Journal of Math-for-Industry, Vol. 3 (2011A-9), pp. 89–92

Math-for-industry
Education & Research Hub

Some relations between Semaev's summation polynomials and Stange's elliptic nets

Tsunekazu Saito, Shun'ichi Yokoyama, Tetsutaro Kobayashi and Go Yamamoto

Received on February 21, 2011 / Revised on March 23, 2011

Abstract. There are two decision methods for the decomposition of multiple points on an elliptic curve, one based on Semaev's summation polynomials and the other based on Stange's elliptic nets. This paper presents some relations between these two methods. Using these relations, we show that an index calculus attack for the elliptic curve discrete logarithm problem (ECDLP) over extension fields via an elliptic net is equivalent to such an attack via Semaev's summation polynomials.

Keywords. Index calculus attack, Semaev's summation polynomials, elliptic nets.

1. Introduction

1.1. Semaev's Summation Polynomials and Index Calculus Attack for the ECDLP over Extension Fields

Let k be a field and E be an elliptic curve defined over k on an affine plane $\mathbb{A}^2(\overline{k})$. For a point $P = (x(P), y(P)) \in E$ and a nonnegative integer m, a evaluation of

$$mP = 0$$

is obtained using the m-division polynomial ψ_m associated with E.

Semaev gave the following theorem for decomposition of multiple points,

$$v_1P_1 + \cdots + v_nP_n = 0,$$

where $v_1, \ldots, v_n$ are integers and $P_1, \ldots, P_n$ are points on E.

Theorem 1 (Semaev [7]). *1. For any elliptic curve defined over arbitrary field k and any integer $n \in \mathbb{Z}_{\geq 2}$, there exists a polynomial*

$$S_n(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n]$$

such that for any points $P_1, \ldots, P_n \in E$, there exist $\epsilon_1, \ldots, \epsilon_n \in \{\pm 1\}$ such that $\epsilon_1P_1 + \cdots + \epsilon_nP_n = 0$ if and only if $S_n(x(P_1), \ldots, x(P_n)) = 0$.

2. Suppose $char(k) \neq 2, 3$ and $E : y^2 = 4x^3 + ax + b$; then polynomial S_n is given explicitly as follows:

$$\begin{aligned} &S_2(X_1, X_2) = X_1 - X_2, \\ &S_3(X_1, X_2, X_3) = (X_1 - X_2)^2X_3^2 \\ &\quad -2\left((X_1 + X_2)\left(\frac{a}{4} + X_1X_2\right) + \frac{b}{2}\right)X_3 \\ &\quad + \left(X_1X_2 - \frac{a}{4}\right)^2 - b(X_1 + X_2), \end{aligned}$$

and

$$S_n(X_1, \ldots, X_n) = Res_X(S_j(X_1, \ldots, X_{j-1}, X), S_{n-j+2}(X_j, \ldots, X_n, X)),$$

for any $n \geq 4$ and $3 \leq j \leq n-1$. Here Res_X stands for resultant with respect to X.

3. The degree of polynomial S_n as a polynomial in X_i is 2^{n-2}.

By Gaudry, it was shown that the Semaev's summation polynomials are useful for an index calculus attack for its elliptic curve discrete logarithm problem over extension fields [5].

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a prime such that $q \neq 2, 3$, and $\mathbb{F}_{q^n}$ is the extension field of degree n. The elliptic curve discrete logarithm problem (ECDLP) over extension fields is for elliptic curve E over the extension field $\mathbb{F}_{q^n}$, for any point $P \in E(\mathbb{F}_{q^n})$ and $A \in \langle P \rangle$, the problem to find the minimal integer m such that $A = mP$. If q is a pseudo-Mersenne prime number and the extension field has a binomial or trinomial as its minimal polynomial, a protocol in elliptic curve cryptography based on the ECDLP over extension fields results in faster running algorithms than that based on the ECDLP over prime fields because the modular reduction of finite fields can be computed [2].

It is important to analyze how secure a high-level cryptography technique is. Therefore we build an algorithm to solve the ECDLP over extension fields efficiently, and calculate the algorithmic calculation complexity. In the process, we will make use of a famous algorithm for the index calculus attack on the ECDLP over extension fields via Semaev's summation polynomials [5].

Now we define the factor basis of $E(\mathbb{F}_{q^n})$,

$$\mathfrak{F} = \{P \in E(\mathbb{F}_{q^n}) |\ x(P) \in \mathbb{F}_q\},$$

and let s be the size of $\mathfrak{F}$. An index calculus attack for the ECDLP over extension fields is defined by the following steps:

Step 1. For $i = 1 \ldots, s$ and random integers $m_i \in \mathbb{Z}/\mathrm{ord}P\mathbb{Z}$ we assume the relation given by $m_i P = \sum_{F \in \mathfrak{F}} f_{iF} F$.

Step 2. Compute values $\log_P F_i$ from the linear equation

$$\begin{pmatrix} m_1 \\ m_2 \\ \cdots \\ m_s \end{pmatrix} P = (f_{ij}) \begin{pmatrix} F_1 \\ F_2 \\ \cdots \\ F_s \end{pmatrix}$$

Step 3. For random $m, m' \in \mathbb{Z}/\mathrm{ord}P\mathbb{Z}$ redefine the relation by

$$mA + m'P = \sum_{F \in \mathfrak{F}} f_F F.$$

Step 4. Compute $\log_P A$ using the form given in step 3 and $\log_P F_i$.

To obtain a relation between a random point $m_i P \in E(\mathbb{F}_{q^n})$ and points of the factor basis $\mathfrak{F}$, Gaudry gave a decomposition algorithm using Semaev's summation polynomial S_n.

Theorem 2 (Gaudry [5]). *For any point P in $E(\mathbb{F}_{q^n})$ and $Q_1, \ldots, Q_n \in \mathbb{F}_q$, the following three conditions are equivalent.*

(1). There are points $F_1, \ldots, F_n \in \mathfrak{F}$ such that $x(F_1) = Q_1, \ldots, x(F_n) = Q_n$ and $P = F_1 + \cdots + F_n$.

(2). For the $(n+1)$-th Semaev's summation polynomial S_{n+1},

$$S_{n+1}(Q_1, \ldots, Q_n, x(P)) = 0.$$

(3). Let $\{t_i | i = 1, \ldots, n\}$ be a basis of field extension $\mathbb{F}_{q^n}/\mathbb{F}_q$, and

$$S_{n+1}(X_1, \ldots, X_n, x(P)) = \sum_{i=1}^{n} s^i_{n+1,P}(X_1, \ldots, X_n) t_i,$$

where $s^i_{n+1,P} \in \mathbb{F}_q[X_1, \ldots, X_n]$; then $(Q_1, \ldots, Q_n)$ is a $\mathbb{F}_q$ rational point of $V(s^1_{n+1,P}, \ldots, s^n_{n+1,P})$, the variety defined by $s^1_{n+1,P}, \ldots, s^n_{n+1,P}$.

Using this theorem, we will obtain the desired relations by solving algebraic equations using either the Gröbner basis or multipolynomial resultant [3]. This attack was created and estimated by Diem [4] and improved by Nagao, Joux, and Vitse [10],[6].

Stange gave a decision method for the decomposition problem with multi-variable elliptic functions. Let k be a number field, and E be an elliptic curve over k. The Weierstrass σ function is

$$\sigma(z) = z \prod_{\omega \in L_E \setminus \{0\}} \left(1 - \frac{z}{\omega}\right) \exp\left(\frac{z}{\omega} + \frac{z^2}{2\omega^2}\right),$$

where L_E is the lattice on $\mathbb{C}$ associated with the elliptic curve E.

For an integer vector $v = (v_1, \ldots, v_n) \in \mathbb{Z}^n$ and complex variables $z = (z_1, \ldots, z_n) \in \mathbb{C}^n$, Stange defined the multivariable elliptic function

$$\Psi_v(z) = \frac{\sigma(v_1 z_1 + \cdots + v_n z_n)}{\prod_{i=1}^n \sigma(z_i)^{\sum_{j=1}^n 2v_i^2 - v_i v_j} \prod_{1 \le s < t \le n} \sigma(z_s + z_t)^{v_s v_t}}.$$

This function has a period L_E for each variable. We are able to assume a point P on E corresponds to a point on $\mathbb{C}$ by the pullback $\pi^{-1} : E \simeq \mathbb{C}/L_E \longrightarrow \mathbb{C}$. Stange gave the following decision method for decomposition of points by $\Psi_v(z)$.

Theorem 3 (Stange [8]). *For points $P_1, \ldots, P_n \in E$ such that $P_i \neq \pm P_j (i \neq j)$ and an integer vector $v = (v_1, \ldots, v_n)$, $v_1 P_1 + \cdots + v_n P_n = 0$ holds if and only if $\Psi_v(P_1, \ldots, P_n) = 0$.*

Moreover, for fixed points $P_1, \ldots, P_n \in E$ such that $P_i \neq \pm P_j (i \neq j)$, the map

$$\begin{aligned} W : \mathbb{Z}^n &\longrightarrow k, \\ v &\longmapsto \Psi_v(P_1, \ldots, P_n) \end{aligned}$$

is called the elliptic net associated with $P_1, \ldots, P_n$. This elliptic net satisfies the condition that for any integer vectors $p, q, r, s \in \mathbb{Z}^n$,

$$\begin{aligned} &W(p+q+s)W(p-q)W(r+s)W(r) \\ &\quad + W(q+r+s)W(q-r)W(p+s)W(p) \\ &\quad\quad + W(r+p+s)W(r-p)W(q+s)W(q) = 0. \end{aligned}$$

This elliptic net is an expansion of elliptic divisibility sequences which satisfy the following relation:

$$h_{m+n} h_{m-n} h_1^2 = h_{n+1} h_{n-1} h_m^2 + h_{m+1} h_{m-1} h_n^2.$$

2. Relations between Semaev's Summation Polynomials and Stange's Elliptic nets

Let k be a number field and K a rational function field generated by functions $\wp(z_1), \ldots, \wp(z_n)$, where $\wp(z_i)$ is the Weierstrass $\wp$ function. Let

$$L = k(\wp(z_1), \wp'(z_1), \ldots, \wp(z_n), \wp'(z_n))$$

be the Galois extension over K. Then its Galois group $Gal(L/K) = \{\pm 1\}^n$ acts on L as follows: for any $(\epsilon_1, \ldots, \epsilon_n) \in Gal(L/K)$ and $f(z_1, \ldots, z_n) \in L$,

$$(\epsilon_1, \ldots, \epsilon_n).f(z_1, \ldots, z_n) = f(\epsilon_1 z_1, \ldots, \epsilon_n z_n).$$

Semaev's summation polynomial is used to check a decomposition using only x coordinates of points on an elliptic curve. In this case, S_n is regarded as a polynomial in K. On the other hand, $\Psi_v(z)$ is regarded as an element in L in general. Note that for a vector v, $\Psi_v(z)$ is an intermediate field of L/K.

Theorem 4. *For any integer $n \in \mathbb{Z}_{\geq 2}$ and elliptic curve E over a number field k,*

$$N_{L/K}(\Psi_v(z)) = S_n(\wp(v_1z_1),\ldots,\wp(v_nz_n))^2 \times \frac{\prod_{i=1}^n \Psi_{v_i}(z_i)^{2^n}}{\prod_{1\leq s<t\leq n}(\wp(z_s)-\wp(z_t))^{2^{n-1}v_sv_t}}.$$

The left-hand side of the equation in this theorem, which is defined as

$$N_{L/K}(\Psi_v(z)) = \prod_{\epsilon_1,\ldots,\epsilon_n\in\{\pm 1\}} \Psi_v(\epsilon_1z_1,\ldots,\epsilon_nz_n) = \frac{\prod_{\epsilon_1,\ldots,\epsilon_n\in\{\pm1\}}\Psi_{(\epsilon_1v_1,\ldots,\epsilon_nv_n)}(z)}{\prod_{1\leq s<t\leq n}(\wp(z_s)-\wp(z_t))^{2^{n-1}v_sv_t}},$$

checks whether for points $P_1,\ldots,P_n \in E$ such that $P_i \neq \pm P_j, (i\neq j)$ there exist $\epsilon_1,\ldots,\epsilon_n \in \{\pm 1\}$ such that $\epsilon_1v_1P_1+\cdots+\epsilon_nv_nP_n = 0$. Furthermore, the Semaev's summation polynomial S_n is irreducible and is a material providing a method to obtain precise decompositions, the norm $N_{L/K}(\Psi_v(z))$ has $S_n(\wp(v_1z_1),\ldots,\wp(v_nz_n))$ as a factor. On the other hand, the second factor of the right-hand side

$$\frac{\prod_{i=1}^n \Psi_{v_i}(z_i)^{2^n}}{\prod_{1\leq s<t\leq n}(\wp(z_s)-\wp(z_t))^{2^{n-1}v_sv_t}}$$

checks whether $v_iP_i = 0$ and $P_i = \pm P_j, (i\neq j)$ hold. However, this factor is not essential for the decomposition decision.

The above shows that Semaev's summation polynomial S_n and the norm of an elliptic net play the same role for the purpose of decision of the decomposition of points on an elliptic curve. Moreover, to eliminate $\wp'(z_i)$ from $\Psi_v(z)$ and to reduce K for an index calculus attack for the ECDLP using Semaev's summation polynomial and deciding decomposition using only the x coordinate, we compute coefficients of $\mathrm{Irr}(\Psi_v(z), L/K)$. However, arbitrary coefficients of $\mathrm{Irr}(\Psi_v(z), L/K)$ except $N_{L/K}(\Psi_v(z))$ do not have a function for checking a decomposition of points on an elliptic curve.

Lemma 1. *For any $n \in \mathbb{Z}_{\geq 3}$, Semaev's summation polynomial S_n satisfies*

$$\begin{aligned} & S_n(\wp(z_1),\ldots,\wp(z_n)) \\ = \; & S_{n-1}(\wp(z_1),\ldots,\wp(z_{n-1}))^2 \\ & \times \prod_{\epsilon_2,\ldots,\epsilon_{n-1}\in\{\pm1\}} (\wp(z_1+\epsilon_2z_2+\cdots+\epsilon_{n-1}z_{n-1}) \\ & \qquad -\wp(z_n)) \\ = \; & (\wp(z_1)-\wp(z_2))^{2^{n-2}} \\ & \times \prod_{i=1}^{n-2} \prod_{\epsilon_2,\ldots,\epsilon_{n-i}\in\{\pm1\}} (\wp(z_1+\epsilon_2z_2+\cdots+\epsilon_{n-i}z_{n-i}) \\ & \qquad -\wp(z_{n-i+1}))^{2^{i-1}}. \end{aligned}$$

Proof. When $n = 3$, then

$$\begin{aligned} & S_3(\wp(z_1),\wp(z_2),\wp(z_3)) \\ & = S_2(\wp(z_1),\wp(z_2))^2(\wp(z_1+z_2)-\wp(z_3)) \\ & \qquad \times(\wp(z_1-z_2)-\wp(z_3)) \end{aligned}$$

is obvious by the additional formula of the Weierstrass $\wp$ function. We assume that the equation of the lemma is satisfied up to $n-1$.

$$\begin{aligned} & S_n(\wp(z_1),\ldots,\wp(z_n)) \\ = \; & Res_X(S_3(\wp(z_1),\wp(z_2),X), S_{n-1}(\wp(z_3),\ldots,\wp(z_n),X)) \\ = \; & Res_X(S_2(\wp(z_1),\wp(z_2))^2 \prod_{\epsilon_2=\pm1}(\wp(z_1+\epsilon_2z_2)-X), \\ & \quad S_{n-2}(\wp(z_3),\ldots,\wp(z_n))^2 \\ & \qquad \times \prod_{\epsilon_4,\ldots,e_n\in\{\pm1\}} (\wp(z_3+\epsilon_4z_4+\cdots+\epsilon_nz_n)-X)) \\ = \; & S_2(\wp(z_1),\wp(z_2))^{2^{n-2}} S_{n-2}(\wp(z_3),\ldots,\wp(z_n))^{2^2} \\ & \times \prod_{\epsilon_2,\epsilon_4,\ldots,\epsilon_n\in\{\pm1\}} (\wp(z_1+\epsilon_2z_2) \\ & \qquad -\wp(z_3+\epsilon_4z_4+\cdots+\epsilon_nz_n)) \\ = \; & (\wp(z_1)-\wp(z_2))^{2^{n-2}}(\wp(z_3)-\wp(z_4))^{2^{n-2}} \\ & \times \prod_{i=1}^{n-4} \prod_{\epsilon_4,\ldots,\epsilon_{n-1}} (\wp(z_3+\epsilon_4z_4+\cdots+\epsilon_{n-i}z_{n-i}) \\ & \qquad -\wp(z_{n-i+1})) \\ & \times \prod_{\epsilon_2,\epsilon_4,\ldots,\epsilon_n\in\{\pm1\}} (\wp(z_1+\epsilon_2z_2) \\ & \qquad -\wp(z_3+\epsilon_4z_4+\cdots+\epsilon_nz_n)). \end{aligned}$$

Thus, the candidate zeros of $S_n(\wp(z_1),\ldots,\wp(z_n))$ are $\{z\in\mathbb{C}^n | z_1+\epsilon_2z_2\in L_E\}$ with order 2^{n-2}, $\{z\in\mathbb{C}^n | z_3+\epsilon_4z_4+\cdots+\epsilon_{n-i+1}z_{n-i+1}\in L_E\}$ with order 2^{1+i} for $i=1,\ldots,n-3$, and $\{z\in\mathbb{C}^n | z_1+\epsilon_2z_2+\cdots+\epsilon_nz_n\in L_E\}$ with order 1. On the other hand, we can determine the candidates of the poles in the same way. Therefore, the zeros and poles are $\{z\in\mathbb{C}^n | z_1+\epsilon_2z_2+\cdots+\epsilon_nz_n\in L_E\}$ with order 1 and $\{z\in\mathbb{C}^n | z_i\in L_E, \text{for } s=1,\ldots,n-1,\ z_i+\sum_{j=1}^s \epsilon_{i_j}z_{i_j}\notin L_E, (i\neq i_j, j=1,\ldots,s)\}$ with order 2^{n-1}.

The zeros and poles of the right-hand side of the equation given in this lemma,

$$\begin{aligned} & (\wp(z_1)-\wp(z_2))^{2^{n-2}} \\ & \times \prod_{i=1}^{n-2} \prod_{\epsilon_2,\ldots,\epsilon_{n-i}\in\{\pm1\}} (\wp(z_1+\epsilon_2z_2+\cdots+\epsilon_{n-i}z_{n-i}) \\ & \qquad -\wp(z_{n-i+1}))^{2^{i-1}}, \end{aligned}$$

are same as those of the left-hand side.

The zeros and poles of $S_n(\wp(z_1),\ldots,\wp(z_n))$ are the same as the ones of the right-hand side of this equation. We compute the Taylor expansions of both sides of the equation around $z_1+z_2=0$. Both the coefficients of the (-2)-order terms of these series with respect to z_1+z_2 are 1. Therefore, the lemma is true by Liouville's theorem. □

Using Lemma 1, we will prove Theorem 4.

Proof. The claim of this theorem is

$$\begin{aligned} & \prod_{\epsilon_2,\ldots,\epsilon_n} \Psi_{(v_1,\epsilon_2v_2,\ldots,\epsilon_nv_n)}(z_1,\ldots,z_n) \\ & = S_n(\wp(v_1z_1),\ldots,\wp(v_nz_n))\textstyle\prod_{i=1}^n \Psi_{v_i}(z_i)^{2^{n-1}}. \end{aligned}$$

When $n = 2$, this claim is obvious by the additional formula of the σ function.

We assume that this claim is true up to $n-1$. Under this assumption,

$$\begin{aligned}
&\prod_{\epsilon_2,\ldots,\epsilon_n\in\{\pm1\}} \Psi_{(v_1,\epsilon_2 v_2\ldots,\epsilon_n v_n)}(z_1,\ldots,z_n)\\
=\ & \frac{\prod_{\epsilon_2,\ldots,\epsilon_n\in\{\pm1\}}\sigma(v_1z_1+\epsilon_2v_2z_2+\cdots+\epsilon_nv_nz_n)}{\prod_{j=1}^n\sigma(z_i)^{2-\epsilon_i\epsilon_jv_iv_j}\prod_{1\le i<j\le n}\sigma(z_i+z_j)^{\epsilon_i\epsilon_jv_iv_j}}\\
=\ & \prod_{\epsilon_2,\ldots,\epsilon_{n-1}\in\{\pm1\}}\Big((\wp(v_1z_1+\epsilon_2v_2z_2+\ldots\\
&\qquad +\epsilon_{n-1}v_{n-1}z_{n-1})-\wp(v_nz_n))\\
&\times\frac{\sigma(z_1+\epsilon_2z_2+\cdots+\epsilon_{n-1}z_{n-1})^2\sigma(z_n)^2}{\prod_{i=1}^n\sigma(z_i)^{2^{n-1}v_i^2}}\Big)\\
=\ & \Psi_{v_n}(z_n)^{2^{n-1}}\\
&\prod_{\epsilon_2,\ldots,\epsilon_{n-1}\in\{\pm1\}}\Psi_{(v_1,\epsilon_2v_2,\ldots,\epsilon_{n-1}v_{n-1})}(z_1,\ldots,z_{n-1})^2\\
&\times\prod_{\epsilon_2,\ldots,\epsilon_{n-1}\in\{\pm1\}}(\wp(v_1z_1+\epsilon_2v_2z_2+\ldots\\
&\qquad +\epsilon_{n-1}v_{n-1}z_{n-1})-\wp(v_nz_n))\\
=\ & S_{n-1}(\wp(v_1z_1),\ldots,\wp(v_{n-1}z_{n-1}))^2\prod_{i=1}^n\Psi_{v_i}(z_i)^{2^{n-1}}\\
&\times\prod_{\epsilon_2,\ldots,\epsilon_{n-1}\in\{\pm1\}}(\wp(v_1z_1+\epsilon_2v_2z_2+\ldots\\
&\qquad +\epsilon_{n-1}v_{n-1}z_{n-1})-\wp(v_nz_n))\\
=\ & S_n(\wp(v_1z_1),\ldots,\wp(v_nz_n))\prod_{i=1}^n\Psi_{v_i}(z_i)^{2^{n-1}}.
\end{aligned}$$

□

2.1. Some Remarks

In this paper, we assume that an elliptic curve is defined over a number field. This assumption is unnecessary and this theorem is generalized to any finite field, by reduction theory. An index calculus attack for the ECDLP over extension fields via elliptic nets vanishing y coordinate is the same as the one via Semaev's summation polynomials, hence the relation given by Theorem 4.

However, it is an open problem to give relations between random points on an elliptic curve and points on the factor basis for an index calculus attack via elliptic nets directly using a Gröbner basis. For the purpose of determining relations, it is sufficient to solve algebraic equations from the descent of elliptic nets for a base field $\mathbb{F}_q$. For any point $P\in E(\mathbb{F}_{q^n})$, we compute the rational polynomial

$$\Psi_{(1,\ldots,1)}(X_1,Y_1,\ldots,X_n,Y_n,x(P),y(P))\in\mathbb{F}_{q^n}(X_1,Y_1,\ldots,X_n,Y_n).$$

We decompose this rational polynomial for basis field $\mathbb{F}_q$ as follows:

$$\Psi_{(1,\ldots,1)}(X_1,Y_1,\ldots,X_n,Y_n,x(P),y(P))=\sum_{i=1}^n\Phi_P^{(i)}(X_1,Y_1,\ldots,X_n,Y_n)t^i$$

where $\{t^i|i=1,\ldots,n\}$ is a basis of $\mathbb{F}_{q^n}/\mathbb{F}_q$ and $\Phi_P^{(i)}$ is a rational polynomial in $\mathbb{F}_q(X_1,Y_1,\ldots,X_n,Y_n)$. Then, we have given the $\mathbb{F}_q$ rational points of $V(\Phi_P^{(1)},\ldots,\Phi_P^{(n)})$ to obtain relations of decomposition by factor basis.

References

[1] Aoki, K., Kobayashi, T. and Nagai, A.: *Supplemental Document for Odd Characteristic Extension Fields*, Standards for Efficient Cryptography, 2009.

[2] Bailey, D. and Paar, C.: *Optimal Extension Fields for Fast Arithmetic in Public-Key Algorithm*, CRYPTO98, LNCS **1462** (1998), Springer.

[3] Cox, D., Little, J. and O 'Shea, D: *Using Algebraic Geometry*, Springer, 2005.

[4] Diem, C.: *On the discrete logarithm problem in elliptic curves*, Preprint, 2009.

[5] Gaudry, P.: *Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem*, J. Symbolic Computation **44** (2009), 1690–1702.

[6] Joux, A. and Vitse, V.: *Elliptic Curve Discrete Logarithm Problem over Small Degree Extension Fields*, Preprint.

[7] Semaev, I.: *Summation polynomials and the discrete logarithm problem on elliptic curves*, Preprint, 2004.

[8] Stange, K.: *The Tate pairing via elliptic nets*, In Proc. of Pairing 2007.

[9] Ogura, N., Kanayama, N., Uchiyama, S. and Okamoto E.: *Cryptographic Pairings Based on Elliptic Nets*, Preprint.

[10] Nagao, K. I.: *Decomposition Attack for the Jacobian of a Hyperelliptic Curve over an Extension Field*, Algorithmic Number Theory, 2010, Springer.

Tsunekazu Saito and Shun'ichi Yokoyama
Graduate School of Mathematics, Kyushu University, Fukuoka 812-8581, Japan
E-mail: t-saito(at)math.kyushu-u.ac.jp
s-yokoyama(at)math.kyushu-u.ac.jp

Tetsutaro Kobayashi and Go Yamamoto
Nippon Telegraph and Telephone Corporation, Tokyo 180-8585, Japan
E-mail: kobayashi.tetsutaro(at)ntt.lab.co.jp
yamamoto.go(at)ntt.lab.co.jp