Linear homomorphic encryption from class groups of quadratic fields

Guilhem Castagnos

Université de Bordeaux

NIST crypto reading club
June 16, 2021

+30 years of Imaginary Quadratic Fields based Crypto

Non exhaustive timeline :

+30 years of Imaginary Quadratic Fields based Crypto

Non exhaustive timeline :

Buchmann and Williams 88
Diffie Hellman Key exchange
DL in class group $C(\mathscr{O}_{\Delta_K})$

+30 years of Imaginary Quadratic Fields based Crypto

Non exhaustive timeline :

Hafner and Mc-Curley 89
Sub exponential algorithm for DL in $C(\mathcal{O}_{\Delta_K})$
and computing the class number $L_{|\Delta_K|}[1/2, 1 + o(1)]$

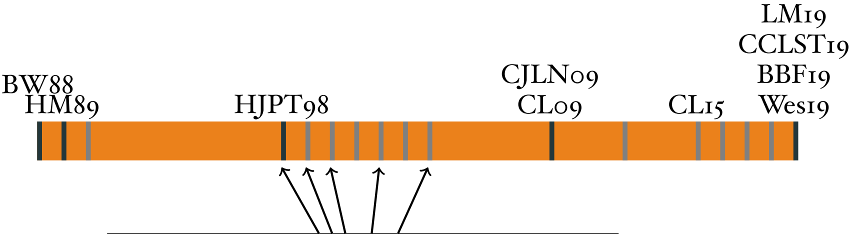
+30 years of Imaginary Quadratic Fields based Crypto

Non exhaustive timeline :

Hühnlein, Jacobson, Paulus and Takagi 98
Class groups of non maximal Orders $C(\mathcal{O}_{\Delta_q})$
$\Delta_q = q^2\Delta_k$

+30 years of Imaginary Quadratic Fields based Crypto

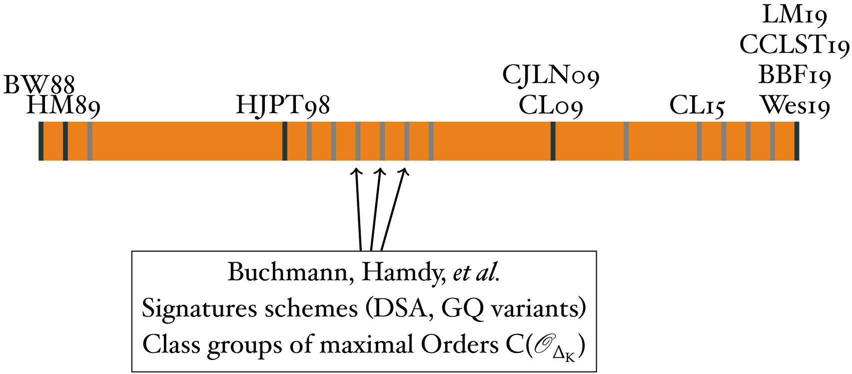
Non exhaustive timeline :



NICE family of cryptosystems
Class groups of non maximal Orders $C(\mathcal{O}_{\Delta_q})$
$\Delta_q = q^2 \Delta_k$
quadratic decryption

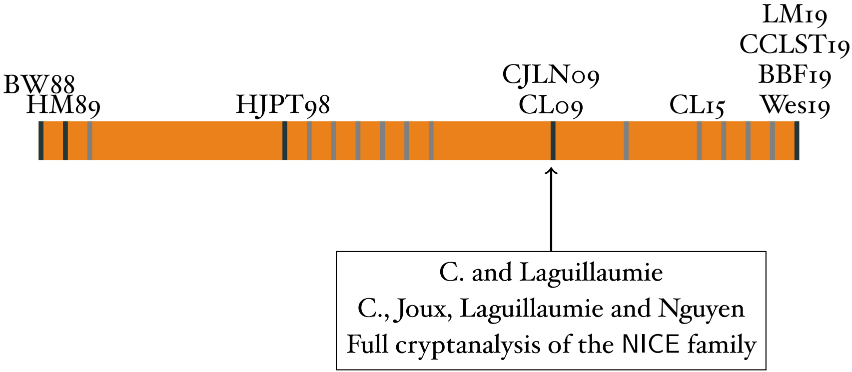
+30 years of Imaginary Quadratic Fields based Crypto

Non exhaustive timeline :



+30 years of Imaginary Quadratic Fields based Crypto

Non exhaustive timeline :



+30 years of Imaginary Quadratic Fields based Crypto

Non exhaustive timeline :

C. and Laguillaumie

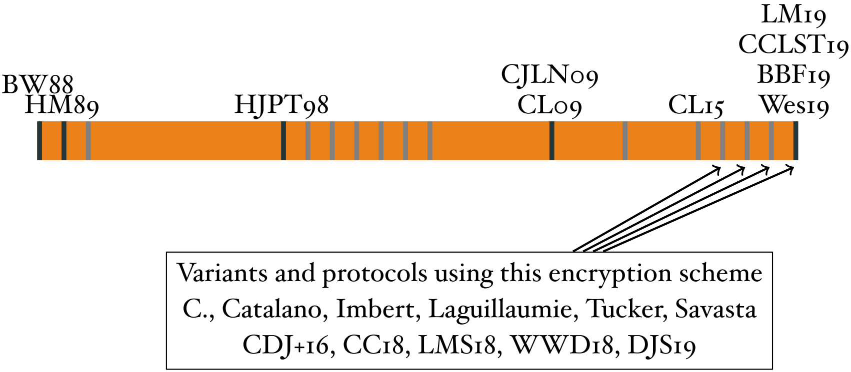
Linearly homomorphic encryption mod q

Class groups of non maximal Orders $C(\mathcal{O}_{\Delta_q})$

$$\Delta_q = -q^2(pq)$$

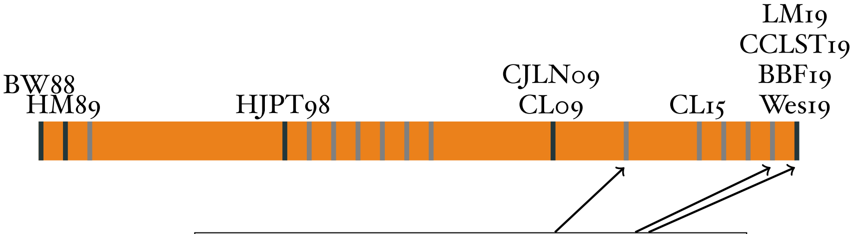
+30 years of Imaginary Quadratic Fields based Crypto

Non exhaustive timeline :



+30 years of Imaginary Quadratic Fields based Crypto

Non exhaustive timeline :



Protocols without trusted setup

Lipmaa 12, Boneh *et al.* 18, Wesolowski 19

Lai and Malavolta 19, Boneh, Bünz and Fisch 19

Class groups of maximal Orders $C(\mathcal{O}_{\Delta_K})$

Outline

Class groups of Maximal Orders of Imaginary Quadratic Fields

Cryptography in Class Groups of Maximal Orders

Class Groups of non Maximal Orders

Linearly Homomorphic Encryption modulo a prime

K and $\mathscr{O}_{\Delta_K}$

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

Ring of integers of K

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

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

Ideals

Ideals of $\mathscr{O}_{\Delta_K}$

- Fractional Ideals: $\mathfrak{a} \subset K$ such that $\exists \alpha \in K^*$, $\alpha\,\mathfrak{a}$ is an ideal of $\mathscr{O}_{\Delta_K}$
- Invertible Fractional Ideals: $\mathfrak{a}$ such that there exists $\mathfrak{b}$ such that $\mathfrak{a}\,\mathfrak{b} = \mathscr{O}_{\Delta_K}$
- Principal Fractional Ideals: $\alpha\,\mathscr{O}_{\Delta_K}$ where $\alpha \in K^*$

Notation

- $I(\mathscr{O}_{\Delta_K})$: group of Invertible Fractional Ideals of $\mathscr{O}_{\Delta_K}$
- $P(\mathscr{O}_{\Delta_K})$: sub-group of Principal Ideals

Class Group

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

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

- Equivalence relation:

$$\mathfrak{a} \sim \mathfrak{b} \iff \exists\, \alpha \in K^*,\ \mathfrak{b} = \alpha\, \mathfrak{a}$$

- Class Number: On average $h(\mathcal{O}_{\Delta_K}) \approx 0.461559\sqrt{|\Delta_K|}$

Representation of the Classes

Representation of (primitive) ideals of $\mathcal{O}_{\Delta_K}$

$$\mathfrak{a} = a\mathbf{Z} + \frac{-b+\sqrt{\Delta_K}}{2}\mathbf{Z} =: (a,b)$$

with $a \in \mathbf{N}$ and $b \in \mathbf{Z}$ such that $b^2 = \Delta_K \mod 4a$

Representation of classes of $C(\mathcal{O}_{\Delta_K})$

- (a,b) is reduced if $-a < b \leq a \leq c$ and $b \geq 0$ if $a = c$ where c is s.t. $\Delta_K = b^2 - 4ac$; moreover $a < \sqrt{|\Delta_K|/3}$
- A unique reduced ideal per class
- Representation of an element of $C(\mathcal{O}_{\Delta_K})$: same bit size as $|\Delta_K|$

Computation in $C(\mathcal{O}_{\Delta_K})$

- Product of ideals followed by reduction
- Efficient algorithms known since Gauss and Lagrange: reduction and composition of Binary Quadratic Forms
- Quadratic complexity or even quasi linear (Schönhage, 91)
- Inverse is for free: $[(a, b)]^{-1} = [(a, -b)]$

Outline

Hard Problems in Imaginary Quadratic Fields

- Computation of $h(\mathcal{O}_{\Delta_K})$, the structure of $C(\mathcal{O}_{\Delta_K})$ and DL
- Sub exponential algorithm of Hafner and Mc-Curley (1989)
- Complexity $L_{|\Delta_K|}[1/2, 1+o(1)]$
- Recent record by Beullens, Kleinjung and Vercauteren (May 2019) : structure of $C(\mathcal{O}_{\Delta_K})$ with a 512 bits $|\Delta_K|$ (52 core years)
- Bit sizes for factoring N vs computing DL in $C(\mathcal{O}_{\Delta_K})$:

Security Parameters	N	Δ_K
112	2048	1348
128	3072	1827
192	7680	3598
256	15360	5971

Biasse, Jacobson and Silvester (10)

Crypto based on DL in $C(\mathcal{O}_{\Delta_K})$

- Buchmann and Williams (88): Diffie-Hellman key exchange and ElGamal
- DSA and GQ signatures adaptations : Biehl, Buchmann, Hamdy, and Meyer (01-02)
- Düllmann, Hamdy, Möller, Pohst, Schielzeth, Vollmer (90-07): Implementation
  - Construct Δ_K a fundamental negative discriminant, in order to minimize to 2-Sylow subgroup 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 $C(\mathcal{O}_{\Delta_K})$

    $\rightsquigarrow$ order of g will be close to $h(\mathcal{O}_{\Delta_K}) \approx \sqrt{|\Delta_K|}$
  - Work in the cyclic group $G = \langle g \rangle \subset C(\mathcal{O}_{\Delta_K})$
- The order of g is unknown!

Paradox of Unknown Order 😐

- DL in a cyclic group $G = \langle g \rangle \subset C(\mathcal{O}_{\Delta_K})$ of unknown order s
- s is divisible by small primes with non negligible probability!
- But s not smooth for cryptographic sizes: no algorithm similar to the $(p-1)$ method
- Uniform sampling in G possible with an upper bound on $h(\mathcal{O}_{\Delta_K}) \geqslant s$
- Can not decide if an element of $C(\mathcal{O}_{\Delta_K})$ is in G

Paradox of Unknown Order 😎

- Cryptographic accumulators (Lipmaa 12), verifiable delay functions (Wesolowski 19), and many others applications without trusted setup
- Example of verifiable delay functions:
  - Slow to compute and easy to verify
  - Based on computing g^{2^t} without knowing the order of g
  - RSA based construction: someone knows $\varphi(n)$! Needs some trusted setup.
  - With class groups, $h(\mathscr{O}_{\Delta_K})$ is really unknown to anyone!
- Another application: linearly homomorphic encryption modulo a prime.

Outline

Class groups of Maximal Orders of Imaginary Quadratic Fields

Cryptography in Class Groups of Maximal Orders

Class Groups of non Maximal Orders

Linearly Homomorphic Encryption modulo a prime

Imaginary Quadratic Orders

Definition

- $K = \mathbf{Q}(\sqrt{\Delta_K})$,
- $\mathscr{O}$ is a subring of K containing 1 and $\mathscr{O}$ is a free $\mathbf{Z}$-module of rank 2

Characterisation

- $\mathscr{O}_{\Delta_K}$: ring of integers of K is the maximal order
- $\mathscr{O} \subset \mathscr{O}_{\Delta_K}$, $\ell := [\mathscr{O}_{\Delta_K} : \mathscr{O}]$ is the conductor,

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

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

Can extend the definition of class groups: $C(\mathscr{O}_{\Delta_\ell})$

Class Groups of Non Maximal Orders

- $\Delta_\ell := \ell^2 \Delta_K$
- There exists a surjection

$$\bar{\varphi}_\ell \ : \ C(\mathcal{O}_{\Delta_\ell}) \twoheadrightarrow C(\mathcal{O}_{\Delta_K})$$

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

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

NICE Family

- Paulus Takagi 98: crypto with non maximal orders
- $\Delta_K = -p$, $\Delta_q = -pq^2$, p, q primes and $p \equiv 3 \pmod 4$

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

- Public key: Δ_q and $h \in \ker \bar{\varphi}_q$, with $\bar{\varphi}_q : C(\mathcal{O}_{\Delta_q}) \to C(\mathcal{O}_{\Delta_K})$
- Secret key: q
- Cryptanalysis : C., Joux, Laguillaumie, Nguyen (09):
  - Each class of $\ker \bar{\varphi}_q$ contains a non reduced ideal (q^2, kq)
  - From $h \in \ker \bar{\varphi}_q$, we find this ideal in polynomial time

A Subgroup with an Easy DL

- C. Laguillaumie 15
- $\Delta_K = -pq$, $\Delta_q = -pq^3$, p, q primes and $pq \equiv 3 \pmod 4$

$$h(\mathcal{O}_{\Delta_q}) = h(\mathcal{O}_{\Delta_K}) \times q$$

- Let $f = [(q^2, q)] \in C(\mathcal{O}_{\Delta_q})$
- $F = \langle f \rangle$ is of order q, and

$$f^m = [(q^2, -L(m)q)]$$

where $L(m) \in [-q, q]$ is odd and $L(m) \equiv m^{-1} \pmod q$

- Moreover if $p > 4q$, the ideals of norm q^2 are reduced

Generation of a group with an easy DL subgroup

- q a prime
- $p > 4q$, $\Delta_K = -pq$, $\Delta_q = -pq^3$, with $pq \equiv -1 \pmod 4$ and $(p/q) = -1$

$$h(\mathcal{O}_{\Delta_q}) = h(\mathcal{O}_{\Delta_K}) \times q$$

  we assume that $\gcd(q, h(\mathcal{O}_{\Delta_K})) = 1$
- Let $\widehat{G}$ be the subgroup of squares of $C(\mathcal{O}_{\Delta_q})$
- $g_q = r^q$ where r is a random element of $\widehat{G}$
- $f = [(q^2, q)] \in \widehat{G}$
- $g = g_q f, G = \langle g \rangle, F = \langle f \rangle, G^q = \langle g_q \rangle$

$$G \simeq F \times G^q$$

  DL easy in F, G^q has unknown order s a divisor of $h(\mathcal{O}_{\Delta_K})$

Outline

Class groups of Maximal Orders of Imaginary Quadratic Fields

Cryptography in Class Groups of Maximal Orders

Class Groups of non Maximal Orders

Linearly Homomorphic Encryption modulo a prime

Framework

Group with an easy discrete logarithm (DL) subgroup

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

$$\mathrm{G} \simeq \mathrm{F} \times \mathrm{G}^q$$

- DL is easy in F:

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

Framework

Group with an easy discrete logarithm (DL) subgroup

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

$$\mathrm{G} \simeq \mathrm{F} \times \mathrm{G}^q$$

- Hard to distinguish elements of G^q:

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

Hard Subgroup Membership Assumption (HSM)

Framework

Group with an easy discrete logarithm (DL) subgroup

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

$$\mathrm{G} \simeq \mathrm{F} \times \mathrm{G}^q$$

- Inspired by Bresson, Catalano, Pointcheval / Camenisch, Shoup (2003) : constructions over Paillier

A Generic Linearly Homomorphic Encryption Scheme

- $\mathscr{M} = \mathbf{Z}/q\mathbf{Z}$
- KeyGen:

  $sk = x \hookleftarrow \mathscr{D}$

  $pk = h \leftarrow g_q^x$
- Encrypt:

  $r \hookleftarrow \mathscr{D}$

  $c = (c_1, c_2) \leftarrow (g_q^r, f^m h^r)$
- Decrypt:

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

- EvalSum:

  $$(c_1 c_1', c_2 c_2') = (g_q^{r+r'}, h^{r+r'} f^{m+m'})$$
- EvalScal:

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

C., Laguillaumie, Tucker (2018)

Indistinguishability à la Cramer Shoup under HSM

$$c = (c_1, c_2) = \left(g_q^r \;, f^m \; h^r \right), \quad h = g_q^x, \quad x, r \hookleftarrow \mathcal{D}$$

Indistinguishability à la Cramer Shoup under HSM

$$c = (c_1, c_2) = \left(g_q^r \, , f^m \boxed{h^r} \right), \quad h = g_q^x, \quad x, r \hookleftarrow \mathscr{D}$$

Indistinguishability à la Cramer Shoup under HSM

$$c = (c_1, c_2) = \left(g_q^r \ , f^m \ c_1^x \right), \quad h = g_q^x, \quad x, r \hookleftarrow \mathscr{D}$$

Compute c with the secret key

Indistinguishability à la Cramer Shoup under HSM

$$c = (c_1, c_2) = \left(\boxed{g_q^r}, f^m \boxed{c_1^x} \right), \quad h = g_q^x, \quad x, r \hookleftarrow \mathscr{D}$$

Indistinguishability à la Cramer Shoup under HSM

$$c = (c_1, c_2) = \left(\mathrm{Z}\ , f^m\ \mathrm{Z}^x \right), \quad h = g_q^x, \quad x \hookleftarrow \mathscr{D}, \quad \mathrm{Z} \hookleftarrow \mathrm{G}^q$$

Use $\mathrm{Z} \hookleftarrow \mathrm{G}^q$ for c_1

Indistinguishability à la Cramer Shoup under HSM

$$c = (c_1, c_2) = \left(\boxed{Z}, f^m \boxed{Z^x}\right), \quad h = g_q^x, \quad x \hookleftarrow \mathscr{D}, \quad \boxed{Z \hookleftarrow G^q}$$

Indistinguishability à la Cramer Shoup under HSM

$$c = (c_1, c_2) = \Big(\mathrm{Z} \,, f^m \, \mathrm{Z}^x \Big), \quad h = g_q^x, \quad x \hookleftarrow \mathscr{D}, \qquad \mathrm{Z} \hookleftarrow \mathrm{G}$$

Under the HSM assumption, replace by $\mathrm{Z} \hookleftarrow \mathrm{G}$

Indistinguishability à la Cramer Shoup under HSM

$$c = (c_1, c_2) = \left(Z , f^m Z^x \right), \quad h = g_q^x, \quad x \hookleftarrow \mathscr{D}, \quad Z \hookleftarrow G$$

Smoothness argument:

- $\mathscr{D}$ close to uniform modulo qs and $\gcd(q, s) = 1$:
  (x mod s) fixed by h but (x mod q) remains uniformly distributed
- $Z = f^a Y$ for some fixed $a \in \mathbf{Z}/q\mathbf{Z}, Y \in G^q$

$$c_2 = f^m Z^x = f^{m+ax} Y^x$$

$\rightsquigarrow m$ is hidden!

Application: Two-Party ECDSA Signing

ECDSA

- Used to sign Bitcoin ₿ transactions
- Stealing signing key $x \rightsquigarrow$ immediate financial loss

- Public params: $(\mathbb{G}, +)$, of prime order q, with generator P
- Secret Key: $x \hookleftarrow \mathbf{Z}/q\mathbf{Z}$ and Public Key: $\mathrm{Q} \leftarrow x \cdot \mathrm{P}$

Application: Two-Party ECDSA Signing

ECDSA

- Used to sign Bitcoin transactions
- Stealing signing key $x \rightsquigarrow$ immediate financial loss

- Public params: $(\mathbb{G}, +)$, of prime order q, with generator P
- Secret Key: $x \hookleftarrow \mathbf{Z}/q\mathbf{Z}$ and Public Key: $\mathrm{Q} \leftarrow x \cdot \mathrm{P}$

Two-Party ECDSA

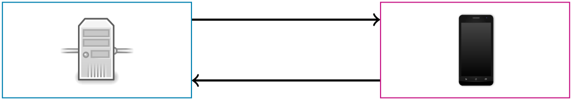
Application: Two-Party ECDSA Signing

ECDSA

- Used to sign Bitcoin transactions
- Stealing signing key $x \rightsquigarrow$ immediate financial loss

- Public params: $(\mathbb{G}, +)$, of prime order q, with generator P
- Secret Key: $x \hookleftarrow \mathbf{Z}/q\mathbf{Z}$ and Public Key: $\mathrm{Q} \leftarrow x \cdot \mathrm{P}$

Two-Party ECDSA



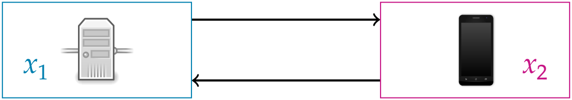
Application: Two-Party ECDSA Signing

ECDSA

- Used to sign Bitcoin transactions
- Stealing signing key $x \rightsquigarrow$ immediate financial loss

- Public params: $(\mathbb{G}, +)$, of prime order q, with generator P
- Secret Key: $x \hookleftarrow \mathbf{Z}/q\mathbf{Z}$ and Public Key: $\mathrm{Q} \leftarrow x \cdot \mathrm{P}$

Two-Party ECDSA



x_1, x_2: shares of x ; Public Key: $\mathrm{Q} \leftarrow x \cdot \mathrm{P}$

Application: Two-Party ECDSA Signing

ECDSA

- Used to sign Bitcoin transactions
- Stealing signing key $x \rightsquigarrow$ immediate financial loss

- Public params: $(\mathbb{G}, +)$, of prime order q, with generator P
- Secret Key: $x \hookleftarrow \mathbf{Z}/q\mathbf{Z}$ and Public Key: $\mathrm{Q} \leftarrow x \cdot \mathrm{P}$

Two-Party ECDSA

m to be signed

x_1 

 x_2

x_1, x_2: shares of x ; Public Key: $\mathrm{Q} \leftarrow x \cdot \mathrm{P}$

Application: Two-Party ECDSA Signing

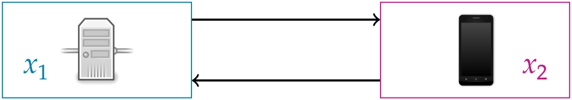
ECDSA

- Used to sign Bitcoin transactions
- Stealing signing key $x \rightsquigarrow$ immediate financial loss

- Public params: $(\mathbb{G}, +)$, of prime order q, with generator P
- Secret Key: $x \hookleftarrow \mathbf{Z}/q\mathbf{Z}$ and Public Key: $Q \leftarrow x \cdot P$

Two-Party ECDSA

m to be signed



x_1, x_2: shares of x ; Public Key: $Q \leftarrow x \cdot P$

Application: Two-Party ECDSA Signing

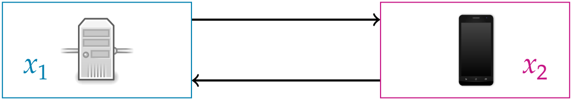
ECDSA

- Used to sign Bitcoin transactions
- Stealing signing key $x \rightsquigarrow$ immediate financial loss

- Public params: $(\mathbb{G}, +)$, of prime order q, with generator P
- Secret Key: $x \hookleftarrow \mathbf{Z}/q\mathbf{Z}$ and Public Key: $\mathrm{Q} \leftarrow x \cdot \mathrm{P}$

Two-Party ECDSA

m to be signed



σ signature of m

x_1, x_2: shares of x ; Public Key: $\mathrm{Q} \leftarrow x \cdot \mathrm{P}$

Difficulty and some Previous works

Unfriendly Equation in ECDSA

$$s \leftarrow k^{-1} \cdot (\mathrm{H}(m) + r \cdot x) \bmod q$$

Lindell (2017)

- Uses Paillier Linearly homomorphic encryption
- Homomorphic mod N an RSA integer (2048 bits)
- ECDSA uses operations mod q (256 bits)
- Drawbacks: Costly range proof, loss in reduction or interactive assumption

Our Two-Party ECDSA Protocol

- C., Catalano, Laguillaumie, Savasta, Tucker (2019)
- Use a linearly homomorphic encryption scheme mod q

  $\rightsquigarrow$ Remove the range proof and some technicalities
- Construction à la Cramer-Shoup: can use an argument based on indistinguishability even if the simulation knows the secret key

  $\rightsquigarrow$ Tight security without *interactive* assumptions
- Better bandwidth and speed (for high level of security)

Comparison: Primitives

- Paillier

Sec. Param.	N (b)	Expo in $\mathbf{Z}/N^2\mathbf{Z}$ (ms)	Ciphertext (b)
112	2048	7	4096
128	3072	22	6144
192	7680	214	15360
256	15360	1196	30720

- C.-Laguillaumie

Sec. Param.	Δ_K (b)	Expo in $C(\mathcal{O}_{\Delta_q})$ (ms)	Ciphertext (b)
112	1348	32	3144
128	1827	55	4166
192	3598	212	7964
256	5971	623	12966

Timings with Pari C Library

Comparison: Two-Party ECDSA

- Lindell

Curve	Sec.	KeyGen (s)	Sign (s)	KeyGen (kb)	Sign (kb)
P-256	128	6.3	0.049	1 317	7.7
P-384	192	65	0.437	3 280	17.7
P-521	256	429	2.4	6 549	33.8

- C. Catalano, Laguillaumie, Savasta, Tucker

Curve	Sec.	KeyGen (s)	Sign (s)	KeyGen (kb)	Sign (kb)
P-256	128	9.3	0.17	227	5.7
P-384	192	35	0.64	427	10.2
P-521	256	103	1.8	688	16.1

Timings with Pari C Library

Questions?