

On Pairing Inversion Problems

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

4 July 2007, Tokyo

Sheet 2 Summary

- * motivation
- * Pairing inversion problems
- * Former works
 - polynomial interpolation
 - η pairing inversion
 - ate pairing inversion
- * the Weil pairing inversion

Sheet 3 Motivation (1)

p : prime, \mathbf{F}_q : the finite field of q elements.
 G_1, G_2 : Abelian groups " $/\mathbf{F}_q$ ", annihilated by a prime l ($\neq p$)
 μ_l : the group of the l -th roots of unity.
 $r := [\mathbf{F}_q(\mu_l) : \mathbf{F}_q]$, the embedding degree
 $e : G_1 \times G_2 \rightarrow \mu_l$, a bilinear, non-degenerate pairing

Assumptions in pairing based cryptographic protocols:
CDHP in G_1 (given $P, aP, bP \in G_1$, compute abP) is difficult.
So are CDHP in G_2 and μ_l .

Some other assumptions:
CBDHP (given $P, aP, bP \in G_1$ and $Q \in G_2$, compute $e(abP, Q)$) is difficult \Rightarrow no harder than CDHP in G_1 .

Sheet 4 Motivation (2)

CDHP in G_1 (resp. G_2, μ_l) is no harder than DLP in G_1 (resp. G_2, μ_l).

Usually: G_1 and G_2 are subgroups of l -torsion points of elliptic curves or Jacobian of hyperelliptic curves or Abelian variety over finite fields.

For simplicity, we consider elliptic curves in this talk.

Sheet 5

Motivation (3)

Curve parameters need to satisfy the following conditions:

- l is so large that square root methods to solve ECDLP in $E[l]$ is infeasible
- $[\mathbf{F}_p(\mu_l):\mathbf{F}_p]$ is so large that index calculus method to solve DLP in $\mathbf{F}_p(\mu_l)$ is infeasible
- $[\mathbf{F}_p(\mu_l):\mathbf{F}_p] \leq r[\mathbf{F}_q:\mathbf{F}_p]$ - r must not be small.

But large r **does not** imply large $[\mathbf{F}_p(\mu_l):\mathbf{F}_p]$ (Hitt).

- r is not too large so that arithmetic operations in $\mathbf{F}_q(\mu_l)$ can be done quickly.
- Otherwise, pairing computation is impractically slow.

Can we believe that CDHP on G_1 (or G_2, μ_l) is difficult under the above assumption?

Sheet 6

Motivation (4)

Elliptic Curve Discrete Log Problem(ECDLP) on "generic" elliptic curves are well studied and widely **believed** to be difficult.

The best known method: square root methods.

However, in pairing based cryptography, we only use special curves, so called "pairing friendly curves".

Special curves with (relatively) easy ECDLP

- supersingular curves (Menezes-Okamoto-Vanstone, Semaev)
- anomalous curves (Semaev, Smart, S.-Araki)

How about for pairing friendly curves?

- not well studied
- less than 10 papers in total??
- only 6 years have passed since Verheul's work

Sheet 7

Pairing Inversion Problems

$$e : G_1 \times G_2 \rightarrow \mu_l.$$

the Verheul map construction (VMC):

Construct a feasibly computable injective group homomorphism $\mu_l \rightarrow G_2$.

Such a homomorphism is called the Verheul map.

Fixed Pairing Inversion (FPI):

Given $P \in G_1$ and $z \in \mu_l$, find $Q \in G_2$ s.t. $e(P, Q) = z$.

Generalized Pairing Inversion (GPI):

Given $z \in \mu_l$, find $P \in G_1$ and $Q \in G_2$ s.t. $e(P, Q) = z$.

If G_2 is **cyclic**, FPI implies VMC.

Sheet 8

Cryptographic Implications(1)

Assume that there is a feasible distortion map $\delta : G_2 \rightarrow G_1$

and that G_1 and G_2 are cyclic groups of order l .

We can solve CDHP on G_1, G_2 and μ_l with $O(\log l)$ evaluations of the Verheul map. (Verheul, 2001)

Sheet 12

Polynomial Interpolation(2)

Verheul map construction:

- degree bound: use of division polynomials.
 - originally developed by Lange, Winterhoff, Kiltz, ... for ECDLP, ECCDHP, ...
- weight bound: coefficients of polynomial interpolation of certain Verheul map are given by a reduction of the modular forms.
 - rather brute force construction: $\omega \in \mu_l, A \in E[l]$.

$$\mu_l \ni z \rightarrow \frac{1}{l} \sum_{n=0}^{l-1} \left(\sum_{m=1}^{l-1} \omega^{-nm\xi(mA)} \right) z^n \quad (\xi : X\text{-coord. funct.})$$

Sheet 13

Eta Pairing Inversion(1)

Galbraith, ÓhÉigeartaigh, Sheedy:

Ref. [13] (to appear in J. Math. Crypt.)

E : **supersingular** curves/ \mathbf{F}_2 , $q := 2^m$, m : odd

- η -pairing itself is a bilinear pairing.
- No final exponentiation is necessary.
- The squaring map is an \mathbf{F}_2 -linear map.

Given $z \in \mu_l$ and $P \in E(\mathbf{F}_q)[l]$, find $Q \in E(\mathbf{F}_q)[l]$ s.t. $\eta(P, Q) = z$.

Take an \mathbf{F}_2 basis $\{\theta_0, \dots, \theta_{m-1}\}$ of \mathbf{F}_q .

Sheet 14

Eta Pairing Inversion(2)

$Q = \left(\sum_{i=0}^{m-1} x_i \theta_i, \sum_{i=0}^{m-1} y_i \theta_i \right)$ where $x_0, \dots, x_{m-1}, y_0, \dots, y_{m-1} \in \mathbf{F}_2$

$$\eta(P, Q) = \frac{\prod_{j=0}^{m-1} \left(\sum_{i=0}^{m-1} (u_{i,j} x_i + v_{i,j} y_i) + w_j \right)}{\prod_{j=0}^{m-1} \left(\sum_{i=0}^{m-1} (a_{i,j} x_i + b_{i,j} y_i) + c_j \right)} \quad \left(\begin{array}{l} a_{i,j}, b_{i,j}, c_j, \\ u_{i,j}, v_{i,j}, w_j \in \mathbf{F}_{q^r} \end{array} \right)$$

To find Q s.t. $\eta(P, Q) = z$, solve

$$z \prod_{j=0}^{m-1} \left(\sum_{i=0}^{m-1} (a_{i,j} x_i + b_{i,j} y_i) + c_j \right) - \prod_{j=0}^{m-1} \left(\sum_{i=0}^{m-1} (u_{i,j} x_i + v_{i,j} y_i) + w_j \right) = 0,$$

$$x_i^2 = x_i, y_i^2 = y_i \quad (i = 1 \sim m)$$

Space requirement is too large ($O(m2^{2m})$)

\Rightarrow infeasible for practical values of m

Sheet 15

Ate Pairing Inversion

Galbraith, Hess, Vercauteren Ref. [12] (IACR e-print 2007/256)

E : an **ordinary** elliptic curve defined over \mathbf{F}_q .

Ate pairing: $f_{t-1,P}(Q)^d$ with $d \in \mathbf{N}$.

$t := \text{Tr}(\text{Fr}_q)$, assumed to be > 1 , $\text{div}(f_{n,P}) = n[P] - [nP] - (n-1)[\mathcal{O}]$.

Decompose an ate pairing inversion problem into two steps

Final Exponentiation Inversion:

Finding correct d -th root of a given value.

- \exists curves s.t. a random root is fine for the next step.

Miller Inversion:

Given $z \in \mu_l$, find Q satisfying $f_{t-1,P}(Q) = z$.

- smaller $t \Rightarrow$ smaller $\text{deg}(f_{t-1,P})$ (as a rational function)
- \exists families of pairing friendly E.C. with small t

Open problem: Do the two families intersect?

Sheet 16

The Weil Pairing Inversion

The Weil Pairing Inversion

Sheet 17

Notation

k : perfect field, E/k : elliptic curve, l : prime, > 3 , $\neq \text{char}(k)$.

$\mathcal{O} \in E(k)$: the identity element of the group structure of E

$\tau \in k(E)$: a k -rational local parameter at \mathcal{O} .

Define $L_{P,Q}$ by

$$\text{div}(L_{P,Q}) = [P] + [Q] + [-P - Q] - 3[\mathcal{O}] \text{ and } \text{lc}(L_{P,Q}) = 1$$

For $P \in E$, define $s_P(Q) := P + Q$: shift by P

In practice, E is given by the Weierstrass equation.

ξ : the X coordinate function

η : the Y coordinate function

$$\tau := -\xi/\eta$$

Then $L_{P,-P} = \xi - \xi(P)$ for $P \neq \mathcal{O}$

Sheet 18

Reviews on a Finite Quotient

Recall: $G \subset E$, finite subgroup

$$\exists E/G : \text{E.C.} \quad \exists \varphi_G \in \text{Isog}(E, E/G) \text{ s.t. } \begin{cases} \varphi_G \text{ is separable} \\ \text{Ker } \varphi_G = G \end{cases}$$

$$\varphi_G^* : k^a(E/G) \xrightarrow{\text{field iso } /k^a} k^a(E)^G \quad (G \text{ acts by shift})$$

In case that E is given by the Weierstrass form, we always use the elliptic curve and the isogeny explicitly constructed by Vélu's formula for E/G and φ_G .

Sheet 19

Construction of a Map (1)

Let $A \in E[l] - \{\mathcal{O}\}$ and put $G := \langle A \rangle$.

$$\text{For } \omega \in \mu_l \subset k^a, \text{ put } F_{\omega,A} := \sum_{n=0}^{l-1} \frac{\omega^n}{L_{A,-A} \circ s_{-nA}}$$

- the Lagrange resolvent for cyclic extension $k^a(E)/k^a(E)^G$.

Key equality: $F_{\omega,A} \circ s_A = \omega F_{\omega,A}$

$$\begin{aligned} F_{\omega,A} \circ s_A &= \sum_{n=0}^{l-1} \frac{\omega^n}{L_{A,-A} \circ s_{-nA} \circ s_A} = \sum_{n=0}^{l-1} \frac{\omega^n}{L_{A,-A} \circ s_{-(n-1)A}} \\ &= \omega \sum_{n=0}^{l-1} \frac{\omega^{n-1}}{L_{A,-A} \circ s_{-(n-1)A}} = \omega \sum_{n=-1}^{l-2} \frac{\omega^n}{L_{A,-A} \circ s_{-nA}} \stackrel{\omega^l = 1}{A \in E[l]} = \omega F_{\omega,A} \end{aligned}$$

$F_{\omega,A}^l$ is G invariant.

$\tilde{F}_{\omega,A} := \varphi_G^{*-1}(F_{\omega,A}^l) \in k^a(\tilde{E})$ where $\varphi_G: E \rightarrow \tilde{E} := E/G$.

Sheet 20

Construction of a Map (2)

$$F_{\omega,A} = \sum_{n=0}^{l-1} \frac{\omega^n}{L_{A,-A} \circ s_{-nA}} \text{ where } A \in E[l] - \{\mathcal{O}\} \text{ and } \omega \in \mu_l.$$

- at most simple poles at points in G : l possible poles
- actually simple poles (observe residue, note $A \neq \mathcal{O}$).

Let R be a zero of $F_{\omega,A}$.

The key equality $F_{\omega,A} \circ s_A = \omega F_{\omega,A}$ implies that

$$R + nA \text{ with } 0 \leq n < l \text{ are also zeros of } F_{\omega,A}.$$

$\deg(\text{div}(F_{\omega,A})) = 0$: No other zeros.

$$\text{div}(F_{\omega,A}) = \sum_{n=0}^{l-1} ([R + nA] - [nA])$$

$$\varphi_G \text{ is separable, hence } \text{div}(\tilde{F}_{\omega,A}) = \text{div}(\varphi_G^{*-1} F_{\omega,A}^l) = l([\varphi_G(R)] - [\mathcal{O}])$$

i.e. $\tilde{F}_{\omega,A}$ has the unique zero.

Denote it by $V_A(\omega)$.

Sheet 21

Homomorphy (1)

Key equality: $F_{z\omega,A} \circ s_A = \omega F_{z\omega,A}$

$$\left(\frac{F_{z\omega,A}}{F_{z,A} F_{\omega,A}} \right) \circ s_A = \frac{z\omega F_{z\omega,A}}{zF_{z,A} \omega F_{\omega,A}} = \frac{F_{z\omega,A}}{F_{z,A} F_{\omega,A}} : G\text{-invariant.}$$

$$\begin{aligned} \text{div } \varphi_G^{*-1} \left(\left(\frac{F_{z\omega,A}}{F_{z,A} F_{\omega,A}} \right)^l \right) &= \text{div} \left(\frac{\tilde{F}_{z\omega,A}}{\tilde{F}_{z,A} \tilde{F}_{\omega,A}} \right) \\ &= l([\mathcal{V}_A(z\omega)] - [\mathcal{O}]) - l([\mathcal{V}_A(z)] - [\mathcal{O}]) - l([\mathcal{V}_A(\omega)] - [\mathcal{O}]) \end{aligned}$$

$\text{Div}(\tilde{E})$ is a free Abelian group:

$$\text{div } \varphi_G^{*-1} \left(\frac{F_{z\omega,A}}{F_{z,A} F_{\omega,A}} \right) = [\mathcal{V}_A(z\omega)] - [\mathcal{V}_A(z)] - [\mathcal{V}_A(\omega)] + [\mathcal{O}]$$

This is principal: $V_A(z\omega) = V_A(z) + V_A(\omega)$ i.e. $V_A \in \text{Hom}(\mu_l, \tilde{E}[l])$.

Sheet 22

Homomorphy (2)

For $m \in \mathbb{Z}$,

$$\left(\frac{F_{\omega, A}^m}{F_{\omega^2, mA}^m} \right) \circ s_{mA} = \frac{(\omega^m F_{\omega, A})^m}{\omega^{m^2} F_{\omega^2, mA}^m} = \frac{F_{\omega, A}^m}{F_{\omega^2, mA}^m} : G\text{-invariant}$$

$$\operatorname{div} \left(\varphi_G^{*-1} \left(\frac{F_{\omega, A}^m}{F_{\omega^2, mA}^m} \right) \right) = m([V_A(\omega)] - [\mathcal{O}]) - ([V_{mA}(\omega^2)] - [\mathcal{O}])$$

Thus

$$V_{mA}(\omega^2) = mV_A(\omega), \quad \text{i.e. } V_{mA}(\omega) = m^{-1}V_A(\omega)$$

Sheet 23

Relation to the Weil Pairing

Recall the definition $\tilde{F}_{\omega, A} = \varphi_G^{*-1}(F_{\omega, A}^l)$.

$$F_{\omega, A}^l = \varphi_G^*(\tilde{F}_{\omega, A}) = \tilde{F}_{\omega, A} \circ \varphi_G$$

Composing $\widehat{\varphi}_G$ (the dual of φ_G) from right, we have

$$(F_{\omega, A}^l) \circ \widehat{\varphi}_G = (F_{\omega, A} \circ \widehat{\varphi}_G)^l = \tilde{F}_{\omega, A} \circ l_{\tilde{E}}$$

Recall $\operatorname{div}(\tilde{F}_{\omega, A}) = l([V_A(\omega)] - [\mathcal{O}])$.

By the very definition of the Weil pairing

$$e_l(B, V_{\widehat{\varphi}_G(B)}(\omega)) = \frac{F_{\omega, \widehat{\varphi}_G(B)}(\widehat{\varphi}_G(X) + \widehat{\varphi}_G(B))}{F_{\omega, \widehat{\varphi}_G(B)}(\widehat{\varphi}_G(X))} \stackrel{\text{Key equality}}{=} \omega$$

for $B \in \tilde{E}[l] - \operatorname{Ker} \widehat{\varphi}_G$.

We have obtained FPI for the Weil pairing inversion.

NOTE ADDED AFTER THE CONFERENCE: In fact, I should be more specific about a definition of the Weil pairing. Let $P, Q \in E[l]$. I followed Chap. XI of

A. Weil:

Variétés abéliennes et courbes algébriques, publications de l'Institut mathématique de l'Université de Strasbourg, vol. 8(1946), Hermann & Cie., Paris, 1948. (combined reprint: Courbes algébriques et variétés abéliennes, Herman, Paris 1971).

For elliptic curves, the definition in the above book becomes

$$e_l(P, Q) := g_Q(X+P)/g_Q(X) \quad \text{where} \quad \operatorname{div}(g_Q) = \sum_{S \in E[l]} ([S+Q'] - [S]), \quad lQ' = Q.$$

This is identical to the definition in Silverman's "Arithmetic of elliptic curves", III.8.

On the other hand, in cryptographic community, the Weil paring is usually defined as follows. Let $D_P := [P+U] - [U]$ and $D_Q := [Q+V] - [V]$ where $U, V \in E$ are chosen so that $\operatorname{supp} D_P \cap \operatorname{supp} D_Q = \emptyset$. Then, the l -th Weil pairing is defined to be

$$\tilde{e}_l(P, Q) = f_P(D_Q)/f_Q(D_P) \quad \text{where} \quad \operatorname{div}(f_P) = lD_P, \quad \operatorname{div}(f_Q) = lD_Q.$$

These two definitions are related by $e_l = 1/\tilde{e}_l$. The proofs of this relation can be found E.W. Howe:

The Weil pairing and the Hilbert symbol, Math. Ann. **305**, 387-392(1996) (in the context of Jacobian varieties of curves)

F. Hess:

Some remarks on the Weil and Tate pairings of curves over finite fields, Theorem 4, unpublished manuscript (extended version of Arch. Math. **82**, 28-32, 2004), available at <http://www.math.tu-berlin.de/~hess/personal/bibliography.html>

This proof is fairly elementary and short.

S. Lang:

Abelian variety, Interscience Publishers Inc, 1959 (reprint from Springer, 1983), Theorem VI.12. (in the context of Abelian varieties.)

Note that two major references

J.H. Silverman:

The arithmetic of elliptic curves, GTM 106, Exercise 3.16(c)

I.F. Blake et al.:

Elliptic curves in cryptography, London Math. Soc. Lect. Notes **265**, §III.5

incorrectly state that $e_l = \tilde{e}_l$. The readers are advised to note this discrepancy of the definitions of the Weil pairing in testing the formulas obtained below by numerical examples. **END NOTE**

Sheet 24 **Behavior under Galois Action (1)**

Assume that E is given by the Weierstrass eq.

For $\sigma \in \text{Gal}(k^a/k)$,

$$\sigma^\circ F_{\omega, A} = \sum_{n=0}^{l-1} \frac{\sigma(\omega^n)}{\sigma^\circ L_{A, -A} \circ S_{-nA}} = \sum_{n=0}^{l-1} \frac{\sigma(\omega^n)}{L_{\sigma(A), -\sigma(A)} \circ S_{-n\sigma(A)}} \circ \sigma = F_{\sigma(\omega), \sigma(A)} \circ \sigma$$

$$\sigma^\circ \tilde{F}_{\omega, A} \circ \varphi_G = \tilde{F}_{\sigma(\omega), \sigma(A)} \circ \varphi_{\langle \sigma(A) \rangle} \circ \sigma = \tilde{F}_{\sigma(\omega), \sigma(A)} \circ \sigma^\circ \varphi_G$$

A zero of $\tilde{F}_{\sigma(\omega), \sigma(A)}$ is unique: $\sigma(V_A(\omega)) = V_{\sigma(A)}(\sigma(\omega))$.

K/k : algebraic extension.

G is defined over $K \Rightarrow \langle V_A(\omega) \rangle$ is defined over K .

Sheet 25 **Behavior under Galois Action (2)**

Let $K = \mathbf{F}_q$ and $[\mathbf{F}_q(\mu_l) : \mathbf{F}_q] > 1$.

π_q : the q -th Frobenius map. $\Rightarrow \pi_q(\omega) = \omega^q$.

$E[l]$ has two non-trivial subgroups defined over K .

$A \in E(\mathbf{F}_q)[l]$

$$\pi_q(A) = A \text{ so } \pi_q(V_A(\omega)) = qV_A(\omega)$$

$$V_A(\omega) \in \text{trace zero sub group}$$

$A \in \text{trace zero subgroup of order } l$

$$\pi_q(A) = qA \text{ so } \pi_q(V_A(\omega)) = V_A(\omega)$$

$$V_A(\omega) \in \tilde{E}(\mathbf{F}_q)[L]$$

Remark: Quotient by $E(\mathbf{F}_q)[L]$ and by trace zero subgroup may differ.

Sheet 26 **Computing V_A (1)**

$$E: Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

For simplicity, $\text{char}(k)=2$ in what follows.

(The same argument holds for at least $\text{char}(k) > 3$ or $= 0$.)

$$x_R := \xi(V_A(\omega)), \quad y_R := \eta(V_A(\omega)), \quad u_n := \xi(nA), \quad v_n = \eta(nA), \quad \Omega_n := \omega^n + \omega^{-n}$$

$$\text{div} \left(\varphi_G^{*-1} \left(\frac{F_{\omega,A}^2}{F_{\omega^4, 2A}} \right) \right) = \text{div} \left(\frac{L_{R,R}}{L_{2R, -2R}} \right)$$

$$F_{\omega,A} = \frac{\Omega_1}{a_1u_1+a_3} \tau^{-1} + \frac{\Omega_1(u_1^2+v_1a_1+a_4)+\omega^{-1}a_1(a_1u_1+a_3)}{(a_1u_1+a_3)^2} + \sum_{n=2}^{(l-1)/2} \frac{\Omega_n}{u_1+u_n} \\ + \left(\frac{\Omega_1}{a_1u+a_3} u_2 + \sum_{n=2}^{(l-1)/2} \frac{\Omega_n(a_1u_1+a_3)}{(u_n+u_1)^2} \right) \tau + \dots$$

By Vélú's formula, $\varphi_G^*(\tilde{\tau}) = \tau(1 + O(\tau^4))$.

Sheet 27 **Computing V_A (2)**

Comparing the coefficients of τ^{-1} , we obtain

$$\frac{F_{\omega,A}^2}{F_{\omega^4, 2A}} = \frac{a_1u_2+a_3}{\Omega_2(a_1u_1+a_3)^2} \frac{L_{R,R}}{L_{2R, -2R}} \circ \varphi_G$$

Comparing the constant terms, we see

$$\frac{x_R^2 + a_1y_R + \tilde{a}_4}{a_1x_R + a_3} = \frac{\Omega_4(u_2^2+v_2a_1+a_4)+\omega^{-4}a_1(a_1u_2+a_3)}{(a_1u_2+a_3)^2} + \sum_{n=2}^{(l-1)/2} \frac{\Omega_{4n}}{u_2-u_{2n}}$$

The case E is ordinary ($a_1 \neq 0$):

$(x_R, y_R) \in \tilde{E} \Rightarrow 6$ pts. This is enough to break CDHP.

The case E is super singular ($a_1 = 0$):

The above formula gives x_R .

NOTE ADDED AFTER THE CONFERENCE: In the above formula, \tilde{a}_4 is the coefficient of X in the Weierstrass eq. of \tilde{E} constructed by Vélú's formula. In case of $a_1 \neq 0$, actually we obtain **2** candidate points rather than 6. **END NOTE**

Sheet 28 **Computing V_A (3)**

Comparing the coefficients of τ^2 we have y_R . w.l.g. $a_2 = 0$.

$$\begin{aligned}
 x_R &= u_2 + \frac{a_3^2}{\Omega_2} \sum_{n=2}^{(l-1)/2} \frac{\Omega_{2n}}{(u_1 - u_n)^2} \\
 y_R &= \frac{(u_2^2 + a_4)}{a_3} (u_4 + u_2) + v_2 + \frac{\omega^4 a_3}{\Omega_4} \\
 &\quad + \frac{a_3(u_2^2 + a_4)}{\Omega_4} \sum_{n=2}^{(l-1)/2} \frac{\Omega_{4n}}{(u_2 - u_{2n})^2} + \frac{a_3^3}{\Omega_4} \sum_{n=2}^{(l-1)/2} \frac{\Omega_{4n}}{(u_2 - u_{2n})^3}
 \end{aligned}$$

Sheet 29

Failed Attempts

Use of -

- division polynomials
- coefficients of higher degree term of $F_{\omega, A}$
- more relations from homomorphy
- Galois theory
- $\psi(V_A(\omega)) = V_{\psi(A)}(\omega)$ for $\psi \in \text{Aut}(E)$.

This is specific to characteristic two.

Sheet 30

Concluding Remarks

In spite of their importance, pairing inversion problems and related problems are not well studied.

Further research is very desirable.

Acknowledgments: I would like to thank Prof. David Lubicz at Université de Rennes and Prof. Loren Olson at Universitet i Tromsø for giving me opportunities to visit. Crucial parts of the work on the Weil pairing inversion were performed there.