1 Slide 1

Title slide

Hello, I am Valeriia Kulynych and my work was conserned on the Supersingular Isogeny Diffie-Hellman key exchange protocol: its idea and what makes this protocol promising. My work was directed by M. Yves Aubry.

2 Slide 2

Outline

We will first briefly discuss notions of the supersingular elliptic curves and isogenies. Then we will focus on the different types of Diffie-Hellman key exchange protocol: classic DH, its Elliptic Curve variation and then we will finally pass to the Supersingular Isogeny Diffie Hellman: its key idea, the problems we face while we construct this, the solutions of these problems and the algorithm itself.

3 Slide 3

Elliptic Curves

An *elliptic curve* is a pair (E, O), where E is a curve of genus 1 and $O \in E$ is a point at infinity.

We won't talk a lot abou elliptic curves in general, but I have to mention that further we will consider curves defined over field K with non-zero characteristic.

We have to mention that the rational points of the curve E has a group structure.

4 Slide 4

Elliptic curves composition law illustration

Composition law on elliptic curves is defined as follows: Let P, Q be the points on the elliptic curve E and L be the line connecting those points. Remark, that L is a tangent line to E if $P = Q$. An let R be the third pont of intersection of L with the curve E. Let L' be the line connecting R and point O. Then $P \oplus Q$ is the point such that L' intersect E at R, O and $P \oplus Q$.

5 Slide 5

Supersingular Elliptic Curves

There is a lot of different but equivalent definitions of the Supersingular Elliptic Curves. We will see now only one of them, but I have mentioned in work the other ones.

So, for every n we define a multiplication map as follows. We denote its kernel by $E[n]$ and it is called n-torsion subgroup of E. Then one can show that for any $r \geq 1$ the group of rational points over field $\bar{K}$ of the p^r-torsion subgroup is either a trivial group or a cyclic group $\mathbb{Z}/p^r\mathbb{Z}$. In the first case, the curve E is called supersingular. Otherwise, it is called ordinary.

6 Slide 6

Isogenies - Definition Slide

Now we will move to the definition of an isogeny.

So, let E_1 nd E_2 be elliptic curves defined over a finite field $\mathbb{F}_q$ of characteristic p. An *isogeny* is a non-constant morphism that maps the identity into the indentity and this morphism is a group homomorphism.

One of the ways to determine whether two curves are isogenous is Sato-Tate theorem. It says, that two elliptic curves are isogenous over the field $\mathbb{F}_q$ if and only if the number of the rational points on these two elliptic curves over the field $\mathbb{F}_q$ is equivalent.

7 Slide 7

Isogenies - Remarks slide

Curves in the same isogeny class are either all supersingular or all ordinary.

The degree of an isogeny ϕ is the degree of ϕ as a morphism (i.e. $\phi : X \to Y$, then the degree of ϕ is the degree of the induced field extension $[K(Y) : K(X)]$).

The thing that is very important for the purpose of this talk is the fact that an isogeny could be identified with its kernel. So, if we are given a subgroup G of E, we can use Velu's formulas to compute an isogeny with such property.

8 Slide 8

Isogeny Graphs

Now we pass to the notion of the isogeny graph. We have a fixed elliptic curve E over a field K. Also we have a set of primes, which is the set of degrees of the isogenies. Then we can construct a graph, where the vertex set is the set of curves that are isogenous to our fixed curve E.And the edges correspond to isogenies between them and are labeled by ℓ by each equivalence classs of ℓ-isogenies for some prime ℓ in the set E.

Isogenies between supersingular curves are also called supersingular.

As we will be dealing with supersingular curves, then what is important for us that supersingular isogeny graphs are alway connected and $\ell + 1$-regular, where ℓ is isogeny degree.

9 Slide 9

Isogeny graph example

It suffices consider supersingular elliptic curves over $\mathbb{F}_{p^2}$ although the isogenies between them are over $\bar{\mathbb{F}}_p$. The amount of supersingular curves over field $\mathbb{F}_p$ is always about $\frac{p}{12}$, the exact number depends on $p \pmod{12}$. Recall, that the nodes are represented by j-invariants of the corresponding curves. The nodes labeled by α and $\bar{\alpha}$ are the primitives of the field extension.

Usually, we treat isogeny graphs as undirected since to every isogeny corresponds its dual. But in this very case we see how it works with the directed graphs.

Note, that for $j(E) = 0$ and $j(E) = 1728 \pmod{83} = 68$ there are three and respectively two non equivalent isogenies mapping from E to another curve E' (i.e. outgoing edge), but their dual isogenies are all equivalent (the reason we have only one incoming edge). We denote these multiple isogenies in the graph using a single arrow together with an integer to indicate the multiplicity. We also have two loop at 28, beacuse they are two isogenies that are dual to each other, but only one loop at 68, because it is dual to itself.

10 Slide 10

Classic Diffie Hellman Algorithm

Diffie Hellman key exchange protocol was one of the first examples of the public key cryptography, that was first introduced in the 1970s. There are two communicating parties, usually named Alice and Bob, and third listening party, usually named Eve. This method allows two parties without prior knowledge of each other establish a shared secret over an insecure channel.

Let's move to the algorithm.

Firstly, Alice and bob agree on a set of public parameters:

- A large enough prime number p, such that $p-1$ has a large enough prime factor;
- A multiplicative generator $g \in \mathbb{Z}/p\mathbb{Z}$.

Then, Alice and Bob perform the following steps:

1. Each chooses a *secret* integer in the interval $]0, p-1[$.
2. They respectively compute $A = g^a$ and $B = g^b$.
3. They exchange A and B over the public channel.
4. They respectively compute the *shared secret* $B^a = A^b = g^{ab}$.

The protocol could be generalized by replacing the multiplicative group with any other cyclic group.

11 Slide 11

Security of DH

Security of DH relies on the hardness of the discrete logarithm problem. So, let G be a cyclic group generated by an element g. For any element $A \in G$, find the discrete logarithm which is defined as follows.

Indeed, we know several algorithms to compute discrete logarithms. One of them requires $O(\sqrt{q})$ computational steps in generic cycliv group G, where q is the greatest prime divisor of $\#G$. That's why to make the procol more secure, we have to choose a very big prime p, which, of course, requires more memory and time to procced all the computational steps.

And if we are dealing with a multiplicative group there are algorithms of even better complexity.

12 Slide 12

Elliptic Curve Diffie Hellman

However, no algorithms better than the generic ones are known for the case when G is a group of rational points on elliptic curve. That is why, Elliptic Curve Diffie Hellman protocol was introduced in the 1980s. It is quite similar to the classic DH:

In this case public parameters of Elliptic Curves Diffie-Hellman (ECDH) protocol are:

- Finite field $\mathbb{F}_p$, with $\log_2 p \simeq 256$;
- Elliptic curve E over the finite field $\mathbb{F}_p$, such that $\#E(\mathbb{F}_p)$ is prime;
- A generator P of $E(\mathbb{F}_p)$.

And then Alice and Bob take the following steps:

1. Each chooses a secret from $]0, \#E(\mathbb{F}_p)[$, where we denote Alice's secret as a, and Bob's as b.
2. They compute public data $A = [a]P$ and $B = [b]P$.
3. Alice and Bob exchange public data.
4. Finally, they compute shared secret $S = [a]B = [b]A$.

It is already known that it is possible to reduce discrete logarithm problem on supersingular elliptic curves to the discrete logarithm problem in finite field. Hence it is possible to reduce the problem to one which is known to have sub-exponential complexity. That is why one should avoid using supersingular curves in ECDH.

13 Slide 13

Background

Before we pass to the main purpose of our talk, that is to say, to the Supersingular Isogeny Diffie-Hellman key exchange protocol, we will first give some background from the graph theory.

Let $G = (V, E)$ be an undirected graph , where V is the set of vertices, and E is the set of edges.

A *random walk* of legth i is a path $v \to \cdots \to v_i$, defined by the random process that selects v_i uniformly at random among the neighbours of v_{i-1}.

we have said that we should avoid supersingular elliptic curve for the ECDH, but it is not the case. And we decide to use supersingular curves and respectively isogenies. Why do we use them?

The first reason is that one isogeny degree is sufficient to obtain an expander graph. We won't emphasise on the expander graphs or even give a strict definition, but for our cryptographic purposes, we have just to admit that expander graphs have short diameter and rapidly mixing walks. This fact allows us to condtruct more efficient protocols.

Secondly, what is even more important reason for creating the whole SIDH protocol, is that there is no action of an abeliaan group on them. This means that it is harder to use quantum computers to speed up the supersingular isogeny path problem.

14 Slide 14

Idea of SIDH

Now we pass to the idea of SIDH.

In this case Alice and Bob take secret random walk in two distinct isogeny graphs on the same vertex set as their secret. Alice's walk has the legth of ε_A and Bob's has legth of ε_B.

On practice, we are choosing a large prime p and small primes ℓ_A and ℓ_B. The vertex set is represented by j-invariants of the supersingular elliptic curves over the field $\mathbb{F}_{p^2}$. Alice's graph consists og ℓ_A-isogenies and Bob's of ℓ_B-isogenies.

The key idea lies in the fact that the walk of length ε_A in the ℓ_A-isogeny graph corresponds to a kernel of a size $\ell_A^{\varepsilon_A}$, and this kernel is cyclic if and only if the walk does not backtrack.

On practice, choosing a secret ealk of length ε_A is equivalent to choosing a secret cyclic subgroup $\langle A \rangle \subset E[\ell_A^{\varepsilon_A}]$.

Since the subgroup $\langle A \rangle + \langle B \rangle = \langle A, B \rangle$ is well-defined, then it defines an isogeny to $E/\langle A, B \rangle$, which is the shared secret.

Since we choose $\ell_A \neq \ell_B$, the group $\langle A, B \rangle$ is cyclic of order $\ell_A^{\varepsilon_A} \ell_B^{\varepsilon_B}$.

15 Slide 15

Example of distinct graph over the same vertex set

Here is a toy exemple of such graphs. The vertex set is represented by j-invariants of the supersingular elliptic curves over the field $\mathbb{F}_{97^2}$. The blue graph consists of 2-isogenies, and we can see that it is 3-regular as it was said before. The red one cosists of 3-isogenies, and it is respectively 4-regular.

16 Slide 16

Illustration of SIDH

Thhis diagram represents the general algorithm. Alice and Bob are given a a fixed supersingular curve E. Then both of them chooses a secret subgroup and computes a secret isogeny. Then they define new isogeny by their kernel which, where their kernels are generated like that, and finally they compute their shared secret.

17 Slide 17

The problems we face

Constructing this protocols we face the next problem.

The first problem is that the points of $\langle A \rangle$ or $\langle B \rangle$ may not be rational.

To make matters worse, the diagram on the previous slide shows no way hov Alice and Bob could compute the shared secret without revealing their respective secrets.

18 Slide 18

Solution of the 1st problem

It turns out that we can control the group structure depending on the field. It is a hard problem in ordinary case, but it is not a big deal if the curve is supersingular.

Then it turns out that since we are dealing with $\mathbb{F}_{p^2}$ then the group of the rational points over our field has the following structure.

Then we try to choose p so that $e)\mathbb{F}_{p^2}$ contains two large torsion subgroups of coprime order.

Once those subgroups are fixed, we look for a prime of the following form, where f is a small co-factor. On practice, we can put $f = 1$, since the primes of the form mentioned before are abundant.

Then $E(\mathbb{F}_{p^2})$ contains $\ell_A^{\varepsilon_A - 1}(\ell_A + 1)$ cyclic subgroup of order $\ell_A^{\varepsilon_A}$ each defining a distinct isogeny. Then a single point $A \in E(\mathbb{F}_q)$ is enough to represent an isogeny walk of length ε_A and we further don't care whether the points of this subgroup are all rational.

19 Slide 19

Solution of the 2nd problem

To solve the second problem we use a very special trick, that puts SIDH apart of all the other DH type protocols. Alice and Bob have to publish some additional data.

They have publicly agreed on a prime and a supersingular elliptic curve of the following form.

Then they publish the bases of their respective torsion groups. Those torsion groups are not cyclic, so we need two points to generate them.

And after thay choose their secrets subgroups generated respectively by points A and B and they have the following form.

20 Slide 20

Solution of the 2nd problem

Once they have choosen their secrets subgroup, or that is to say their secret isogenies, they publish the images of their companions public bases under their own secret isogeny.

Then next step for each of them, is to compute the image of their secret point under ther companions isogenies. And they can easily do this given the knowledge of their public bases images.

They compute new isogenies whose respective kernels are generated this way. And that allows them both to compute the shared secret.

21 Slide 21

Schematizing of the SIDH

All the protocol is schematized on this slide.

So the public parameters are primes ℓ_A, ℓ_B, p, a supersingular curve E and the respective bases of the torsion group.

To start the protocol, Alice and Bob choose a secret point of the certain form, that represents the whole walk on their own isogeny graphs.

Afterwards, they compute their secret isogeny, which could be identified by the kernel generated by the point they have chosen before. They also compute the images of the bases.

They exchange this data.

And finally they computed the shared secret with the help of their new isogenies, whose kernels are generated this way.

22 Slide 22

Security of SIDH

The security of the supersingular isogeny DH reliea on the hardness of the problem called Supersingular Decision DH. This problem concerns in determining from which of the two distribution the suple we are given is sampled.

23 Slide 23

Security of SIDH

We won't emphasise on the SSDDH, but we have to admit that the best known algorithms to solve this problem have exponentional complexity even on quantum computer. And this is what makes this protocol very promising since it is very probable that quantum computers are going to appear in the near future. SIDH is a good example of a quantum-resistant key exchange protocol.

But, we also have to remark, that though there is no algorithms to solve the general problem, several polynomial-time attacks have appeared against variations of SIDH.

24 Slide 24

Analogues between different DH

To sum up, this figure shows us the analogues between different DH instantiations.

In the classic DH elements are integers modulo prime, in elliptic curve variatins they are point on the elliptic curve, and in SIDH they are curves in isogeny class, which are represented as nodes in isogeny graph.

Then the secrets are respectively exponents, scalars and isogenies.

We do the following computation.

And what is a hard problem that makes the algorithm useful for cryptography is to find those things.

25 Slide 25

THANK YOU!