Bulletin of the *Transilvania* University of Braşov • Vol 2(51) - 2009
Series III: Mathematics, Informatics, Physics, 85-92

SOME RECENT APPLICATIONS OF ELLIPTIC CURVES IN CRYPTOGRAPHY

Mireille MARTIN-DESCHAMPS[1]

Communicated to:
9-ème Colloque franco-roumain de math. appl., 28 août-2 sept. 2008, Braşov, Romania

Abstract

Since about 1985, the theory of elliptic curves over finite fields has been applied to various problems in cryptography. One of the main reasons for interest in cryptosystems based on elliptic curves is that they can provide (a huge number of) finite abelian groups having a rich algebraic structure.
In this paper we give three recent applications of the Weil-pairing on an elliptic curve in crytography :
- the MOV attack (discrete logarithm on a supersingular elliptic curve),
- the tripartite Diffy-Helmann key exchange,
- identity based cryptography.

2000 *Mathematics Subject Classification*: 11G20, 14H52, 94A60.

1 Cryptology

1.1 Definitions

Cryptology is the science of encoded messages, which will be sent through an unsafe channel. Its fundamental aim is to protect a piece of information so that only a specific person (or machine) can access it.
Cryptology has two faces : cryptography and cryptanalysis.
Cryptography is the study of methods of encoding (or encrypting) messages so that only the intended recipients can read them.
Cryptanalysis is the study of methods of cracking the codes.

1.2 Private key cryptography

The situation involves two persons, traditionally called Alice and Bob. Alice wants to send a secret message to Bob. Using encryption, she converts it into a form that a spy, Oscar, cannot understand. Then Bob receives the message and deciphers it.

[1] CNRS UMR 8100, Université de Versailles Saint-Quentin, F-78035 Versailles, France

The original message is the **plaintext**, the disguised message (obtained after encryption) is the **ciphertext**.
Until the late seventies, all cryptography message transmission was by what can be called "*private key*". This means that someone who has enough information to encrypt messages automatically has enough information to decipher messages as well. As a result, any two users of the system who want to communicate secretly must have exchanged keys in a safe way.

1.3 Public key cryptography

In 1976, Diffie and Helmann invented an entirely new type of cryptography, called "*public key*". At the heart of this concept is the idea of using a one-way function for encryption.

Definition 1.1. *A function $f : X \to Y$ is a one-way function if it is easy to compute $f(x)$ for all $x \in X$, but hard to compute $f^{-1}(y)$ for most randomly selected y.*

Example 1.2. *Let G be a finite abelian group, with group law $*$, identity element e_G. If $g \in G$ and $n \in \mathbb{N}^*$, define :*

- $g^n = g * \cdots * g$ *(n times)*
- $g^{-n} = (g^{-1})^n$
- $g^0 = e_G$

The function

$$f : \mathbb{Z} \to G \quad , \quad f(a) = g^a$$

is a one-way function. Computing a from g^a is the **discrete logarithm problem**.

The first algorithms in public key cryptography were based on the discrete logarithm in finite fields.

Example 1.3. *(Diffie-Hellman key exchange) ([3])*
A (Alice) and B(Bob) want to agree upon a large integer to serve as a key for some private key cryptosystem. This must be done using open communication channels. They agree on **public** *data : a prime number p and an element g in $\mathbf{F}_p^*$ (p and $\operatorname{ord} g$ big enough).*
Alice secretly chooses a random positive integer $k_A < p$ (her secrete key) and sends g^{k_A} to Bob.
Bob does likewise : he chooses k_B and sends g^{k_B} to Alice.
Their common secret is $g^{k_A k_B} = (g^{k_A})^{k_B} = (g^{k_B})^{k_A}$.
The problem for an eavesdropper is : given g, g^{k_A}, g^{k_B}, find $g^{k_A k_B}$.

People think that this problem is equivalent to the discrete logarithm problem, but it not proven yet.

1.4 Safety

In order to estimate the safety, one rates the complexity of known algorithms which can solve the discrete log problem (dlp).

Proposition 1.4. *([3]) If $G = \mathbb{Z}/n\mathbb{Z}$, the dlp is polynomial : its complexity is $\mathcal{O}((\log_2 n)^2)$. If $G = \mathbb{F}_p^*$ (multiplicative group of the finite field $\mathbb{F}_p$), where p is a prime number, the dlp is sub-exponential : its complexity is*

$$\mathcal{O}(\exp(\beta(\log_2 p)^{1/3}(\log_2 \log_2 p)^{2/3}))$$

where β is some (known) constant. The same holds for any finite field.
If G is a "generic" finite abelian group (with no exploitable structure), the dlp is exponential : its complexity is $\mathcal{O}(\sqrt{\#G})$.

The complexity of solving the dlp is a very relative notion. Today the dlp in a finite field is difficult if $p \gg 0$ (at least 150 digits).
As soon as these systems developed, and at the same time the computers became more and more powerful and fast, people tried to find new groups in order to improve the safety. It turns out that the elliptic curves can provide a tremendous number of "generic" finite abelian groups having a rich algebraic structure. For each q, there is only one $\mathbf{F}_q^*$, and there are many elliptic curves group $E/\mathbf{F}_q$. Moreover, there is no subexponential algorithm to break the system if E is suitably chosen.

The elliptic curve cryptosystems are now well developed, and there are many usable implementations.

2 Elliptic curves

2.1 Definitions

Let $\mathbb{K}$ be a (perfect) field and $\overline{\mathbb{K}}$ its algebraic closure. For the properties of elliptic curves in this second paragraph, see [5].

Definitions 2.1. *A Weierstrass polynomial is an element f of the polynomial ring $\mathbb{K}[X, Y]$ of the following form :*

$$f = Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6.$$

An elliptic curve $E(\mathbb{K})$ over $\mathbb{K}$ is the union of

- *the set of pairs (x, y) in $\mathbb{K}^2$ such that $f(x, y) = 0$ where f is a Weierstrass polynomial and $f, \partial f/\partial X, \partial f/\partial Y$ have no common solution in $\overline{\mathbb{K}}$,*
- *and a point called infinity (of the y-axis) and denoted by O.*

Remark 2.2. *For algebraic geometers there is an intrinsic definition : an elliptic curve $E(\mathbb{K})$ over $\mathbb{K}$ is a projective smooth irreducible curve of genus equal to 1.*

Definitions 2.3. *If $\mathbb{K}$ is a subfield of $\mathbb{K}'$, the same Weierstrass polynomial defines two elliptic curves $E(\mathbb{K}) \subset E(\mathbb{K}')$. We say that $E(\mathbb{K})$ (resp. $E(\mathbb{K}')$) is the set of points of the elliptic curve E with value in $\mathbb{K}$ (resp. in $\mathbb{K}'$).*

Remark 2.4. *If $\mathbb{K}$ is finite, the number of points of $E(\mathbb{K})$ is also finite, but in general it is not possible to know it exactly. There are only bounds, except for special curves, called supersingular.*
If E is supersingular, $\#E(\mathbf{F}_p) = p + 1$.

2.2 Group law on an elliptic curve

Definition 2.5. *Let P, Q two points of $E(\mathbb{K})$.*
If we agree that the point O is on any line with equation $X = a$, for all $P, Q \in E(\mathbb{K})$, there exists a unique $R \in E(\mathbb{K})$ such that P, Q, R are on a line (If 2 or 3 points meet, the line is tangent).
Let S such that R, O, S are on a line. Define $P +_E Q = S$.

Theorem 2.6. *This defines a group structure on the elliptic curve $E(\mathbb{K})$, with neutral element O.*
If $\mathbb{K} \subset \mathbb{K}'$, $E(\mathbb{K})$ is a subgroup of $E(\mathbb{K}')$.

Definition 2.7. *(Torsion subgroups) Let P a point of $E(\mathbb{K})$. If $m \in \mathbb{N}^*$, we can define :*

$$[m]P = P +_E \cdots +_E P \qquad (m \text{ terms})$$

The m-torsion subgroup of E, denoted $E[m]$, is the subgroup of points $P \in E(\overline{\mathbb{K}})$ such that $[m]P = O$.

These subgroups are well known. We have the following result :

Proposition 2.8. *Let p be the characteristic of the field $\mathbb{K}$.*

- *If $p = 0$, or if m and p are relatively prime,*

$$E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

- *If $p > 0$, there are two possibilities :*
  - *either $\forall r \in \mathbb{N}^*$, $E[p^r] \simeq \mathbb{Z}/p^r\mathbb{Z}$,*
  - *either $\forall r \in \mathbb{N}^*$, $E[p^r] = 0$ and we say that the elliptic curve E is supersingular.*

2.3 Weil pairing on an elliptic curve

Let $m \in \mathbb{N}^*$ relatively prime with p. The Weil-pairing is a map :

$$e_m : E[m] \times E[m] \to \mu_m(\overline{\mathbb{K}}) \subset \overline{\mathbb{K}}^* \quad (= m^{th} \text{ roots of } 1)$$

which has the following properties :

- bilinear : $e_m(S, T_1 +_E T_2) = e_m(S, T_1).e_m(S, T_2)$;
- alternating : $e_m(T, T) = 1$ ($\Rightarrow e_m(T, S) = e_m(S, T)^{-1}$) ;
- non degenerate : if $e_m(S, T) = 1$ for all $S \in E[m]$ then $T = O$;
- Galois-invariant : if $S, T \in E(\mathbb{K})$, then $e_m(S, T) \in \mathbb{K}$.

It is possible to compute explicitely this pairing.

3 Applications in cryptology

3.1 Discrete logarithm problem (dlp)

Elliptic curves on finite fields provide a lot of new groups wich are "generic". There is no known algorithm to solve the dlp using more that the group structure.
These groups can be used for any cryptosystem based on the discrete log problem, and they are smaller with the same level of security.

3.2 MOV attack of the dlp on a supersingular elliptic curve

Supersingular elliptic curves are frequently used in cryptosystem based on the discrete log problem for many reasons :

- the computations are easy on these curves (this can't be explained here in detail) ;
- their number of points is exactly known : if E is a a supersingular curve on the finite field $\mathbf{F}_p$, then $\#E(\mathbf{F}_p) = p + 1$;
- they have a non trivial automorphism (see the following examples).

Example 3.1. *If $p \equiv 3[4]$, (then -1 is not a square in $\mathbf{F}_p$), the elliptic curve E defined on $\mathbf{F}_p$ by $Y^2 = X^3 + X$ is supersingular.*
It has an automorphism ψ defined by $\psi(x, y) = (-x, iy)$ where $i = \sqrt{-1} \in \overline{\mathbf{F}_p}$.

Example 3.2. *If $p \equiv 2[4]$, (then -1 is not a cube in $\mathbf{F}_p$), the elliptic curve E defined on $\mathbf{F}_p$ by $Y^2 = X^3 + 1$ is supersingular.*
It has an automorphism ψ defined by $\psi(x, y) = (jx, y)$ where $j = \sqrt[3]{-1} \in \overline{\mathbf{F}_p}$.

The MOV (Menezes, Okamoto and Van Stone) attack ([4]) proves that
the dlp on a supersingular curve on the field $\mathbf{F}_p$ can be reduced to the dlp in the field $\mathbf{F}_{p^2}$. We describe it briefly below.

The problem is the following : let $P \in E(\mathbf{F}_p)$, $Q = xP$, **find** x.
We can suppose that P is in a subgroup de $E(\mathbf{F}_p)$ of prime order ℓ, which divides $\#E(\mathbf{F}_p) = p + 1$. Then :

- $P \in E[\ell]$,

- we can consider the Weil-paitring $e_\ell : E[\ell] \times E[\ell] \to \mu_\ell(\overline{\mathbf{F}_p})$,
- ℓ divides $p^2 - 1$, therefore $\mu_\ell(\overline{\mathbf{F}_p}) \subset \mathbf{F}_{p^2}$ because $\mathbf{F}_{p^2}$ is the splitting field on $\mathbf{F}_p$ of the polynomial $X^{p^2} - X$.

Now we can choose another point $R \in E[\ell]$ such that $e_\ell(P, R) \neq 1$.
Then $e_\ell(Q, R) = e_\ell(xP, R) = e_\ell(P, R)^x \in \mathbf{F}_{p^2}$.
So we can find x by solving the dlp in $\mathbf{F}_{p^2}$.

3.3 Tripartite Diffie-Hellman key exchange

We explained in 1.3 the Diffie-Hellman key exchange for two persons, A and B. The question is : is it possible to adapt it for three persons ?
We fix a prime number p and an element g in $\mathbf{F}_p^*$. We suppose that A has a secret key k_A, B a secret key k_B and C a secret key k_C, and we would like $g^{k_A k_B k_C}$ to be their be common secret ? So the question is :
is it possible to compute $g^{k_A k_B k_C}$ if you know k_A, g^{k_B} and g^{k_C} ?
The answer is : Yes, but with a second "round" :
A sends $g^{k_A k_B}$ to C and $g^{k_A k_C}$ to B, B sends $g^{k_B k_C}$ to A.
$g^{k_A k_B k_C} = (g^{k_B k_C})^{k_A} = (g^{k_A k_C})^{k_B}) = (g^{k_A k_B})^{k_C})$.

Using the Weil pairing on a supersingular elliptic curve on $\mathbf{F}_p$, Antoine Joux defined in 2004 a **Tripartite Diffie-Hellman key exchange**. We describe it briefly below.

Let p be a prime number and ℓ be an integer relatively prime with p, E a supersingular elliptic curve on $\mathbf{F}_p$, with an automorphism ψ defined as above.
First we define a **modified Weil pairing** on $E[\ell]$ by

$$\hat{e_\ell}(P, Q) = e_\ell(P, \psi(Q)).$$

This new pairing has an interesting property : $P \neq 0 \Rightarrow \hat{e_\ell}(P, P) \neq 1$.
First, A, B and C agree on **public** data : E, ℓ and $P \in E[\ell]$.
Then A secretly chooses a random positive integer a (secrete key) and sends aP to B and C, B chooses b and sends bP to A and C, C chooses c and sends cP to A and B.
Their common secret is $\hat{e_\ell}(P, P)^{abc} = \hat{e_\ell}(bP, cP)^a$.

3.4 Identity based cryptography

The original motivation for identity-based encryption (idea of Shamir, 1984) is to help the deployment of a public key infrastructure and to simplify systems that manage a large number of public keys. Rather than storing a big database of public keys the system can derive these public keys from usernames or electronic addresses.
The first practical identity based encryption IBE scheme was proposed by Boneh and Franklin in 2001 ([1]). Again we describe it briefly below.

A key generator chooses an elliptic curve E over $\mathbf{F}_q$, a number ℓ relatively prime with p, a point $P \in E(\mathbf{F}_q)$ and an integer s.
The **public** data are : E, P and $Q = sP$.
There is a function which associates to every user Bob (defined for example by his e-mail address bob@bob.com) a point P_B of E.
Alice chooses a random integer r and sends rP to Bob.
The key generator sends sP_B to Bob (his secrete key).
Their common secret is

$$e_\ell(rQ, P_B) = e_\ell(rsP, P_B) = e_\ell(P, P_B)^{rs} = e_\ell(rP, sP_B).$$

For more details, see : http://crypto.stanford.edu/ibe/

References

[1] Boneh B. and Franklin M., *Identity based encryption from the Weil pairing*, Crypto, Springer-Verlag, LNCS **2139** (2001), 213-229.

[2] Joux A., *A one round protocol for tripartite Diffie-Hellman*, Journal of cryptology **17**, n4 (2004), 263-276.

[3] Koblitz, N., *Algebraic aspects of Cryptography*, Springer - Algorithms and Computation in Mathematics 3, 1999.

[4] Menezes A., Okamoto T. and Van Stone S., Reducing elliptic curve logarithms to logarithms in a finite field, IEEE Transactions on Information Theory **39**, n5 (1993), 1639-1646.

[5] Silverman J.H., **The Arithmetic of Elliptic Curves**, Springer, Graduate texts in Mathematics 106, 1992.