Computing optimal pairings on abelian varieties with theta functions

David Lubicz[1,2], **Damien Robert**[3]

[1]CÉLAR

[2]IRMAR, Université de Rennes 1

[1]LFANT Team, IMB & Inria Bordeaux Sud-Ouest

10/02/2011 (Luminy)

Outline

Discrete logarithm

Definition (DLP)

Let $G = \langle g \rangle$ be a cyclic group of prime order. Let $x \in \mathbb{N}$ and $h = g^x$. The discrete logarithm $\log_g(h)$ is x.

- Exponentiation: $O(\log p)$. DLP: $\widetilde{O}(\sqrt{p})$ (in a generic group).
- The DLP is supposed to be difficult to solve in $\mathbb{F}_q^*$, $E(\mathbb{F}_q)$, $J(\mathbb{F}_q)$, $A(\mathbb{F}_q)$.

$\Rightarrow$ The DLP yields good candidates for one way functions.

Pairings

Definition

Let G_1 and G_2 be two cyclic groups of prime order. A pairing is a (non degenerate) bilinear application $e : G_1 \times G_1 \to G_2$.

- If the pairing e can be computed easily, the difficulty of the DLP in G_1 reduces to the difficulty of the DLP in G_2.

$\Rightarrow$ MOV attacks on elliptic curves.

Cryptographic applications of pairings

- Identity-based cryptography [BF03].
- Short signature [BLS04].
- One way tripartite Diffie–Hellman [Jou04].
- Self-blindable credential certificates [Ver01].
- Attribute based cryptography [SW05].
- Broadcast encryption [GPSW06].

Example (Identity-based cryptography)

- Master key: (P, sP), s. $\quad s \in \mathbb{N}, P \in G_1$.
- Derived key: Q, sQ. $\quad Q \in G_1$.
- Encryption, $m \in G_2$: $m' = m \oplus e(Q, sP)^r$, rP. $\quad r \in \mathbb{N}$.
- Decryption: $m = m' \oplus e(sQ, rP)$.

The Weil pairing on elliptic curves

- Let $E: y^2 = x^3 + ax + b$ be an elliptic curve over k ($\operatorname{car} k \neq 2,3$).
- Let $P, Q \in E[\ell]$ be points of ℓ-torsion.
- The divisor $[\ell]^*(Q-0)$ is trivial, let $g_Q \in k(E)$ be a function associated to this principal divisor.
- The function $x \mapsto \frac{g_Q(x+P)}{g_Q(x)}$ is constant and is equal to a ℓ-th root of unity $e_{W,\ell}(P,Q)$ in $\overline{k}^*$.

Proof.

If f_Q is a function associated to the principal divisor $\ell Q - \ell 0$, we have $(g_Q^\ell) = [\ell](g_Q) = [\ell]^*[\ell](Q-0) = [\ell]^*(f_Q) = (f_Q \circ [\ell])$ so $g_Q(x+P)^\ell = f_Q(\ell x + \ell P) = f_Q(\ell x) = g_Q(x)^\ell$ and $e_{W,\ell}(P,Q)^\ell = 1$. □

- The application $e_{W,\ell}: E[\ell] \times E[\ell] \to \mu_\ell(\overline{k})$ is a non degenerate pairing: the Weil pairing.

Computing the Weil pairing

- Let f_P be a function associated to the principal divisor $\ell(P-0)$, and f_Q to $\ell(Q-0)$.
- By Weil reciprocity, we have:

$$e_{W,\ell}(P,Q) = \frac{f_Q(P-0)}{f_P(Q-0)}.$$

- We need to compute the functions f_P and f_Q. More generally, we define the Miller's functions:

Definition

Let $\lambda \in \mathbb{N}$ and $X \in E[\ell]$, we define $f_{\lambda,X} \in k(E)$ to be a function thus that:

$$(f_{\lambda,X}) = \lambda(X) - ([\lambda]X) - (\lambda-1)(0).$$

Miller's algorithm

- The key idea in Miller's algorithm is that

$$f_{\lambda+\mu,X} = f_{\lambda,X} f_{\mu,X} \mathfrak{f}_{\lambda,\mu,X}$$

where $\mathfrak{f}_{\lambda,\mu,X}$ is a function associated to the divisor

$$([\lambda+\mu]X) - ([\lambda]X) - ([\mu]X) + (0).$$

- We can compute $\mathfrak{f}_{\lambda,\mu,X}$ using the addition law in E: if $[\lambda]X = (x_1, y_1)$ and $[\mu]X = (x_2, y_2)$ and $\alpha = (y_1 - y_2)/(x_1 - x_2)$, we have

$$\mathfrak{f}_{\lambda,\mu,X} = \frac{y - \alpha(x - x_1) - y_1}{x + (x_1 + x_2) - \alpha^2}.$$

Tate pairing

Definition

- Let $E/\mathbb{F}_q$ be an elliptic curve of cardinal divisible by ℓ. Let d be the smallest number thus that $\ell \mid q^d - 1$: we call d the embedding degree. $\mathbb{F}_{q^d}$ is constructed from $\mathbb{F}_q$ by adjoining all the ℓ-th root of unity.
- The Tate pairing is a non degenerate bilinear application given by

$$\begin{array}{rcl} e_T\colon E(\mathbb{F}_{q^d})/\ell E(\mathbb{F}_{q^d}) \times E[\ell](\mathbb{F}_q) & \longrightarrow & \mathbb{F}^*_{q^d}/\mathbb{F}^{*\,\ell}_{q^d} \\ (P,Q) & \longmapsto & f_Q((P)-(0)) \end{array}.$$

- If $\ell^2 \nmid E(\mathbb{F}_{q^d})$ then $E(\mathbb{F}_{q^d})/\ell E(\mathbb{F}_{q^d}) \simeq E[\ell](\mathbb{F}_{q^d})$.
- We normalise the Tate pairing by going to the power of $(q^d-1)/\ell$.
- This final exponentiation allows to save some computations. For instance if $d = 2d'$ is even, we can suppose that $P = (x_2, y_2)$ with $x_2 \in E(\mathbb{F}_{q^{d'}})$. Then the denominators of $f_{\lambda,\mu,Q}$ are ℓ-th powers and are killed by the final exponentiation.

Miller's algorithm

Computing Tate pairing

Input: $\ell \in \mathbb{N}$, $Q=(x_1,y_1)\in E[\ell](\mathbb{F}_q)$, $P=(x_2,y_2)\in E(\mathbb{F}_{q^d})$.

Output: $e_T(P,Q)$.

- Compute the binary decomposition: $\ell := \sum_{i=0}^{I} b_i 2^i$. Let $T=Q, f_1=1, f_2=1$.
- For i in $[I..0]$ compute
  - α, the slope of the tangent of E at T.
  - $T=2T$. $T=(x_3,y_3)$.
  - $f_1=f_1^2(y_2-\alpha(x_2-x_3)-y_3)$, $f_2=f_2^2(x_2+(x_1+x_3)-\alpha^2)$.
  - If $b_i=1$, then compute
    - α, the slope of the line going through Q and T.
    - $T=T+Q$. $T=(x_3,y_3)$.
    - $f_1=f_1^2(y_2-\alpha(x_2-x_3)-y_3)$, $f_2=f_2(x_2+(x_1+x_3)-\alpha^2)$.
- Return

$$\left(\frac{f_1}{f_2}\right)^{\frac{q^d-1}{\ell}}.$$

Abelian varieties

Definition

An Abelian variety is a complete connected group variety over a base field k.

- Abelian variety = points on a projective space (locus of homogeneous polynomials) + an abelian group law given by rational functions.

Example

- Elliptic curves= Abelian varieties of dimension 1.
- If C is a (smooth) curve of genus g, its Jacobian is an abelian variety of dimension g.

Pairing on abelian varieties

- Let $Q \in \widehat{A}[\ell]$. By definition of the dual abelian variety, Q is a divisor of degree 0 on A such that ℓQ is principal. Let $f_Q \in k(A)$ be a function associated to ℓQ.
- Let $P \in A[\ell]$. Since $\widehat{\widehat{A}} \simeq A$, we can see P as a divisor of degree 0 on $\widehat{A}$. $\ell(P)$ is then a principal divisor (f_P) where $f_P \in k(\widehat{A})$.
- We can then define the Weil pairing:

$$\begin{aligned} e_{W,\ell} : A[\ell] \times \widehat{A}[\ell] &\longrightarrow \mu_\ell(\overline{k}) \\ (P,Q) &\longmapsto \frac{f_Q(P)}{f_P(Q)} \end{aligned}.$$

- Likewise, we can extend the Tate pairing to abelian varieties.

Pairings and polarizations

- If Θ is an ample divisor, the polarisation φ_Θ is a morphism $A \to \widehat{A}, x \mapsto t_x^*\Theta - \Theta$.
- We can then compose the Weil and Tate pairings with φ_Θ:

$$\begin{array}{rcl} e_{W,\Theta,\ell}: A[\ell] \times A[\ell] & \longrightarrow & \mu_\ell(\overline{k}) \\ (P,Q) & \longmapsto & e_{W,\ell}(P, \varphi_\Theta(Q)) \end{array} .$$

- More explicitly, if f_P and f_Q are the functions associated to the principal divisors $\ell t_P^*\Theta - \ell\Theta$ and $\ell t_Q^*\Theta - \ell\Theta$ we have

$$e_{W,\Theta,\ell}(P,Q) = \frac{f_Q(P-0)}{f_P(Q-0)}.$$

Cryptographic usage of pairings on abelian varieties

- The moduli space of abelian varieties of dimension g is a space of dimension $g(g+1)/2$. We have more liberty to find optimal abelian varieties in function of the security parameters.
- Supersingular elliptic curves have a too small embedding degree. [RS09] says that for the current security parameters, optimal supersingular abelian varieties of small dimension are of dimension 4.
- If A is an abelian variety of dimension g, $A[\ell]$ is a $(\mathbb{Z}/\ell\mathbb{Z})$-module of dimension $2g \Rightarrow$ the structure of pairings on abelian varieties is richer.

Computing pairings on abelian varieties

- If J is the Jacobian of an hyperelliptic curve H of genus g, it is easy to extend Miller's algorithm to compute the Tate and Weil pairing on J.
- For instance if $g = 2$, the function $f_{\lambda,\mu,Q}$ is of the form

$$\frac{y - l(x)}{(x - x_1)(x - x_2)}$$

where l is of degree 3.

- If P is a degenerate divisor (P is a sum of only one point on the curve H), the evaluation $f_Q(P)$ is faster than for a general divisor (which would be a sum of g points on the curve H).

$\Rightarrow$ Pairings on Jacobians of genus 2 curves can be competitive with pairings on elliptic curves.

- What about more general abelian varieties? We don't have Mumford coordinates.

Complex abelian varieties

- Abelian variety over $\mathbb{C}$: $A = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$, where $\Omega \in \mathcal{H}_g(\mathbb{C})$ the Siegel upper half space.
- The theta functions with characteristic give a lot of analytic (quasi periodic) functions on $\mathbb{C}^g$.

$$\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\Omega) = \sum_{n\in\mathbb{Z}^g} e^{\pi i \, {}^t(n+a)\Omega(n+a)+2\pi i \, {}^t(n+a)(z+b)} \qquad a,b \in \mathbb{Q}^g$$

Quasi-periodicity:

$$\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z+m_1\Omega+m_2,\Omega) = e^{2\pi i({}^t a\cdot m_2 - {}^t b\cdot m_1) - \pi i \, {}^t m_1\Omega m_1 - 2\pi i \, {}^t m_1\cdot z}\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\Omega).$$

- Projective coordinates:

$$\begin{array}{ccc} A & \longrightarrow & \mathbb{P}^{n^g-1}_{\mathbb{C}} \\ z & \longmapsto & (\vartheta_i(z))_{i\in Z(\overline{n})} \end{array}$$

where $Z(\overline{n}) = \mathbb{Z}^g/n\mathbb{Z}^g$ and $\vartheta_i = \vartheta\left[\begin{smallmatrix} 0 \\ \frac{i}{n} \end{smallmatrix}\right](., \frac{\Omega}{n})$.

The differential addition law ($k = \mathbb{C}$)

$$\Big(\sum_{t \in Z(\overline{2})} \chi(t)\vartheta_{i+t}(x+y)\vartheta_{j+t}(x-y)\Big).\Big(\sum_{t \in Z(\overline{2})} \chi(t)\vartheta_{k+t}(0)\vartheta_{l+t}(0)\Big) =$$

$$\Big(\sum_{t \in Z(\overline{2})} \chi(t)\vartheta_{-i'+t}(y)\vartheta_{j'+t}(y)\Big).\Big(\sum_{t \in Z(\overline{2})} \chi(t)\vartheta_{k'+t}(x)\vartheta_{l'+t}(x)\Big).$$

where $\chi \in \hat{Z}(\overline{2}), i, j, k, l \in Z(\overline{n})$

$$(i', j', k', l') = A(i, j, k, l)$$

$$A = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Example: addition in genus 1 and in level 2

Doubling Algorithm:
Input: $P=(x:z)$.
Output: $2.P=(x':z')$.

1. $x_0=(x^2+z^2)^2$;
2. $z_0=\frac{A^2}{B^2}(x^2-z^2)^2$;
3. $x'=(x_0+z_0)/a$;
4. $z'=(x_0-z_0)/b$;
5. Return $(x':z')$.

Differential Addition Algorithm:
Input: $P=(x_1:z_1)$, $Q=(x_2:z_2)$ and $R=P-Q=(x_3:z_3)$ with $x_3z_3\neq 0$.
Output: $P+Q=(x':z')$.

1. $x_0=(x_1^2+z_1^2)(x_2^2+z_2^2)$;
2. $z_0=\frac{A^2}{B^2}(x_1^2-z_1^2)(x_2^2-z_2^2)$;
3. $x'=(x_0+z_0)/x_3$;
4. $z'=(x_0-z_0)/z_3$;
5. Return $(x':z')$.

Arithmetic with low level theta functions (car $k \neq 2$)

	Mumford [Lan05]	Level 2 [Gau07]	Level 4
Doubling	$34M+7S$	$7M+12S+9m_0$	$49M+36S+27m_0$
Mixed Addition	$37M+6S$		

Multiplication cost in genus 2 (one step).

	Montgomery	Level 2	Jacobians	Level 4
Doubling	$5M+4S+1m_0$	$3M+6S+3m_0$	$3M+5S$	$9M+10S+5$
Mixed Addition			$7M+6S+1m_0$	

Multiplication cost in genus 1 (one step).

The Weil and Tate pairing with theta coordinates [LR10]

P and Q points of ℓ-torsion.

0_A	P	$2P$	$\dots$	$\ell P = \lambda_P^0 0_A$
Q	$P \oplus Q$	$2P+Q$	$\dots$	$\ell P + Q = \lambda_P^1 Q$
$2Q$	$P+2Q$			
$\dots$	$\dots$			
$\ell Q = \lambda_Q^0 0_A$	$P + \ell Q = \lambda_Q^1 P$			

- $e_{W,\ell}(P,Q) = \frac{\lambda_P^1 \lambda_Q^0}{\lambda_P^0 \lambda_Q^1}$.
  If $P = \Omega x_1 + x_2$ and $Q = \Omega y_1 + y_2$, then $e_{W,\ell}(P,Q) = e^{-2\pi i \ell ({}^t x_1 \cdot y_2 - {}^t y_1 \cdot x_2)}$.
- $e_{T,\ell}(P,Q) = \frac{\lambda_P^1}{\lambda_P^0}$.

Why does it works?

$$\begin{array}{ccccc} 0_A & \alpha P & \alpha^4(2P) & \dots & \alpha^{\ell^2}(\ell P) = \lambda'^0_P 0_A \\ \beta Q & \gamma(P \oplus Q) & \frac{\gamma^2\alpha^2}{\beta}(2P+Q) & \dots & \frac{\gamma^\ell \alpha^{\ell(\ell-1)}}{\beta^{\ell-1}}(\ell P+Q) = \lambda'^1_P \beta Q \\ \beta^4(2Q) & \frac{\gamma^2\beta^2}{\alpha}(P+2Q) & & & \\ \dots & \dots & & & \\ \beta^{\ell^2}(\ell Q) = \lambda'^0_Q 0_A & \frac{\gamma^\ell \beta^{\ell(\ell-1)}}{\alpha^{\ell-1}}(P+\ell Q) = \lambda'^1_Q \alpha P & & & \end{array}$$

We then have

$$\lambda'^0_P = \alpha^{\ell^2}\lambda^0_P, \quad \lambda'^0_Q = \beta^{\ell^2}\lambda^0_Q, \quad \lambda'^1_P = \frac{\gamma^\ell \alpha^{(\ell(\ell-1)}}{\beta^\ell}\lambda^1_P, \quad \lambda'^1_Q = \frac{\gamma^\ell \beta^{(\ell(\ell-1)}}{\alpha^\ell}\lambda^1_Q,$$

$$e'_{W,\ell}(P,Q) = \frac{\lambda'^1_P \lambda'^0_Q}{\lambda'^0_P \lambda'^1_Q} = \frac{\lambda^1_P \lambda^0_Q}{\lambda^0_P \lambda^1_Q} = e_{W,\ell}(P,Q),$$

$$e'_{T,\ell}(P,Q) = \frac{\lambda'^1_P}{\lambda'^0_P} = \frac{\gamma^\ell}{\alpha^\ell\beta^\ell}\frac{\lambda^1_P}{\lambda^0_P} = \frac{\gamma^\ell}{\alpha^\ell\beta^\ell} e_{T,\ell}(P,Q).$$

The case $n = 2$

- If $n = 2$ we work over the Kummer variety K, so $e(P,Q) \in \overline{k}^{*,\pm 1}$.
- We represent a class $x \in \overline{k}^{*,\pm 1}$ by $x + 1/x \in \overline{k}^{*}$. We want to compute the symmetric pairing

$$e_s(P,Q) = e(P,Q) + e(-P,Q).$$

- From $\pm P$ and $\pm Q$ we can compute $\{\pm(P+Q), \pm(P-Q)\}$ (need a square root), and from these points the symmetric pairing.
- e_s is compatible with the $\mathbb{Z}$-structure on K and $\overline{k}^{*,\pm 1}$.
- The $\mathbb{Z}$-structure on $\overline{k}^{*,\pm}$ can be computed as follow:

$$(x^{\ell_1+\ell_2} + \frac{1}{x^{\ell_1+\ell_2}}) + (x^{\ell_1-\ell_2} + \frac{1}{x^{\ell_1-\ell_2}}) = (x^{\ell_1} + \frac{1}{x^{\ell_1}})(x^{\ell_2} + \frac{1}{x^{\ell_2}})$$

Comparison with Miller algorithm

$g=1$	$7\mathbf{M}+7\mathbf{S}+2\mathbf{m_0}$
$g=2$	$17\mathbf{M}+13\mathbf{S}+6\mathbf{m_0}$

Tate pairing with theta coordinates, $P,Q \in A[\ell](\mathbb{F}_{q^d})$ (one step)

		Miller		Theta coordinates
		Doubling	Addition	One step
$g=1$	d even	$1\mathbf{M}+1\mathbf{S}+1\mathbf{m}$	$1\mathbf{M}+1\mathbf{m}$	$1\mathbf{M}+2\mathbf{S}+2\mathbf{m}$
	d odd	$2\mathbf{M}+2\mathbf{S}+1\mathbf{m}$	$2\mathbf{M}+1\mathbf{m}$	
$g=2$	Q degenerate + d even	$1\mathbf{M}+1\mathbf{S}+3\mathbf{m}$	$1\mathbf{M}+3\mathbf{m}$	$3\mathbf{M}+4\mathbf{S}+4\mathbf{m}$
	General case	$2\mathbf{M}+2\mathbf{S}+18\mathbf{m}$	$2\mathbf{M}+18\mathbf{m}$	

$P \in A[\ell](\mathbb{F}_q)$, $Q \in A[\ell](\mathbb{F}_{q^d})$ (counting only operations in $\mathbb{F}_{q^d}$).

Ate pairing

- Let $G_1 = E[\ell] \bigcap \mathrm{Ker}(\pi_q - 1)$ and $G_2 = E[\ell] \bigcap \mathrm{Ker}(\pi_q - [q])$.
- We have $f_{ab,Q} = f_{a,Q}^b f_{b,[a]Q}$.
- Let $P \in G_1$ and $Q \in G_2$ we have $f_{a,[q]Q}(P) = f_{a,Q}(P)^q$.
- Let $\lambda \equiv q \mod \ell$. Let $m = (\lambda^d - 1)/\ell$. We then have

$$\begin{aligned} e_T(P,Q)^m &= f_{\lambda^d,Q}(P)^{(q^d-1)/\ell} \\ &= \left(f_{\lambda,Q}(P)^{\lambda^{d-1}} f_{\lambda,[q]Q}(P)^{\lambda^{d-2}} \dots f_{\lambda,[q^{d-1}]Q}(P)\right)^{(q^d-1)/\ell} \\ &= \left(f_{\lambda,Q}(P)^{\sum \lambda^{d-1-i} q^i}\right)^{(q^d-1)/\ell} \end{aligned}$$

Definition

Let $\lambda \equiv q \mod \ell$, the (reduced) ate pairing is defined by

$$a_\lambda : G_1 \times G_2 \to \mu_\ell, (P,Q) \mapsto f_{\lambda,Q}(P)^{(q^d-1)/\ell}.$$

It is non degenerate if $\ell^2 \nmid (\lambda^k - 1)$.

Optimal ate [Ver10]

- Let $\lambda = m\ell = \sum c_i q^i$ be a multiple of ℓ with small coefficients c_i. $(\ell \nmid m)$
- The pairing

$$\begin{aligned} a_\lambda \colon G_1 \times G_2 &\longrightarrow \mu_\ell \\ (P, Q) &\longmapsto \left(\prod_i f_{c_i, Q}(P)^{q^i} \prod_i f_{\sum_{j>i} c_j q^j, c_i q^i, Q}(P) \right)^{(q^d - 1)/\ell} \end{aligned}$$

  is non degenerate when $m d q^{d-1} \not\equiv (q^d - 1)/r \sum_i i c_i q^{i-1} \mod \ell$.
- Since $\varphi_d(q) = 0 \mod \ell$ we look at powers $q, q^2, \ldots, q^{\varphi(d)-1}$.
- We can expect to find λ such that $c_i \approx \ell^{1/\varphi(d)}$.

Ate pairing with theta functions

- Let $P \in G_1$ and $Q \in G_2$.
- In projective coordinates, we have $\pi_q^d(P+Q) = P + \lambda^d Q = P + Q$.
- Unfortunately, in affine coordinates, $\pi_q^d(\widetilde{P+Q}) \neq \widetilde{P+\lambda^d Q}$.
- But if $\pi_q^d(\widetilde{P+Q}) = C * \widetilde{P+\lambda^d Q}$, then C is exactly the (non reduced) ate pairing!

Miller functions with theta coordinates

- We have

$$f_{\mu,Q}(P) = \frac{\vartheta(Q)}{\vartheta(P+\mu Q)} \left(\frac{\vartheta(P+Q)}{\vartheta(P)} \right)^{\mu}.$$

- So

$$\mathfrak{f}_{\lambda,\mu,Q}(P) = \frac{\vartheta(P+\lambda Q)\vartheta(P+\mu Q)}{\vartheta(P)\vartheta(P+(\lambda+\mu)Q)}.$$

- We can compute this function using a generalised version of Riemann's relations:

$$\Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{i+t}(P+(\lambda+\mu)Q)\vartheta_{j+t}(\lambda Q)\Big).\Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{k+t}(\mu Q)\vartheta_{l+t}(P)\Big) =$$

$$\Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{-i'+t}(0)\vartheta_{j'+t}(P+\mu Q)\Big).\Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{k'+t}(P+\lambda Q)\vartheta_{l'+t}((\lambda+\mu)Q)\Big).$$

Perspectives

- Characteristic 2 case (especially for supersingular abelian varieties of characteristic 2).
- Optimized implementations (FPGA, ...).
- Look at special points (degenerate divisors, ...).

Bibliography

[BF03] D. Boneh and M. Franklin. “Identity-based encryption from the Weil pairing”. In: *SIAM Journal on Computing* 32.3 (2003), pp. 586–615 (cit. on p. 5).

[BLS04] D. Boneh, B. Lynn, and H. Shacham. “Short signatures from the Weil pairing”. In: *Journal of Cryptology* 17.4 (2004), pp. 297–319 (cit. on p. 5).

[Gau07] P. Gaudry. “Fast genus 2 arithmetic based on Theta functions”. In: *Journal of Mathematical Cryptology* 1.3 (2007), pp. 243–265 (cit. on p. 19).

[GPSW06] V. Goyal, O. Pandey, A. Sahai, and B. Waters. “Attribute-based encryption for fine-grained access control of encrypted data”. In: *Proceedings of the 13th ACM conference on Computer and communications security*. ACM. 2006, p. 98 (cit. on p. 5).

[Jou04] A. Joux. “A one round protocol for tripartite Diffie–Hellman”. In: *Journal of Cryptology* 17.4 (2004), pp. 263–276 (cit. on p. 5).

[Lan05] T. Lange. “Formulae for arithmetic on genus 2 hyperelliptic curves”. In: *Applicable Algebra in Engineering, Communication and Computing* 15.5 (2005), pp. 295–328 (cit. on p. 19).

[LR10] D. Lubicz and D. Robert. “Efficient pairing computation with theta functions”. In: *Algorithmic Number Theory*. Lecture Notes in Comput. Sci. 6197 (July 2010). Ed. by G. Hanrot, F. Morain, and E. Thomé. 9th International Symposium, Nancy, France, ANTS-IX, July 19-23, 2010, Proceedings. DOI: 10.1007/978-3-642-14518-6_21. URL: http://www.normalesup.org/~robert/pro/publications/articles/pairings.pdf. Slides http://www.normalesup.org/~robert/publications/slides/2010-07-ants.pdf (cit. on p. 20).

[RS09] K. Rubin and A. Silverberg. “Using abelian varieties to improve pairing-based cryptography”. In: *Journal of Cryptology* 22.3 (2009), pp. 330–364 (cit. on p. 14).

[SW05] A. Sahai and B. Waters. “Fuzzy identity-based encryption”. In: *Advances in Cryptology–EUROCRYPT 2005* (2005), pp. 457–473 (cit. on p. 5).

[Ver10] F. Vercauteren. "Optimal pairings". In: *IEEE Transactions on Information Theory* 56.1 (2010), pp. 455–461 (cit. on p. 25).

[Ver01] E. Verheul. "Self-blindable credential certificates from the Weil pairing". In: *Advances in Cryptology—ASIACRYPT 2001* (2001), pp. 533–551 (cit. on p. 5).