponentiations:
 - NUCOMP, NUDUPL Shanks NATO NTA'89
 - Inversion are free ~> adapt exponentiation optimizations of ECC
 - Fixed base exponentiation

Class Groups

CL 0000 Threshold CL 00000000

CL versus Paillier

Sec. level		CL	Paillier
	ciphertext	2694 bits	4096 bits
	setup	0.300 s	-
112	keygen	0.011 s	0.039 s
	encrypt	4.39 ms	6.57 ms
	decrypt	9.70 ms	6.56 ms
128	ciphertext	3509 bits	6144 bits
	setup	0.586 s	-
	keygen	0.019 s	0.121 s
	encrypt	7.68 ms	20.9 ms
	decrypt	17.8 ms	20.8 ms

Threshold CL

Threshold CL					
	n	10	100	1000	
	Dealing	24	241	17 325	
DKG	Check	63	3 609	351 540	
	Extract	7	467	46 338	
	total comp.	93	4318	415 203	
	total comm.	2	30	1 849	
	Partial Dec.	13	32	352	
Decryption	Verify	14	28	253	
	Combine	2	59	6 922	
	total comp.	29	119	7 527	
	total comm.	1	1	2	

• In ms/KB for a single party at 112 bits security with t = n/2 - 1

Class Groups

CL 0000



Threshold CL

- Ongoing "clean" implementation (better batched ZKP) by Bouvier and Combal
- Stay tuned on

https://gite.lirmm.fr/crypto/bicycl