Pre-Computation Scheme of Window τNAF for Koblitz Curves Revisited

Wei Yu, Guangwu Xu

Institute of Information Engineering, Chinese Academy of Sciences
yuwei_1_yw@163.com

Eurocrypt 2021

Abstract

- Introduction

Abstract

- Introduction
- Frobenius Map τ

Abstract

- Introduction
- Frobenius Map τ
- The Complex Conjugate of τ

Abstract

- Introduction
- Frobenius Map τ
- The Complex Conjugate of τ
- Novel Pre-Computation

Abstract

- Introduction
- Frobenius Map τ
- The Complex Conjugate of τ
- Novel Pre-Computation
- Scalar Multiplication

Introduction:NIST Standard

NIST recommends 4 Koblitz curves

1. NIST FIPS 186-5(draft): digital signature standard (October of 2019)
2. NIST SP 800-56A: pair-wise key-establishment schemes (April of 2018)
3. NIST SP 800-57: key management (May of 2020)

Elliptic curve over $\mathbb{F}_2$:

$$y^2 + xy = x^3 + ax^2 + 1 \text{ with } a \in \mathbb{F}_2$$

$\mathbb{F}_{2^m}$-rational points: $\{(x,y)|y^2 + xy = x^3 + ax^2 + 1, x, y \in \mathbb{F}_{2^m}\} \cup \infty$
$E_a(\mathbb{F}_2)$ is a subgroup of $E_a(\mathbb{F}_{2^m})$
$|E_a(\mathbb{F}_{2^m})| = |E_a(\mathbb{F}_2)| \cdot p$.

The Weil Conjecture

Table: The value of m makes p a prime($m < 2000$)

$a=0$	233	239	277	283	349
	409	571	1249	1913	
$a=1$	163	283	311	331	347
	359	701	1153	1597	1621

Introduction:Scalar Multiplication

Scalar multiplication $Q = nP$

$$n = \sum_{i=1}^{l} c_i 2^{b_i}, \; c_i \in \mathscr{C} = \{\pm 1\}, \; b_l > b_{l-1} > \ldots > b_1 \geq 0$$

Horner's algorithm:

$$nP = \sum_{i=1}^{l} c_i 2^{b_i} P$$

Introduction:Scalar Multiplication

$$
\begin{aligned}
31 &= \lfloor \Pi \times 10 \rfloor \\
31 &= 2^4 + 2^3 + 2^2 + 2^1 + 1 \\
&= 2^5 - 1 \\
31P &= 2^4P + 2^3P + 2^2P + 2^1P + P \\
31P &= 2(2(2(2P + P) + P) + P) + P
\end{aligned}
$$

Introduction:Scalar Multiplication

Frobenius(Koblitz,Solinas)

$$n = \sum_{i=0}^{l-1} \epsilon_i u_i \tau^i, \epsilon_i \in \{0,1\}$$

Double base number system for multi-scalar multiplications
EUROCRYPT 2009

↓

On the optimal pre-computation of window τNAF for Koblitz curves
IEEE Transactions on Computers 2016

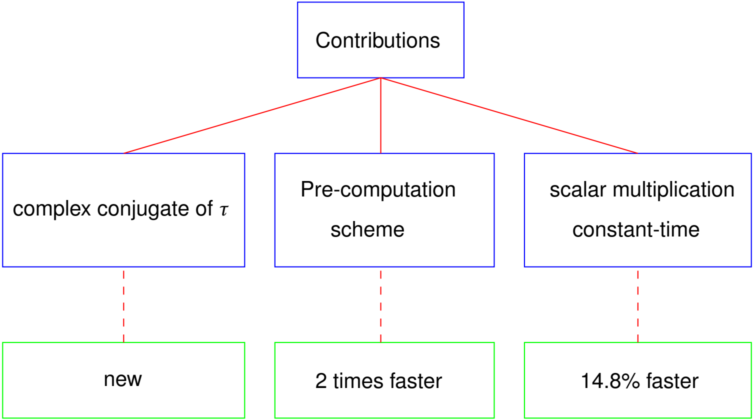
↓

Twisted μ_4-Normal Form for Elliptic Curves
EUROCRYPT 2017

↓

Pre-Computation Scheme of Window τNAF for Koblitz Curves Revisited
EUROCRYPT 2021

Introduction:Contributions



Frobenius map τ

The Frobenius map τ is an endomorphism of $E_a(\mathbb{F}_{2^m})$

$$\tau(x,y) = (x^2, y^2)$$

For each point P in $E_a(\mathbb{F}_{2^m})$,

$$\tau^2(P) + 2P = \mu\tau(P), \mu = (-1)^{1-a}$$

Frobenius map τ

M

1. the main subgroup of $E_a(F_{2^m})$
2. order p
3. $\delta(P) = \mathcal{O}$ for every $P \in M$, $\delta = \frac{\tau^m - 1}{\tau - 1}$
4. $\rho \equiv n \pmod{\delta}, \rho \in \mathbb{Z}[\tau] \Rightarrow \rho P = nP$

Frobenius map τ

Window τNAF

1. Reduction: $\rho \in \mathbb{Z}[\tau]$ satisfying $\rho \equiv n \pmod{\delta}$
2. Window τNAF with width w:

$$\rho = \sum_{i=0}^{l-1} \epsilon_i u_i \tau^i, \epsilon_i \in \{-1, 1\}$$

   $\{u_k, u_{k+1}, \ldots, u_{k+w-1}\}$ contains at most one nonzero element
3. Pre-computation: Compute $Q_i = c_i P$ for each $i \in I_w$
4. Computing nP: Employ Horner's algorithm to calculate nP

The Complex Conjugate of τ

Avanzi, Dimitrov, Doche, and Sica and Doche, Kohel, and Sica used complex multiplication $\bar{\tau}P$ in double-base representation. Our $\mu\bar{\tau}P$ 2**M**$+2$**S** μ_4-Koblitz curve

$$\mu\bar{\tau}P = \left((X_0+X_2)^2 : (X_0X_3+X_1X_2) : (X_1+X_3)^2 : (X_0X_1+X_2X_3)\right)$$

Table: Costs of point operations on Koblitz curves

Coordinates	$\tau(P)$	τ-affine operation	addition	mixed addition
LD coordinates	3**S**	2**S**	13**M**$+4$**S**	8**M**$+5$**S**
λ-coordinates	3**S**	2**S**	11**M**$+2$**S**	8**M**$+2$**S**
μ_4-Koblitz curve ($a=0$)	4**S**	3**S**	7**M**$+2$**S**	6**M**$+2$**S**
μ_4-Koblitz curve ($a=1$)	4**S**	3**S**	8**M**$+2$**S**	7**M**$+2$**S**

Novel Pre-Computation

- $R_i = \{g + h\tau | g + h\tau \equiv i \pmod{\tau^w}, N(g + h\tau) < 2^w\}$
- $I_w = \{1, 3, \cdots, 2^{w-1} - 1\}$
- $C = \{c_i | c_i \in R_i,\ i \in I_w\},\ c_1 = 1$

pre-computation: $Q_i = c_i P$ with $c_i \in C$ for all $i \in I_w$.

Table: Novel pre-computation for width 4

	c_i		Q_i	$a = 0/a = 1$
				6**M**+6**S**
$w = 4$	$c_5 = -1 + \mu\tau$	$c_5 = -\mu\bar{\tau}$	$Q_5 = -\mu\bar{\tau}P$	2**M**+2**S**
	$c_7 = 1 + \mu\tau$	$c_7 = \mu\bar{\tau}c_5$	$Q_7 = -(\mu\bar{\tau})^2 P$	2**M**+2**S**
	$c_3 = -3 + \mu\tau$	$c_3 = -\mu\bar{\tau}c_7$	$Q_3 = (\mu\bar{\tau})^3 P$	2**M**+2**S**

Novel Pre-Computation

Table: Cost of pre-computations on a μ_4-Koblitz curve

		$w=4$	$w=5$	$w=6$
$a=0$	Solinas	$15\mathbf{M}+15\mathbf{S}$	$38\mathbf{M}+38\mathbf{S}$	-
	Hankerson,Menezes,Vanstone	$15\mathbf{M}+15\mathbf{S}$	$40\mathbf{M}+35\mathbf{S}$	$89\mathbf{M}+67\mathbf{S}$
	Trost, Xu	$15\mathbf{M}+12\mathbf{S}$	$39\mathbf{M}+20\mathbf{S}$	$87\mathbf{M}+36\mathbf{S}$
	Ours	$6\mathbf{M}+6\mathbf{S}$	$18\mathbf{M}+17\mathbf{S}$	$44\mathbf{M}+32\mathbf{S}$
$a=1$	Solinas	$18\mathbf{M}+15\mathbf{S}$	$45\mathbf{M}+38\mathbf{S}$	-
	Hankerson,Menezes,Vanstone	$18\mathbf{M}+15\mathbf{S}$	$47\mathbf{M}+35\mathbf{S}$	$104\mathbf{M}+67\mathbf{S}$
	Trost, Xu	$18\mathbf{M}+12\mathbf{S}$	$46\mathbf{M}+20\mathbf{S}$	$102\mathbf{M}+36\mathbf{S}$
	Ours	$6\mathbf{M}+6\mathbf{S}$	$19\mathbf{M}+17\mathbf{S}$	$47\mathbf{M}+32\mathbf{S}$

Two times faster, compared to the state-of-the-art

Scalar Multiplication

Table: Time cost of scalar multiplications using μ_4-Koblitz curves in μs

		K1-163(w)	K-233(w)	K-283(w)	K-409(w)	K-571(w)
	τNAF	70.42	98.6	171.9	384.2	424.6
	Trost, Xu	48.9(5)	70.23(5)	114.9(5)	225(6)	268.4(6)
	Ours	44.75(6)	64.05(6)	104.3(6)	207.4(7)	243.3(7)
constant-time	regular τNAF	173.7	265.6	432.4	860.1	1038.5
	Trost, Xu	63.95(6)	88.7(6)	143.6(6)	283.6(6)	336.2(6,M)
	Ours	54.77(6)	78.67(7)	126.2(7)	248.8(7)	294.7(7)

Scalar Multiplication

Technique

1. novel pre-computation scheme
2. bigger window width

Result

1. 33.5%: LD coordinates
2. 28.6%: λ-coordinates
3. 14.8%: μ_4-Koblitz curve

Conclusion

1. Our pre-computation scheme is about two times faster based on $\mu\bar{\tau}$-operations.
2. Increase the width for window τNAF to 7 for a better scalar multiplication.
3. Our results push the scalar multiplication of Koblitz curves, a very well-studied and long-standing research area, to a significant new stage.

Any questions please send email to:`yuwei_1_yw@163.com`
Thanks for your time!