12. Elliptic curve cryptography.

A. Ushakov

MA503, April 20, 2022

Contents

Here we discuss the elliptic curve discrete logarithm problem (ECDLP) and basic protocols that use computational hardness of the ECDLP.

- The elliptic curve discrete logarithm problem (ECDLP).
- ECDLP: complexity.
- Babystep-giantstep algorithm: example.
- Pohlig–Hellman algorithm: example.
- Elliptic Diffie–Hellman key exchange. Example.
- Elliptic curve computational DH problem (ECCDH).
- Elliptic ElGamal PKC. Example.

The elliptic curve discrete logarithm problem (ECDLP)

DLP in a finite field F is an algorithmic question for given h, g to find $n \in \mathbb{N}$ satisfying $h = g^n$ in F.

The discrete logarithm problem (DLP) in $\mathcal{E}$ *is an algorithmic question for given h, g to find $n \in \mathbb{N}$ satisfying $h = n \cdot g$.*

For instance, for $y^2 = x^3 + 3x + 8$ over $\mathbb{Z}_{13}$ and $g = (1, 5)$ we have

$$
\begin{array}{llll}
0(1,5) = \mathcal{O} & \log_{(1,5)}(\mathcal{O}) = 0 & 5(1,5) = (12,11) & \log_{(1,5)}(12,11) = 5 \\
1(1,5) = (1,5) & \log_{(1,5)}(1,5) = 1 & 6(1,5) = (9,6) & \log_{(1,5)}(9,6) = 6 \\
2(1,5) = (2,10) & \log_{(1,5)}(2,10) = 2 & 7(1,5) = (2,3) & \log_{(1,5)}(2,3) = 7 \\
3(1,5) = (9,7) & \log_{(1,5)}(9,7) = 3 & 8(1,5) = (1,8) & \log_{(1,5)}(1,8) = 8 \\
4(1,5) = (12,2) & \log_{(1,5)}(12,2) = 4 & 9(1,5) = \mathcal{O}. &
\end{array}
$$

If $h = n \cdot g$ has a solution, then it has infinitely many solutions of the form $[n]_{|g|}$.

ECDLP: complexity

ECDLP (the problem to compute $\log_g(\cdot)$ *for* $g \in \mathcal{E}$*) has no faster than* $O(\sqrt{|g|})$ *solutions.*

There are several general algorithms for ECDLP.

- Babystep-giantstep algorithm solves ECDLP in $O(\sqrt{|g|})$ time.
- Pohlig–Hellman algorithm solves ECDLP efficiently if $|g|$ is a product of small prime powers.

There are no index calculus algorithms known for the ECDLP.

ECDLP can be solved in polynomial-time on a quantum computer.

Babystep-giantstep algorithm: example

To compute $\log_g(h)$ *for* $g, h \in \mathcal{E}$, *compute* $n = 1 + \lfloor\sqrt{|g|}\rfloor$ *and construct two lists*

- **(babysteps)** $\mathcal{O}, 1\cdot g, 2\cdot g, 3\cdot g, \ldots, n\cdot g$,
- **(giantsteps)** $h, h - n\cdot g, h - 2n\cdot g, h - 3n\cdot g, \ldots, h - n^2\cdot g$.

Find a match $i\cdot g = h - jn\cdot g$ *and output* $jn + i$.

The curve $\mathcal{E}$ defined by $y^2 = x^3 + 2x + 9$ over $\mathbb{Z}_{67}$ has 75 elements and $(8,1)$ is primitive in $\mathcal{E}$. To compute $\log_{(8,1)}(61,7)$ we compute $n = 1 + \lfloor\sqrt{|(8,1)|}\rfloor = 9$.

(Babysteps)

$$\begin{array}{lll} 0\cdot g = \mathcal{O} & 3\cdot g = (0,64) & 6\cdot g = (15,8) \\ 1\cdot g = (8,1) & 4\cdot g = (9,32) & 7\cdot g = (45,29) \\ 2\cdot g = (13,50) & 5\cdot g = (6,61) & 8\cdot g = (11,42). \end{array}$$

(Giantsteps)

$$\begin{array}{rrr} h = (61,7) & h - 27\cdot g = (15,8) & h - 54\cdot g = (30,66) \\ h - 9\cdot g = (26,4) & h - 36\cdot g = (0,3) & h - 63\cdot g = (66,26) \\ h - 18\cdot g = (17,47) & h - 45\cdot g = (5,12) & h - 72\cdot h = (46,35). \end{array}$$

Hence, $6\cdot g = h - 27\cdot g$. Therefore, $h = 33\cdot g$.

Pohlig–Hellman algorithm: example

Pohlig–Hellman algorithm can be used to solve ECDLP.

- Consider the curve $\mathcal{E}$ defined by $y^2 = x^3 + x + 5$ of order $|\mathcal{E}| = 30 = 2 \cdot 3 \cdot 5$.
- The point $g = (12, 11)$ is primitive on $\mathcal{E}$, i.e., its order is 30.

Let $h = (21, 6)$. To compute $\log_g(h)$ using Pohlig–Hellman we compute the following:

$$
\begin{array}{llll}
N_1 = 15 & g_1 = 15g = (10,0) & h_1 = 15h = (10,0) & \log_{(10,0)}((10,0)) = 1 = k_1 \\
N_2 = 10 & g_2 = 10g = (26,2) & h_2 = 10h = (26,27) & \log_{(26,2)}((26,27)) = -1 = k_2 \\
N_3 = 6 & g_3 = 6g = (6,13) & h_3 = 6h = (16,12) & \log_{(6,13)}((16,12)) = k_3.
\end{array}
$$

We can compute $\log_{(6,13)}((16,12))$ directly by computing multiples of $(6,13)$ (it is better than computing multiples of g) and get $k_3 = 2$. Finally we reconstruct $k = \log_g(h)$ using CRT

$$
\begin{cases}
k \equiv_2 1 \\
k \equiv_3 -1 \\
k \equiv_5 2
\end{cases}
$$

and get $k = 17$.

Pohlig–Hellman algorithm is efficient if $|g|$ is a product of small powers $p_i^{a_i}$.

Elliptic Diffie–Hellman key exchange

Recall that the goal of a key exchange protocol is to allow two parties establish a common shared key.

Key generation (performed by Alice or by Bob):

- Choose sufficiently large prime field $F = \mathbb{Z}_p$.
- Choose an elliptic curve $\mathcal{E}$ over $\mathbb{Z}_p$ (i.e., a Weierstrass equation).
- Choose a primitive element $g \in \mathcal{E}$.

Encryption step performed by Alice:

- Choose a random $a \in \mathbb{N}$ (Alice's private key);
  compute $A = a \cdot g$ (Alice's public key);
  send A to Bob.

Encryption step performed by Bob:

- Choose a random $b \in \mathbb{N}$ (Bob's private key);
  compute $B = b \cdot g$ (Bob's public key);
  send B to Alice.

Computing the shared key (performed by Alice): $K = a \cdot B$.
Computing the shared key (performed by Bob): $K = b \cdot A$.

It is easy to check that

$$a \cdot B = (ab) \cdot g = b \cdot A,$$

i.e., Alice and Bob get the same element K.

DH: example

For instance, for the curve $\mathcal{E}$ defined by $y^2 = x^3 + 2x + 9$ over $\mathbb{Z}_{13}$.

	$\mathcal{O}$	(0, 3)	(0, 10)	(1, 5)	(1, 8)	(3, 4)	(3, 9)	(4, 4)	(4, 9)	(5, 1)	(5, 12)	(6, 4)	(6, 9)	(8, 2)	(8, 11)	(11, 6)	(11, 7)
$\mathcal{O}$	$\mathcal{O}$	(0, 3)	(0, 10)	(1, 5)	(1, 8)	(3, 4)	(3, 9)	(4, 4)	(4, 9)	(5, 1)	(5, 12)	(6, 4)	(6, 9)	(8, 2)	(8, 11)	(11, 6)	(11, 7)
(0, 3)	(0, 3)	(3, 9)	$\mathcal{O}$	(3, 4)	(11, 7)	(0, 10)	(1, 8)	(5, 12)	(8, 11)	(4, 9)	(5, 1)	(11, 6)	(8, 2)	(4, 4)	(6, 4)	(1, 5)	(6, 9)
(0, 10)	(0, 10)	$\mathcal{O}$	(3, 4)	(11, 6)	(3, 9)	(1, 5)	(0, 3)	(8, 2)	(5, 1)	(5, 12)	(4, 4)	(8, 11)	(11, 7)	(6, 9)	(4, 9)	(6, 4)	(1, 8)
(1, 5)	(1, 5)	(3, 4)	(11, 6)	(8, 11)	$\mathcal{O}$	(6, 4)	(0, 10)	(11, 7)	(4, 4)	(8, 2)	(6, 9)	(5, 1)	(3, 9)	(1, 8)	(5, 12)	(4, 9)	(0, 3)
(1, 8)	(1, 8)	(11, 7)	(3, 9)	$\mathcal{O}$	(8, 2)	(0, 3)	(6, 9)	(4, 9)	(11, 6)	(6, 4)	(8, 11)	(3, 4)	(5, 12)	(5, 1)	(1, 5)	(0, 10)	(4, 4)
(3, 4)	(3, 4)	(0, 10)	(1, 5)	(6, 4)	(0, 3)	(11, 6)	$\mathcal{O}$	(6, 9)	(5, 12)	(4, 4)	(8, 2)	(4, 9)	(1, 8)	(11, 7)	(5, 1)	(8, 11)	(3, 9)
(3, 9)	(3, 9)	(1, 8)	(0, 3)	(0, 10)	(6, 9)	$\mathcal{O}$	(11, 7)	(5, 1)	(6, 4)	(8, 11)	(4, 9)	(1, 5)	(4, 4)	(5, 12)	(11, 6)	(3, 4)	(8, 2)
(4, 4)	(4, 4)	(5, 12)	(8, 2)	(11, 7)	(4, 9)	(6, 9)	(5, 1)	(1, 5)	$\mathcal{O}$	(0, 10)	(3, 4)	(3, 9)	(6, 4)	(11, 6)	(0, 3)	(1, 8)	(8, 11)
(4, 9)	(4, 9)	(8, 11)	(5, 1)	(4, 4)	(11, 6)	(5, 12)	(6, 4)	$\mathcal{O}$	(1, 8)	(3, 9)	(0, 3)	(6, 9)	(3, 4)	(0, 10)	(11, 7)	(8, 2)	(1, 5)
(5, 1)	(5, 1)	(4, 9)	(5, 12)	(8, 2)	(6, 4)	(4, 4)	(8, 11)	(0, 10)	(3, 9)	(0, 3)	$\mathcal{O}$	(11, 7)	(1, 5)	(3, 4)	(1, 8)	(6, 9)	(11, 6)
(5, 12)	(5, 12)	(5, 1)	(4, 4)	(6, 9)	(8, 11)	(8, 2)	(4, 9)	(3, 4)	(0, 3)	$\mathcal{O}$	(0, 10)	(1, 8)	(11, 6)	(1, 5)	(3, 9)	(11, 7)	(6, 4)
(6, 4)	(6, 4)	(11, 6)	(8, 11)	(5, 1)	(3, 4)	(4, 9)	(1, 5)	(3, 9)	(6, 9)	(11, 7)	(1, 8)	(4, 4)	$\mathcal{O}$	(0, 3)	(8, 2)	(5, 12)	(0, 10)
(6, 9)	(6, 9)	(8, 2)	(11, 7)	(3, 9)	(5, 12)	(1, 8)	(4, 4)	(6, 4)	(3, 4)	(1, 5)	(11, 6)	$\mathcal{O}$	(4, 9)	(8, 11)	(0, 10)	(0, 3)	(5, 1)
(8, 2)	(8, 2)	(4, 4)	(6, 9)	(1, 8)	(5, 1)	(11, 7)	(5, 12)	(11, 6)	(0, 10)	(3, 4)	(1, 5)	(0, 3)	(8, 11)	(6, 4)	$\mathcal{O}$	(3, 9)	(4, 9)
(8, 11)	(8, 11)	(6, 4)	(4, 9)	(5, 12)	(1, 5)	(5, 1)	(11, 6)	(0, 3)	(11, 7)	(1, 8)	(3, 9)	(8, 2)	(0, 10)	$\mathcal{O}$	(6, 9)	(4, 4)	(3, 4)
(11, 6)	(11, 6)	(1, 5)	(6, 4)	(4, 9)	(0, 10)	(8, 11)	(3, 4)	(1, 8)	(8, 2)	(6, 9)	(11, 7)	(5, 12)	(0, 3)	(3, 9)	(4, 4)	(5, 1)	$\mathcal{O}$
(11, 7)	(11, 7)	(6, 9)	(1, 8)	(0, 3)	(4, 4)	(3, 9)	(8, 2)	(8, 11)	(1, 5)	(11, 6)	(6, 4)	(0, 10)	(5, 1)	(4, 9)	(3, 4)	$\mathcal{O}$	(5, 12)

Since $|\mathcal{E}| = 17$, every nontrivial element is primitive. So, let's choose $g = (0, 3)$.

- **Encryption step performed by Alice:** Alice chooses her private key $a = 6$, and sends $A = 6 \cdot (0, 3) = (8, 2)$ to Bob.
- **Encryption step performed by Bob:** Bob chooses his private key $b = 5$, and sends $B = 5 \cdot (0, 3) = (6, 9)$ to Alice.

Alice computes the shared key: $K = 6 \cdot (6, 9) = (11, 6)$.
Computing the shared key (performed by Bob): $K = 5 \cdot (8, 2) = (11, 6)$.

Elliptic curve computational DH problem (ECCDH)

A passive eavesdropper Eve collects public information:

- The initial information: description of $\mathcal{E}$ and the base element $g \in \mathcal{E}$.
- Alice's public key: $a \cdot g$.
- Bob's public key: $b \cdot g$.

Eve's goal is to the find the shared key $(ab) \cdot g$.

(ECCDH for an elliptic curve $\mathcal{E}$)

Given $(g, a \cdot g, b \cdot g)$ *compute* $(ab) \cdot g$.

Security of elliptic curve Diffie-Hellman key-exchange relies on computational hardness of ECCDH.

Elliptic ElGamal PKC

Key generation (performed by Alice):

- Choose sufficiently large prime field $F = \mathbb{Z}_p$.
- Choose an elliptic curve $\mathcal{E}$ over $\mathbb{Z}_p$ (i.e., a Weierstrass equation).
- Choose a primitive element $g \in \mathcal{E}$.
- Choose $a \in \mathbb{N}$ (**Alice's private key**) and compute $A = a \cdot g$.

Finally, Alice publishes the triple $(\mathcal{E}, g, A)$, called the **Alice's public key**.

Encryption (performed by Bob):

To encrypt the message $m \in \mathcal{E}$ Bob

- picks a (secret) random $j \in \mathcal{E}$;
- computes $c_1 = j \cdot g$ and $c_2 = m + j \cdot A$;
- sends the pair (c_1, c_2) to Alice.

Decryption (performed by Alice):

- Alice computes $c_2 - a \cdot c_1$. The obtained point is m.

It is easy to check that $m = c_2 - a \cdot c_1$ because

$$c_2 - a \cdot c_1 = (m + j \cdot A) - (aj) \cdot g = m + aj \cdot g - aj \cdot g = m.$$

Alice, indeed, obtains Bob's plaintext m.

Elliptic ElGamal PKC: example

Key generation (Alice): choose $\mathcal{E}$ defined by $y^2 = x^3 + 2x + 9$ over $\mathbb{Z}_{13}$.

	$\mathcal{O}$	$(0,3)$	$(0,10)$	$(1,5)$	$(1,8)$	$(3,4)$	$(3,9)$	$(4,4)$	$(4,9)$	$(5,1)$	$(5,12)$	$(6,4)$	$(6,9)$	$(8,2)$	$(8,11)$	$(11,6)$	$(11,7)$
$\mathcal{O}$	$\mathcal{O}$	$(0,3)$	$(0,10)$	$(1,5)$	$(1,8)$	$(3,4)$	$(3,9)$	$(4,4)$	$(4,9)$	$(5,1)$	$(5,12)$	$(6,4)$	$(6,9)$	$(8,2)$	$(8,11)$	$(11,6)$	$(11,7)$
$(0,3)$	$(0,3)$	$(3,9)$	$\mathcal{O}$	$(3,4)$	$(11,7)$	$(0,10)$	$(1,8)$	$(5,12)$	$(8,11)$	$(4,9)$	$(5,1)$	$(11,6)$	$(8,2)$	$(4,4)$	$(6,4)$	$(1,5)$	$(6,9)$
$(0,10)$	$(0,10)$	$\mathcal{O}$	$(3,4)$	$(11,6)$	$(3,9)$	$(1,5)$	$(0,3)$	$(8,2)$	$(5,1)$	$(5,12)$	$(4,4)$	$(8,11)$	$(11,7)$	$(6,9)$	$(4,9)$	$(6,4)$	$(1,8)$
$(1,5)$	$(1,5)$	$(3,4)$	$(11,6)$	$(8,11)$	$\mathcal{O}$	$(6,4)$	$(0,10)$	$(11,7)$	$(4,4)$	$(8,2)$	$(6,9)$	$(5,1)$	$(3,9)$	$(1,8)$	$(5,12)$	$(4,9)$	$(0,3)$
$(1,8)$	$(1,8)$	$(11,7)$	$(3,9)$	$\mathcal{O}$	$(8,2)$	$(0,3)$	$(6,9)$	$(4,9)$	$(11,6)$	$(6,4)$	$(8,11)$	$(3,4)$	$(5,12)$	$(5,1)$	$(1,5)$	$(0,10)$	$(4,4)$
$(3,4)$	$(3,4)$	$(0,10)$	$(1,5)$	$(6,4)$	$(0,3)$	$(11,6)$	$\mathcal{O}$	$(6,9)$	$(5,12)$	$(4,4)$	$(8,2)$	$(4,9)$	$(1,8)$	$(11,7)$	$(5,1)$	$(8,11)$	$(3,9)$
$(3,9)$	$(3,9)$	$(1,8)$	$(0,3)$	$(0,10)$	$(6,9)$	$\mathcal{O}$	$(11,7)$	$(5,1)$	$(6,4)$	$(8,11)$	$(4,9)$	$(1,5)$	$(4,4)$	$(5,12)$	$(11,6)$	$(3,4)$	$(8,2)$
$(4,4)$	$(4,4)$	$(5,12)$	$(8,2)$	$(11,7)$	$(4,9)$	$(6,9)$	$(5,1)$	$(1,5)$	$\mathcal{O}$	$(0,10)$	$(3,4)$	$(3,9)$	$(6,4)$	$(11,6)$	$(0,3)$	$(1,8)$	$(8,11)$
$(4,9)$	$(4,9)$	$(8,11)$	$(5,1)$	$(4,4)$	$(11,6)$	$(5,12)$	$(6,4)$	$\mathcal{O}$	$(1,8)$	$(3,9)$	$(0,3)$	$(6,9)$	$(3,4)$	$(0,10)$	$(11,7)$	$(8,2)$	$(1,5)$
$(5,1)$	$(5,1)$	$(4,9)$	$(5,12)$	$(8,2)$	$(6,4)$	$(4,4)$	$(8,11)$	$(0,10)$	$(3,9)$	$(0,3)$	$\mathcal{O}$	$(11,7)$	$(1,5)$	$(3,4)$	$(1,8)$	$(6,9)$	$(11,6)$
$(5,12)$	$(5,12)$	$(5,1)$	$(4,4)$	$(6,9)$	$(8,11)$	$(8,2)$	$(4,9)$	$(3,4)$	$(0,3)$	$\mathcal{O}$	$(0,10)$	$(1,8)$	$(11,6)$	$(1,5)$	$(3,9)$	$(11,7)$	$(6,4)$
$(6,4)$	$(6,4)$	$(11,6)$	$(8,11)$	$(5,1)$	$(3,4)$	$(4,9)$	$(1,5)$	$(3,9)$	$(6,9)$	$(11,7)$	$(1,8)$	$(4,4)$	$\mathcal{O}$	$(0,3)$	$(8,2)$	$(5,12)$	$(0,10)$
$(6,9)$	$(6,9)$	$(8,2)$	$(11,7)$	$(3,9)$	$(5,12)$	$(1,8)$	$(4,4)$	$(6,4)$	$(3,4)$	$(1,5)$	$(11,6)$	$\mathcal{O}$	$(4,9)$	$(8,11)$	$(0,10)$	$(0,3)$	$(5,1)$
$(8,2)$	$(8,2)$	$(4,4)$	$(6,9)$	$(1,8)$	$(5,1)$	$(11,7)$	$(5,12)$	$(11,6)$	$(0,10)$	$(3,4)$	$(1,5)$	$(0,3)$	$(8,11)$	$(6,4)$	$\mathcal{O}$	$(3,9)$	$(4,9)$
$(8,11)$	$(8,11)$	$(6,4)$	$(4,9)$	$(5,12)$	$(1,5)$	$(5,1)$	$(11,6)$	$(0,3)$	$(11,7)$	$(1,8)$	$(3,9)$	$(8,2)$	$(0,10)$	$\mathcal{O}$	$(6,9)$	$(4,4)$	$(3,4)$
$(11,6)$	$(11,6)$	$(1,5)$	$(6,4)$	$(4,9)$	$(0,10)$	$(8,11)$	$(3,4)$	$(1,8)$	$(8,2)$	$(6,9)$	$(11,7)$	$(5,12)$	$(0,3)$	$(3,9)$	$(4,4)$	$(5,1)$	$\mathcal{O}$
$(11,7)$	$(11,7)$	$(6,9)$	$(1,8)$	$(0,3)$	$(4,4)$	$(3,9)$	$(8,2)$	$(8,11)$	$(1,5)$	$(11,6)$	$(6,4)$	$(0,10)$	$(5,1)$	$(4,9)$	$(3,4)$	$\mathcal{O}$	$(5,12)$

- Since $|\mathcal{E}| = 17$, every nontrivial element is primitive. Choose $g = (0,3)$.
- Choose $a = 7 \in \mathbb{N}$ and compute $A = 7 \cdot (0,3) = (4,4)$.

Alice publishes her public key $(\mathcal{E}, (0,3), (4,4))$.

Encryption (performed by Bob):

To encrypt the message $m = (8,11) \in \mathcal{E}$ Bob

- chooses $j = 2 \in \mathbb{N}$ and computes
  $c_1 = j \cdot g = (3,9)$ and $c_2 = m + j \cdot A = (8,11) + 2 \cdot (4,4) = (5,12)$.
- sends the pair $((3,9),(5,12))$ to Alice.

Decryption (performed by Alice): $m = c_2 - a \cdot c_1 = (5,12) - 7(3,9) = (8,11)$.