On Interpolation of Inverse Paring Maps

Takakazu Satoh
Graduate school of Mathematics
Tokyo Institute of Technology

佐藤 孝和
理工学研究科数学専攻
東京工業大学

20 september 2005, DTU, København
(revision 8 december 2005)

Sheet 2 Summary

* motivation
* polynomial interpolation
  classical DL, ECDL, the Verheul isomorphism
* statement of a result
* outline of proof

Sheet 3 Motivation: MOV Reduction

$E/\mathbf{F}_q$: an elliptic curve
$B \in E(\mathbf{F}_q)$, order N: prime, $\neq p$
$r : \langle B \rangle \to \mathbf{F}_{q^k}^{\times}$ (k: embedding degree), an injective homomorphism.

Using the Weil pairing or the Tate pairing, we can evaluate r in probabilistic polynomial time (w.r.t. $k \log q$).
The relation $P = nB$ is mapped to $r(P) = r(B)^n$.
$\Rightarrow$ ECDLP for $\langle B \rangle$ is not more difficult than FF-DLP for $\mathbf{F}_{q^k}^{\times}$.

We want to say FF-DLP is not more difficult than ECDLP,
(don't we?)
We need a feasible algorithm to compute an inverse direction isomorphism $\langle \zeta \rangle \to \langle B \rangle$ where ζ is a primitive N-th root of the unity.

Sheet 4 Motivation: Results of Verheul

E. Verheul: Evidence that XTR is more secure than supersingular elliptic curve cryptosystems, EuroCrypt 2001.

> Let G_1, G_2, H be cyclic groups of a same order of known factorization (e.g. prime order).
> Assume existence of efficient algorithms to compute:
> $D : G_1 \to G_2$, an isomorphism (distortion map)
> $e : G_1 \times G_2 \to H$, a non-degenerate bilinear pairing
> $v : H \to G_1$, an isomorphism

$\Rightarrow$ CDHP on H is efficiently computable.

He constructed D for the CTP elliptic curves over $\mathbf{F}_p$ (in this context, G_1, $G_2 \subset E(\mathbf{F}_{p^3})$, H is the XTR subgroup of $\mathbf{F}_{p^3}$).

He concluded that, in this case, v is unlikely to exist since CDHP on XTR subgroup is *believed* to be difficult.

Sheet 5 **Open Problems**

- Is Verheul's conjecture true?
- What is computational complexity to compute a homomorphism from a subgroup of $\mathbf{F}_q^\times$ to $E(\mathbf{F}_q)$?
- What if E is restricted to a curve in a certain special family (say, supersingular curves, curves with small embedding degrees)?

I don't have any answers at least for now.

Sheet 6 **Verheul Isomorphism**

Following

N. Koblitz, A. Menezes: Pairing based cryptography at high security levels, IACR e-print 2005/076

we adopt the following definition.

Definition. Let N be a prime.
Let $E/\mathbf{F}_q$ be an elliptic curve,
Let $B \in E$ be a point of order N.
Let $\zeta \in \mathbf{F}_q^a$ be the primitive N-th root of the unity.

We call a group isomorphism $\langle\zeta\rangle \to \langle B\rangle$ the **Verheul isomorphism**.

Sheet 7 **Polynomial Interpolation: Finite Field(1)**

Finite field case:
$\omega \in \mathbf{F}_q^\times$: generator.

The function $\mathbf{F}_q^\times \ni x \to \log_\omega x \in \mathbf{Z}/(q-1)\mathbf{Z} \to \mathbf{F}_p$ for all $x \in \mathbf{F}_q^\times$
(the last map: $m \bmod (q-1) \to m \bmod p$ for $0 \le m < q-1$, $m \in \mathbf{N}$)
is represented as a polynomial function.
This is obvious because of Lagrange's polynomial interpolation formula.

If such a polynomial function is evaluated quickly, we can solve DLP. So, we need to confirm at least
- the degree of such a polynomial is large
- the polynomial is dense
- etc. etc...

Sheet 8 Polynomial Interpolation: Finite Field(2)

For the finite field case, we have an explicit formula:

$$\log_\omega(x) = -1 + \sum_{j=1}^{q-2} \frac{x^j}{\omega^{-j}-1}$$

Ref.

A. L. Wells, Jr.:

A polynomial form for logarithms modulo a prime, IEEE Trans. IT. **30**(1984), 845-846.

G. L. Mullen, D. White:

A polynomial representation for logarithms in $GF(q)$, Acta Arith. **47**(1986), 255-261

H. Niederreiter:

A short proof for explicit formulas for discrete logarithms in finite fields, Appl. Alg. Eng. Comm. Comput. **1**(1990), 55-57.

Sheet 9 Polynomial Interpolation: Finite Field(3)

Of course these results does not give hardness of DLP.

Indeed, the index calculus method computes DL function with sub-exponential computational time.

The consideration on polynomial interpolations just gives a circumstance evidence that DLP is hard.

However:
- It is a proved result without assuming any unproved conjecture, hypothesis, belief or whatsoever.
- It has number theoretic interests.

Sheet 10 Polynomial Interpolation: EC(1)

T. Lange, A. Winterhof:

Interpolation of the elliptic curve Diffie-Hellman mapping, *Proc. AAECC 2003*, Lect. Notes Comput. Sci., **2643**(2003), 51-60.

Theorem. Let $E/\mathbf{F}_p$ be an elliptic curve and assume $p \geq 7$.
Let B be a point of order N. For a subset $S \subset \{1, \dots, [N/4]\}$, let $F_S(X) \in \mathbf{F}_p[X]$ satisfy

$$F_S(\xi(nB)) = n \quad \textit{and} \quad F_S(\xi(2nB)) = 2n, \quad n \in S.$$

Here ξ is the X-coordinate function.

Then $\deg F_S \geq \frac{{}^{\#}S}{4}$.

Sheet 11 Polynomial Interpolation: EC(2)

Some other results:

T. Lange, A. Winterhof: Polynomial interpolation of the elliptic curve and XTR discrete

logarithm, Proc. COCOON 2002, Lect. Notes Comput Sci., **2387**(2002), 137-143.
T. Lange, A. Winterhof: Interpolation of the discrete logarithm in $\mathbf{F}_q$ by boolean functions and by polynomial in several variables modulo a divisor of $q-1$, *Discrete Appl. Math.*, **128**(2003), 193-206.
E. Kiltz, A. Winterhof: On the interpolation of bivariate polynomials related to the Diffie-Hellman mapping, *Bull. Austral. Math. Soc.*, **69**(2004), 305-315.
T. Satoh: On degrees of polynomial interpolation related to elliptic curve cryptography, *Proc. Workshop on Coding and Cryptography*, Bergen, 2005, 55-61.

Sheet 12 **Polynomial Interpolation: EC(3)**

Previously known results:

lower bounds of degrees of interpolated polynomial for
ECDL, or the X-coordinate of the Verheul isomorphism.

In extreme case, an interpolating polynomial may be a monomial so that it can be evaluated very quickly.

Sheet 13 **Statement of a Result**

p, N: primes, satisfying $p \geq 5$, $N \neq p$ and $\sqrt{12p} \leq N < \frac{2}{\sqrt{3}}p$.
$E/\mathbf{F}_p$: an ordinary elliptic curve
ζ: a primitive N-th root of unity.
$C \subset E$: a cyclic subgroup of order N.
β: a generator of C.
Let $\varphi_{E,\beta}(t)$ be the polynomial satisfying

(1) $\varphi_{E,\beta}(\zeta^n) = \xi(n\beta)$ for all $1 \leq n < N$.
i.e. $\varphi_{E,\beta}$ is the polynomial interpolation of the X-coordinate of the Verheul isomorphism for $1 \leq n < N$.

(2) $\varphi_{E,\beta}(1) = 0$.

Then, none of coefficients of $\varphi_{E,\beta}$ vanishes for at least 28% of such pairs (E, C).
cf. changing β and/or ζ only permutes coefficients.

Sheet 14 **Cryptographic Implication?**

It's a still long way to cryptography.

- For now, the result says nothing on a particular pair (E, C).
- It is certainly not bad to prove that an obvious algorithm to compute the Verheul isomorphism fails.
- But all cryptographically useful pairs (E, C) may fall where the result does not cover.

Sheet 15 **Outline of Proof**

(1) Work over $\mathbf{C}$: Let H be the complex upper half plane.

$$E_\tau \;:\; Y^2 \;=\; X^3 - \frac{E_4(\tau)}{48}X + \frac{E_6(\tau)}{864} \;\ni\; B_\tau \;:=\; \left(\frac{\wp(1/N;\tau)}{(2\pi i)^2},\, \frac{\wp'(1/N;\tau)}{(2\pi i)^3}\right)$$

Key point: the product of coefficients for all non-constant terms of φ_{E_τ, B_τ} is a modular form of weight $2(N-1)$ for $\Gamma_0(N)$. Hence it has exactly $(N^2-1)/6$ zeros (with counting multiplicity correctly) on $X_0(N) := \widehat{\Gamma_0(N)\backslash H}$.

(2) Apply reduction modulo p to obtain the result over $\mathbf{F}_p$.
Key point: If $\sqrt{12p} < N \le \frac{2}{\sqrt{3}}p$, reduction preserves orders of zeros and poles for most of imaginary quadratic values of τ.

Sheet 16 — Modular Forms (1): Definition

For $\tau \in H$, $f : H \to \mathbf{C}$ and $M := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbf{R})_+$, put

$$M\langle\tau\rangle \;:=\; \frac{a\tau+b}{c\tau+d},$$
$$\left(f\,|_k M\right)(\tau) \;:=\; \det(M)^{k/2}(c\tau+d)^{-k} f(M\langle\tau\rangle)$$

$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbf{Z}) \;\middle|\; c \equiv 0 \bmod N \right\},$
$\chi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) := \chi(d)$ for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$, the Dirichlet char. $\chi \bmod N$

Modular forms of weight k and character χ for $\Gamma_0(N)$:

$$M_k(\Gamma_0(N), \chi) \;:=\; \left\{ f \in \mathrm{Hol}(H) \;\middle|\; \begin{array}{l} f\,|_k M \;=\; \chi(M) f \text{ for all } M \in \Gamma_0(N) \\ f \text{ is holomorphic at each cusps} \end{array} \right\}$$

$M_k(\Gamma_0(N)) := M_k(\Gamma_0(N), \chi_0)$. ($\chi_0$: the principal character mod N)

Sheet 17 — Modular Forms (2): Properties

* $f \in M_k(\Gamma_0(N), \chi)$, $g \in M_l(\Gamma_0(N), \psi) \;\Rightarrow\; fg \in M_{k+l}(\Gamma_0(N), \chi\psi)$.
  in particular, $f \in M_k(\Gamma_0(N)) \Rightarrow f^n \in M_{kn}(\Gamma_0(N))$.

* $f \in M_k(\Gamma_0(N)) \;\Rightarrow\; f$ has $\dfrac{k[SL(2, \mathbf{Z}) : \Gamma_0(N)]}{12}$ zeros (counting with multiplicity) over $\widehat{\Gamma_0(N)\backslash H}$.

  $[SL(2, \mathbf{Z}) : \Gamma_0(N)] = N+1$ for a prime N.

Sheet 18 — Modular Forms (3): Examples

* Ramanujan's Δ

$$\Delta(\tau) \;:=\; \mathbf{e}(\tau)\prod_{n=1}^{\infty}(1 - \mathbf{e}(\tau)^n)^{24} \;\in\; M_{12}(SL(2, \mathbf{Z}))$$

  where $\mathbf{e}(\tau) := \exp(2\pi i\tau)$.
  The function Δ has no zeros on H and has a simple zero at ∞.

* The Eisenstein series of weight k (k: even, ≥ 4):

$$E_k(\tau) := \frac{1}{2} \sum_{\substack{\gcd(c,d)=1 \\ c \equiv 0 \bmod N}} \frac{1}{(c\tau+d)^k} \in M_k(\Gamma_0(N))$$

This does *not* converge for $k=2$. But this is the case we need.

Sheet 19 **Modular Forms (4): Hecke's Trick**

E. Hecke: Theorie der Eisensteinschen Riehen höherer Stufe und ihre Anwendung auf Funktionentheorie und Arithmetik, *Abh. Math. Sem. Hamburg*, **5**(1927), 199-224.

$$G_{(m,n)}(\tau\,;s) := \sum_{u \equiv m(N),\ v \equiv n(N)} \frac{1}{(u\tau+v)^2 |u\tau+v|^s}$$

Abs. conv. for $\mathrm{Re}(s) > 0$, meromorphically extended to s plane.
Put $G_{(m,n)}(\tau) := G_{(m,n)}(\tau\,;0)$. **This is not holomorphic on τ.**
But the following linear combinations are holomorphic on τ.

$$E_{\chi_0}(\tau) := -\frac{N^2}{8\pi^2}\left(\sum_{t=1}^{N-1} G_{(0,t)} - (N-1)G_{(0,0)}\right) \in M_2(\Gamma_0(N))$$

$$E_{\chi}(\tau) := -\frac{N^2}{8\pi^2}\sum_{t=1}^{N-1} \chi^{-1}(t) G_{(0,t)} \in M_2(\Gamma_0(N), \chi) \qquad (\chi \neq \chi_0)$$

Sheet 20 **Modular Forms (5): Fourier Expansion**

$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_0(N)$.
f: modular form for $\Gamma_0(N)$, of weight k, character χ
$\Rightarrow f(\tau+1) = f(\tau)$
It is expanded by the Fourier series:

$$f(\tau) = \sum_{n=-\infty}^{\infty} a_n \mathbf{e}(n\tau).$$

The number a_n is called **the n-th Fourier coefficient** of f.
$\mathbf{e}(\tau)$ is a local parameter at ∞.

Sheet 21 **Relations to Elliptic Curves**

(1) $N^{-2}\wp\left(\frac{m\tau+n}{N}, \tau\right) = G_{(m,n)}(\tau) - G_{(0,0)}(\tau)$

(2) Let f be modular **function** for $\Gamma_0(N)$, i.e.,
  (a) f is meromorphic on H and at all cusps
  (b) $f\,|_0 M = f$ for all $M \in \Gamma_0(N)$
  Then, $f \in \mathbf{C}(j, j\circ[N])$. ($[N]$: the multiplication by N map)
  The meromorphic function f is a rational function of an affine curve $\Phi_N(X, Y) = 0$.

(3) If all the Fourier coefficients satisfies certain algebraic conditions, f is a rational function of j and $j\circ[N]$ with algebraic coefficients.
  This is a key to define reduction of a modular function.

Sheet 22 — Polynomial Interpolation over C

$$E_\tau\ :\ Y^2 = X^3 - \frac{E_4(\tau)}{48}X + \frac{E_6(\tau)}{864}\ \ni\ B_\tau := \left(\frac{\wp(1/N;\tau)}{(2\pi i)^2}, \frac{\wp'(1/N;\tau)}{(2\pi i)^3}\right)$$

$\varphi_{E_\tau, B_\tau}(t) := \sum_{m=0}^{N-1} A_m(\tau)t^m$: polynomial interpolation of the X-coord. of the Verheul isomorphism sending $\mathbf{e}(1/N)$ to $\xi(B_\tau)$. Then

$$A_m = \begin{cases} 2\sum_\chi \dfrac{\mathfrak{g}(\chi^{-1})}{N-1}\chi(m)E_{\chi^{-1}} & (m \neq 0,\ \mathfrak{g}(\chi^{-1}): \text{the Gauss sum}), \\ 2E_{\chi_0} & (m = 0). \end{cases}$$

$A_m \in M_2(\Gamma_1(N))$ where $\Gamma_1(N) = \left\{\begin{pmatrix} a & b \\ c & d\end{pmatrix} \in \Gamma_0(N) : a \equiv d \equiv 1(N)\right\}$

$\prod_{m=1}^{N-1} A_m \in M_{2(N-1)}(\Gamma_0(N)) \Rightarrow (N^2-1)/6$ zeros on $X_0(N)$.

Except for these zeros, none of $A_m(\tau)$ vanishes.

Sheet 23 — Normalization(1)

In order to apply "reduction mod p" to results on **C**, we redefine E_τ and B_τ as:

$$E_\tau\ :\ Y^2 = X^3 - \frac{E_4(\tau)}{48\Delta(\tau)^{1/3}}X + \frac{E_6(\tau)}{864\Delta(\tau)^{1/2}}$$

$$B_\tau := \left(\frac{\wp(1/N;\tau)}{(2\pi i)^2\Delta(\tau)^{1/6}}, \frac{\wp'(1/N;\tau)}{(2\pi i)^3\Delta(\tau)^{1/4}}\right)$$

$$A_m := \text{coefficient of the degree } m \text{ term in } \varphi_{E_\tau, B_\tau}$$

to make everything algebraic.

Sheet 24 — Normalization (2)

For simplicity, we assume $N \equiv 1 \bmod 6$ in what follows.

$$\prod_{m=1}^{N-1} A_m = \Delta^{-(N-1)/6} \prod_{m=1}^{N-1}\left(2\sum_\chi \frac{\mathfrak{g}(\chi^{-1})}{N-1}\chi(m)E_{\chi^{-1}}\right).$$

This is a modular function for $\Gamma_0(N)$, i.e. a rational function on $X_0(N)$. (Note $(N-1)/6 \in \mathbf{Z}$.)

Modular functions can have arbitrary large order poles and zeros. But the sum of orders are zero.

- Δ is non zero except at ∞ (simple) and 0 (order N).
- $\prod_{m=1}^{N-1}\left(2\sum_\chi \frac{\mathfrak{g}(\chi^{-1})}{N-1}\chi(m)E_{\chi^{-1}}\right)$ is holomorphic on $X_0(N)$.

We can recover the same results: none of $A_1(\tau)$, ..., $A_{N-1}(\tau)$ is zero except for $(N^2-1)/6$ values of τ.

Sheet 25 **Reduction (1)**

$E/\mathbf{F}_p$: an ordinary elliptic curve
$C \subset E$: a subgroup of order N

By the Deuring lifting theorem,
$\exists \tau \in H$, $\exists K$: an algebraic number field
$\exists \mathfrak{p}$: a prime ideal of K
s.t. $E = \overline{E_\tau}$ ($\overline{}$ = reduction modulo $\mathfrak{p}$), $C = \overline{\langle B_\tau \rangle}$

Put $\zeta := \overline{\mathbf{e}(1/N)}$, $\beta = \overline{B_\tau}$.
Consider polynomial interpolation $\varphi_{E,C}(t) := \sum_{m=0}^{N-1} \alpha_m t^m$ of the Verheul isomorphism satisfying $\varphi_{E,C}(\zeta) = \xi(\beta)$.

Then, $\alpha_m = \overline{A_m(\tau)}$ (reduction of a $\mathfrak{p}$-integral algebraic number).
Problem: We cannot reduce an arbitrary meromorphic function on H modulo $\mathfrak{p}$.

Sheet 26 **Reduction (2)**

Recall $h(\tau) := \prod_{m=1}^{N-1} A_m(\tau)$ is a modular function for $\Gamma_0(N)$.
We can regard h as a rational function of the affine curve $\Phi_N(X,Y) = 0$. (Φ_N: the N-th modular polynomial.)

Replace K by its finite extension if necessary (and $\mathfrak{p}$ by its extension to a new K) so that $h \in K(j, j \circ [N])$.

We can reduce a rational function h on $\Phi_N(X,Y) = 0$ to $\bar{h}$ which is a rational function on the affine curve $\overline{\Phi_N}(X,Y) = 0$.
(Note $\Phi_N(X,Y) \in \mathbf{Z}[X,Y]$.)

New obstacles:
(1) $\Phi_N(X,Y) = 0/\mathbf{Q}$ and $\overline{\Phi_N}(X,Y) = 0/\mathbf{F}_p$ are not smooth.
At singular points, orders of zeros are not defined.
(2) In general, reduction does not preserve orders of zeros.

Sheet 27 **Cryptographic Constraint**

A number of singular points is not so large.

But the case $C = E(\mathbf{F}_p)$ **always** corresponds to a singular point of $\overline{\Phi_N}(X,Y) = 0$.

If we consider cryptographic application,
we cannot exclude such points from our results.

Sheet 28 **Spots**

k: perfect field, K/k: finite extension
$\mathscr{C}/k$: an algebraic curve

An equivalence class of valuations on the function field $K(\mathscr{C})$ trivial on k is called a **spot** of $K(\mathscr{C})/k$.

Fact: If $\mathscr{C}$ is smooth

$$\{\text{spots of } K(\mathscr{C})/k\} \xleftrightarrow{1:1} \mathscr{C}/\mathrm{Gal}(K^a/K)$$

In our context: we can talk about an order of zero of a rational function on $\Phi_N(X,Y)=0$ by using a spot,
without its explicit smooth model.

For an imaginary quadratic τ, we can define a valuation $\overline{\mathrm{ord}}_\tau$ on the function field of $\overline{\Phi_N}(X,Y)=0/\mathbf{F}_p$.

Sheet 29 **Reductions and Orders**

Let R be the ring of $\mathfrak{p}$-integral elements in K. Let $\tau \in H$ be an imaginary quadratic. Assume
(1) $j(\tau)j(N\tau)(j(\tau)-1728)(j(N\tau)-1728) \not\equiv 0 \bmod \mathfrak{p}$
(2) $\exists P \in R[[T]]$ s.t. $j\circ[N]=P(j-j(\tau))+j(N\tau)$
(3) $(\partial_Y \Phi_N)(j(\tau)+T, j(N\tau)+P(T)) \in R((T))^\times$
Then, for a rational function f on $\Phi_N(X,Y)=0$,

$$\overline{\mathrm{ord}}_\tau \bar{f} \;\geq\; \mathrm{ord}_\tau f. \qquad (*)$$

The condition $N \leq \frac{2}{\sqrt{3}}p$ in our result ensures (2) and (3).
At the cusps (0 and ∞), we obtain similar inequalities to (*).

The condition (1) is more delicate. The number of such points is at most 6 under $N > \sqrt{12p}$. The sums of orders of zeros on such points is non-negative.

Sheet 30 **Final Remarks**

- By considering $\prod_{m=1}^{N-1}(A_m - c\Delta^{-1/6}E_{\chi_0})$ for a constant c, we see $A_1(\tau), \ldots, A_{N-1}(\tau)$ takes several values provided if $E_{\chi_0}(\tau)\neq 0$.
- Nevertheless, modular forms have various arithmetic properties and structures. Their special values may behave far from randomly.
- Of particular interest is to see what happens when

$$(\partial_Y \Phi_N)(j(\tau)+T, j(N\tau)+P(T)) \;\notin\; R((T))^\times.$$

Sheet 31 **Acknowledgments**

Special Thanks to:

Steven Galbraith
Tanja Lange
Igor Semaev
Universitiet i Tromsø