The Decisional Diffie-Hellman problem for class group actions

Jana Sotáková

QuSoft

June 12, 2020

Joint work with Wouter Castryck and Frederik Vercauteren

Diffie-Hellman using groups

Alice and Bob wish to establish a shared secret over an insecure channel.

They agree on a group G and an element $g \in G$ that generates a multiplicative subgroup of size N.

Alice

- $a \leftarrow \mathbb{Z}/N\mathbb{Z}$
- computes g^a
- receives g^b
- computes $(g^b)^a$

insecure channel

- G, g of order N
- $\xleftarrow{g^b}$ $\xrightarrow[g^a]{}$

Bob

- $b \leftarrow \mathbb{Z}/N\mathbb{Z}$
- computes g^b
- receives g^a
- computes $(g^a)^b$

So both Alice and Bob share g^{ab}.

Assumptions for the Diffie-Hellman exchange

Cyclic group $G = \langle g \rangle$ generated by an element of order n and $a, b, c \in \mathbb{Z}/N$.

Secret keys (discrete logarithm problem)

If the adversary sees (G, g, g^a), she should not be able to compute a.

Intercepted transcript (computational Diffie-Hellman assumption)

If the adversary sees the transcript of the conversation (G, g, g^a, g^b), she should not able to compute the shared value g^{ab}.

Shared secret (decisional Diffie-Hellman)

The adversary cannot distinguish between (G, g, g^a, g^b, g^{ab}) and (G, g^a, g^b, g^c) for $a, b, c \xleftarrow{\$} \mathbb{Z}/N$.

Some (polynomial) reductions

We have a cyclic group $G = \langle g \rangle$ of prime order N:

- discrete logarithm: $(g, g^a) \to a$,
- computational Diffie-Hellman: $(g, g^a, g^b) \to g^{ab}$,
- decisional Diffie-Hellman: $(g, g^a, g^b, g^c) \to ab \stackrel{?}{=} c$ in $\mathbb{Z}/N$.

Reductions independent of the group G:

- CDH implies DLP (compute a, b from g^a, g^b and then compute g^{ab}) ,
- DDH implies DLP (compute a, b, c from g^a, g^b, g^c and compare $ab \stackrel{?}{=} c$),
- DDH implies CDH (compute g^{ab} from g^a, g^b and compare $g^{ab} \stackrel{?}{=} g^c$).

Other reductions:

- DLP implies CDH if $N - 1$ is smooth [Den Boer],
- DLP implies CDH if there exist suitable elliptic curve over $\mathbb{F}_N$ [Maurer-Wolf],
- CDH does not imply DDH: there are group for which DDH is easy (pairings of elliptic curves).

Where do we see these assumptions

We have a cyclic group $G = \langle g \rangle$ of prime order N:

- discrete logarithm: $(g, g^a) \to a$,
- computational Diffie-Hellman: $(g, g^a, g^b) \to g^{ab}$,
- decisional Diffie-Hellman: $(g, g^a, g^b, g^c) \to ab \stackrel{?}{=} c$.

1. The discrete logarithm problem is the most natural mathematically, so a lot of effort into breaking DLP.
2. CDH is the 'advertised' assumption for DH-based protocols, e.g. ECDH,
3. CDH ony guarantees 1 'hardcore' bit that is not predictable:
   if we want g^{ab} to look random to the attacker, we need DDH,
4. DDH used in ElGamal encryption, Cramer-Shoup cryptosystem, signatures, ...,
5. DDH in a group of size $N > 2^n$ gives g^{ab} with n bits of computational entropy, hashing produces random-looking strings.

And Shor's algorithm breaks DLP in cyclic groups.

Group actions

Commutative group G and $G \times X \to X$ be a free and transitive group action:

$$(g, x) \mapsto g \star x.$$

- group action: $g \star (h \star x) = (g \cdot h) \star x$ for any $g, h \in G$ and $x \in X$.
- free and transitive: for any $x, x' \in X$ there exists a unique $g \in G$:

$$x' = g \star x.$$

transport of structure from the group G to a set X.

Group-action based cryptography: secrets=computing in the group G, public = points of X

Diffie-Hellman	Group action Diffie-Hellman
cyclic group G	group G acting on a set X
choose generator g of order n	choose a starting point $x \in X$
sample random $a, b \in \mathbb{Z}/n$	sample random $g_a, g_b \in G$
exchange g^a, g^b	exchange $g_a \star x, g_b \star x$
compute $(g^a)^b = g^{ab} = (g^b)^a$	$g_b \star (g_a \star x) = (g_a \cdot g_b) \star x = g_a \star (g_b \star x)$

Non-example

Textbook Diffie-Hellman

We have a cyclic group $G = \langle g \rangle$ of prime order N.

The group $\mathrm{Aut}(G) \cong (\mathbb{Z}/N\mathbb{Z})^\times$ acts on the set $X = \{g, g^2, g^3, \ldots, g^{N-1}\}$ by

$$a \star g = g^a.$$

$$a \star (b \star g) = a \star (g^b) = g^{ab} = (ab) \star g$$

Problem: X still has too much structure:

Indeed, $X \subset G$ so we can still multiply elements of X:

$$(a \star g) \cdot (b \star g) = g^a \cdot g^b = g^{a+b} \in G$$

Group actions in isogeny-based cryptography

Setting of [C'06, RS'06, DKS'18, CSIDH, CSURF]:

- group: class group $\mathrm{Cl}(\mathcal{O})$ of an order $\mathcal{O}$ in an imaginary quadratic field,
- set: elliptic curves defined over a finite field $\mathbb{F}_q$ with CM by $\mathcal{O}$.

First we choose an order:

$$\mathcal{O} = \mathbb{Z}[\pi] = \{a + b\pi : a, b \in \mathbb{Z}\}$$

for some π satisfying

$$\pi^2 - t\pi + q = 0 \qquad \text{with } \ t, q \in \mathbb{Z} \text{ and } t^2 - 4q. < 0$$

The elliptic curves:

$$E : y^2 = x^3 + ax + b, \qquad a, b \in \mathbb{F}_q \quad \text{and } 4a^3 + 27b^2 \neq 0$$

satisfying

$$\#E(\mathbb{F}_q) = 1 + \#\{(u, v) \in \mathbb{F}_q \times \mathbb{F}_q : v^2 = u^3 + au + b\} = 1 - t + q.$$

Endomorphism rings

$\mathcal{O} = \mathbb{Z}[\pi]$ and $\pi^2 - t\pi + q = 0$ and elliptic curves E such that $\#E(\mathbb{F}_q) = 1 - t + q$.

Elliptic curves give finite abelian groups $E(\mathbb{F}_q)$.

Isogenies: homomorphisms of elliptic curves $\varphi : E \to E'$ as abelian groups, given by rational maps

$$(x, y) \mapsto (f(x, y), g(x, y)) \qquad \text{for } f, g \in \mathbb{F}_q(x, y)$$

We want elliptic curves such that

$$\mathcal{O} \cong \mathrm{End}(E) = \{\text{isogenies } \varphi : E \to E\}$$

Denote the set of such elliptic curves (up to $\mathbb{F}_q$-isomorphism) $\mathcal{E}\ell\ell_q(\mathcal{O}, t)$.

What is the relationship between $\mathcal{E}\ell\ell_q(\mathcal{O}, t)$ a $\mathcal{O}$?

1. For any $E, E' \in \mathcal{E}\ell\ell_q(\mathcal{O}, t)$, any isogeny $\varphi : E \to E'$ corresponds to an ideal $\mathfrak{a} \subset \mathcal{O}$ and vice versa.
2. The principal ideals $(\alpha) \subset \mathcal{O}$ correspond to endomorphisms $\varphi : E \to E$.

ℓ-isogenies

$\mathcal{O} = \mathbb{Z}[\pi]$ and $\pi^2 - t\pi + q = 0$ and $\mathcal{E}\ell\ell_q(\mathcal{O}, t)$ is the set of elliptic curves E such that $\#E(\mathbb{F}_q) = 1 - t + q$.

What is an isogeny corresponding to an ideal?

Modern setting

Only need isogenies corresponding to ideals $\mathfrak{a} = (\ell, \pi - 1)$ for primes $\ell || 1 - t + q$:

- We have $\ell | \#E(\mathbb{F}_q)$ but $\ell^2 \nmid \#E(\mathbb{F}_q)$,
- there is a unique cyclic subgroup $H \subset E(\mathbb{F}_q)$ of order ℓ,
- the isogeny $\varphi : E \to E'$ is the one given by the group homomorphism $E \to E/H$.

Description of $H \longrightarrow$ reconstruct the rational maps in $O(\sqrt{\ell})$.

Main advantage

This description does not need any ideals $\mathfrak{a} \subset \mathcal{O}$, only ℓ-torsion points for $\ell | \#E(\mathbb{F}_q)$.

All other isogenies are given by sequences of isogenies

$$E_1 \overset{\varphi_1}{\to} E_2 \ldots E_n \overset{\varphi_n}{\to} E_{n+1}$$

where φ_i are constructed as above (+ small technical details).

Zoology of proposals

$\mathcal{O} = \mathbb{Z}[\pi]$ and $\pi^2 - t\pi + q = 0$ and $\mathcal{E}\ell\ell_q(\mathcal{O}, t)$ is the set of elliptic curves E such that $\#E(\mathbb{F}_q) = 1 - t + q$.

The class group $\mathrm{Cl}(\mathcal{O})$ acts on $\mathcal{E}\ell\ell_q(\mathcal{O}, t)$ via $([\mathfrak{a}], E) \mapsto a \star E$.

Proposals differ in choosing q and t.

- [C'06, RS'06] allow ordinary $(t \neq 0)$ elliptic curves over $\mathbb{F}_q$, any t and $\mathcal{O}$.
- [DKS'18] use ordinary elliptic curves over a prime field $\mathbb{F}_p$ with $\#E(\mathbb{F}_p) = q + 1 - t$ divisible by lots of small primes, eg. with points of order ℓ for every

$$\ell \in \{3, 5, 7, 11, 13, 17, 103, 523, 821, 947, 1723\}.$$

- CSIDH [BLMPR'18] uses supersingular elliptic curves $(t = 0)$ over $\mathbb{F}_p$ with $p \equiv 3 \bmod 8$, order $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ and $\#E(\mathbb{F}_p) = p + 1$ divisible by lots of small primes, e.g.

$$p = 4 \cdot 3 \cdot 5 \cdot \ldots \cdot 373 \cdot 587 - 1$$

- CSURF [DW'19] uses supersingular elliptic curves over $\mathbb{F}_p$ with $p \equiv 7 \bmod 8$, order $\mathcal{O} = \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$ and $\#E(\mathbb{F}_p) = p + 1$ divisible by lots of small primes, e.g.

$$p = 8 \cdot 3^2 \cdot \ldots \cdot \widehat{347} \cdot \ldots \cdot \widehat{359} \cdot \ldots \cdot 389 - 1$$

Complex multiplication

$\mathcal{O} = \mathbb{Z}[\pi]$ and $\pi^2 - t\pi + q = 0$ and $\mathcal{E}\ell\ell_q(\mathcal{O}, t)$ is the set of elliptic curves E such that $\#E(\mathbb{F}_q) = 1 - t + q$.

Theorem (Main theorem of complex multiplication)

For the order $\mathcal{O}$ and elliptic curves $\mathcal{E}\ell\ell_q(\mathcal{O}, t)$, consider the mapping

$$\begin{aligned} (\{\text{ideals of } \mathcal{O}\},\ \mathcal{E}\ell\ell_q(\mathcal{O}, t)) &\to \mathcal{E}\ell\ell_q(\mathcal{O}, t) \\ (\mathfrak{a}, E) &\longmapsto E' \end{aligned}$$

where $\varphi : E \to E'$ is the isogeny corresponding to $\mathfrak{a}$. This mapping factors though the classgroup $\mathrm{Cl}(\mathcal{O})$ and induces a free and transitive action

$$\begin{aligned} \mathrm{Cl}(\mathcal{O}) \times \mathcal{E}\ell\ell_q(\mathcal{O}, t) &\longrightarrow \mathcal{E}\ell\ell_q(\mathcal{O}, t) \\ ([\mathfrak{a}], E) &\longmapsto [\mathfrak{a}] \star E. \end{aligned}$$

So we finally have a group $\mathrm{Cl}(\mathcal{O})$ acting on a set $\mathcal{E}\ell\ell_q(\mathcal{O}, t)$ freely and transitively.

Assumptions for the group action Diffie-Hellman

$\mathcal{O} = \mathbb{Z}[\pi]$ and $\pi^2 - t\pi + q = 0$ and $\mathcal{E}\ell\ell_q(\mathcal{O}, t)$ is the set of elliptic curves E such that $\#E(\mathbb{F}_q) = 1 - t + q$.

The class group $\mathrm{Cl}(\mathcal{O})$ acts on $\mathcal{E}\ell\ell_q(\mathcal{O}, t)$ via $([\mathfrak{a}], E) \mapsto a \star E$.

Group action Diffie-Hellman	Commutative isogeny schemes
group G acting on a set X	class group $\mathrm{Cl}(\mathcal{O})$ acting on $\mathcal{E}\ell\ell_q(\mathcal{O}, t)$
choose a starting point $x \in X$	choose starting curve, e.g. $E : y^2 = x^3 + x$
sample random $g_a, g_b \in G$	sample random $[\mathfrak{a}], [\mathfrak{b}], \xleftarrow{\$} \mathrm{Cl}(\mathcal{O})$
exchange $g_a \star x, g_b \star x$	exchange $[\mathfrak{a}] \star E, [\mathfrak{b}] \star E$

Vectorization/Group Action Inverse Problem (discrete logarithm problem)

If the adversary sees $(E, [\mathfrak{a}] \star E)$, she should not be able to compute $[a]$.

Parallelization (computational Diffie-Hellman assumption)

If the adversary sees the transcript of the conversation $(E, [\mathfrak{a}] \star E, [\mathfrak{b}] \star E)$, she should not able to compute the shared value $[\mathfrak{a}\mathfrak{b}] \star E$.

Decisional Diffie-Hellman (decisional Diffie-Hellman)

The adversary cannot distinguish between $(E, [\mathfrak{a}] \star E, [\mathfrak{b}] \star E, [\mathfrak{a}\mathfrak{b}] \star E)$ and $(E, [\mathfrak{a}] \star E, [\mathfrak{b}] \star E, [\mathfrak{c}] \star E)$ for $[\mathfrak{a}], [\mathfrak{b}], [\mathfrak{c}] \xleftarrow{\$} \mathrm{Cl}(\mathcal{O})$.

Decisional Diffie-Hellman problem

$\mathcal{O} = \mathbb{Z}[\pi]$ and $\pi^2 - t\pi + q = 0$ and $\mathcal{E}\ell\ell_q(\mathcal{O}, t)$ is the set of elliptic curves E such that $\#E(\mathbb{F}_q) = 1 - t + q$.

The class group $\mathrm{Cl}(\mathcal{O})$ acts on $\mathcal{E}\ell\ell_q(\mathcal{O}, t)$ via $([\mathfrak{a}], E) \mapsto a \star E$.

Castryck-S.-Vercauteren

The group action $E \mapsto [\mathfrak{a}] \star E$ does not hide the group perfectly.

There are (well-understood) quadratic characters

$$\chi : \mathrm{Cl}(\mathcal{O}) \longrightarrow \{\pm 1\}.$$

We show how to

compute $\chi([\mathfrak{a}])$ directly from the elliptic curves $E, E' = [\mathfrak{a}] \star E$,

without knowing $[\mathfrak{a}]$ or even without knowing anything about the class group.

Breaking DDH for class group actions

Given a tuple of elliptic curves, decide whether they are a 'Diffie-Hellman' sample:

$$(E, [\mathfrak{a}] \star E, [\mathfrak{b}] \star E, [\mathfrak{c}] \star E) \longrightarrow [\mathfrak{a}\mathfrak{b}] \stackrel{?}{=} [\mathfrak{c}]$$

We always have $\chi([\mathfrak{a}\mathfrak{b}]) = \chi([\mathfrak{a}]) \cdot \chi([\mathfrak{b}])$. So, for a DH tuple, we always have $\chi([\mathfrak{a}]) \cdot \chi([\mathfrak{b}]) = \chi([\mathfrak{c}])$; for a random $[\mathfrak{c}]$ this holds* with probability $1/2$.

When does our attack work?

$\mathcal{O} = \mathbb{Z}[\pi]$ and $\pi^2 - t\pi + q = 0$ and $\mathcal{E}\ell\ell_q(\mathcal{O}, t)$ is the set of elliptic curves E such that $\#E(\mathbb{F}_q) = 1 - t + q$.
The class group $\mathrm{Cl}(\mathcal{O})$ acts on $\mathcal{E}\ell\ell_q(\mathcal{O}, t)$ via $([\mathfrak{a}], E) \mapsto a \star E$.

We need non-trivial characters

From the tuple $(E, [\mathfrak{a}] \star E, [\mathfrak{b}] \star E, [\mathfrak{c}] \star E)$ we compute $\chi([\mathfrak{a}]), \chi([\mathfrak{b}])$ and $\chi([\mathfrak{c}])$ and check

$$\chi([\mathfrak{c}]) \stackrel{?}{=} \chi([\mathfrak{a}]) \cdot \chi([\mathfrak{b}]) = \chi([\mathfrak{a}\mathfrak{b}]).$$

There exist non-trivial characters for a density 1 of orders $\mathcal{O}$ and there is a character computable in time polynomial in $\log q$ if and only if there is a small divisor of $t^2 - 4q$.

This attack works

1. for ordinary curves [C'06, RS'06, DKS'18]: whenever $\# \mathrm{Cl}(\mathcal{O})$ is even and there is a small odd divisor of $\mathrm{disc}(\mathcal{O})$, which is (heuristically) a density 1 set of orders $\mathcal{O}$. In praticular, it works for all setups proposed in [DKS'18],
2. for supersingular curves: whenever $p \equiv 1 \bmod 4$. This is not the case for CSIDH or CSURF (they use $p \equiv 3 \bmod 4$).

Thank you!

eprint: 2020/151
Breaking the decisional Diffie-Hellman problem for class group actions using genus theory
Wouter Castryck and Jana Sotáková and Frederik Vercauteren
https://eprint.iacr.org/2020/151