CS548 Advanced Information Security

Efficient Algorithms for Pairing-Based Cryptosystems

Paulo S. L. M. Barreto, Hae Y. Kim, Ben Lynn, and Michael Scott

Proceedings of Crypto, 2002

2010. 04. 22.

Kanghoon Lee, AIPR Lab., KAIST

Contents

KAIST

Introduction

- Problems of Pairing-Based Cryptosystems
  - Expensive bilinear pairing computations (e.g. Weil or Tate pairing)

- Goals
  - To make entirely practical systems
  - Theoretical guarantees
  - Several efficient algorithms for the arithmetic operations

- Contributions of this paper
  - Definition of point tripling → *<u>Faster scalar multiplication in characteristic 3</u>*
  - Improved square root computation over F_{p^m} → *<u>Important for the point compression</u>*
  - A variant of Miller's algorithm → *<u>Efficient computation of Tate pairing</u>*

    (In characteristics 2 and 3, complexity reduction of Tate pairing is from $O(m^3)$ to $O(m^2)$)

KAIST

Mathematical Preliminaries (1)

- Finite Field, F_{p^m} : the field with p^m elements
  - p (prime number) : <u>*characteristic*</u> of F_{p^m}
  - m (positive integer) : <u>*extension degree*</u>
  - $F_q^* \equiv F_q - \{0\}$ (simply write F_q with $q=p^m$)

- Elliptic Curve $E(F_q)$
  - The set of solutions *(x, y)* over F_q to an equation of form
    $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ with additional *point at infinity*, *O*
  - There exists an abelian group law on *E*, $P_3 = P_1 + P_2$

- The number of points of $E(F_q)$, $n = \#E(F_q)$, called <u>*order*</u> of the curve over the field F_q
- The order of point *P* : the least nonzero integer *r* such that *rP=O*
- $E[r]$: the set of all points of order *r* in *E*
  - $E(K)[r]$: the set of all points of order r to the particular subgroup *E(K)*

Mathematical Preliminaries (2)

- *Security multiplier k*
  - If $r \mid q^k-1$ and r *does not divide* q^s-1 for any $0 < s < k$

- Some cryptographically interesting supersingular elliptic curves

curve equation	underlying field	curve order	k
$E_{1,b}: y^2 = x^3 + (1-b)x + b,\ b \in \{0,1\}$	$\mathbb{F}_p$	$p+1$	2
$E_{2,b}: y^2 + y = x^3 + x + b,\ b \in \{0,1\}$	$\mathbb{F}_{2^m}$	$2^m + 1 \pm 2^{(m+1)/2}$	4
$E_{3,b}: y^2 = x^3 - x + b,\ b \in \{-1,1\}$	$\mathbb{F}_{3^m}$	$3^m + 1 \pm 3^{(m+1)/2}$	6

- *Divisor* : a formal sum of points on the curve F_{p^m}
- *The degree of a divisor* $A = \sum_P a_P(P)$ is the sum $A = \sum_P a_P$

Mathematical Preliminaries (3)

- Tate Pairing
  - Let *l* be a natural number coprime to *q*
  - The *Tate pairing of order l* is the map $e_l : E(F_q)[l] \times E(F_{q^k})[l] \rightarrow F^*_{q^k}$ as $e_l(P,Q) = f_P(A_Q)^{(q^k-1)/l}$

- Tate pairing satisfies the following properties
  - (Bilinearity) $e_\ell(P_1 + P_2, Q) = e_\ell(P_1, Q) \cdot e_\ell(P_2, Q)$ and $e_\ell(P, Q_1 + Q_2) = e_\ell(P, Q_1) \cdot e_\ell(P, Q_2)$ for all $P, P_1, P_2 \in E(\mathbb{F}_q)[\ell]$ and all $Q, Q_1, Q_2 \in E(\mathbb{F}_{q^k})[\ell]$. It follows that $e_\ell(aP, Q) = e_\ell(P, aQ) = e_\ell(P, Q)^a$ for all $a \in \mathbb{Z}$.
  - (Non-degeneracy) If $e_\ell(P, Q) = 1$ for all $Q \in E(\mathbb{F}_{q^k})[\ell]$, then $P = O$. Alternatively, for each $P \neq O$ there exists $Q \in E(\mathbb{F}_{q^k})[\ell]$ such that $e_\ell(P, Q) \neq 1$.
  - (Compatibility) Let $\ell = h\ell'$. If $P \in E(\mathbb{F}_q)[\ell]$ and $Q \in E(\mathbb{F}_{q^k})[\ell']$, then $e_{\ell'}(hP, Q) = e_\ell(P, Q)^h$.

Scalar Multiplication in Characteristic 3 (1)

✓ Arithmetic on the curve $E_{3,b}$

- Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, $P_3 = (x_3, y_3)$
- By definition, $-O = O$, $-P_1 = (x_1, -y_1)$, $O + P_1 = P_1 + O = P_1$
- Furthermore,

$$
\begin{aligned}
&P_1 = -P_2 && \Rightarrow P_3 = O. \\
&P_1 = \quad P_2 && \Rightarrow \lambda \equiv 1/y_1,\ x_3 = x_1 + \lambda^2,\ y_3 = -(y_1 + \lambda^3). \\
&P_1 \neq -P_2,\ P_2 && \Rightarrow \lambda \equiv \frac{y_2 - y_1}{x_2 - x_1},\ x_3 = \lambda^2 - (x_1 + x_2),\ y_3 = y_1 + y_2 - \lambda^3.
\end{aligned}
$$

✓ Double-and-add method : $V = kP,\ k \in Z$, $k = (k_t \dots k_1\, k_0)_2$ where $k_i \in \{0,1\}$

Double-and-add scalar multiplication:

set $V \leftarrow P$
for $i \leftarrow t-1, t-2, \dots, 1, 0$ do {
  set $V \leftarrow 2V$
  if $k_i = 1$ then set $V \leftarrow V + P$
}
return V

Scalar Multiplication in Characteristic 3 (2)

- Point Tripling for $E_{3,b}$
  - $P = (x, y)$
  - $3P = (x_3, y_3)$ with the folumas,

$$x_3 = (x^3)^3 - b$$
$$y_3 = -(y^3)^3$$

- Triple-and-add method : $V = kP,\ k \in Z$, k = $(k_t \ldots k_1\ k_0)_3$ where $k_i \in \{-1, 0, 1\}$

Triple-and-add scalar multiplication:

set $V \leftarrow P$ if $k_t = 1$, or $V \leftarrow -P$ if $k_t = -1$
for $i \leftarrow t-1, t-2, \ldots, 1, 0$ do {
    set $V \leftarrow 3V$
    if $k_i = 1$ then set $V \leftarrow V + P$
    if $k_i = -1$ then set $V \leftarrow V - P$
}
return V

KAIST

Square Root Extraction

- ✓ Elliptic curve equation $E : y^2 = f(x)$ over F_q
- ✓ In a finite field F_{p^m} where $p \equiv 3 \pmod 4$ and odd *m*, the best algorithm to compute a square root → $O(m^3)$
- ✓ A solution of $x^2 = a$, is given by $x = a^{(p^m+1)/4}$
  - If *m = 2k+1* for some *k* , $$\frac{p^m+1}{4} = \frac{p+1}{4}\left[p(p-1)\sum_{i=0}^{k-1}(p^2)^i + 1\right],$$

    so that $$a^{(p^m+1)/4} = [(a^{\sum_{i=0}^{k-1}(p^2)^i})^{p(p-1)} \cdot a]^{(p+1)/4}.$$
- ✓ $a^{\sum_{i=0}^{k-1} u^i}$ where $u = p^2$ can be verified by induction

$$a^{1+u+\cdots+u^{k-1}} = \begin{cases} (a^{1+u+\cdots+u^{\lfloor k/2 \rfloor-1}}) \cdot (a^{1+u+\cdots+u^{\lfloor k/2 \rfloor-1}})^{u^{\lfloor k/2 \rfloor}}, & k \text{ even}, \\ ((a^{1+u+\cdots+u^{\lfloor k/2 \rfloor-1}}) \cdot (a^{1+u+\cdots+u^{\lfloor k/2 \rfloor-1}})^{u^{\lfloor k/2 \rfloor}})^u \cdot a, & k \text{ odd}. \end{cases}$$

- ✓ $O(m^2 \log m)$ F_p operations

KAIST

Computing the Tate Pairing

- Tate Pairing, $e_l : E(F_q)[l] \times E(F_{q^k})[l] \rightarrow F_{q^k}^*$
  - Let $P \in E(F_q)[l]$, $Q \in E(F_{q^k})[l]$
  - $e_l(P,Q) = f_P(A_Q)^{(q^k-1)/l}$
- To find the function f_P and then evaluate its value at A_Q
- Miller's Formula [1, Theorem 2]

Theorem 2 (Miller's formula). *Let P be a point on $E(\mathbb{F}_q)$ and f_c be a function with divisor $(f_c) = c(P) - (cP) - (c-1)(O)$, $c \in \mathbb{Z}$. For all $a, b \in \mathbb{Z}$, $f_{a+b}(Q) = f_a(Q) \cdot f_b(Q) \cdot g_{aP,bP}(Q)/g_{(a+b)P}(Q)$.*

where

$$(g_{aP,bP}) = (aP) + (bP) - (-(a+b)P) - 3(O),$$

$$(g_{(a+b)P}) = ((a+b)P) + (-(a+b)P) - 2(O).$$

Miller's Algorithm

- **Miller's algorithm:**

$$
\begin{aligned}
&\text{set } f \leftarrow 1 \text{ and } V \leftarrow P \\
&\text{for } i \leftarrow t-1, t-2, \ldots, 1, 0 \text{ do } \{ \\
&\quad \text{set } f \leftarrow f^2 \cdot g_{V,V}(Q)/g_{2V}(Q) \text{ and } V \leftarrow 2V \\
&\quad \text{if } \ell_i = 1 \text{ then set } f \leftarrow f \cdot g_{V,P}(Q)/g_{V+P}(Q) \text{ and } V \leftarrow V + P \\
&\} \\
&\text{return } f
\end{aligned}
$$

- Example Computation of the Tate Pairing [2, Appendix B]
  - $p = 43$, $k = 2$, $l = 11$
  - Supersingular elliptic curve $E : y^2 = x^3 + x$, order = 44
  - Distortion map $\phi(x, y) = (-x, iy)$
  - $P = (23,8)$, $Q=(20,8t)$
  - Using the Miller's algorithm,
    $t([2]P, Q)^{(p^2+1)/l} = (40t+28)^{168} = 23t + 26$, $t(P, Q)^{(p^2+1)/l} = (13t+38)^{168} = 3t + 11$
  - We know that $t([2]P, Q) = t(P, Q)^2$

Improvement of Miller's Algorithm (1)

✓ Irrelevant denominators

- When computing $e_n(P,\phi(Q))$ and ϕ is a distortion map,
  the g_{2V} and g_{V+P} denominators in Miller's algorithm can be discarded
- Distorsion maps

curve (see table 1)	underlying field	distortion map	conditions
$E_{1,0}$	$\mathbb{F}_p,\ p>3$	$\phi_1(x,y)=(-x,iy)$	$i\in\mathbb{F}_{p^2}$, $i^2=-1$
$E_{2,b},\ b\in\{0,1\}$	$\mathbb{F}_{2^m}$	$\phi_2(x,y)=(x+s^2,y+sx+t)$	$s,t\in\mathbb{F}_{2^{4m}}$, $s^4+s=0$, $t^2+t+s^6+s^2=0$
$E_{3,b},\ b\in\{-1,1\}$	$\mathbb{F}_{3^m}$	$\phi_3(x,y)=(-x+r_b,iy)$	$r_b,i\in\mathbb{F}_{3^{6m}}$, $r_b^3-r_b-b=0$, $i^2=-1$

✓ Evaluation of f_n with more efficient ***triple-and-add*** method in characteristic 3

- $(f_{3a})=(f_a)+(g_{aP,aP})+(g_{2aP,aP})-(g_{2aP})-(g_{3aP})$
- With discarding the irrelevant denominators

$$f_{3b}(Q)=f_b^3(Q)\cdot g_{aP,aP}(Q)\cdot g_{2aP,aP}(Q)$$

KAIST

Improvement of Miller's Algorithm (2)

- Speeding up the Final Powering
  - Evaluation of the Tate pairing $e_n(P,Q)$ includes a final raising to the power of $(p^{km}-1)/n$
  - Exponent part → similar way to the square root algorithm

- Fixed-base Pairing Precomputation
  - When computing $e_n(P,Q)$, P is either fixed (e.g. base point on the curve) or used repeatedly (e.g. public key)
  - Precompute $e_n(P,Q)$

KAIST

Experimental Results

- ✓ Timings for Boneh-Lynn-Shacham (BLS) verification and Boneh-Franklin identity-based encryption (IBE) (ms)

operation	original [3, 14]	ours
BLS verification	2900	53
IBE encryption	170	48 (preprocessed: 36)
IBE decryption	140	30 (preprocessed: 19)

- ✓ Future works
  - Apply to more general algebraic curves, e.g., a fast *n*-th root algorithm

KAIST

References

[1] Paulo S. L. M. Barreto, Hae Y. Kim, Ben Lynn, and Michael Scott, Efficient Algorithms for Pairing-Based Cryptosystems, Proceedings of Crypto, 2002

[2] Marcus Stogbauer, Efficient Algorithms for Pairing-Based Cryptosystems, Diploma Thesis, Darmastay University of Technology, 2004