

Elliptic Curve Ordered Digital Signature

Alexander Rostovtsev Elena Makhovenko
Olga Shemyakina

8th April 2004

Department of Information Security of Computer Systems
St. Petersburg State Polytechnic University,
Polytechnicheskaya st., 29, St. Petersburg, 195251, Russia
{rostovtsev, helen, olga}@ssl.stu.neva.ru

Abstract. New cryptographic primitive, ordered digital signature, is proposed. It allows ordering the documents being signed without any timestamping or numeration. This primitive can be based both on ECDSA or Schnorr protocol. To order signatures, elliptic curve equation is being changed with small order isogenies, corresponding to elliptic curve homomorphisms. Initial elliptic curve number of points is a multiple of 2 or 3, and connected component of isogeny graph is large. Once current document is signed, j -invariant of the next curve is computed, isogenous to the current curve, and the next curve is chosen. Isogeny is also used for base point and public key computation. The next isogeny can be chosen at random or deterministically. It can be computed only from the previous one, so the set of signed documents is linearly ordered.

Key words: Elliptic curve, isogeny, digital signature, ECDSA.

1 Introduction

Digital signature is a multi-purpose cryptographic tool for e-documents authentication. ECDSA is one of the most widely used digital signature standards [1]. Its security depends on elliptic curve discrete logarithm problem.

Let p be a large prime, \mathbf{F}_p be a field of p elements and $f(x)$ be a cubic polynomial, having no multiple roots over algebraic closure $\bar{\mathbf{F}}_p$ of the field \mathbf{F}_p . Elliptic curve $E(\mathbf{F}_p)$ is given by equation

$$y^2 \equiv f(x) \pmod{p}. \quad (1)$$

The set of elliptic curve points includes the solutions of equation (1) and the point at infinity P_∞ . Elliptic curve points form finite additive Abelian group with zero element P_∞ . According to Hasse's theorem, inequality holds for the group order: $|p + 1 - \#E(\mathbf{F}_p)| < 2\sqrt{p}$ [2].

Let $Q \in E(\mathbf{F}_p)$ be the base point in the cyclic group G of large prime order $r > \sqrt{\#E(\mathbf{F}_p)}$. Then elliptic curve point group has unique subgroup of order r . According to ECDSA, primes p and r are of 256 and 160 bit length respectively.

Elliptic curve discrete logarithm problem is: given points $P, Q \in G$ of order r find logarithm w such that $P = wQ$. If the group G cannot be embedded into the field \mathbf{F}_p additive group or into the field \mathbf{F}_p finite extension multiplicative group of small degree [3] [4], then Pollard's algorithm [5] of complexity $O(\sqrt{r})$ is the best for discrete logarithm computing.

Digital signature protocol ECDSA makes use of the following parameters: elliptic curve $E(\mathbf{F}_p)$ and base point Q . Secret key is logarithm w . Public key is point $P = wQ$.

Digital signature generation is performed as follows.

1. Integer $k, 0 < k < r$, is generated at random.
2. Point $R = (x_R, y_R) = kQ$ is computed. If the congruence $x_R \equiv 0 \pmod{r}$ holds then go to step 1.
3. For the message M hash-function $e = h(M)$ is computed.
4. Element s is computed from the congruence $e \equiv wx_R + ks \pmod{r}$. If the congruence $s \equiv 0 \pmod{r}$ holds then go to step 1.
5. Output: $(M, x_R \pmod{r}, s)$.

Digital signature verification is performed as follows.

1. If $0 < s, x_R < r$ does not hold, then digital signature is invalid.
2. $s^{-1} \pmod{r}$ is computed.
3. For the message M hash-function $e = h(M)$ is computed.
4. Point $R' = (x_{R'}, y_{R'}) = s^{-1}eQ - (s^{-1}x_R \pmod{r})P$ is computed.
5. If the congruence $x_{R'} \equiv x_R \pmod{r}$ holds then digital signature is valid else it is invalid.

Sometimes information systems are to allow ordering the documents being signed. For example, how one can determine which of two signed documents was signed later? In that case the signer changes the document and adds auxiliary fields, containing current time or number of the document. It is inconvenient, for example, when blind signature is used.

Blind signature means that the signer does not know the text to be signed. Corresponding protocol is based on one-way invertible transformation of digital signature equation (hash function is not used). Then digital signature generation protocol is as follows.

1. Signer generates at random exponent $\hat{k}, 0 < \hat{k} < r$, computes point $\hat{R} = \hat{k}Q$ and sends \hat{R} to the client.

2. Client generates at random mask $\alpha, 0 < \alpha < r$, and computes point $R = \alpha\hat{R}$, computes mask β solving congruence $x_{\hat{R}} \equiv \alpha^{-1}\beta x_R \pmod{r}$, computes masked message $\hat{m} \equiv \alpha^{-1}\beta m \pmod{r}$ and sends \hat{m} to the signer. Notice that this implies $R = kQ$, where $k \equiv \alpha\hat{k} \pmod{r}$.
3. Signer computes s as solution of congruence $\hat{m} \equiv wx_{\hat{R}} + \hat{k}s \pmod{r}$ and sends it to client.
4. Client verifies that signature $(\hat{s}, x_{\hat{R}})$ is valid and then deletes mask from signature: $s \equiv \beta^{-1}\hat{s} \pmod{r}$. Then (x_R, s) is valid signature for message m .

This protocol corresponds to congruence $\alpha^{-1}\beta m \equiv w\alpha^{-1}\beta x_R + \alpha^{-1}\beta ks \pmod{r}$, reducing by multiple $\alpha^{-1}\beta$ gives correct digital signature equation. It is easy to see that signer cannot join additional information such as time stamp or number of the message. So verifier has no obvious way to determine which of two signed messages is earliest.

We propose ECDSA modification, which allows checking the order of the documents being signed without any numerators or time stamps. We call this primitive *ordered digital signature*.

2 Elliptic curve isogenies

Let $p > 3$. Then invertible affine change of variables converts polynomial $f(x)$ in (1) to $f(x) = x^3 + Ax + B$, where $4A^3 + 27B^2 \not\equiv 0 \pmod{p}$. Isomorphism of elliptic curves $y^2 = x^3 + Ax + B$ and $y'^2 = x'^3 + A'x' + B'$ is given by the formulae $y' = u^3y, x' = u^2x, A' = u^4A, B' = u^6B$ for any $u \neq 0$.

Any elliptic curve defines function field $\mathbf{F}_p(E) = \mathbf{F}_p(x, y)/(y^2 - f(x))$ and is defined by invariant $j = 12^3 \cdot 4A^3 / (4A^3 + 27B^2) \pmod{p}$ up to isomorphism. One-to-one correspondence can be established between elliptic curve and j -invariant, for example, by choosing minimal possible integer A .

Characteristic equation over the complex number field \mathbf{C} holds for elliptic curve $E(\bar{\mathbf{F}}_p)$:

$$\pi^2 - T\pi + p = 0, \tag{2}$$

where $\pi(x, y) = (x^p, y^p)$ is Frobenius endomorphism and $T = p + 1 - \#E(\mathbf{F}_p)$. Let $D_\pi = T^2 - 4p$ be discriminant of Frobenius equation.

Isogeny of elliptic curves $E_1(\mathbf{F}_p)$ and $E_2(\mathbf{F}_p)$ is a map $\varphi : E_1(\mathbf{F}_p) \rightarrow E_2(\mathbf{F}_p), \varphi \in (\mathbf{F}_p(E))^2$, for which $\varphi(P_\infty) = P_\infty$. Isogeny kernel includes points, mapped into P_∞ . The degree $\deg(\varphi)$ of isogeny φ is equal to kernel cardinality over algebraic closed field. Isogeny kernel for isogeny of prime degree l coincides with cyclic torsion group of order l . Isogeny is uniquely determined by its kernel. As there are $l + 1$ cyclic groups of order l in fundamental parallelogram, there exist $l + 1$ isogenies of degree l over algebraic closed field.

Elliptic curves are isogenous if and only if they have the same number of points [2]. Each elliptic curve has $O(\sqrt{p})$ isogenous curves. Each isogeny φ has

a dual one $\hat{\varphi} : E_2(\mathbf{F}_p) \rightarrow E_1(\mathbf{F}_p)$ of the same degree, where $\varphi\hat{\varphi}$ is $E_2(\mathbf{F}_p)$ -point multiplication by l , and $\hat{\varphi}\varphi$ is $E_1(\mathbf{F}_p)$ -point multiplication by l .

Elliptic curve isogeny gives homomorphism of corresponding Abelian groups. If isogeny degree is not a multiple of r , then isogeny gives isomorphism of cyclic groups of order r . If $\varphi : E_1(\mathbf{F}_p) \rightarrow E_2(\mathbf{F}_p)$ is isogeny then

$$\varphi(wQ) = w\varphi(Q). \quad (3)$$

So if $P = wQ$ for E_1 -points, then $\varphi(P) = w\varphi(Q)$ for E_2 -points.

Given isogeny of degree l , j -invariants of isogenous elliptic curves are defined as the roots over \mathbf{F}_p of symmetric modular polynomials $\Phi_l(u, v) \in \mathbf{Z}[u, v]$, constructed according to the theory of modular functions [6]. Modular polynomials for $l = 2, 3$ are:

$$\begin{aligned} \Phi_2(u, v) = & u^3 + v^3 - u^2v^2 + 1488uv(u + v) - 162000(u^2 + v^2) + \\ & + 40773375uv + 8748 \cdot 10^6(u + v) - 157464 \cdot 10^9; \end{aligned}$$

$$\begin{aligned} \Phi_3(u, v) = & u^4 + v^4 - u^3v^3 + 2232u^2v^2(u + v) - 1069956uv(u^2 + v^2) + \\ & + 36864000(u^3 + v^3) + 2587918086u^2v^2 + 8900222976000uv(u + v) + \\ & + 452984832 \cdot 10^6(u^2 + v^2) - 770845966336 \cdot 10^6uv + 1855425871872 \cdot 10^9(u + v). \end{aligned}$$

If j is j -invariant of given elliptic curve, then j -invariants of isogenous curves are the roots of polynomial $\Phi_l(u, j)$ over the field \mathbf{F}_p . For the prime $l \neq 2$ polynomial Φ_l has two roots if $(\frac{D_\pi}{l}) = 1$, has no roots if $(\frac{D_\pi}{l}) = -1$, has one or $l + 1$ roots if $D_\pi \equiv 0 \pmod{l}$. Isogeny multiplication is associative and commutative [7].

For $l = 2$ we can set $E_1(\mathbf{F}_p) : y^2 \equiv x^3 + ax^2 + bx \pmod{p}$, where $b \neq 0$ and $a^2 - 4b \neq 0$, $E_2(\mathbf{F}_p) : v^2 \equiv u^3 - 2au^2 + (a^2 - 4b)u \pmod{p}$ for the equation (2).

Isogeny with the kernel $\{(0, 0)\} \cup P_\infty$ is:

$$\begin{aligned} \varphi : E_1 & \rightarrow E_2, \\ (u, v) & = \left(\frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2} \right). \end{aligned}$$

With a change of variable x to $x - a/3$, elliptic curve $E_1(\mathbf{F}_p)$ is reduced to ordinary form $y^2 \equiv x^3 + Ax + B \pmod{p}$.

Let $E_1 : y^2 = x^3 + Ax + B$, $E_2(K) : v^2 = u^3 + A_1u + B_1$ and let $(x_R, y_R) \in E_1$ be affine point of order 3 (point of inflection). Isogeny of degree 3 is given as

$$u = \frac{x^2(2x_R - x) + x(2A + 5x_R^2) + 4B + 2Ax_R - 2x_R^3}{(x - x_R)^2};$$

$$v = y \frac{x^2(3x_R - x) - x(2A + 9x_R^2) - 8B - 6Ax_R - x_R^3}{(x - x_R)^3};$$

$$A_1 = -9A - 30x_R^2; B_1 = -27B - 70x_R^3 - 42Ax_R.$$

Elliptic curve isogeny of prime degree $l \geq 5$ can be computed in such a way [8]. Let $E_1(K) : y^2 = x^3 + Ax + B; E_2(K) : v^2 = u^3 + A_1u + B_1$; let $(x_R, y_R) \in E_1(K)$ be affine point of order l . Isogeny kernel includes affine points of order l from the set $R \cup -R$, where $R \cap -R = \emptyset$. So R consists of $(l-1)/2$ points.

For $Q \in R$ we set $g_{Q,x} = 3x_Q^2 + A; g_{Q,y} = -2y_Q; s_Q = 4x_Q^3 + 4Ax_Q + 4B; t_Q = 6x_Q^2 + 4A$. Then isogeny is given as

$$u = x + \sum_{Q \in R} \left(\frac{t_Q}{x - x_Q} + \frac{s_Q}{(x - x_Q)^2} \right);$$

$$v = y - \sum_{Q \in R} \left(\frac{2y s_Q}{(x - x_Q)^3} + \frac{(y - y_Q)t_Q}{(x - x_Q)^2} - \frac{g_{Q,x}g_{Q,y}}{(x - x_Q)^2} \right).$$

Elliptic curve $E_2(K)$ coefficients are

$$A_1 = A - 5 \sum_{Q \in R} t_Q, \quad B_1 = B - 7 \sum_{Q \in R} (s_Q + x_Q t_Q).$$

Given elliptic curve $E_1(\mathbf{F}_p)$ and isogeny of degree l , one can define the set of isogenous elliptic curves, taking isogeny composition into account. The set of isogenous elliptic curves can be described by isogeny graph, with the vertices corresponding to elliptic curves and the edges corresponding to isogenies of degree l . As each isogeny has a dual one, isogeny graph is non-directed. In practice, isogeny graph consists of isomorphic trees, joined together by a cycle.

Elliptic curve is defined by its conductor m , where conductor is positive integer for which $\mathbf{Z}[m\sqrt{D}]$ is endomorphisms ring of elliptic curve over \mathbf{F}_p and D is square-free divisor of D_π . Elliptic curves, forming isogeny graph cycle, have the same m value [7].

Ordered digital signature uses isogenous elliptic curves from isogeny graph cycle $E_1(\mathbf{F}_p) \rightarrow E_2(\mathbf{F}_p) \rightarrow \dots$

3 Ordered signature

Ordered digital signature is based on ECDSA. The difference is that elliptic curve is to have large cycle of isogenies of small degree l . ECDSS allows such type of curves.

Elliptic curve, used for digital signature, is to have isogeny of small degree l (for example, $l = 3$), for which polynomial Φ_l has exactly two roots over the field \mathbf{F}_p . Once the message is signed, current elliptic curve $E_i(\mathbf{F}_p)$ is changed: new elliptic curve is computed, its invariant j_{i+1} is a root of polynomial $\Phi_l(j_{i+1}, j_i) \pmod{p}$. Let $P_i, Q_i \in E_i(\mathbf{F}_p)$ be images of initial points P, Q . Then $P_{i+1} =$

$\varphi(P_i), Q_{i+1} = \varphi(Q_i)$. If an equality $P = wQ$ holds for initial elliptic curve, then an equality $P_i = wQ_i$ holds for all i according to equation (3). So, elliptic curve modification does not modify secret key w .

Ordered digital signature protocol makes use of the following parameters (all signatures are checked by the same prover): initial elliptic curve $E(\mathbf{F}_p)$ with j -invariant j , j -invariant j_1 of the next elliptic curve and initial point Q . Invariant j_1 is used to define direction in j -invariant cycle. Isogeny is to keep elliptic curve conductor invariable. Logarithm w is a secret key. Point $P = wQ$ is initial public key.

Digital signature generation is performed as follows.

1. Integer $k, 0 < k < r$, is generated at random.
2. Point $R = (x_R, y_R) = kQ$ is computed. If congruence $x_R \equiv 0 \pmod{r}$ holds then go to step 1.
3. For the message M hash-function $e = h(M)$ is computed.
4. Element s is computed from the congruence $e \equiv wx_R + ks \pmod{r}$. If the congruence $s \equiv 0 \pmod{r}$ holds then go to step 1.
5. Output: $(M, x_R \pmod{r}, s)$.
6. j -invariant of the next elliptic curve, different from j -invariant of the current curve, is computed as a root of modular polynomial $\Phi_l(u, j) \pmod{p}$. Elliptic curve equation is changed.
7. Points $Q \leftarrow \varphi(Q), P \leftarrow \varphi(P)$ are computed.

(Steps 6, 7 modify elliptic curve, base point and public key.)

Digital signature verification is performed as follows.

1. If $0 < s, x_R < r$ does not hold, then signature is invalid.
2. $s^{-1} \pmod{r}$ is computed.
3. For the message M hash-function $e = h(M)$ is computed.
4. Point $R' = (x_{R'}, y_{R'}) = s^{-1}eQ - s^{-1}x_R \pmod{r}P$ is computed.
5. If the congruence $x_{R'} \equiv x_R \pmod{r}$ holds then digital signature is valid else it is invalid.
6. If digital signature is valid then j -invariant of the next elliptic curve, different from j -invariant of the current curve, is computed as a root of modular polynomial $\Phi_l(u, j) \pmod{p}$. Elliptic curve equation is changed and the points $Q \leftarrow \varphi(Q), P \leftarrow \varphi(P)$ are computed.

(Step 6 modifies elliptic curve, base point and public key.)

If we want to find out which of two documents was signed first, we are to compute isogeny sequence for all elliptic curves, beginning from initial one, and to verify digital signature according to ECDSA. Cyclic structure of isogeny graph gives natural linear ordering of elliptic curves and induces linear ordering of digital signatures.

The primitive suggested can be based on different elliptic curve signature schemes, for example ElGamal [9] or Schnorr [10] protocol. Elliptic curve modification is performed similarly.

Using isogenies for elliptic curve modification does not decrease digital signature strength, because isogenies do not simplify elliptic curve discrete logarithm problem.

References

- [1] ANSI X9.62–1998, Public key cryptography for the financial industry: the elliptic curve digital signature algorithm (ECDSA)
- [2] Silverman, J.H.: The arithmetic of elliptic curves, Springer–Verlag, 1986
- [3] Menezes, A., Okamoto, T., Vanstone, S.: Reducing elliptic curve logarithms to logarithms in finite fields. *IEEE Transactions on Information Theory*, **39** (1993) 1639–1636
- [4] Semaev, I.: Evaluation of discrete logarithms in a group of p -torsion points of an elliptic curve in characteristic p . *Mathematics of Computation*, **67** (1998) 353–356
- [5] Pollard, J.M.: Monte Carlo methods for index computation (mod p). *Mathematics of Computation*, **32** (1978) 918–924
- [6] Lang, S.: *Elliptic functions*. Springer-Verlag. 1987
- [7] Kohel, D.: Endomorphism rings of elliptic curves over finite fields. PhD Thesis, David Kohel, Berkeley, December 1996
- [8] Lercier, R., Morain, F.: Algorithms for computing isogenies between elliptic curves. *Computational perspectives on number theory. AMS/IP Studies on Advanced Mathematics. Vol. 7*
- [9] ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, **IT–31** (1985) 469–472
- [10] Schnorr, C.P.: Efficient identification and signatures for smart cards. *Advances in Cryptology — CRYPTO’ 89. LNCS, 435* (1990), Springer-Verlag, 239–252