Efficient pairing computation with theta functions.

ANTS IX

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

[1]CÉLAR

[2]IRMAR, Université de Rennes 1

[3]Caramel Team, Nancy Université, CNRS, Inria Nancy Grand Est

21/07/2010

Pairings in cryptography

Definition

A pairing is a bilinear application $e : G_1 \times G_1 \to G_2$.

- Identity-based cryptography [BF03].
- Short signature [BLS04].
- One way tripartite Diffie–Hellman [Jou04].
- Anonymous credentials [Ver01].
- Attribute based cryptography [SW05].
- Broadcast encryption [Goy+06].

Pairings on abelian varieties

- $(A, \mathcal{L})$ a principally polarised abelian variety.
- Θ the theta divisor associated to $\mathcal{L}$.
- $P \in A[\ell]$. $\exists f_P \in k(A) \mid$
$$(f_P) = \ell\,(t_P^*\Theta - \Theta)\,.$$
- Weil pairing $e_W : A[\ell] \times A[\ell] \to \mu_\ell$
$$e_W(P, Q) = \frac{f_P(Q - 0_A)}{f_Q(P - 0_A)}.$$
- Tate pairing: $e_T : A[\ell] \times A(k)/\ell A(k) \to k^*/k^{*\ell}$
$$e_T(P, Q) = f_P(Q - 0_A).$$

Miller algorithm

- $P \in A[\ell]$. $\exists f_{n,P} \in k(A) \mid$

$$(f_{n,P}) = n.t_P^* \Theta - t_{nP}^* \Theta - (n-1)\Theta.$$

- $\exists f_{n_1.P, n_2.P} \in k(A) \mid$

$$(f_{n_1.P,n_2.P}) = t_{n_1.P}^* \Theta + t_{n_2.P}^* \Theta - t_{(n_1+n_2).P}^* \Theta - \Theta.$$

- $$f_{(n_1+n_2),P} = f_{n_1,P} f_{n_2,P} f_{n_1.P,n_2.P}$$

$\Rightarrow$ Evaluate $f_{\ell,P}(Q)$ via a Miller loop.

Remark

Only used with Mumford coordinates $\Rightarrow$ need to work on a Jacobian of an hyperelliptic curve.

Theta functions

- Abelian variety over $\mathbb{C}$: $A = \mathbb{C}^g / (\mathbb{Z}^g + \Omega\mathbb{Z}^g)$; $\Omega \in \mathcal{H}_g(\mathbb{C})$ the Siegel upper half space (Ω symmetric, $\operatorname{Im}\Omega$ positive definite).
- Theta functions with characteristics:

$$\vartheta(z,\Omega) = \sum_{n \in \mathbb{Z}^g} e^{\pi i \, {}^t n \Omega n + 2\pi i \, {}^t n z},$$

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

- Theta functions of level 4: $\left(\vartheta\left[\begin{smallmatrix} i/2 \\ j/2 \end{smallmatrix}\right](2z,\Omega)\right)_{i,j \in Z(\overline{2})}$, coordinates on A.
- Theta functions of level 2: $\left(\vartheta\left[\begin{smallmatrix} 0 \\ i/2 \end{smallmatrix}\right](z,\Omega/2)\right)_{i \in Z(\overline{2})}$, coordinates on the Kummer variety $A/\pm 1$.

Duplication formula

$$\vartheta\left[\begin{smallmatrix}0\\ \frac{i}{2}\end{smallmatrix}\right](z_1+z_2,\Omega)\vartheta\left[\begin{smallmatrix}0\\ \frac{j}{2}\end{smallmatrix}\right](z_1-z_2,\Omega)=\sum_{t\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}\vartheta\left[\begin{smallmatrix}\frac{t}{2}\\ \frac{i+j}{4}\end{smallmatrix}\right](2z_1,2\Omega)\vartheta\left[\begin{smallmatrix}\frac{t}{2}\\ \frac{i-j}{4}\end{smallmatrix}\right](2z_2,2\Omega)$$

$$\vartheta\left[\begin{smallmatrix}\chi/2\\ i/(4)\end{smallmatrix}\right](2z_i,2\Omega)\vartheta\left[\begin{smallmatrix}0\\ j/(4)\end{smallmatrix}\right](0,2\Omega)=$$
$$\frac{1}{2^g}\sum_{t\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}e^{-2i\pi\,{}^t\chi\cdot t}\vartheta\left[\begin{smallmatrix}2\chi\\ \frac{i+j}{4}+t\end{smallmatrix}\right](z_i,\Omega)\vartheta\left[\begin{smallmatrix}0\\ \frac{i-j}{4}+t\end{smallmatrix}\right](z_i,\Omega).$$

The differential addition law

$$\Big(\sum_{t \in Z(\overline{2})} \chi(t)\vartheta_{i+t}(z_1+z_2)\vartheta_{j+t}(z_1-z_2)\Big).\Big(\sum_{t \in Z(\overline{2})} \chi(t)\vartheta_{k+t}(0)\vartheta_{l+t}(0)\Big) = \Big(\sum_{t \in Z(\overline{2})} \chi(t)\vartheta_{-i'+t}(z_2)\vartheta_{j'+t}(z_2)\Big).\Big(\sum_{t \in Z(\overline{2})} \chi(t)\vartheta_{k'+t}(z_1)\vartheta_{l'+t}(z_1)\Big).$$

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

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

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

Arithmetic with level two 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 coordinates
Doubling	$5M + 4S + 1m_0$	$3M + 6S + 3m_0$	$3M + 5S$
Mixed Addition			$7M + 6S + 1m_0$

Multiplication cost in genus 1 (one step).

Miller functions with theta coordinates

Proposition

- $$f_{n,P} = \frac{\vartheta \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix} \right] (z)}{\vartheta \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix} \right] (z + nz_P)} \left(\frac{\vartheta \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix} \right] (z + z_P)}{\vartheta \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix} \right] (z)} \right)^n .$$

- $$f_{n_1.P, n_2.P} = \frac{\vartheta(z + n_1.z_P)\vartheta(z + n_2.z_P)}{\vartheta(z)\vartheta(z + (n_1 + n_2).z_P)}.$$

Corollary

$$e_W(P, Q) = \frac{\vartheta(\ell z_P + z_Q)\vartheta(0)}{\vartheta(z_Q)\vartheta(\ell z_P)} \cdot \frac{\vartheta(z_P)\vartheta(\ell z_Q)}{\vartheta(z_P + \ell z_Q)\vartheta(0)}$$
$$= \exp(2\pi i \ell(z_{P,1} z_{Q,2} - z_{P,2} z_{Q,1}))$$

with $z_P = z_{P,1}\Omega + z_{P,2}$ and $z_Q = z_{Q,1}\Omega + z_{Q,2}$.

Fast pairing computation with theta functions of level 2

P and Q points of ℓ-torsion.

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

- $e_W(P,Q)^2 = \frac{\lambda_P^1 \lambda_Q^0}{\lambda_P^0 \lambda_Q^1}$.
- $e_T(P,Q)^2 = \frac{\lambda_P^1}{\lambda_P^0}$.

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 + denominator elimination	$1\mathbf{M} + 1\mathbf{S} + 3\mathbf{m}$	$1\mathbf{M} + 3\mathbf{m}$	$3\mathbf{M} + 4\mathbf{S} + 4\mathbf{m}$
	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 $\mathbb{F}_{q^d}$).

How to compute $P + Q$?

- Work in level 4, and go back to level 2 once we know $P + Q$.

$\Rightarrow$ Impose the 4-torsion on A to be rational
(In level 2: only impose the 2-torsion to be rational).

- Stay in level 2 and compute the symmetric pairing:

$$e_{T,s} = e_T(P,Q) + e_T(P,-Q).$$

- $\mathbb{Z}$-action on $k^{*,\pm 1}$:

$$x^{n_1+n_2} + \frac{1}{x^{n_1+n_2}} = \left(x^{n_1} + \frac{1}{x^{n_1}}\right) \cdot \left(x^{n_2} + \frac{1}{x^{n_2}}\right) - \left(x^{n_1-n_2} + \frac{1}{x^{n_1-n_2}}\right).$$

Computing $P \pm Q$

- The even theta null point are non zero $\Leftrightarrow$ the Kummer variety is projectively normal.
- Generically the case (but not for Jacobians of hyperelliptic curves of genus $g \geqslant 3$).
- We can then compute $\vartheta_i(P+Q)\vartheta_j(P-Q) + \vartheta_j(P+Q)\vartheta_i(P-Q)$.

$\Rightarrow$ Recover $P \pm Q$ with a square root.

$\Rightarrow$ Alternatively, compute $\ell P + Q$ in the algebra of degree 2

$$k[X]/\left((X - \vartheta_0(P+Q))(X - \vartheta_0(P-Q))\right).$$

Perspectives

- Degenerate divisors: should be even faster!
- Ate pairing, optimal ate?
- Miller algorithm directly on the theta coordinates.

Personal announcement

- I will defend my PhD Thesis "Theta functions and applications in cryptography", Wednesday 21 at 17h00, in C005 (Loria).
- Talk will be in French, but slides in English.

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. 2).

[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. 2).

[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. 8).

[Goy+06] V. Goyal et al. "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. 2).

[Jou04] A. Joux. "A one round protocol for tripartite Diffie–Hellman". In: *Journal of Cryptology* 17.4 (2004), pp. 263–276. (Cit. on p. 2).

[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. 8).

[SW05] A. Sahai and B. Waters. "Fuzzy identity-based encryption". In: *Advances in Cryptology–EUROCRYPT 2005* (2005), pp. 457–473. (Cit. on p. 2).

[Ver01] E. Verheul. "Self-blindable credential certificates from the Weil pairing". In: *Advances in Cryptology—ASIACRYPT 2001* (2001), pp. 533–551. (Cit. on p. 2).