Elliptic Curves and their application in Cryptography

Matthijs Coster

MIVD (MISS)

october 3, 2002

Contents

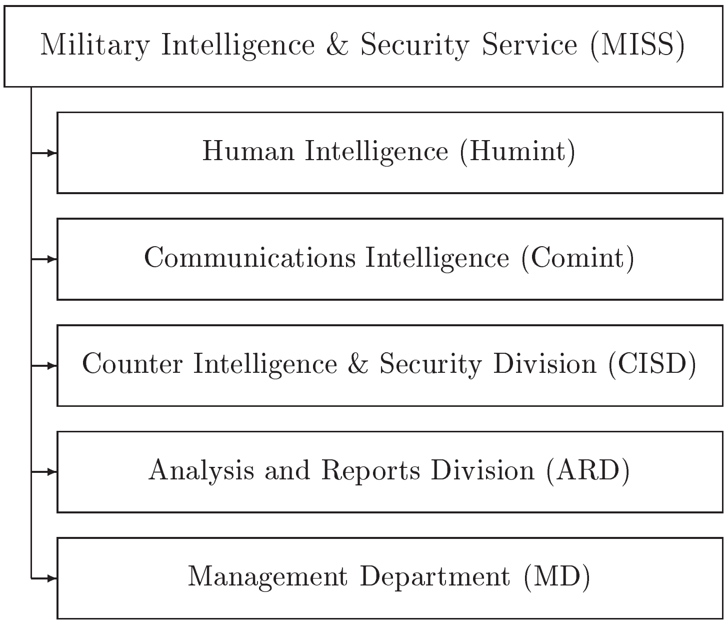
1 Tasks of the MIVD (Military Intelligence & Security Service)

[1]On may 30, 2002 the Intelligence and Security Services Act took effect. This new ISS Act defines the following tasks for the Military Intelligence and Security Service: Conduct investigations: into the potential and the armed

[1]Copied from the Annual Report MIS 2001

forces of foreign powers to ensure the adequate build-up and the effective use of the Netherlands armed forces; into factors that influence or can exercise influence on sustaining and strengthening the international rule of law, as far as the armed forces are or can be involved; Conduct security clearance investigations in compliance with the Security Investigations Act. Conduct investigations needed for taking measures: to prevent activities aimed at harming the security or combat readiness of the armed forces; to promote a proper process of mobilisation and concentration of the armed forces; to promote the undisturbed preparation and deployment of the armed forces as referred to sub a, second dash. Promote measures for the protection of the interests referred to sub c, including measures to protect the secrecy of classified military information. Conduct investigations on foreign countries concerning military-relevant subjects as defined, in concordance with the relevant ministers, by the Dutch Prime Minister-cum-Minister of General Affairs.
The "old" Intelligence and Security Services Act defined the MIS tasks as comprehending an Intelligence and a Counter Intelligence and Security task. This report reviews both tasks.

1.1 Organogram



1.2 Organisation

To implement its tasks the MIS is organised into divisions that are principally charged with collecting and processing information into intelligence products including intelligence reports, risk analyses and briefings serving

as basis for the planning and support of military operations.
The Communications Intelligence (Comint) and Human Intelligence (Humint) Divisions collect the information that is passed on to the Analysis and Reports Division (ARD) and the Counter Intelligence and Security Division (CISD). The modus operandi comprehends the subsequent selection, analysis, adaptation and processing of the information. The ISS Act and the Intelligence Investigations Act define the specific powers of the MISS.

2 Introduction

2.1 Public Key Cryptography

At the moment there are 3 main PKC–systems:

1. Discrete Logarithm (1976, Diffie, Hellman)
2. RSA (1977, Rivest, Shamir, Adleman)
3. Elliptic Curves (1985, Miller, Koblitz)

Almost all of the other PKC–systems have been broken between their announcement and now. There are many reasons to assume that these three PKC–systems will also be used in the future. All three systems are based on hard mathematical problems. The background of the first two problems is more common knowledge than elliptic curves. This hour I will say a little bit about the elliptic curve cryptosystem (ECC). The world of ECC is changing continuously. In comparison to RSA and DL much more research have been published during the last few years. My impression is that the participation of elliptic curves in the world of cryptography is growing.

3 Elliptic curves

The name "elliptic curve" is based on the ellipse. However it is easy to calculate the surface of the ellipse, it is hard to calculate the circumference of the ellipse. The calculation can be reduced to an integral:

$$\int \frac{1}{\sqrt{x^3 + Ax + B}} \mathbf{d}x.$$

This integral, which cannot be solved easily, was the reason to consider the curve

$$Y^2 = X^3 + AX + B$$

This was done already during the 18th century. Probably, it was Abel in ca. 1820 who introduced the addition of points on the curve. At the moment there are several definitions for an elliptic curve. However the following definition is used usually:

Definition. *An elliptic curves E, defined over an arbitrary field k, is a non-singular plain projective third degree curve over k with a k-rational point O (i.e. with coordinates in k) over E.*

Such a curve can be described by its so-called **Weierstraß form**, in homogeneous coordinates x, y, z,

$$\boxed{E : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3}$$

where $a_1, \cdots, a_6 \in k$, such that the **discriminant** $\Delta \neq 0$. This discriminant[2] is a polynomial expression in the coefficients $a_1, \ldots, a_6$. The restriction $\Delta \neq 0$ is necessary and sufficient for E in order to be non-singular. The curve E has exactly one k-rational point at 'infinity', i.e. $z = 0$, the point $(0 : 1 : 0)$. This point plays the rôle of O (origin). Sometimes we want to express that a curve E is based over field k. We will do this by the notation E/k.

In general we will restrict ourself to the affine part ($z \neq 0$) of elliptic curves E:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

For fields k of characteristic > 2 such as $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{F}_p$ with $p > 3$ we can transform the Weierstraß form for the affine curve by the coordinate transformation

$$X = x + \frac{a_1^2 + 4a_2}{12} \quad \text{and} \quad Y = y + \frac{a_1}{2}x + \frac{a_3}{2}$$

to a curve of the form

$$\boxed{E/k : y^2 = x^3 + Ax + B}$$

with $A, B \in k$ such that the discriminant $\Delta = 4A^3 + 27B^2 \neq 0$. This form will be used in the latter.

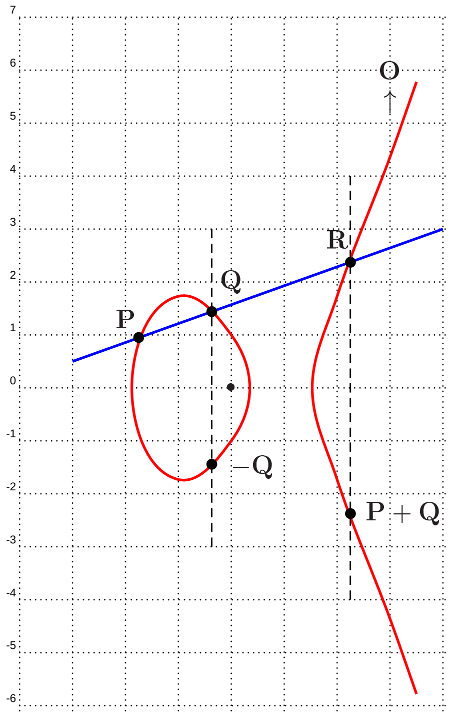
Remark. For practical applications finite fields of the form $k = GF(2^n) = \mathbb{F}_{2^n}$ are very important. For such elliptic curves the theory as mentioned above has to be modified.

3.1 The group of points on elliptic curves

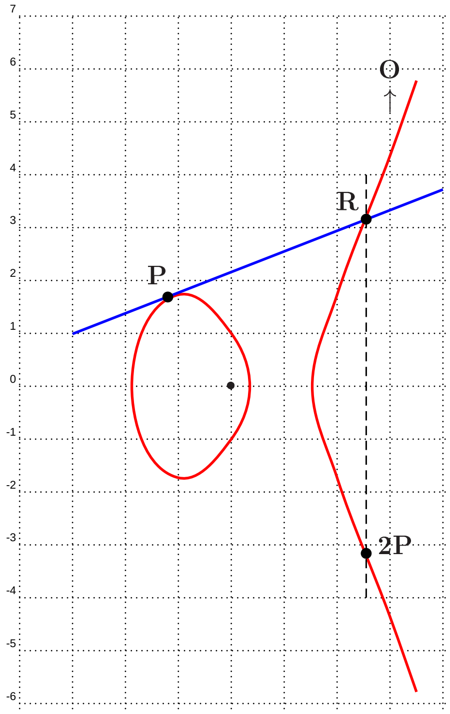
What is the reason that elliptic curves are such interesting objects in algebraic geometry? On each elliptic curve E defined over a field k, the points $E(k)$ form an **abelian group**. The addition of two points P and Q can be

[2]Compare the discriminant $\Delta = b^2 - 4ac$ of the quadratic expression $ax^2 + bx + c$.

shown clearly in the figure below. (here we assume that $k = \mathbb{R}$).



In order to construct the point $2P = P + P$ we draw the tangent in P to the curve:



We will transform this construction into a formula:

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P} \text{ if } P \neq Q, \quad \text{en} \quad \lambda = \frac{3x_P^2 + A}{2y_P} \text{ if } P = Q,$$

here λ is the coefficient of the line through P and Q, resp. of the tangent in P as long as $y_P \neq 0$. If $y_P = 0$ then: $2P = O$. From a straightforward (but simple) calculation with the λ calculated above, follows:

$$\boxed{x_{P+Q} = \lambda^2 - (x_P + x_Q)} \quad \text{and} \quad \boxed{y_{P+Q} = -y_Q - \lambda(x_{P+Q} - x_Q)}$$

and

$$\boxed{x_{2P} = \lambda^2 - 2x_p} \quad \text{and} \quad \boxed{y_{2P} = -\lambda^3 - y_P + 3\lambda x_P}$$

These formulas consist of additions, subtractions and multiplications in the field in which P and Q are defined. Therefore the coordinates of $P + Q$ and $2P$ are in the same field. Of course in order to prove that the points $E(k)$ on an elliptic curve form an abelian group, one has to check the axiomas of an abelian group.[3] The neutral element is the point at infinity $O = (0 : 1 : 0)$. It is easy to calculate the inverse $-P$ of the point $P = (x, y)$: $-P = (x, -y)$. The sum of three points on a line is O. The points P, $-P$ and O are on one line.

3.2 Counting points on elliptic curves

A user of ECC will be interested to know the structure of the group, especially he would like to know the number of points, $\#E(\mathbb{F}_q)$. If he knows $\#E(\mathbb{F}_q)$ he knows whether the Pohlig–Hellman–attack can be applied. It is impossible to write down all points for large q. But it is not neccessary at all. The formula of **Hasse–Weil** can be applied, which reduces the amount of work enormously.

THEOREM. *Let E be an elliptic curve over $\mathbb{F}_q$, then:*

$$\boxed{q + 1 - 2\sqrt{q} \leq \#(E(\mathbb{F}_q)) \leq q + 1 + 2\sqrt{q}}$$

Using this formula and the baby–step–giant–step method of Shanks it is feasable upto 100 bits to calculate the number of points $\#E(\mathbb{F}_q)$. This method chooses an arbitrary point and calculates for a random point P the points P, $2P$, $\ldots$, kP. The X–coordinates of these points are placed in memory. Next kmP, $k(m+1)P$, $\ldots$, $k(m+n)P$ are calculated, until the X–coordinate matches an element from memory. Now we have $k(m+j)P = \pm iP$, for some i, j. From this we deduce that $\#E(\mathbb{F}_q) = k(m + j) \mp i$

For larger values of q we need the help of an algorithm developed by René Schoof. This algorithm will be explained in the sequel, but before we need some definitions.

[3]The associativity is hardly to prove.

3.3 The Frobenius endomorphism

A map which plays a crucial rôle in the theory of elliptic curves over finite fields is the **Frobenius endomorphism**. For a curve $E/\mathbb{F}_q$ we consider the map

$$\begin{array}{rcl} \varphi_q : E(\overline{\mathbb{F}_q}) & \to & E(\overline{\mathbb{F}_q}), \\ \varphi_q : (x,y) & \mapsto & (x^q, y^q) \\ \varphi_q : O & \mapsto & O. \end{array}$$

For two points $P, Q \in E(\overline{\mathbb{F}_q})$ we have $\varphi_q(P+Q) = \varphi_q(P) + \varphi_q(Q)$. It is easy to see that the set $E(\mathbb{F}_q)$ is the set of points which are invariant under φ_q, i.e. for $P \in E(\overline{\mathbb{F}_q})$ we have $P \in E(\mathbb{F}_q) \iff \varphi_q(P) = P$.

The Frobenius endomorphism $\varphi_q : E(\overline{\mathbb{F}_q}) \to E(\overline{\mathbb{F}_q})$ satisfies the characteristic equation

$$\boxed{\varphi_q^2 - t\varphi_q + q = 0}$$

which can be interpretated in the sense of operators which work on the group of points of E:

$$(x^{q^2}, y^{q^2}) - t \cdot (x^q, y^q) + q \cdot (x,y) = O, \quad \forall\ (x,y) \in E(\overline{\mathbb{F}_q}).$$

The integer t which appears in this formula is called **trace of Frobenius**, and is denoted by $\mathrm{Tr}(\varphi_q)$. The following theorem explains the relation between t and the number of points:

Theorem. $\#(E/\mathbb{F}_q) = q + 1 - \mathrm{Tr}(\varphi_q)$.

3.4 The group of torsion points

Let $E/\mathbb{F}_q$ be an elliptic curve. For $n \in \mathbb{N}_{\geq 2}$ we write $E[n] := E(\overline{\mathbb{F}_q})[n]$ for the group of the n-**torsion points** of $E(\overline{\mathbb{F}_q})$, i.e. the points $P \in E(\overline{\mathbb{F}_q})$ with $nP = O$. The structure of the group $E[n]$ is well-known:

$$E[n] \cong \mathbb{Z}/n \oplus \mathbb{Z}/n, \quad \text{if } \gcd(n,q) = 1.$$

3.5 SEA

It is obvious that if we can calculate the trace $\mathrm{Tr}(F_q)$ of Frobenius, then we have information about $E/\mathbb{F}_q$. The calculation of the trace of Frobenius is the kernel of the SEA-algorithm. Recent methods are based on the work of the Dutch mathematician René Schoof done in 1984, they were improved by A.O.L. Atkin and N. Elkies in the years 90 of the last century. Advanced methods from arithmetical algebraic geometry (modulair forms) are used intensively. Finally this method is called **SEA-algorithm** (**S**choof-**E**lkies-**A**tkin). SEA can be used in order to calculate the number of points on an elliptic curve over $\mathbb{F}_p$ for large values of p.

Schoof studied for a prime $\ell \neq p$ the torsion group $E[\ell]$. Then he considered how the Frobenius endomorphism works on $E[\ell]$. The characteristic equation of Frobenius can be reduced modulo ℓ. We have

$$\varphi_q^2 - t_\ell \varphi_q + q_\ell = 0,$$

here $t_\ell \equiv t \bmod \ell$ en $q_\ell \equiv q \bmod \ell$. This equation can be rewritten to

$$t_\ell \varphi_q = \varphi_q^2 + q_\ell.$$

We consider a (generic) point $P = (x, y)$. We calculate the righthandside and lefthandside of previous equation for this point. We find for the righthandside

$$(\varphi_q^2 + q_\ell)(x, y) = (x^{q^2} + \frac{f_1(x,y)}{g_1(x,y)}, y^{q^2} + \frac{f_2(x,y)}{g_2(x,y)}).$$

We eliminate the y in the x-coordinate, since $y^2 = x^3 + Ax + B$. the x-coordinate can be rewritten as the quotient $\frac{F(x)}{G(x)}$. The lefthandside can be rewritten as the quotient $\frac{K_{t_\ell}(x)}{L_{t_\ell}(x)}$. In the lefthandside t_ℓ is unknown. If the correct value of t_ℓ is chosen then $F(x)$ and K_{t_ℓ} have a common non–trivial divisor. We have to chose $t_\ell = 0, 1, 2, \ldots$ until t_ℓ fits. Now by varying ℓ we find related values t_ℓ. t can be calculated using the Chinese Remainder Theorem.

3.6 Satoh

Satoh invented another algorithm for counting points on an elliptic curve, based on the *Verschiebung*. Fouquet, Gaudry en Harley improved this algorithm. The algorithm can be used to count the points on curves E over fields $\mathbb{F}_q$ with $q = p^n$ and n large.

3.7 Monsky–Washnitzer–cohomology

Recently Kedlaya invented an algorithm which is rather comparable to the algorithm of Satoh. It is based on the Monsky–Washnitzer–cohomology. The algorithm is a little bit slower, but the algorithm can be applied in much more circumstances.

3.8 AGM

Mèstre invented another algorithm for counting points on an elliptic curve. It is based on the Algebraic–Geometric–Mean. The method is so new that there are no papers about this algorithm. Harley improved this algorithm and used this algorithm in order to calculated the number of points on a curve over the field $\mathbb{F}_{2^{32003}}$ (august 2002).

3.9 The group structure

If $\#(E(\mathbb{F}_q))$ and its factorisation are known, then a (probabilistic) algorithm due to V. Miller can be used to calculate the group structure of $E(\mathbb{F}_q)$ in about $(ln\, ln\, q)^2$ steps, assumed that q and $\#(E(\mathbb{F}_q))$ have no common divisors.

THEOREM. *$E(\mathbb{F}_q)$ is an abelian group of rank 1 or 2, and can be written as*

$$E(\mathbb{F}_q) = \mathbb{Z}/n_1 \oplus \mathbb{Z}/n_2,$$

where $n_2|n_1$ and $n_2|(q-1)$.

For an arbitrary curve E, n_2 is 1 or 2.

4 Cryptography

4.1 The discrete logarithm (DL)

In an (abelian) group G (multiplicatively written) we can consider the equation $y = x^n$, $x, y \in G$, $n \in \mathbb{Z}$. If x and n are given then y can be calculated easily, however if x en y are given then in general it is hard to calculate n. This is equivalent to the well-known real logarithm we call n the **discrete logaritme** of y related to the base x.

4.2 Diffie–Hellman for elliptic curves (ECDL)

In 1985, V. Miller and, —independently— N. Koblitz suggested a cryptographic protocol based on elliptic curves (ECC). ECC could be an equivalent of DL. Elliptic curves have been studied in mathematics since long time. If you compare elliptic curves˜to RSA and DL you find many advantages: to obtain the same security one can use smaller fields for elliptic curves. Therefore elliptic curves can be implemented easier and faster. This will be the subject of section 4.5.

The Discrete Logarithm for elliptic curves can be applied in the same sense as the "usual" Discrete Logarithm. Suppose that **A**lice and **B**ob would like to exchange a message, and they would like to do this in a cryptographic secure way. They are able to apply the protocol of Diffie–Hellman for creating a common secret key. Then they can use this key for DES or AES, or any other cryptographic protocol.

We show how they can use Diffie–Hellman in order to find a common secret key.

We suppose that **A**lice and **B**ob chose a prime p, a curve E over $\mathbb{F}_p$ and a point P.

- **A**lice choses a secret key k_A and calculates k_AP.
- **A**lice publishes k_AP.
- **B**ob choses a secret key k_B and calculates k_BP.

• **B**ob publishes $k_B P$.
• **A**lice calculates with the information got from **B**ob $k_A(k_B P)$.
• **A**lice and **B**ob decide to use the x–coordinate of the point $k_A k_B P$ being the secret key.

4.3 ElGamal for elliptic curves

Instead of Diffie–Hellman, **A**lice and **B**ob can also decide to use the protocol of ElGamal. This protocol differs from Diffie–Hellman. ElGamal does not create a common key, but using ElGamal a message can be sent from **A**lice to **B**ob. T. ElGamal suggested his Public Key encryption scheme in 1984, before elliptic curves were introduced in cryptography.

Alice would like to send a message to **B**ob.

1. **A**lice and **B**ob agree to a prime p, a curve E and a pointt P,
2. **B**ob chooses a secret key k_B,
3. **B**ob publishes $B = k_B \cdot P$,
4. **A**lice has message m which has to be sent, and calculates the related point M.
5. **A**lice chooses a random number k,
6. **A**lice calculatest $K = k \cdot P$ and $C = M + k \cdot B$,
7. **A**lice sends (K, C),
8. **B**ob calculates $M = C - k_B \cdot K =$
   $(M + k \cdot k_B \cdot P) - k_B \cdot k \cdot P$.

It is not trivial to find a point M for the message m. It is impossible to choose for m the x-coordinate of M. In about 50% of the cases m will not appear as x-coordinate. This problem can be avoided by adding a few bits to m, which can be chosen arbitrarily. If an x-coordinate is known, then it is easy to calculate the related y.

4.4 Attacks on ECC

ECC is a special Discrete Logarithm. Therefore all possible attacks on DL are applicable on ECC as well. We summarise some (well-known) attacks on DL:

1. Exhausted search
2. Baby–step Giant–step

3. Pollard's rho
4. Pohlig–Hellman
5. Index calculus

In order to save ECC against the first three attacks it is important to chose q large enough. In practice q is chosen $q > 2^{160}$ (at least 50 digits). Pohlig–Hellman works if $\#E(\mathbb{F}_q)$ consist of (non–trivial) primedivisors. This can be avoided by varying the parameters of E until the number of points is a prime or a small multiple of a prime. The index calculus works if and only if a *factor base* can be created. Silverman suggested in 1998 a factor base. But unfortunately he failed to use the factor base for an attack. If a good factor base has been found, this will imply that q has to be chosen (much) larger.

Another problem is related to the curve itself. We consider in a separated section the attention on several families of curves which can be attacked with less effort.

4.5 Attacks in Cryptography

In this section we will compare theoretical attacks on symmetric cryptosystems (DES, AES) and asymmetric cryptosystems (RSA, DL, ECC). Before comparing the attacks we will introduce the L–function which is used to express the run time.

$$L_x(v, \lambda) = \exp\left(\lambda (\log x)^v (\log \log x)^{1-v}\right)$$

Here x, v and λ are real numbers with $x > e$ and $0 \leq v \leq 1$. If $v = 1$ then L_x behaves as an polynomial in x while if $v = 0$ then L_x behaves as an polynomial in $\log x$, in formulas

$$\begin{aligned} L_x(1, \lambda) &= x^\lambda \\ L_x(0, \lambda) &= (\log x)^\lambda \end{aligned}$$

Notice that

$$\log \log L_x(v, \lambda) = v \cdot \log \log L_x(1, \lambda) + (1 - v) \cdot \log \log L_x(0, \lambda)$$

interpolates between powers of x and powers of $\log x$. x can be replaced by 2^n in case of an n–bit symmetric cryptosystem, by N, the modulus, in case of RSA or by q in case of finite field $\mathbb{F}_q$.

We have the following list of known attacks:

Crypto	size	year	method	run–time
DES	56 bits	1997	exhausted search	$L_{2^{55}}(1, 1)$
RSA	512 bits	1999	NFS (number field sieve)	$L_N(\frac{1}{3}, 1.9)$
ECC	108 bits	2000	Birthday	$L_{2^{109}}(\frac{1}{2}, \lambda)$

In order to compare attacks in cryptography we compare run times related to the cryptosystems which were broken and we extrapolate these results to larger sizes. Approximately, we get:

•	RSA/DL:	512	640	1024	2048	4096
•	ECC:	103	113	137	181	242
•	AES:	60	63	72	88	110.
	source	*Lenstra/Verheul* (cf. [12])				

5 Which elliptic curves can be chosen?

5.1 Supersingular elliptic curve [Trace 0]

A elliptic curve $E/\mathbb{F}_q$, $q = p^m$, is called **supersingular** if $\mathrm{Tr}(\varphi_q)$ is divisable by p. We restrict ourself to the case $q = p$. In this case we have $\mathrm{Tr}(\varphi_q) = 0$ or $\#(E(\mathbb{F}_p)) = p + 1$.

In 1993 A. Menezes, T. Okamoto and S. Vanstone (cf. [13]) published a remarkable construction in order to reduce the ECDLP to a DLP in an extension of $\mathbb{F}_p$. This construction is based on advanced algebraic geometry for elliptic curves. It appears that the degree of the extension is 2 for supersingular curves over $\mathbb{F}_p$. The ECDLP can be solved in subexponential time. To avoid this attack larger fields have to be used, in order to guarantee the same cryptographic security, which reduces the speed.

The crucial step in the construction of Menezes, Okamoto and Vanstone is based on the use of the **Weil pairing**. Let P, Q and R be points of order n, i.e. $nP = nQ = nR = O$. Let $k \in \mathbb{N}$ such that $E[n] \subset E(\mathbb{F}_{p^k})$. The Weil pairing e_n is a map which sends a pair of points to a n-th power of unity. This n-th power of unity can be embedded in $\mathbb{F}_{p^k}$. Therefore the Weil pairing can be defined by: $e_n : E[n] \times E[n] \to \mathbb{F}_{p^k}$. The Weil pairing has the following proporties:

(i) $e_n(P, O) = 1$,
(ii) $e_n(P, P) = 1$,
(iii) $e_n(P, Q) \cdot e_n(Q, P) = 1$,
(iv) $e_n(P, R) \cdot e_n(Q, R) = e_n(P + Q, R)$.

Suppose that $Q = mP$. Then for arbitrary points R we have $e_n(P, R)^m = e_n(Q, R)$. The problem to find an m such that $Q = mP$ is reduced to the problem to find an m such that $x^m = y$ over $\mathbb{F}_{p^k}$, for $x = e_n(P, R)$ and $y = e_n(Q, R)$.

In the case of supersingular curves over $\mathbb{F}_p$ the ECDLP can be reduced to a “normal” discrete logarithm over $\mathbb{F}_{p^2}$. Menezes, Okamoto en Vanstone were able to deduce that in the case of supersingular curves over $\mathbb{F}_q$, the ECDLP can be reduced to a DL over a field of maximal $\mathbb{F}_{q^6}$.

5.2 Anomalous elliptic curves [Trace 1]

Elliptic curves $E/\mathbb{F}_q$ with $\mathrm{Tr}(\varphi_q) = 1$ are called **anomalous**. If $q = p$, then it could be a good idea to chose an anomalous elliptic curve for cryptographic purposes, because the attack of Pohlig–Hellman cannot be applied. At the end of the last century G. Frey & H.-G. Rück, I. Semaev, T. Satoh & K. Araki and N. Smart simplified the isomorphism between $E(\mathbb{F}_p)$ and the additive group of $\mathbb{F}_p$. In the last group the discrete logarithm problem can be solved easily. It occurs that an explicit isomorphism $\psi : E(\mathbb{F}_p) \xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p^+$ can be found easily.

$$\begin{array}{rcl} \psi : E(\mathbb{F}_p) & \to & \mathbb{F}_p \\ P & \mapsto & \psi(P) \end{array}$$

If we would like to calculate a value m for two points P en Q such that $Q = mP$, then this can be done by $m = \psi(Q)/\psi(P)$.

5.3 Trace 2

Work of G. Frey, M. Müller and H.-G. Rück (1998), based on work of J. Tate and S. Lichtenbaum, has interesting applications in the ECDLP. This result is in fact an extension on the work of Menezes, Okamoto and Vanstone for supersingular curves. If p is a prime such that $p' = \dfrac{p-1}{2}$ is prime as well, and $E/\mathbb{F}_p$ is an elliptic curve with $\mathrm{Tr}(F_p) = 2$, i.e. $\#(E(\mathbb{F}_p)) = p - 1$, then the ECDLP can be solved directly and reduced to the DLP in $\mathbb{F}_p$ in polynomial ($\log m$) time[4]. The used definitions and technics are based on advanced algebraic geometry and are too difficult to explain in this paper.

5.4 Curves on special fields

Recently a complete new set of curves has to be proved to be less secure in use. In 1998 Frey explained at ECC his ideas about replacing elliptic curves by variaties. His ideas have been evaluated by Gaudry, Hess, Smart and Galbraith (cf. [7]).

Their idea is to replace the Elliptic Curve $\mathcal{E}$ over $\mathbb{F}_{q^m}$ by an m-dimensional abelian variety $\mathcal{W}$ over $\mathbb{F}_q$ (here $q = p^l$, in general $p = 2$). Sometimes it is possible to intersect the abelian variety by $m - 1$ hyperplanes, in such a way that the intersection is a special curve, the so called *hyperelliptic curve*. On the hyperelliptic curve it is easier to solve the discrete logarithm problem.

Let $K = \mathbb{F}_{2^n}$, and let the elliptic curve

$$\mathcal{E} : Y^2 + XY = X^3 + AX^2 + B$$

[4]The result of mentioned authors is more general.

be defined over K, i.e. $A, B \in K$. Suppose $n = lm$. Let $q = 2^l$, $k = \mathbb{F}_q$, then K is an extension of k of degree m. Hence there exists a k–basis $\psi_0, \psi_1, \ldots, \psi_{m-1}$. We can express A, B, X, Y in terms of the elements of the k–basis:

$$\begin{aligned} A &= a_0\psi_0 + a_1\psi_1 + \ldots a_{m-1}\psi_{m-1} \\ B &= b_0\psi_0 + b_1\psi_1 + \ldots b_{m-1}\psi_{m-1} \\ X &= x_0\psi_0 + x_1\psi_1 + \ldots x_{m-1}\psi_{m-1} \\ Y &= y_0\psi_0 + y_1\psi_1 + \ldots y_{m-1}\psi_{m-1} \end{aligned}$$

After substituting these equations in the equation of the elliptic curve, we get an equation of a variety $\mathcal{W}$ over k in $2m$ variables. $\mathcal{W}$ is called the *Weil restriction*, and the process is called the *Weil descent*.

The next step is to find a hyperelliptic curve $\mathcal{H}_q$ as a sub–variety in $\mathcal{W}$. This is rather complicated. At the moment a KASH-program of Hess is available (cf. [8]).

6 Implementations

Most of all crypto–sellers either sell elliptic–curve–software as well or have plans to do such in the nearby future. On the internet we couldn't find much information on this kind of information. We tried to find smartcards (chipcards) which could be used for ECC. In general the chips have been produced by other organisations. We found several organisations how produces chips on which ECC has been implemented. We mention: Certicom, Infineon, Motorola, Philips and Siemens. In comparison to RSA it takes a long time to make an ECC–Point–computation:

Below the sizes and calculation–speed of the Infineon–chip SLE 66CX–640P are mentioned:

Crypto	# bits	speed
RSA	1024	220 ms
ECC	160	83 ms
ECC	256	234 ms

Infineon explains these times theirselves because they are not allowed to use the main patents for ECC. (almost all patents for ECC–calculations belong to Certicom.)

References

[1] *A Course in Number Theory and Cryptography*, **N. Koblitz**, GTM 114, Springer-Verlag (199?).

[2] *Elliptic Curve Public Key Cryptosystems*, **A. Menezes**, Kluwer Academic Publishers (1993).

[3] *The Arithmetic of Elliptic Curves*, **J. Silverman**, GTM 106, Springer-Verlag (1986).

Advanced Literature

[4] *Elliptic Curves in Cryptography*, **Ian Blake, Gadiel Seroussi, Nigel P. Smart**, book (1997).

[5] *Schoof's algorithm and isogeny cycles*, **Couveignes, Morain**, (1994) (ANTS I).

[6] *On Satoh's algorithm and its implementation*, **Mireille Fouquet, Pierrick Gaudry, Robert Harley**, (2000).

[7] *Constructive and destructive facets of Weil descent on elliptic curves*, **Pierrick Gaudry, F. Hess, Nigel P. Smart**, (199?).

[8] *An extension of the GHS attack*, **Florian Hess**, (2001) (ECC2001).

[9] *Analysis of the Xedni Calculus Attack*, **Michael J. Jacobson, Neal Koblitz, Joseph H. Silverman, Andreas Stein, Edlyn Teske** Designs, Codes & Cryptography, (2000).

[10] *Solving elliptic curve discrete logarithm problems using Weil descent*, **Michael J. Jacobson, Alfred Menezes, Andreas Stein**, (2001).

[11] *The State of Elliptic Curve Cryptography*, **Neal Koblitz, Alfred Menezes, Scott Vanstone**, Designs, Codes & Cryptography, (2000).

[12] *Selecting Cryptographic Key Sizes*, **Arjen Lenstra, Erik Verheul**, Journal of Cryptology, (2000).

[13] *Reducing elliptic curve logarithms to logarithms in a finite field*, **A. Menezes, T. Okamoto, S. Vanstone**, (1991) (Proceedings of the 23rd Annual ACM Symposium on Theory of Computing)

[14] *Elliptic curves and their use in cryptography*, **Miller**, (1998) (ECC98)

[15] *The Xedni Calculus and the Elliptic Curve Discrete Logarithm Problem*, **Joseph H. Silverman**, (1998) (ECC98)

[16] *Elliptic curve discrete logarithms and the index calculus* , **Joseph H. Silverman**, (1998) (ECC98)

[17] *Satoh point counting in characteristic 2*, **Berit Skjernaa**, (2000)

[18] *The Past Fifteen Years of Public-Key Cryptography*, **Scott Vanstone**, (2000) (ECC2000)

Software

[19] *LiDIA*, ftp.informatik.tu-darmstadt.de/pub/TI/systems/LiDIA/current/, (freeware).

[20] *MAGMA*, www.maths.usyd.edu.au:8000/comp/magma/Overview.html.

[21] *Maple+package APECS* Maple: www.maplesoft.com, APECS: Ian Connell email:connell@math.mcgill.ca (freeware).

[22] *Miracl*, ftp.compapp.dcu.ie/pub/crypto/miracl.zip (freeware)

[23] *NumberTheory Libary (NTL, Victor Shoup) + Elliptic Curve–package (SVIC, Matthijs Coster)*, www.shoup.net/ntl/index.html + www.coster.demon.nl/ntl/ (freeware)

[24] *Pari/GP*, ftp://megrez.math.u-bordeau.fr/pub/pari/ (freeware)

Internetsites

[25] www.coster.demon/elliptic/index.html, Matthijs Coster, Information about elliptic curves.

[26] www.tml.hut.fi/ helger/crypto/link/public/elliptic/, Helger, Elliptic Curves Pointers.

[27] www.ecstr.com, Comparison of keysizes of symmetric and asymmetric cryptographic systems, Arjen Lenstra, Erik Verheul.