

Elliptic curves and discrete logarithm problem

Franck Leprévost

Franck.Leprevost@uni.lu

Université du Luxembourg, LACS, Luxembourg



2 mai 2007

Outlines

- 1 Cryptology
- 2 Discrete Logarithm Problem
- 3 Elliptic Curves and ECDLP
- 4 General methods for solving ECDLP
- 5 Specific methods for solving the ECDLP

Cryptology

- Cryptology = Cryptography + Cryptanalysis
- Cryptography = Build
 - Secret-Key Cryptosystems
 - Public-Key Cryptosystems
- Cryptanalysis = Find attacks, weaknesses
- Alice, Bob and Oscar

Secret-Key Cryptology

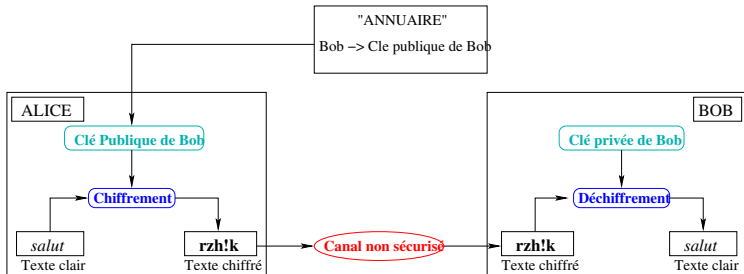


- Fundamental principle : one unique key for encryption and decryption
 - Stream ciphers
 - Block ciphers
- Many limitations

Principles of Public-Key Cryptology

- Fundamental principle : two keys
 - A public key (for the encryption and verification of signatures)
 - A secret key (for the decryption and the signature)
- Allows encryption, digital signature, key exchange
- Security is based on mathematical problems

Encryption



Digital Signature

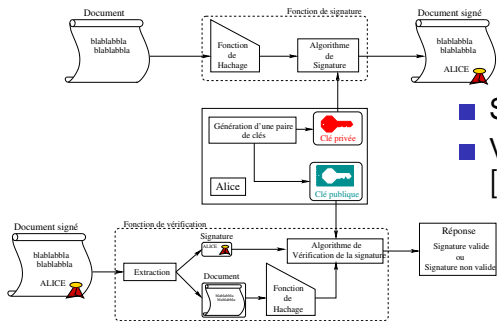
■ Alice signs M using :

- $h_M = H(M)$ the hash of M
- her secret key K_d .
- the decryption function D .
- Result $s(M) = D_{K_d}(h_M)$

■ Signed document : $[M, s(M)]$

■ Verification of the signature $[M, s(M)]$:

- uses the public-key K_e of Alice and the decryption-function E
- $E_{K_e}(s(M)) = h_M =? H(M)$
- Only Alice can produce $s(M)$



PKC and related mathematical problems

- IF : RSA, Rabin-Williams
- DLP : DSA, El Gamal, Diffie-Hellman
- ECDLP : ECDSA, EC-El Gamal, EC-DH
- DLP in other groups

Discrete Logarithm Problem

Let $h \in (G, \cdot) = \langle g \rangle$ a finite group.

The Discrete Logarithm Problem (DLP) is :

Knowing

$$G, g, h,$$

Find $x \in \mathbb{Z}$ (denoted $x = \log_g h$) such that

$$h = g^x.$$

Diffie-Hellman Key Exchange Protocol

Let G , $n = |G|$ and g be public data.

- Alice chooses an integer $1 \leq a \leq n - 1$ at random.
- Alice computes $A = g^a$ and sends it to Bob.
- Bob chooses an integer $1 \leq b \leq n - 1$ at random.
- Bob computes $B = g^b$ and sends it to Alice.
- Alice computes B^a , and Bob computes A^b .

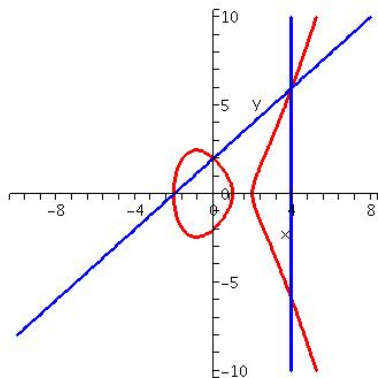
The common key is hence

$$K = g^{ab} = A^b = B^a.$$

Security of DHP

- DHP : Knowing G , g , $A = g^a$ and $B = g^b$, compute $K = g^{ab}$.
- Solve first DLP, then DHP
- However, there may be other ways.
- One can express DLP and DHP in any cyclic group G :
 $G = \mathbb{F}_p^*$, $G \subset E(\mathbb{F}_p)$, etc.
- Pay attention to the choice of the parameters.

Elliptic curves : Weierstrass form and Group law



The (short) Weierstrass form of an elliptic curve over a field K (where $6 \neq 0$) is :

$$Y^2 = X^3 + aX + b,$$

where $a, b \in K$ are such that

$$\Delta = -16(4a^3 + 27b^2) \neq 0.$$

Group law

If $P_1 = (x_1, y_1) \in E(K)$, then

$$-P_1 = (x_1, -y_1).$$

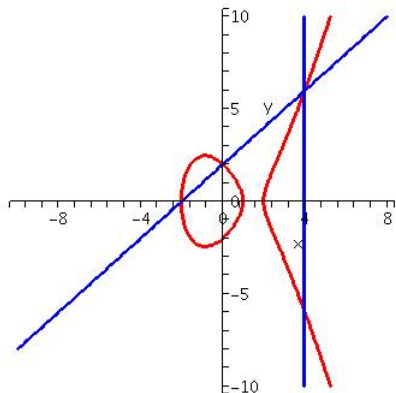
Let

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } x_1 \neq x_2 \\ \frac{3x_1^2 + a}{2y_1} & \text{if } x_1 = x_2 \text{ and } y_1 \neq 0 \end{cases}$$

Let $P_3 = (x_3, y_3) = P_1 + P_2 \neq \mathcal{O}$, then

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = (x_1 - x_3)\lambda - y_1 \end{cases}$$

Example



Let E be of equation
 $y^2 = (x + 2)(x - 1)(x - 2)$,
 and let $P = (-2, 0)$, and
 $Q = (0, 2)$.
 Then $P + Q = (4, -6)$.

Multiplication

- If $m \geq 1$, then

$$[m]P = \underbrace{P + \dots + P}_{m \text{ times}};$$

- Of course, if $m = 0$

$$[0]P = \mathcal{O};$$

- If $m \leq -1$, then

$$[m]P = [-m](-P)$$

Example

Let E defined by

$$y^2 = x^3 + 5x + 3.$$

Let $P = (1, 3)$. One has

- $[2]P = \left(-\frac{2}{9}, -\frac{37}{27}\right)$
- $[3]P = \left(\frac{1453}{121}, -\frac{56385}{1331}\right)$
- $[4]P = \left(\frac{195793}{49284}, \frac{101205953}{10941048}\right)$
- $[5]P = \left(-\frac{97988579}{177395761}, \frac{623326948653}{2362734140759}\right)$

Elliptic curves over finite fields

- $\#E(\mathbb{F}_p) = p + 1 - t$, where $|t| \leq 2\sqrt{p}$.
- The computation of $\#E(\mathbb{F}_p)$ amounts to the computation of t .

For this, one can use

- CM methods
- so-called Koblitz-curves
- SEA, cohomology methods, ...

ECDLP

Let E be an elliptic curve defined over a finite field \mathbb{F}_p

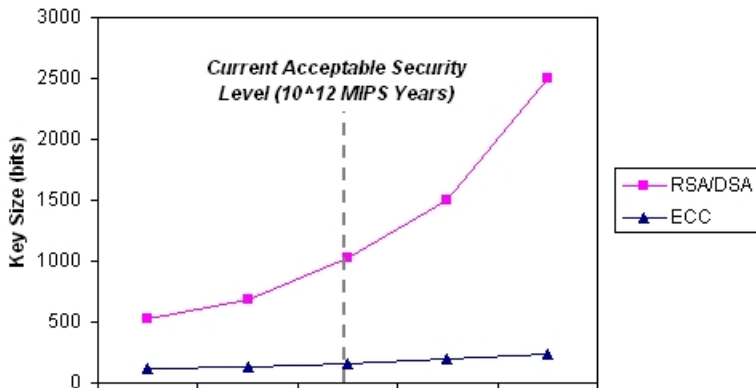
Let $G = \langle P \rangle$ be a cyclic subgroup of $E(\mathbb{F}_p)$.

Let $Q \in G$, ECDLP is the problem of finding $n \in \mathbb{Z}$ such that

$$Q = [n]P.$$

ECDLP vs RSA/DLP

COMPARISON OF SECURITY LEVELS of ECC and RSA & DSA



General methods for solving ECDLP

- Pohlig-Hellman's reduction
- Baby Step Giant Step



Other general methods for solving ECDLP

- Kangoroos
- Xedni



Pohlig-Hellman's reduction

This requires the knowledge of the factorization of

$$n = |G| = \prod_{i=1}^k p_i^{e_i}.$$

The reduction

- DLP in G (of order n) amounts to many DLPs in groups of order $p \in \mathcal{P}$, $p \leq n$.
- This requires to solve these DLP using other methods !
- The reduction proceeds in 2 steps :
 - 1 Step 1 : Reduction from n to $p_i^{e_i}$.
 - 2 Step 2 : Reduction from $p_i^{e_i}$ to p_i .

Step 1 : Reduction from n to $p_i^{e_i}$

Step 1

- For $i \in [1, k]$, let $n_i = \frac{n}{p_i^{e_i}}$, $g_i = g^{n_i}$ and $h_i = h^{n_i}$. Then $h_i = (g_i)^x \in G_i = \langle g_i \rangle$ of order $p_i^{e_i}$.
Hence $\exists x(p_i) \in [0, p_i^{e_i} - 1] / h_i = (g_i)^{x(p_i)}$ in G_i .
- If $e_i > 1$, one computes $\{x(p_i)\}_{1 \leq i \leq k}$ with step 2.
- All this leads to the k equations :

$$\begin{cases} x \equiv x(p_1) \pmod{p_1^{e_1}} \\ \vdots \\ x \equiv x(p_k) \pmod{p_k^{e_k}} \end{cases} \quad \text{CRT gives } x \pmod{n}$$

Step 2 : Reduction from $p_i^{e_i}$ to p_i

Step 2 : find $x \in [0, p^e - 1] / h = g^x \in G = \langle g \rangle ; |G| = p^e$

- One has $x_i \in [0, p - 1] / x = x_0 + x_1 \cdot p + \dots + x_{e-1} p^{e-1}$
- Computation of x_0 :
 - $p^{e-1} \cdot x = p^{e-1} \cdot x_0 + p^e (x_1 + \dots + x_{e-1} p^{e-2})$
 - $|G| = p^e \implies h^{p^{e-1}} = g^{p^{e-1} \cdot x} = (g^{p^{e-1}})^{x_0}$
 - $\text{ord}(g^{p^{e-1}}) = p$: this reduces to a DLP in G' of order p
 - ⋮
- Computation of x_j (one assumes x_0, \dots, x_{j-1} already known) :
 - $h_j = hg^{-(x_0 + x_1 p + \dots + x_{j-1} p^{j-1})} \implies (g^{p^{e-1}})^{x_j} = (h_j)^{p^{e-1-j}}$
 - $\text{ord}(g^{p^{e-1}}) = p$: this reduces to a DLP in G' of order p

Pohlig-Hellman : Example

Let E defined over \mathbb{F}_{1009} by

$$Y^2 = X^3 + 71X + 602.$$

One has

$$\#E(\mathbb{F}_{1009}) = 1060 = 2^2 \cdot 5 \cdot 53$$

Let

$$P = (1, 237), \quad \text{and} \quad Q = (190, 271).$$

One looks for m such that

$$Q = [m]P.$$

Pohlig-Hellman

The order of P is $530 = 2 \cdot 5 \cdot 53$ in $E(\mathbb{F}_{1009})$

One computes

- $m \bmod 2$
- $m \bmod 5$
- $m \bmod 53$

Then one finds m , using the CRT.

Pohlig-Hellman : modulo 2

One multiplies P and Q by

$$\frac{n}{2} = \frac{530}{2} = 265.$$

This leads to

$$\begin{cases} P_2 = [265]P = (50, 0) \\ Q_2 = [265]Q = (50, 0) \end{cases}$$

The DLP to solve is simply :

$$Q_2 = [m \bmod 2]P_2,$$

hence

$$m \equiv 1 \pmod{2}.$$

Pohlig-Hellman : modulo 5

One multiplies P and Q by

$$\frac{n}{5} = \frac{530}{5} = 106.$$

This leads to

$$\begin{cases} P_5 = [106]P = (639, 160) \\ Q_5 = [106]Q = (639, 849) \end{cases}$$

The DLP to solve is then

$$Q_5 = [m \bmod 5]P_5,$$

hence

$$m \equiv 4 \pmod{5}$$

Pohlig-Hellman : modulo 53

One multiplies P and Q by

$$\frac{n}{53} = \frac{530}{53} = 10.$$

This leads to

$$\begin{cases} P_{53} = [10]P = (32, 737) = P' \\ Q_{53} = [10]Q = (592, 97) = Q' \end{cases}$$

The DLP to solve is then :

$$Q_{53} = [m \bmod 53]P_{53}.$$

One can show that

$$m \equiv 48 \pmod{53}$$

Pohlig-Hellman : solution

One has

$$\begin{cases} m \equiv 1 \pmod{2} \\ m \equiv 4 \pmod{5} \\ m \equiv 48 \pmod{53} \end{cases}$$

Using the CRT, one finally finds :

$$m = 419$$

Solving ECDLP : BSGS

Description of the method

- Soit $m = \lceil \sqrt{n} \rceil$. Division of x by m :

$$\exists q, r \in \mathbb{Z} : x = qm + r, \text{ with } 0 \leq r < m.$$
- Principle : find q and r (hence x) using :

$$hg^{-r} = (g^m)^q$$
 - 1 Baby Step : $B = \{(hg^{-r}, r)\}_{0 \leq r < m}$
 - if $\exists r \in [0, m[/ (1, r) \in B$, then $x = r$.
 - 2 Giant Step : Let $t = g^m$. For $q = 1, 2, \dots$ do
 - if $\exists r \in [0, m[/ (t^q, r) \in B$, then $x = qm + r$.
- Complexity : memory $\mathcal{O}(\sqrt{n})$; operations $\mathcal{O}(\sqrt{n})$

BSGS : Example

let E defined over \mathbb{F}_{1009} by

$$Y^2 = X^3 + 71X + 602.$$

Find r such that

$$Q' = (592, 97) = [r](32, 737) = [r]P'$$

Baby Steps...

Because $\lceil \sqrt{53} \rceil = 8$, one needs 8 Baby Steps :

b	$R_b = Q' - [b]P'$
0	(592, 97)
1	(728, 450)
2	(537, 344)
3	(996, 154)
4	(817, 136)
5	(365, 715)
6	(627, 606)
7	(150, 413)

... and Giant Steps

One computes the Giant Steps : $[a]([8]P')$:

a	$[a]([8]P')$
1	(996, 855)
2	(200, 652)
3	(378, 304)
4	(609, 357)
5	(304, 583)
6	(592, 97)

BSGS

One notices an identity with $a = 6$, and $b = 0$, what leads to :

$$r = 8a + b = 8 \cdot 6 + 0 = 48$$

and we are done.

One also could have noticed that

$$[8]P' = -R_3 = -Q' + [3]P'$$

and hence

$$Q' = [3]P' - [8]P' = -[5]P' = [48]P'$$

Last slide : Specific methods for solving the ECDLP

- Anomalous curves : p -adic elliptic logarithm and cohomology
- Supersingular curves : cohomology and Weil's pairing