A Digital Signature Scheme for Long-Term Security

Dimitrios Poulakis and Robert Rolland

August 25, 2012

Introduction

Many applications of the Information Technology, such as encryption of sensitive medical data or digital signatures for contracts, need long term cryptographic security. Today's cryptography provides strong tools only for short term security.

Introduction

Many applications of the Information Technology, such as encryption of sensitive medical data or digital signatures for contracts, need long term cryptographic security. Today's cryptography provides strong tools only for short term security.

In order to achieve the goal of long-term security for the signatures, Mageberg in his thesis (Technische Universitat Darmstadt 2002) suggested the use of more than one independent signature schemes.

Introduction

Many applications of the Information Technology, such as encryption of sensitive medical data or digital signatures for contracts, need long term cryptographic security. Today's cryptography provides strong tools only for short term security.

In order to achieve the goal of long-term security for the signatures, Mageberg in his thesis (Technische Universitat Darmstadt 2002) suggested the use of more than one independent signature schemes.

Thus, if one of them is broken, then it can be replaced by a new secure one and the document has to be re-signed. Mageberg has proposed protocols that support multiple signatures including the update management in the case of a break.

In this talk we propose a signature scheme which provides an efficient solution to the above problem.

In this talk we propose a signature scheme which provides an efficient solution to the above problem.

It is based on the problems of the integer factorization and the discrete logarithm for elliptic curves. If any of these problems is broken, the other will still be valid and hence the signature will be protected (as long as quantum computers are not present).

Elliptic Curves

An *elliptic curve* over a field K is a smooth curve defined by an equation of the form

$$y^2 + a_1 yx + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

where $a_1, a_3, a_2, a_4, a_6 \in K$.

Elliptic Curves

An *elliptic curve* over a field K is a smooth curve defined by an equation of the form

$$y^2 + a_1 yx + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

where $a_1, a_3, a_2, a_4, a_6 \in K$.

The set of points $E(K)$ of E over K has an abelian group stucture defined by

$$P \oplus Q \oplus R = 0 \iff P, Q, R \text{ collinear.}$$

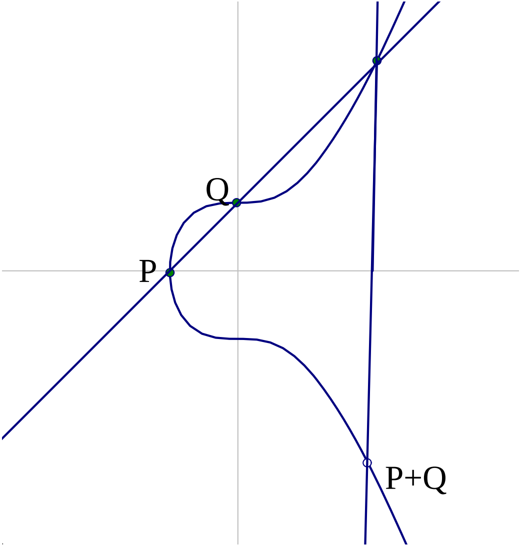

Figure: sum of $P = (-1, 0)$ and $Q = (0, 1)$ over $Y^2 = X^3 + 1$.

Weil pairing

Let E be an elliptic curve over a field K, $\bar{K}$ the algebraic closure of K, and $n \in \mathbb{Z}^+$ with $char(K) \not| n$. Consider the sets

$$\mu_n = \{x \in \bar{K} / \ x^n = 1\}, \quad E[n] = \{P \in E(\bar{K}) / \ nP = 0\}.$$

Weil pairing

Let E be an elliptic curve over a field K, $\bar{K}$ the algebraic closure of K, and $n \in \mathbb{Z}^+$ with $char(K) \not| n$. Consider the sets

$$\mu_n = \{x \in \bar{K} / \ x^n = 1\}, \quad E[n] = \{P \in E(\bar{K}) / \ nP = 0\}.$$

The *Weil pairing* is an application $e_n : E[n] \times E[n] \to \mu_n$, which can be efficiently constucted, s. t.

Weil pairing

Let E be an elliptic curve over a field K, $\bar{K}$ the algebraic closure of K, and $n \in \mathbb{Z}^+$ with $char(K) \not| n$. Consider the sets

$$\mu_n = \{x \in \bar{K} /\ x^n = 1\}, \quad E[n] = \{P \in E(\bar{K}) /\ nP = 0\}.$$

The *Weil pairing* is an application $e_n : E[n] \times E[n] \to \mu_n$, which can be efficiently constucted, s. t.

1. e_n is bilinear;

Weil pairing

Let E be an elliptic curve over a field K, $\bar{K}$ the algebraic closure of K, and $n \in \mathbb{Z}^+$ with $char(K) \not| n$. Consider the sets

$$\mu_n = \{x \in \bar{K} / \ x^n = 1\}, \quad E[n] = \{P \in E(\bar{K}) / \ nP = 0\}.$$

The *Weil pairing* is an application $e_n : E[n] \times E[n] \to \mu_n$, which can be efficiently constucted, s. t.

1. e_n is bilinear;
2. $e_n(S, T) = e_n(T, S)^{-1}, \ \ \forall S, T \in E[n]$;

Weil pairing

Let E be an elliptic curve over a field K, $\bar{K}$ the algebraic closure of K, and $n \in \mathbb{Z}^+$ with $char(K) \nmid n$. Consider the sets

$$\mu_n = \{x \in \bar{K} / \ x^n = 1\}, \quad E[n] = \{P \in E(\bar{K}) / \ nP = 0\}.$$

The *Weil pairing* is an application $e_n : E[n] \times E[n] \to \mu_n$, which can be efficiently constucted, s. t.

1. e_n is bilinear;
2. $e_n(S, T) = e_n(T, S)^{-1}, \quad \forall S, T \in E[n]$;
3. $e_n(S, T) = 1, \ \forall S \in E[n] \iff T = 0$;

Weil pairing

Let E be an elliptic curve over a field K, $\bar{K}$ the algebraic closure of K, and $n \in \mathbb{Z}^+$ with $char(K) \not| n$. Consider the sets

$$\mu_n = \{x \in \bar{K} / \ x^n = 1\}, \quad E[n] = \{P \in E(\bar{K}) / \ nP = 0\}.$$

The *Weil pairing* is an application $e_n : E[n] \times E[n] \to \mu_n$, which can be efficiently constucted, s. t.

1. e_n is bilinear;
2. $e_n(S, T) = e_n(T, S)^{-1}, \ \ \forall S, T \in E[n]$;
3. $e_n(S, T) = 1, \ \forall S \in E[n] \iff \ T = 0$;
4. $e_n(S^\sigma, T^\sigma) = e_n(S, T)^\sigma, \ \ \forall \sigma \in Gal(\bar{K}/K)$.

Weil pairing

Let E be an elliptic curve over a field K, $\bar{K}$ the algebraic closure of K, and $n \in \mathbb{Z}^+$ with $char(K) \not| n$. Consider the sets

$$\mu_n = \{x \in \bar{K} / \ x^n = 1\}, \quad E[n] = \{P \in E(\bar{K}) / \ nP = 0\}.$$

The *Weil pairing* is an application $e_n : E[n] \times E[n] \to \mu_n$, which can be efficiently constucted, s. t.

1. e_n is bilinear;
2. $e_n(S, T) = e_n(T, S)^{-1}, \quad \forall S, T \in E[n]$;
3. $e_n(S, T) = 1, \ \forall S \in E[n] \iff T = 0$;
4. $e_n(S^\sigma, T^\sigma) = e_n(S, T)^\sigma, \quad \forall \sigma \in Gal(\bar{K}/K)$.

Note that they are also Tate pairing, eta, ate and omega pairings.

The Proposed Scheme

A user $\mathcal{A}$, who wants to create a public and a private key selects:

The Proposed Scheme

A user $\mathcal{A}$, who wants to create a public and a private key selects:

1. primes p_1, p_2 s.t. the factorization of $n = p_1 p_2$ is infeasible;

The Proposed Scheme

A user $\mathcal{A}$, who wants to create a public and a private key selects:

1. primes p_1, p_2 s.t. the factorization of $n = p_1 p_2$ is infeasible;
2. an elliptic curve $E/\mathbb{F}_q$, $P \in E(\mathbb{F}_q)$ with $\mathrm{ord}(P) = n$ and a pairing e_n on E s.t. $e_n(P, P)$ is a primitive n-th root of 1;

The Proposed Scheme

A user $\mathcal{A}$, who wants to create a public and a private key selects:

1. primes p_1, p_2 s.t. the factorization of $n = p_1 p_2$ is infeasible;
2. an elliptic curve $E/\mathbb{F}_q$, $P \in E(\mathbb{F}_q)$ with $\mathrm{ord}(P) = n$ and a pairing e_n on E s.t. $e_n(P, P)$ is a primitive n-th root of 1;
3. $g, a, b \in \{1, \ldots, n\}$ with $\gcd(g, n) = 1$ and computes
   $$Q = g^a P, \quad r = g^b \bmod n, \quad R = g^{a-ab} P;$$

The Proposed Scheme

A user $\mathcal{A}$, who wants to create a public and a private key selects:

1. primes p_1, p_2 s.t. the factorization of $n = p_1 p_2$ is infeasible;
2. an elliptic curve $E/\mathbb{F}_q$, $P \in E(\mathbb{F}_q)$ with $\mathrm{ord}(P) = n$ and a pairing e_n on E s.t. $e_n(P, P)$ is a primitive n-th root of 1;
3. $g, a, b \in \{1, \ldots, n\}$ with $\gcd(g, n) = 1$ and computes
$$Q = g^a P, \quad r = g^b \bmod n, \quad R = g^{a-ab} P;$$
4. hash functions $H : \{0, 1\}^* \rightarrow < P >$ and $h : \{0, 1\}^* \rightarrow \{0, \ldots, n-1\}$.

The Proposed Scheme

A user $\mathcal{A}$, who wants to create a public and a private key selects:

1. primes p_1, p_2 s.t. the factorization of $n = p_1 p_2$ is infeasible;
2. an elliptic curve $E/\mathbb{F}_q$, $P \in E(\mathbb{F}_q)$ with $\mathrm{ord}(P) = n$ and a pairing e_n on E s.t. $e_n(P, P)$ is a primitive n-th root of 1;
3. $g, a, b \in \{1, \ldots, n\}$ with $\gcd(g, n) = 1$ and computes
   $$Q = g^a P, \quad r = g^b \bmod n, \quad R = g^{a-ab} P;$$
4. hash functions $H : \{0,1\}^* \to < P >$ and
   $h : \{0,1\}^* \to \{0, \ldots, n-1\}$.

$\mathcal{A}$ publishes E, e_n, h and H.

The Proposed Scheme

A user $\mathcal{A}$, who wants to create a public and a private key selects:

1. primes p_1, p_2 s.t. the factorization of $n = p_1 p_2$ is infeasible;
2. an elliptic curve $E/\mathbb{F}_q$, $P \in E(\mathbb{F}_q)$ with $\mathrm{ord}(P) = n$ and a pairing e_n on E s.t. $e_n(P, P)$ is a primitive n-th root of 1;
3. $g, a, b \in \{1, \ldots, n\}$ with $\gcd(g, n) = 1$ and computes
   $$Q = g^a P, \quad r = g^b \bmod n, \quad R = g^{a-ab} P;$$
4. hash functions $H : \{0,1\}^* \to < P >$ and $h : \{0,1\}^* \to \{0, \ldots, n-1\}$.

$\mathcal{A}$ publishes E, e_n, h and H.
Public key : (g, P, Q, R, r, n).

The Proposed Scheme

A user $\mathcal{A}$, who wants to create a public and a private key selects:

1. primes p_1, p_2 s.t. the factorization of $n = p_1 p_2$ is infeasible;
2. an elliptic curve $E/\mathbb{F}_q$, $P \in E(\mathbb{F}_q)$ with $\mathrm{ord}(P) = n$ and a pairing e_n on E s.t. $e_n(P, P)$ is a primitive n-th root of 1;
3. $g, a, b \in \{1, \ldots, n\}$ with $\gcd(g, n) = 1$ and computes
$$Q = g^a P, \quad r = g^b \bmod n, \quad R = g^{a-ab} P;$$
4. hash functions $H : \{0,1\}^* \rightarrow < P >$ and $h : \{0,1\}^* \rightarrow \{0, \ldots, n-1\}$.

$\mathcal{A}$ publishes E, e_n, h and H.
Public key : (g, P, Q, R, r, n).
Private key : (a, b, p_1, p_2).

Signature generation

$\mathcal{A}$ wants to sign a message $m \in \{0, 1\}^*$.

Signature generation

$\mathcal{A}$ wants to sign a message $m \in \{0,1\}^*$.

Then he computes

$$(x, y) = g^{ab}H(m)$$

and

$$s = bh(m) + a - ab \bmod \phi(n).$$

Signature generation

$\mathcal{A}$ wants to sign a message $m \in \{0,1\}^*$.

Then he computes

$$(x, y) = g^{ab} H(m)$$

and

$$s = bh(m) + a - ab \mod \phi(n).$$

The signature of m is the couple (x, s).

Verification

Suppose that (x, s) is the signature of m.

Verification

Suppose that (x, s) is the signature of m.

The receiver determines y such that $\Sigma = (x, y) \in E(\mathbb{F}_q)$.

Verification

Suppose that (x, s) is the signature of m.

The receiver determines y such that $\Sigma = (x, y) \in E(\mathbb{F}_q)$.

He accepts the signature if and only if

$$e_n(\pm g^s \Sigma, P) = e_n(r^{h(m)} H(m), Q)$$

Verification

Suppose that (x, s) is the signature of m.

The receiver determines y such that $\Sigma = (x, y) \in E(\mathbb{F}_q)$.

He accepts the signature if and only if

$$e_n(\pm g^s \Sigma, P) = e_n(r^{h(m)} H(m), Q)$$

and

$$g^s r^{-h(m)} P = R.$$

Security

If an attacker wants to compute a and b from the public key, he has to compute

Security

If an attacker wants to compute a and b from the public key, he has to compute

- a discrete logarithm in the group $< P >$

Security

If an attacker wants to compute a and b from the public key, he has to compute

- a discrete logarithm in the group $< P >$
- two discrete logarithms modulo n.

Security

If an attacker wants to compute a and b from the public key, he has to compute

- a discrete logarithm in the group $< P >$
- two discrete logarithms modulo n.

Note that an algorithm which computes the discrete logarithm modulo n implies an algorithm which breaks the Composite Diffie-Hellman key distribution scheme for n and any algorithm which break this scheme can be used to factorize n.

Suppose there is an oracle $\mathcal{O}$ such that given a public key and a message m provides a signature for m.

Suppose there is an oracle $\mathcal{O}$ such that given a public key and a message m provides a signature for m.

We shall use $\mathcal{O}$ in order to factorize n which is the product of two (unknown) primes.

Suppose there is an oracle $\mathcal{O}$ such that given a public key and a message m provides a signature for m.

We shall use $\mathcal{O}$ in order to factorize n which is the product of two (unknown) primes.

Let $p(d, a)$ be the smallest prime of the arithmetic progression $\{a + kd/\ k \geq 0\}$. Put

$$p(d) = \max\{p(d, a)/\ 1 \leq a < d,\ \gcd(a, d) = 1\}.$$

Suppose there is an oracle $\mathcal{O}$ such that given a public key and a message m provides a signature for m.

We shall use $\mathcal{O}$ in order to factorize n which is the product of two (unknown) primes.

Let $p(d,a)$ be the smallest prime of the arithmetic progression $\{a+kd/\ k \geq 0\}$. Put

$$p(d) = \max\{p(d,a)/\ 1 \leq a < d,\ \gcd(a,d) = 1\}.$$

Conjecture

(Heath-Brown, 1978) $p(d) < Cd(\log d)^2$.

It follows that there is $j < C(\log 4n)^2$ s. t. $q = 4nj + 4n - 1$ is a prime.

It follows that there is $j < C(\log 4n)^2$ s. t. $q = 4nj + 4n - 1$ is a prime.

We can find q in polynomial time, using a primality test $O((\log n)^2)$ times.

It follows that there is $j < C(\log 4n)^2$ s. t. $q = 4nj + 4n - 1$ is a prime.

We can find q in polynomial time, using a primality test $O((\log n)^2)$ times.

Since $q \equiv 3 \pmod 4$, the elliptic curve $y^2 = x^3 + x$ on $\mathbb{F}_q$ is supersingular. Thus

$$|E(\mathbb{F}_q)| = q + 1 = 4n(j + 1)$$

and so, $E(\mathbb{F}_q)$ has a point P of order n.

We consider $g, a, b \in \{1, \dots, n-1\}$ and we compute

$$r = g^b \bmod n, \quad Q = g^a P, \quad R = g^{a-ab} P.$$

(g, P, Q, R, r, n) is a public key for our system.

We consider $g, a, b \in \{1, \ldots, n-1\}$ and we compute

$$r = g^b \bmod n, \quad Q = g^a P, \quad R = g^{a-ab} P.$$

(g, P, Q, R, r, n) is a public key for our system.

Then $\mathcal{O}$ gives signatures (S_i, s_i) for the messages m_i $(i = 1, \ldots, k)$ and so, we have

$$s_i = bh(m_i) + a - ab \bmod \phi(n).$$

It follows that $\phi(n)$ divides the gcd d of the above numbers.

We consider $g, a, b \in \{1, \ldots, n-1\}$ and we compute

$$r = g^b \bmod n, \quad Q = g^a P, \quad R = g^{a-ab} P.$$

(g, P, Q, R, r, n) is a public key for our system.

Then $\mathcal{O}$ gives signatures (S_i, s_i) for the messages m_i $(i = 1, \ldots, k)$ and so, we have

$$s_i = bh(m_i) + a - ab \bmod \phi(n).$$

It follows that $\phi(n)$ divides the gcd d of the above numbers.

Assuming the numbers $s_i - bh(m_i) - a + ab$ follow the uniform distribution, the probability that two such numbers has gcd $> \phi(n)$ is quite small. Thus, $\phi(n)$ can be easily computed and so the factorization of n.

We consider the following problem:

We consider the following problem:

Computational co-Diffie - Hellman on (G_1, G_2). Let G_1 and G_2 be two (multiplicative) cyclic groups of prime order p; g_1 is a fixed generator of G_1 and g_2 is a fixed generator of G_2; ψ is an isomorphism from G_2 to G_1, with $\psi(g_2) = g_1$. Given γ_2, $\gamma_2^{\alpha} \in G_2$ and $h \in G_1$ as input, compute $h^{\alpha} \in G_1$.

We consider the following problem:

Computational co-Diffie - Hellman on (G_1, G_2). Let G_1 and G_2 be two (multiplicative) cyclic groups of prime order p; g_1 is a fixed generator of G_1 and g_2 is a fixed generator of G_2; ψ is an isomorphism from G_2 to G_1, with $\psi(g_2) = g_1$. Given γ_2, $\gamma_2^\alpha \in G_2$ and $h \in G_1$ as input, compute $h^\alpha \in G_1$.

The best known algorithm for solving the above problem is to compute discrete logarithm in G_2.

We consider the following problem:

Computational co-Diffie - Hellman on (G_1, G_2). Let G_1 and G_2 be two (multiplicative) cyclic groups of prime order p; g_1 is a fixed generator of G_1 and g_2 is a fixed generator of G_2; ψ is an isomorphism from G_2 to G_1, with $\psi(g_2) = g_1$. Given γ_2, $\gamma_2^{\alpha} \in G_2$ and $h \in G_1$ as input, compute $h^{\alpha} \in G_1$.

The best known algorithm for solving the above problem is to compute discrete logarithm in G_2.

We solve this problem, using $\mathcal{O}$, for the subgroups of order p_1 and p_2 of the group of $< P >$.

Let $P_i \in E(\mathbb{F}_q)$ with $\mathrm{ord}(P_i) = p_i$ $(i = 1, 2)$. We take $g_i \in \{1, \ldots, p_i - 1\}$ and $a, b \in \{1, \ldots, \phi(n)\}$ and we compute

$$Q_i = g_i^a P_i, \quad R_i = g_i^{a-ab} P_i, \quad r_i = g_i^b \bmod p_i, \quad (i = 1, 2).$$

Let $P_i \in E(\mathbb{F}_q)$ with $\mathrm{ord}(P_i) = p_i$ $(i = 1, 2)$. We take $g_i \in \{1, \ldots, p_i - 1\}$ and $a, b \in \{1, \ldots, \phi(n)\}$ and we compute

$$Q_i = g_i^a P_i, \quad R_i = g_i^{a-ab} P_i, \quad r_i = g_i^b \bmod p_i, \quad (i = 1, 2).$$

Let $g, r \in \{1, \ldots, n-1\}$ such that $g \equiv g_i \pmod{p_i}$, $r \equiv r_i \pmod{p_i}$, $(i = 1, 2)$. We set

$$P = P_1 + P_2, \quad Q = Q_1 + Q_2, \quad R = R_1 + R_2.$$

It follows that

$$Q = g^a P, \quad R = g^{a-ab} P.$$

Let $P_i \in E(\mathbb{F}_q)$ with $\mathrm{ord}(P_i) = p_i$ $(i = 1, 2)$. We take $g_i \in \{1, \ldots, p_i - 1\}$ and $a, b \in \{1, \ldots, \phi(n)\}$ and we compute

$$Q_i = g_i^a P_i, \quad R_i = g_i^{a-ab} P_i, \quad r_i = g_i^b \bmod p_i, \quad (i = 1, 2).$$

Let $g, r \in \{1, \ldots, n-1\}$ such that $g \equiv g_i \pmod{p_i}$, $r \equiv r_i \pmod{p_i}$, $(i = 1, 2)$. We set

$$P = P_1 + P_2, \quad Q = Q_1 + Q_2, \quad R = R_1 + R_2.$$

It follows that

$$Q = g^a P, \quad R = g^{a-ab} P.$$

(g, P, Q, R, r, n) is a public key for our signature scheme.

We apply $\mathcal{O}$ on (g, P, Q, R, r, n) and $m \in \{0,1\}^*$, and we get the signature (S, s) for m.

We apply $\mathcal{O}$ on (g, P, Q, R, r, n) and $m \in \{0,1\}^*$, and we get the signature (S, s) for m.

Thus, $S = g^{ab}H(m)$, whence $g^s r^{-h(m)} S = g^a H(m)$.

We apply $\mathcal{O}$ on (g, P, Q, R, r, n) and $m \in \{0,1\}^*$, and we get the signature (S, s) for m.

Thus, $S = g^{ab}H(m)$, whence $g^s r^{-h(m)} S = g^a H(m)$.

Set $S = S_1 + S_2$, $H(m) = H_1 + H_2$, where $S_i, H_i \in < P_i >$ $(i = 1, 2)$.

We apply $\mathcal{O}$ on (g, P, Q, R, r, n) and $m \in \{0,1\}^*$, and we get the signature (S, s) for m.

Thus, $S = g^{ab}H(m)$, whence $g^s r^{-h(m)} S = g^a H(m)$.

Set $S = S_1 + S_2$, $H(m) = H_1 + H_2$, where $S_i, H_i \in < P_i >$ $(i = 1, 2)$.

Then,

$$g_i^s r_i^{-h(m)} S_i = g_i^a H_i,$$

and so, $g_i^s r_i^{-h(m)} S_i$ is the solution of the computational problem co-Diffie-Hellman with $\gamma_2 = P_i$, $\alpha = g_i^a$ and $h = H_i$ $(i = 1, 2)$.

The elliptic curve and the pairing

The construction of an elliptic curve $E/\mathbb{F}_q$, having $P \in E(\mathbb{F}_q)$ with $\mathrm{ord}(P) = n$ is achieved by the following algorithm:

The elliptic curve and the pairing

The construction of an elliptic curve $E/\mathbb{F}_q$, having $P \in E(\mathbb{F}_q)$ with $\mathrm{ord}(P) = n$ is achieved by the following algorithm:

1. select large prime numbers p_1, p_2 s.t. the factorization of $p_1 - 1$, $p_2 - 1$ is known and the computation of the factorization of $n = p_1 p_2$ is infeasible;

The elliptic curve and the pairing

The construction of an elliptic curve $E/\mathbb{F}_q$, having $P \in E(\mathbb{F}_q)$ with $\mathrm{ord}(P) = n$ is achieved by the following algorithm:

1. select large prime numbers p_1, p_2 s.t. the factorization of $p_1 - 1$, $p_2 - 1$ is known and the computation of the factorization of $n = p_1 p_2$ is infeasible;
2. select a random prime number p and compute $m = \mathrm{ord}_n(p)$;

The elliptic curve and the pairing

The construction of an elliptic curve $E/\mathbb{F}_q$, having $P \in E(\mathbb{F}_q)$ with $\mathrm{ord}(P) = n$ is achieved by the following algorithm:

1. select large prime numbers p_1, p_2 s.t. the factorization of $p_1 - 1$, $p_2 - 1$ is known and the computation of the factorization of $n = p_1 p_2$ is infeasible;
2. select a random prime number p and compute $m = \mathrm{ord}_n(p)$;
3. find, using Broker's algorithm, a supersingular elliptic curve E over $\mathbb{F}_{p^{2m}}$ with trace $t = 2p^m$;

The elliptic curve and the pairing

The construction of an elliptic curve $E/\mathbb{F}_q$, having $P \in E(\mathbb{F}_q)$ with $\mathrm{ord}(P) = n$ is achieved by the following algorithm:

1. select large prime numbers p_1, p_2 s.t. the factorization of $p_1 - 1$, $p_2 - 1$ is known and the computation of the factorization of $n = p_1 p_2$ is infeasible;
2. select a random prime number p and compute $m = \mathrm{ord}_n(p)$;
3. find, using Broker's algorithm, a supersingular elliptic curve E over $\mathbb{F}_{p^{2m}}$ with trace $t = 2p^m$;
4. return $\mathbb{F}_{p^{2m}}$ and E.

The elliptic curve and the pairing

The construction of an elliptic curve $E/\mathbb{F}_q$, having $P \in E(\mathbb{F}_q)$ with $\mathrm{ord}(P) = n$ is achieved by the following algorithm:

1. select large prime numbers p_1, p_2 s.t. the factorization of $p_1 - 1$, $p_2 - 1$ is known and the computation of the factorization of $n = p_1 p_2$ is infeasible;
2. select a random prime number p and compute $m = \mathrm{ord}_n(p)$;
3. find, using Broker's algorithm, a supersingular elliptic curve E over $\mathbb{F}_{p^{2m}}$ with trace $t = 2p^m$;
4. return $\mathbb{F}_{p^{2m}}$ and E.

Since $t = 2p^m$ and $m = \mathrm{ord}_n(p)$, we get $|E(\mathbb{F}_{p^{2m}})| = (p^m - 1)^2$ and $n | p^m - 1$. Hence $E(\mathbb{F}_{p^{2m}})$ contains a point of order n.

The elliptic curve and the pairing

The construction of an elliptic curve $E/\mathbb{F}_q$, having $P \in E(\mathbb{F}_q)$ with $\mathrm{ord}(P) = n$ is achieved by the following algorithm:

1. select large prime numbers p_1, p_2 s.t. the factorization of $p_1 - 1$, $p_2 - 1$ is known and the computation of the factorization of $n = p_1 p_2$ is infeasible;
2. select a random prime number p and compute $m = \mathrm{ord}_n(p)$;
3. find, using Broker's algorithm, a supersingular elliptic curve E over $\mathbb{F}_{p^{2m}}$ with trace $t = 2p^m$;
4. return $\mathbb{F}_{p^{2m}}$ and E.

Since $t = 2p^m$ and $m = \mathrm{ord}_n(p)$, we get $|E(\mathbb{F}_{p^{2m}})| = (p^m - 1)^2$ and $n | p^m - 1$. Hence $E(\mathbb{F}_{p^{2m}})$ contains a point of order n.

Under the assumption of the Generalized Riemman Hypothesis, the time complexity of this algorithm is polynomial.

For the pairing we take ϵ_n to be one of the pairings of Weil, Tate, eta, ate, omega on $E[n]$ together with a distortion map ψ such that the points P and $\psi(P)$ is a generating set for $E[n]$ and we consider the pairing

$$e_n(P, Q) = \epsilon_n(P, \psi(Q)).$$

Another method for the construction of the elliptic curve E which is quite practical is given by the following algorithm:

Another method for the construction of the elliptic curve E which is quite practical is given by the following algorithm:

1. draw at random a prime number p_1 of a given size l;

Another method for the construction of the elliptic curve E which is quite practical is given by the following algorithm:

1. draw at random a prime number p_1 of a given size l;
2. draw at random a number p_2 of size l;

Another method for the construction of the elliptic curve E which is quite practical is given by the following algorithm:

1. draw at random a prime number p_1 of a given size l;
2. draw at random a number p_2 of size l;
3. repeat $p_2 = \mathrm{NextPrime}(p_2)$ until $4p_1p_2 - 1$ is prime;

Another method for the construction of the elliptic curve E which is quite practical is given by the following algorithm:

1. draw at random a prime number p_1 of a given size l;
2. draw at random a number p_2 of size l;
3. repeat $p_2 = \mathrm{NextPrime}(p_2)$ until $4p_1p_2 - 1$ is prime;
4. return $p = 4p_1p_2 - 1$.

Another method for the construction of the elliptic curve E which is quite practical is given by the following algorithm:

1. draw at random a prime number p_1 of a given size l;
2. draw at random a number p_2 of size l;
3. repeat $p_2 = \mathrm{NextPrime}(p_2)$ until $4p_1p_2 - 1$ is prime;
4. return $p = 4p_1p_2 - 1$.

The elliptic curve $E : y^2 = x^3 + ax$, where $-a$ is not a square in $\mathbb{F}_p$, is supersingular and so $|E(\mathbb{F}_p)| = p + 1 = 4p_1p_2$. Hence there is $P \in E(\mathbb{F}_p)$ with $\mathrm{ord}(P) = p_1p_2$.

Another method for the construction of the elliptic curve E which is quite practical is given by the following algorithm:

1. draw at random a prime number p_1 of a given size l;
2. draw at random a number p_2 of size l;
3. repeat $p_2 = \mathrm{NextPrime}(p_2)$ until $4p_1p_2 - 1$ is prime;
4. return $p = 4p_1p_2 - 1$.

The elliptic curve $E : y^2 = x^3 + ax$, where $-a$ is not a square in $\mathbb{F}_p$, is supersingular and so $|E(\mathbb{F}_p)| = p + 1 = 4p_1p_2$. Hence there is $P \in E(\mathbb{F}_p)$ with $\mathrm{ord}(P) = p_1p_2$.

If ϵ is one of the previous pairings on $E[n]$, then we use the distortion map $\psi(Q) = \psi(x, y) = (-x, iy)$ with $i^2 = -1$ and so, we have the pairing:

$$e(P, Q) = \epsilon(P, \psi(Q)).$$

An Example

Let $n = p_1 p_2$, where p_1, p_2 are 256-bits primes given by

$$p_1 = 6648101541610901309221290229437670283577419589920755980686054166957863749 4231$$

and

$$p_2 = 1157385760891529093145823398348422486009642738646439842030828553445799070 38313.$$

The number

$q = 4p_1p_2 - 1 = 30777672244885922298367181451455799589815604954364949152875842939564481247670869579707155280684905464796492983111143287609791419983028317761589419333889211$

is a prime.

The number

$q = 4p_1p_2 - 1 = 30777672244885922298367181451455799589815604954364949152875842939564481247670869579707155280684905464796492983111143287609791419983028317761589419333889211$

is a prime.

Since $q \equiv 3 \pmod 4$, the elliptic curve

$$E : y^2 = x^3 + x$$

over $\mathbb{F}_q$ is superesingular.

The point $P = (x(P), y(P))$, where

$$x(P) = 2492343830287910304155093376887381755381585900 7663$$

$$6972230312491954089508938594293101431086136135995118826 70$$

$$676138255514518447219689120752272772341649471097,$$

$$y(P) = 7379969973486764966658607017040721934904356153827 9$$

$$2210827517600538539755358116422263315026068694342336247 34$$

$$779779132109106217320985031461076144560383831 00$$

has order $n = p_1 p_2$.

We take $g = 2$,

$$a = 2^{256} + 2^{9} + 1 = 115792089237316195423570985008687907853269984665640564039457584007913129640449,$$

$$b = 2^{128} + 2^{100} + 1 = 340282368188589063691604008928471416833.$$

We have

$$r = 2^b \bmod n = 60604738311804190280025275442744666692049$$

$$836109319481630443372486036335615842187469452441526711 22$$

$$84647646590300127020573917994700502444986860669431119 5640,$$

We have

$r = 2^b \bmod n = 60604738311804190280025275442744666692049$

$8361093194816304433724860363356158421874694524415267112 2$

$846476465903001270205739179947005024449868606694311195640,$

$2^a \bmod n = 30170327810598461233195990938464557925983833 0$

$0588875602809811232191097667270756706255964182155241639 5$

$5319907854573382245426564094874852045289557121519086 7,$

We have

$$r = 2^b \bmod n = 6060473831180419028002527544274466692049$$

$$8361093194816304433724860363356158421874694524415267112 2$$

$$84647646590300127020573917994700502444986860669431119564 0,$$

$$2^a \bmod n = 3017032781059846123319599093846455792598383 30$$

$$0588875602809811232191097667270756706255964182155241639 5$$

$$5319907854573382245426564094874852045289557121519086 7,$$

$$2^{a(1-b)} \bmod n = 6901235301332732306263093894248462771489 18$$

$$2738937811099893935523975261846628680897065414699668317 0$$

$$3048453509930121476438921649862265355773278725114764186 4.$$

We consider the points $Q = 2^a P = (x(Q), y(Q))$, where

$$x(Q) = 7260248943743510410597070580439186623312590993698497282989406963716051852174477547835747074046966659229829111355206667689244366615968601129874346167442208,$$

$$y(Q) = 1804789523816175348587711731174083153281119499241138802179335269409050631413675108169733886226831548047728894457761544353817492371971818591598163063576179 8$$

and $R = 2^{a-ab}P = (x(R), y(R))$, where

$$x(R) = 10151186689439654567058518823964915155717966972$$

$$738632185569449759143395815855509840876862062561458081$$

$$97532841580391886676491297127195784414219665252153884 0,$$

$$y(R) = 11830609568816187455064602957532997672345403803 7$$

$$42470622163211050426407526147503476874128489377669604 87$$

$$30660200567015539148455811330398091422405264826631 37.$$

Public key : $(2, P, Q, R, r, n)$.
Private key : (a, b, p_1, p_2).

Public key : $(2, P, Q, R, r, n)$.
Private key : (a, b, p_1, p_2).

We use the Weil or Tate pairing with the distorsion map $\psi(x, y) = (-x, iy)$ with $i^2 = -1$.

THANK YOU