Breaking the Decisional Diffie-Hellman problem for class group actions

Jana Sotáková

QuSoft

April 17, 2020

Joint work with Wouter Castryck and Frederick Vercauteren

The textbook Diffie-Hellman exchange

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

They agree to on a prime $p = 1009$ and a number $g = 515$.

There are $n = 252$ different powers of $g = 515$ modulo $p = 1009$: $515, 867, 527, 993, 841, 254, 649, 256, 670, \ldots$

Alice	insecure channel	Bob
	$p = 1009$, $g = 515$, $n = 252$	
► $113 \leftarrow \mathbb{Z}/252\mathbb{Z}$		► $89 \leftarrow \mathbb{Z}/252\mathbb{Z}$
► $515^{113} \pmod{1009} = 402$	$\xleftarrow{735}$	► $735^{89} \pmod{1009} = 735$
► receives 735	$\xrightarrow[402]{}$	► receives 402
► $735^{113} \pmod{1009} = 663$.		► $402^{89} \bmod 1009 = 663$.

So Alice and Bob now share the value 663.

Diffie-Hellman using groups

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

They agree to on a group G and an element $g \in G$ that generates a multiplicative subgroup of size n.
(We had $G = (\mathbb{Z}/1009\mathbb{Z})^{\times}$, $g = 515$ and $n = 252$.)

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

Important assumption (discrete logarithm assumption)

The adversary should not be able to compute the secret keys, that is, if she knows (G, g, g^a), she should not be able to compute a.

But the shared value is g^{ab}.

Actual assumption (computational Diffie-Hellman)

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

Decisional Diffie-Hellman assumption

- How much of a secret g^{ab} actually is?
- Ideally, g^{ab} is indistinguishable from a random element/string.

Decisional Diffie-Hellman problem

Suppose you are given a tuple (g, g^a, g^b, g^c), can you determine whether $g^c = g^{ab}$?

More precisely, you are given (g, g^a, g^b, g^c) where c is random with probability $1/2$ and $c = ab$ with probability $1/2$. Can you tell in which situation you are?

DDH assumption

No computationally bounded adversary can succeed with a significantly better success rate than a random guess.

How secure is the Diffie-Hellman key exchange?

Let G be an abelian group used in cryptography nowadays, e.g. a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ or of an elliptic curve over a finite field.

Shor's attack on the discrete logarithm problem

If the attacker sees (G, g, g^a), she can compute a in quantum polynomial time.

Then it is easy to solve DDH (or CDH): from (g, g^a, g^b, g^c) compute a, b, c and check whether $ab = c$ (or compute (g^{ab}).

A workaround

Using group actions, we represent the group by a set.

Example: Affine spaces

The affine space A is acted on by its vector space V:

$$A \times V \mapsto A \qquad (a, v) \mapsto a + v$$

1. (action) for any vectors $v, v' \in V$ and point $a \in A$, we have

$$(a + v) + v' = a + (v + v'),$$

2. (free action) for every vectors $v, v' \in V$ and a point $a \in A$, if

$$a + v = a + v' \longrightarrow v = v',$$

3. (transitive action) for every $a, a' \in A$ there is $v \in V$ such that

$$a + v = a'.$$

Hiding structure

Affine space

By choosing an origin $a \in A$, there is a bijection $A \cong V$:
write every $a' \in A$ as $a' = a + v$ for some $v \in V$, then

$$a' = a + v \longmapsto v \in V.$$

So affine spaces $\approx$ vector spaces before the choice of an origin.

Diffie-Hellman exchange from group actions

'Diffie-Hellman' from group actions

Let $G \times X \to X$ be a (transitive, free) group action by a commutative group G:

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

We choose a point $y \in X$. Then Alice can choose a random $a \in G$ and compute $a \star y$, Bob can choose a random $b \in G$ and compute $b \star y$.
If they exchange their values, Alice can compute

$$a \star (b \star y) = (ab) \star y$$

and Bob can compute $b \star (a \star y) = (ba) \star y = (ab) \star y$.

Textbook Diffie-Hellman again

We phrased the problem in terms of the exponents:
$(g, g^a, g^b, g^c) \longrightarrow ab \stackrel{?}{=} c$.
Say n is the order of g and n is prime. Then the group $G = (\mathbb{Z}/n\mathbb{Z})^\times$ acts on the set $\{g, g^2, g^3, \ldots, g^{n-1}\}$ by

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

Group actions in isogeny-based cryptography

The setting [C'97, RS'06, DKS'18, CSIDH, CSURF]

1. **Group:** We start with an order in an imaginary quadratic field:

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

   for some $\pi \notin \mathbb{Z}$. This is a ring that does not admit unique factorization into primes.

   Introduce ideals = ideal numbers, we basically add missing gcd's for all pairs $a + b\pi, c + d\pi \in \mathcal{O}$:

   $$\mathfrak{a} = (a + b\pi, c + d\pi)$$

   We can multiply ideals to obtain other ideals. We have principal ideals $(a + b\pi, a + b\pi)$: take the gcd with youself.
   Every time a product of ideals is a principal ideal, we obtain a relation. And we quotient by all those relations:

   $$\mathrm{Cl}(\mathcal{O}) = \{\text{ideal numbers, with multiplication}\}/\sim$$

The group action, continued

We have a **group**: ideal class group $\mathrm{Cl}(\mathcal{O})$, elements are classes $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})$.
Define the **set**: elliptic curves over a finite field $\mathbb{F}_p$ with CM by $\mathcal{O}$; elements are equations $E : y^2 = x^3 + ax^2 + bx$, $a, b \in \mathbb{F}_p$
Group action:

$$\begin{aligned} \mathrm{Cl}(\mathcal{O}) \times \{\text{elliptic curves}\} &\to \{\text{elliptic curves}\} \\ ([\mathfrak{a}], E) &\mapsto [\mathfrak{a}] \star E \end{aligned}$$

and this action is free and transitive.

For $\mathcal{O} = \mathbb{Z}[\pi]$ and $\mathfrak{a} = (2, \pi - 1)$:

the ideal class $[(2, \pi - 1)]$ acts as $E \mapsto [\mathfrak{a}] \star E$

$$y^2 = x^3 + ax^2 + bx \longmapsto y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$$

Decisional Diffie-Hellman problem

DDH for class group actions

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

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

Characters of the class group

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

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 $1/2$.

Our work

We show how to compute the characters $\chi([\mathfrak{a}])$ directly from the elliptic curves $E, E' = [\mathfrak{a}] \star E$, that is, without knowing $[\mathfrak{a}]$.

Attacking the DDH from class group actions

Recall the DDH problem: given elliptic curves over $\mathbb{F}_p$

$$(E, [\mathfrak{a}] \star E, [\mathfrak{b}] \star E, [\mathfrak{c}] \star E), \quad \text{does } [\mathfrak{c}] = [\mathfrak{a}\mathfrak{b}]?$$

We pick a character χ, compute the character values from the elliptic curves and check

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

The running time depends on the choice of the characters χ. So when does the attack run in polynomial time in $\log p$?

This attack works

1. for ordinary curves [C'97, 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`