Improved algorithms for an efficient arithmetic on some categories of elliptic curves

Mustapha Hedabou

Department Computer Science,
ENSA de Safi,
University of Marrakech, Morocco
E-mail: mhedabou@gmail.com

Abstract: The Frobenius endomorphism τ is known to be useful for an efficient scalar multiplication on elliptic curves $E(\mathbb{F}_{q^m})$ defined either over fields with small characteristics or over optimal extension fields. In this paper, we will present two techniques that aim to enhance the Frobenius-based methods for computing the scalar multiplication on these curves. The first method, called the generalised τ-adic method, is dedicated to improve the efficiency of the generalised τ-adic method when the elliptic curves are defined over fields of small characteristics. The generalised τ-adic with even digits improves substantially the computation time and the number of stored points whereas the generalised τ-adic with odd digits reduces only the number of stored points but it offers better resistance against the SPA attacks. The generalised τ-adic method is particularly efficient when the trace of the used curve is small. The second method allows to reduce by about 50% the number of the stored points by the Frobenius-based algorithm on elliptic curve defined over optimal extension fields. Finally, we show that there are a lot of curves which are well suited for cryptography, and for which the proposed methods can be applied.

Keywords: elliptic curve; scalar multiplication; Frobenius map; normal basis; τ-adic expansion; precomputed table.

Reference to this paper should be made as follows: Hedabou, M. (2016) 'Improved algorithms for an efficient arithmetic on some categories of elliptic curves', *Int. J. Computational Complexity and Intelligent Algorithms*, Vol. 1, No. 1, pp.54–67.

Biographical notes: Mustapha Hedabou received his MSc in Mathematics from the University of Paul Sabatier, Toulouse, France. In 2006, he received his PhD in Computer Science from INSA de Toulouse, France. He is currently an Associate Professor at ENSA de Safi, University of Marrakech in Morroco. His area interest covers information security, public key cryptography based on elliptic curves and identity-based cryptography.

1 Introduction

Since they provide the same level of security as other systems for keys with shorter length, elliptic curve cryptosystems (ECC) are of great interest for cryptographic applications on devices with small resources such as smart cards. The dominant operation in the process of the implementation of an ECC is the computation of the scalar multiplication kP, where k is a positive integer and P is a point of the elliptic curve.

One of the important techniques for improving the computation of the scalar multiplication on the categories of elliptic defined over field $\mathbb{F}_{q^m}$, where q is a power of prime integer, is the use of the Frobenius map. The first Frobenius-based method for computing the scalar multiplication on elliptic curves was proposed by Koblitz (1991) for $q = 2$. Müller (1998), Smart (1997) and others (Aranha et al., 2012; Roy et al., 2011) have extended this technique for q which is a small power of two respectively of prime integer.

Under reasonable assumptions, each integer $k \in \mathbb{F}_{q^m}$ can be expressed as

$$k = \sum_{i=0}^{i=m-1} k_i \tau^i,$$

where $k_i \in [-q, q]$. To perform the scalar multiplication on the categories of elliptic defined over fields of small characteristic, the Frobenius-based algorithms store the points $P_i = k_i P$ for $= 1, \cdots, q$ and compute the scalar multiplication kP in the same way as the classical width-w method (Blake et al., 1999). When q is a prime integer close to the word size of the processor, Sarkar et al. (2004) and Chung et al. (2007) have proposed a new method for computing the scalar multiplication based on the use of the Frobenius map and a new look-up table. In this paper we propose to enhance the efficiency of these methods.

Our first approach aims to improve the efficiency of the generalised τ-adic method on the elliptic curves defined over fields of small characteristic by reducing the computation time and the size of the required precomputed table. For this purpose, we modify the τ-adic representation of the secret scalar k by eliminating all its odd digits. This method offers better performances than the original generalised τ-adic method but it is particularly efficient when the trace t of the underlying curve is small. The use of a new τ-adic expansion of the scalar that contains only odd digits allows also to improve the performances of the generalised τ-adic method even if it is less efficient than the previous one. On the other hand, the second method offers better resistance against the SPA attacks Kocher et al. (1999) since the scalar representation does not contain any zero digits. Although the SPA attacks are out of this paper interest, we will introduce the generalised τ-adic based on the use of the expansion that contains only odd digits.

In Kobayashi et al. (1999), the authors have proposed a scalar multiplication method combining the Frobenius map and a special precomputed table for elliptic curves defined over optimal extension fields ($q = p^n$, where $p > 2$ is a prime number). Sarkar et al. (2004), have introduced a new method that exploit the speed up arisen from the efficient arithmetic given by the special OEF fields. In this paper, we propose to modify the τ-adic representation of k in order to get only an odd digits k_i. The binary representation of each odd digit k_i will be modified by following the scheme introduced by Hedabou

et al. (2005). Our algorithm allows to halve the number of points stored by the method of Sarkar et al. (2004).

For security requirement, it is necessary to mention that all the considered curves are defined over composite or optimal extension fields, which means that they may be vulnerable to the attacks based on the Weil descent, especially to the GHS attack (Gaudry et al., 2002). To deal with this threat, we will identify the curves that may succumb to these attacks and show that we can find a lot of such curves that are suited for use in cryptography.

The paper is organised as follows: Section 2 recalls some properties of the Frobenius map in the setting of ECC and describes the Frobenius-based methods for computing the scalar multiplication. In Section 3, we introduce our proposed techniques for improving the efficiency of the Frobenius-based scalar multiplication methods. The security of the considered curves will be discussed in Section 4. Finally we conclude in Section 5.

2 Preliminaries

Let $E(\mathbb{F}_q)$ an elliptic curve defined over a finite field $\mathbb{F}_q$. We define the q-th power Frobenius (Menezes, 1992) map τ on $E(\mathbb{F}_q)$ as follows

$$\tau : (x, y) \mapsto (x^q, y^q).$$

The following properties are equivalent:

1 $\#E(\mathbb{F}_q) = q + 1 - t$

2 the trace of τ is t

3 $\tau^2 - t\tau + q = 0$.

Koblitz (1991) showed that the use of the Frobenius map τ can speed up the multiplication of a point P by a scalar k on certain categories of elliptic curves defined over fields with a characteristic $q = 2$ (Koblitz curves) by introducing the τ-adic method. Müller (1998) has generalised the τ-adic method for elliptic curves defined over fields $\mathbb{F}_{q^m}$ with $q = 2^n$, by showing the following theorem.

Theorem 2.1: Let $q \geq 4$ and let $k \in \mathbb{Z}[\tau]$. If we set $s = \lceil 2log_q||k|| \rceil + 3$, then there exist a rational integer $k_i \in \{-q/2, \cdots, q/2\}$, $0 \leq i \leq s$, such that

$$k = \sum_{i=0}^{s} k_i \tau^i$$

where $||k|| := \sqrt{k\overline{k}}$ and $\overline{k}$ is the conjugate of k and $\lceil x \rceil$ is the minimum integer greater than or equal to x.

For the special cases $q = 8, 32$ and 16, Müller has showed that we can write

$$k = \sum_{i=0}^{m-1} k_i \tau^i,$$

where $k_i \in \{-q/2 \cdots, q/2\}$ and $m = \lceil log_q(k) \rceil$.

The computation of the scalar multiplication kP on these curves is done as follows (Müller, 1998):

Algorithm 1 Generalised τ-adic method

Input : an integer k, and a point $P \in E(\mathbb{F}_{q^m})$.
Output : kP.
1. *Computation of the* τ*-adic expansion:* $k = \sum_{i=0}^{m-1} k_i \tau^i$, *with* $k_i \in \{-q/2, \cdots, q/2\}$.
2. **Precomputation**. *Compute and store the points* $P_i = iP$, *for* $i = 0, \cdots, q/2$.
3. **Left-to-right point multiplication**
   3.1 $Q \leftarrow P_{k_{m-1}}$.
   3.2 *for* $i = m-1$ *down to* 0 *do*
   3.2.1 *if* $k_i \geq 0$ *then* $Q \leftarrow \tau(Q) + P_{k_i}$.
   3.2.2 *else* $Q \leftarrow \tau(Q) - P_{|k_i|}$.
4. *Return* Q.

In Kobayashi et al. (1999), the authors have noticed that the proof of Theorem 2.1 does not assume that q is a small power of two. By using the following equations

$$\tau^m = \mathbf{1} \text{ in } End_E,$$
$$\sum_{i=0}^{i=m-1} \tau^i(P) = 0 \text{ for all } P \in E(\mathbb{F}_{q^m}) \setminus E(\mathbb{F}_q),$$

they have shown that we can write

$$k = \sum_{i=0}^{m-1} k_i \tau^i, \text{ where } k_i \in \{-q \cdots, q\}.$$

For the choice of q satisfying the following properties :

- q is prime close to the word size of the processor
- $q = 2^s \pm c$, where $log_2(c) \leq s/2$
- an irreducible binomial $f(x) = x^m - w$ exist, consequently, they have presented an efficient algorithm for the evaluation of the Frobenius map when the elements of the field are represented with a polynomial basis.

To compute the scalar multiplication kP for such q, they have also proposed a new scalar multiplication method over $\mathbb{F}_{q^m}$, where q is close to word size of the processor ($2^{16}, 2^{32}$ or 2^{64}). The scalar k is expressed as $k = \sum_{i=0}^{i=m-1} k_i \tau^i$, where $k_i \in [-q, q]$, and each k_i is represented by its signed binary representation : $k_i = \sum_{j=0}^{A} k_{i,j} 2^j$, where $k_{i,j} \in \{-1, 0, 1\}$. The scalar k can be then represented by a matrix with m rows and A columns, and the algorithm will processes k columnwise. The expression of kP can be written as

$$\begin{aligned} kP = &(k_{0,0} + k_{0,1}2 + \cdots + k_{0,A}2^A)P \\ &+ (k_{1,0} + k_{1,1}2 + \cdots + k_{1,A}2^A)\tau(P) \\ &\vdots \\ &+ (k_{m-1,0} + k_{m-1,1}2 + \cdots + k_{m-1,A}2^A)\tau^{m-1}(P), \end{aligned}$$

and the computation of kP is done as follows:

Algorithm 2 Method of Kobayashi et al.

Input : a τ-adic representation $(k_{m-1}, \cdots, k_0)$ integer k, and a point $P \in E(\mathbb{F}_{p^m})$.
Output : kP.
1. For $0 \leq i \leq m-1$ and $0 \leq j \leq A$ compute $k_{i,j}$.
2. Compute $P_i \leftarrow \tau^i(P)$.
3. $Q \leftarrow \mathcal{O}$, $j \leftarrow A+1$.
4. $Q \leftarrow 2Q$.
5. While $j \geq 0$, if $k_{i,j} = 1$ then $Q \leftarrow Q + P_i$.
6. $j \leftarrow j - 1$.
7. Return Q.

3 The proposed methods

In this section, we will introduce our proposed techniques for improving the efficiency the Frobenius-based methods on elliptic curves defined over fields of a small characteristic and over optimal extension fields. From the previous sections, it is clear that in general cases, the scalar k can be expressed as: $k = \sum_{i=0}^{i=m-1} k_i \tau^i$, where $k_i \in [-q, q]$. In the following, we will use this general τ-adic representation of the scalar, but for special cases, we will rather consider the improved one:

$$k = \sum_{i=0}^{i=m-1} k_i \tau^i,$$

where $k_i \in \{-q/2, \cdots, q/2\}$.

To enhance the efficiency of the generalised τ-adic method, we will use two new expansions of the secret scalar k. The first expansion contains only the even digits and the second one only the odd digits. The generalised τ-adic method combined with the first expansion allows to reduce both the size of the precomputed table and the running time, while when it is combined with the second one it allows to reduce only the size of the precomputed table. We call these methods the generalised τ-adic method with even digits respectively with odd digits.

3.1 *The generalised τ-adic method for the curves $E(\mathbb{F}_{q^m})$, where q is a small power of 2*

Our main idea, is to change the τ-adic representation of the secret scalar k. Let $(k_{m-1}, \cdots, k_0)$ be the τ-adic representation, i.e., $k = \sum_{i=0}^{i=m-1} k_i \tau^i$, where $k_i \in [-q, q]$, and let $\tau^2 - t\tau + q = 0$ be the characteristic equation of the Frobenius map. Finally, let us assume that q is a small power of two, the trace t is then an odd integer (Müller, 1998).

3.1.1 The generalised τ-adic method with even digits

Our algorithm proposes to eliminate all the odd digits k_i from the τ-adic representation of k. We will proceed as follows: first let us assume that the least significant digit k_0 of the τ-adic representation of k is an even integer. When we meet the first odd digit k_i then we set

$$\begin{cases} k_i \leftarrow k_i + \text{sign}(k_{i-1})t \\ k_{i+1} \leftarrow k_{i+1} - \text{sign}(k_{i-1}) \\ k_{i-1} \leftarrow k_{i-1} - \text{sign}(k_{i-1})q \end{cases}$$

Since the trace t of the curve is an odd integer, it is clear that the new obtained digit k_i by this process is an even integer.

Remark 3.1: If we denote k'_{i-1}, k'_i, k'_{i+1} the obtained digits, then we have

$$\begin{aligned} & k'_{i-1}\tau^{i-1} + k'_i\tau^i + k'_{i+1}\tau^{i+1} \\ &= (k_{i-1} - sign(k_{i-1})q)\tau^{i-1} + (k_i + sign(k_{i-1})t)\tau^i \\ &\quad + \ (k_{i+1} - sign(k_{i-1}))\tau^{i+1} \\ &= k_{i-1}\tau^{i-1} + k_i\tau^i + k_{i+1}\tau^{i+1} - sign(k_{i-1})\tau^{i-1}(\tau^2 - t\tau + q) \\ &= k_{i-1}\tau^{i-1} + k_i\tau^i + k_{i+1}\tau^{i+1} - 0 \\ &= k_{i-1}\tau^{i-1} + k_i\tau^i + k_{i+1}\tau^{i+1}. \end{aligned}$$

Thus, we can conclude that this process does not change the value of k.

In order to eliminate all odd digits, we continue this process until we touch the digit k_{m-2}. If the obtained k_{m-1} is an even digit then we are sure that all obtained digits are even. In the other case we modify the digit k_{m-1} by the doing the described process above. The new digit k_{m-1} is an even integer, but the new τ-adic representation will contain an additional digit k_m which may be 1 or -1 depending on the sign of the new digit k_{m-2}. Since we are looking for a new representation with only even digits, we propose to use the following process to deal with this problem.

As explained before, for every point P of the curve $E(\mathbb{F}_{q^m})$ the Frobenius map satisfies $\tau^m(P) = P$. Thus, the digit k_m can be removed from the new τ-adic representation of k, and compensate this operation by performing a more adding or subtraction by the point P.

The first digit k_0 is assumed to be an even integer, which mean that we have either set $k \leftarrow k + 1$ or $k \leftarrow k - 1$ depending on the original value of k_0 (the even value of k_0 must be in $[-q, q]$). To summarise, in order to get the new τ-adic representation of k with only odd digits, we have either set $k \leftarrow k + 1$ or $k \leftarrow k - 1$ and removed the value of k_m, which is 1 or -1, from the new representation of k. To recover the correct value of the scalar multiplication kP, we have possibly to add or subtract P or $2P$ to the point output by the generalised τ-adic method combined with this new τ-adic representation of k. For example if we have set $k \leftarrow k + 1$ and the value of the removed digit k_m is -1 we have to subtract $2P$. On the other hand the point output is the correct value of the scalar multiplication kP if we have set $k \leftarrow k - 1$ and the value of the removed k_m is -1, etc.

Finally, this process outputs a new representation $(k'_m, \cdots, k_0)$, where each $k'_i \in [-q-|t|-1, q+|t|+1]$ is an even integer. To compute the scalar multiplication kP, we will use an intermediate element k' of $\mathbb{Z}[\tau]$. Let k' be the element of $\mathbb{Z}[\tau]$ represented by the new τ-adic expansion that contains only even digits $(k'_{m-1}, \cdots, k'_0)$, i.e., $k' = \sum_{i=0}^{i=m-1} k'_i \tau^i$. It is clear that we have $k = k' + k'_m - (k'_0 - k_0)$. Thus, to compute kP, we will first compute $Q = k'P$ and recover the kP by performing the operation $Q - (k'_0 - k_0 - k'_m)P$.

The following algorithm implements in detail the computation of the scalar multiplication kP by the generalised τ-adic method with even digits.

Algorithm 3 Generalised τ-adic method with even digits

Input : the τ-adic expansion $(k_{m-1}, \cdots, k_0)$ of an integer k, and a point $P \in E(\mathbb{F}_{q^m})$.
Output : kP.

I. **Generation of the τ-adic expansion with even digits**

1. If k_0 is an odd integer and $-q \leq k_0 - 1 \leq q$ set $k'_0 \leftarrow k_0 - 1$ else set $k'_0 \leftarrow k_0 + 1$.
2. for $i = 1$ to $m - 2$
2.1 if k_i is an odd integer set $k'_i \leftarrow k_i + sign(k'_{i-1})t, k'_{i+1} \leftarrow k_{i+1} - sign(k'_{i-1})$, $k'_{i-1} \leftarrow k'_{i-1} - sign(k'_{i-1})q$.
3. If k'_{m-1} is an odd integer set $k'_{m-1} \leftarrow k'_{m-1} + sign(k'_{m-2})t, k'_m \leftarrow -sign(k'_{m-2})$, $k'_{m-2} \leftarrow k'_{m-2} - sign(k'_{m-2})q$.
4. Let k' be the element of $\mathbb{Z}[\tau]$ represented by the new τ-adic expansion that contains only even digits $(k'_{m-1}, \cdots, k'_0)$, i.e., $k' = \sum_{i=0}^{i=m-1} k'_i \tau^i$.

II. **Computation of the scalar multiplication $k'P$**

1. Precomputation. Compute and store the points $P_i = iP$, for $i = 2, \cdots, q + |t| + 1$.
2. Use the step 3 of Algorithm 1 to compute $Q = k'P$.
3. Return $Q - (k'_0 - k_0 - k'_m)P$.

Now, we will evaluate the efficiency of our proposed algorithm in term of computation time and the size of the used space memory. As explained before the generalised τ-adic method stores in the precomputed table q points. The new τ-adic expansion of the scalar k contains only even digits k_i where $k_i \in [-q-|t|-1, q+|t|+1]$, hence the generalised τ-adic method with even digits will require the storage of $\frac{q+|t|+1}{2}$ points. Since the trace t of the curve satisfies $|t| \leq 2\sqrt{q}$ [Hasse theorem (Blake et al., 1999)] and q is a small power of two, then we have $\frac{q+|t|+1}{2} \leq q$ for $q \geq 8$. Thus in average, the number of stored points is reduced by $q - \frac{q+|t|+1}{2} = \frac{q-|t|-1}{2}$

The proposed method offers an optimal gain when the trace of the used curves is small integer. Indeed, for example when $t = 1$, we have $\frac{q-|t|-1}{2} = \frac{q}{2} - 1$, which means that the use of the modified τ-adic representation allows to reduce the size of required space memory by about 50%.

Since the digits of the new τ-adic expansion of k are all even integers and belong to $[-q-|t|-1, q+|t|+1]$, then the number of the expected zero digits k_i is $\frac{2log_q(k)}{(q+|t|+1)}$. If we denote by A and F an adding respectively an evaluation of the Frobenius operation, then the complexity of the generalised τ-adic method with even digits is

$$\left[log_q(k) - \left\lfloor \frac{2log_q(k)}{(q+|t|+1)} \right\rfloor\right] A + [log_q(k)]F,$$

which means that the generalised τ-adic method with even digits allows to save $\lfloor \frac{2log_q(k)}{(q+|t|+1)} - \frac{log_q(k)}{q} \rfloor$ points additions.

Consequently, the improvement of the computation time is also optimal when the trace t of the considered elliptic curves is small.

3.1.2 The generalised τ-adic method with odd digits

By using the process described above, we can also generate a new expansion of the scalar k that contains only odd digits. Without loss of generality, we will assume that the least significant digit k_0 is an odd number and we will apply the process described in the previous sections when we meet an even digit.

By using the same arguments, we can see that the number of stored points is reduced by $q - \frac{q+|t|+1}{2} = \frac{q-|t|-1}{2}$. On the other hand, the running time of the the generalised τ-adic method with odd digits is

$$log_q(k)A + log_q(k)F,$$

which means that it penalises the running time of the generalised τ-adic method by $\frac{log_q(k)}{q}$ points adding operations. On the other hand it is important to notice that the generalised τ-adic method with odd digits allows to thwart SPA attacks.

3.1.3 Efficiency

For several values of q and the trace t, Tables 1 and 2 give some numerical values about the running time and the size of the precomputed table. T and S will denote in percentage the gain of the computation time and of the number of the stored points that can be saved by our proposed methods with respect to the original generalised τ-adic one. We assume that the elements of the underlying field are represented by a normal basis, which means that the cost of the evaluation of the Frobenius operation may be negligible.

Table 1 Performances comparison: generalised τ-adic method *with even digits* with respect to generalised τ-adic method for elliptic curvves $E(\mathbb{F}_{q^m})$, where q is a small power of 2

The trace	$q = 8$		$q = 16$		$q = 32$		$q = 64$		$q = 256$	
	S	*T*	*S*	*T*	*S*	*T*	*S*	*T*	*S*	*T*
$t = \pm 1$	37%	8.5%	43%	5.7%	46%	2.8%	48%	1.4%	49%	0.3%
$t = \pm 3$	25%	4.7%	37%	4 %	43%	2.5%	46%	1.4%	49%	0.3%
$t = \pm 5$	12%	2%	31%	3%	40%	2.2%	45%	1.3%	48%	0.3%
$t = \pm 7$	-	-	25%	2.2%	37%	1.94%	43%	1.2%	48%	0.3%
$t = \pm 9$	-	-	-	-	34%	1.9%	42%	1.1%	48%	0.3%
$t = \pm 11$	-	-	-	-	31%	1.9%	40%	1%	47%	0.3%
$t = \pm 13$	-	-	-	-	-	-	39%	1%	47%	0.3%
$t = \pm 23$	-	-	-	-	-	-	-	-	45%	0.3%
$t = \pm 31$	-	-	-	-	-	-	-	-	43%	0.3%

Table 2 Performances comparison: generalised τ-adic method *with odd digits* with respect to generalised τ-adic method for elliptic curvves $E(\mathbb{F}_{q^m})$, where q is a small power of 2

La trace	$q=8$		$q=16$		$q=32$		$q=64$		$q=256$	
	S	*T*	*S*	*T*	*S*	*T*	*S*	*T*	*S*	*T*
$t=\pm1$	37%	–12.5%	43%	–6.25%	46%	–3.25%	48%	–1.56%	49%	–0.39%
$t=\pm3$	25%	–12.5%	37%	–6.25 %	43%	–3.25%	46%	–1.56%	49%	–0.33%
$t=\pm5$	12%	–12.5%	31%	–6.25%	40%	–3.25%	45%	–1.56%	48%	–0.39%
$t=\pm7$	-	-	25%	–6.25%	37%	–3.25%	43%	–1.56%	48%	–0.39%
$t=\pm9$	-	-	-	-	34%	–3.25%	42%	–1.56%	48%	–0.39%
$t=\pm11$	-	-	-	-	31%	–3.25%	40%	–1.56%	47%	–0.39%
$t=\pm13$	-	-	-	-	-	-	39%	–1.56%	47%	–0.39%
$t=\pm23$	-	-	-	-	-	-	-	-	45%	–0.39%
$t=\pm31$	-	-	-	-	-	-	-	-	43%	–0.39%

The values given in this table take in account the more additional adding operations that may be performed to recover the result of the scalar multiplication kP from $k'P$.

3.1.4 The generalised τ-adic method for the special curves

In this section, we will study the generalised τ-adic method with even digits when the special curves are considered. As explained before, for the these curves we can write $k=\sum_{i=0}^{i=m-1} k_i\tau^i$ where $k_i \in [-q/2, q/2]$, for $q=8,\ 16$, or 32.

Without loss of generality, it is clear that by using Algorithm 3 we can write $k=\sum_{i=0}^{i=m-1} k_i\tau^i$, where each $k_i \in [-\frac{q}{2}-|t|-1, \frac{q}{2}+|t|+1]$ is an even integer. The complexity of the generalised τ-adic method with even digits is then

$$\left[log_q(k) - \left\lfloor \frac{2log_q(k)}{\left(\frac{q}{2}+|t|+1\right)} \right\rfloor\right] A + [log_q(k)]F,$$

which means that it allows to save $\lfloor \frac{2log_q(k)}{(\frac{q}{2}+|t|+1)} - \frac{2log_q(k)}{q} \rfloor$ points additions.

This method requires the storage of $\frac{\frac{q}{2}+|t|+1}{2}$ points, which means that it allows to reduce the number of stored points by $\frac{q}{2} - \frac{\frac{q}{2}+|t|+1}{2} = \frac{\frac{q}{2}-|t|-1}{2}$.

On these curves, the generalised τ-adic method with even digits allows also to reduce considerably the number of the stored points especially when the trace of the curve is small. The reduction percentage of the used precomputed table is less important than that obtained on the general curves. On the other hand, the percentage of the running time reduction is more important. Table 3 gives some numerical values.

The generalised τ-adic method with odd digits allows to reduce the same number of the stored points as the generalised τ-adic method with even digits, but the percentage of the running time augmentation is slightly higher.

Table 3 Performances comparison: generalised τ-adic method *with even digits* with respect to generalised τ-adic method for the special curves

La trace	$q=8$		$q=16$		$q=32$		$q=64$		$q=256$	
	S	*T*	*S*	*T*	*S*	*T*	*S*	*T*	*S*	*T*
$t=\pm1$	25%	11%	37%	8.5%	43%	5.7%	46%	2.8%	49%	0.7%
$t=\pm3$	0%	0%	25%	4.7%	37%	4 %	43%	2.5%	48%	0.7%
$t=\pm5$	–25%	–6%	12%	2%	31%	3%	40%	2.2%	47%	0.7%
$t=\pm7$	-	-	0%	0%	25%	2.2%	37%	1.94%	46%	0.6%
$t=\pm9$	-	-	-	-	19%	1.5%	34%	1.9%	46%	0.6%
$t=\pm11$	-	-	-	-	-	-	32%	1.4%	45%	0.6%
$t=\pm13$	-	-	-	-	-	-	28%	1.2%	44%	0.6%
$t=\pm23$	-	-	-	-	-	-	-	-	40%	0.5%
$t=\pm31$	-	-	-	-	-	-	-	-	37%	0.4%

3.2 The generalised τ-adic method for the curves $E(\mathbb{F}_{q^m})$, where q is a small prime number

This section introduces a new process for generating an expansion of k that contains only odd respectively even digits when the considered curve is $E(\mathbb{F}_{q^m})$, where q is a small prime number.

Smart (1997) showed that, for every scalar k, we can write

$$k = \sum_{i=0}^{i=m-1} k_i \tau^i,$$

where $k_i \in \{-q, -q+1, \cdots, q\}$.

We recall that the technique described in the previous section for curves defined over fields with characteristic two is based on the fact that the trace of the curve is an odd integer. In this section we will explain how we can generate a new expansion of k that contains only odd digits (respectively even digits) even if the trace of the considered curve is an even integer.

To eliminate all the even digits k_i from the τ-adic expansion of k, we will also use the Frobenius equation $\tau^2 - t\tau + q = 0$. We will modify the digits from the most significant digit k_{m-1} to the second last significant one k_2, by following this process.

If the digit k_i is even, we set

$$\begin{cases} k_i \leftarrow k_i - \text{sign}(k_{i-2}) \\ k_{i-1} \leftarrow k_{i-1} + \text{sign}(k_{i-2})t \\ k_{i-2} \leftarrow k_{i-2} - \text{sign}(k_{i-2})q, \end{cases}$$

and we keept the digits k_{i-1}, k_i, k_{i+1} inchanged otherwise.

From Remark 3.1, it is clear that this process does not change the value of the scalar k.

When the digit k_2 is touched, it is clear that the digits k'_i for $i = 2, \cdots, m-1$ of the new τ-adic expansion τ-adic $(k'_{m-1}, \cdots, k'_0)$ are odd integers. On the other hand we can not predict wether the digits k'_0 and k'_1 are odd integer or not. If the digit k'_0 or k'_1 respectively the both are even integers, we propose to replace k'_0 by $k'_0 \pm 1$ or k'_1 by $k'_1 \pm 1$ respectively k'_0 and k'_1 by $k'_0 \pm 1$, k'_1 by $k'_1 \pm 1$.

Let $k' \in \mathbb{Z}[\tau]$ be the element represented by the τ-adic expansion $(k'_{m-1}, \cdots, k'_0)$ obtained after this last modification. To compute the scalar multiplication kP, first we compute $k'P$, and after we recover kP by performing possibly two adding operations and one evaluation of the Frobenius. Indeed, we have only to add or to subtract P, $\tau(P)$ or $P \pm \tau(P)$ according to the operations performed to transform k'_0 and k'_1 into odd integers.

This process can easily adapted to generate a new τ-adic expansion of k that contains only even integers.

The generalised τ-adic methods with odd or even digits on the curves $E(\mathbb{F}_{q^m})$, where q is a small prime number, compute the scalar multiplication kP with a more additional evaluation of the Frobenius than on the curves $E(\mathbb{F}_{q^m})$, where q is small power of two. Consequently, all results and comments given in the previous sections are also valid for the generalised τ-adic methods with odd or even digits on the curves $E(\mathbb{F}_{q^m})$, where q is small prime number.

3.3 The proposed method for the curves $E(\mathbb{F}_{q^m})$, where $\mathbb{F}_{q^m}$ is an optimal extension field

Sarkar et al. (2004) have proposed an improvement of Algorithm 2 by storing the points $[b_0, b_1, \cdots, b_{m-1}]P = b_0P + b_1\tau(P) + b_2\tau^2(P) + \cdots + b_{m-1}\tau^{m-1}(P)$ for all $(b_{m-1}, \cdots, b_1, b_0) \in \{-1, 0, 1\}^m$. If this table is available, the computation of kP becomes easy by using the following algorithm.

Algorithm 4 Method of Sarkar et al.

Input : a τ-adic representation $(k_{m-1}, \cdots, k_0)$ integer k, and a point $P \in E(\mathbb{F}_{q^m})$.
Output : kP.
1. Set $Q \leftarrow [k_{0,A}, \cdots, k_{m-1,A}]P$
2. For $j = A - 1$ down to 0
3. $Q \leftarrow 2Q$
4. $Q \leftarrow Q + [k_{0,j}, \cdots, k_{m-1,j}]P$
5. return Q.

As mentioned before, this algorithm stores all the points $[b_0, b_1, \cdots, b_{m-1}]P = b_0P + b_1\tau(P) + b_2\tau^2(P) + \cdots + b_{m-1}\tau^{m-1}(P)$ for all $(b_{m-1}, \cdots, b_1, b_0) \in \{-1, 0, 1\}^m$, which means that the number of stored points is $3^m - 1$. With the use of the unsigned binary representation for each digit k_i, we remark that Algorithm 4 will require only the storage of $2^m - 1$ points. In the following, we will compare the efficiency of our proposed method with that of the improved Algorithm 4.

The improvement that aims to reduce by about 50% the number of the stored points by the improved Algorithm 4 will be achieved in two steps. In the first time, we generate a new τ-adic representation of k that contains only the odd digits, by using the process described in Section 3.2. After that, we modify the binary representation of each

odd digits by following the scheme proposed by Hedabou et al. (2005). This scheme eliminates all zero bits of binary representation of each odd integer and replaces them by 1 or -1. This is done by following this process: the first bit k'_0 of an integer k' is assumed to be odd, let k'_j be the first bit equal to 0. We then replace k'_j by $k'_j + 1 = 1$ and k'_{j-1} by $k'_{j-1} - 2 = -k'_{j-1} = -1$. This modification does not change the value of k'.

After these modifications, the set of points stored in the precomputed table

$$\{[b_{m-1}, \cdots, b_1, b_0]P, \text{ for all } b_i = \pm 1\},$$

can be represented as $\{-Q, Q\}$, where $Q = \{[b_{m-1}, \cdots, b_1, b_0]P$, with $b_0 = 1\}$. Hence, we need to store in the precomputed table only the points $[b_{m-1}, \cdots, b_1, 1]P$ with $b_i = \pm 1$. Consequently, the number of the points stored in the precomputation phase of the proposed scheme is 2^{m-1}, which is about the half of what is required by the original method.

The new odd digits k_i obtained after the modification of the τ-adic representation of k are in $[-q - |t| - 1, q + |t| + 1]$. Since $|t| \leq 2\sqrt{q}$, it is clear that $log_2(k_i) \leq log_2(q)$ for $i = 0, \cdots, m-1$, which means that the length of the odd digits binary representation is the same as that of the original ones. Thus, the modification of the τ-adic representation penalises the computation time only by at most 2 adding and 1 Frobenius evaluation operations. These additional operations are possibly required for recovering the correct value of the scalar multiplication kP.

Now, we will compare the performances of the proposed method with respect to the method of Sarkar et al. We assume that the sizes of the used scalars are approximately the same as those of the fields $\mathbb{F}_{q^m}$ on which the elliptic curves are defined, i.e., $log_2(k) = \lceil log_2(q) \rceil \times m$, and that the points are represented with projective coordinates. We denote by S and T the percentage of the gain in term of the computation time and the number of the stored points that can be saved by our proposed method with respect to the method of Sarkar et al.

The numerical values given by Table 4 show clearly that the proposed method allows to reduce by about 50% the number of the stored points by the τ-base method. The running time increase does not exceed 7%.

Table 4 Performances comparison: the proposed method with respect to Sarkar et al. one's for Elliptic curves $E(\mathbb{F}_{q^m})$, where $\mathbb{F}_{q^m}$ is an optimal extension field

$q = 2^{17} - 1, m = 9$		$q = 2^{31} - 1, m = 6$		$q = 2^{31} - 1, m = 7$		$q = 2^{61} - 1, m = 3$	
S	*T*	*S*	*T*	*S*	*T*	*S*	*T*
9.9%	–7.3%	49.2%	–4.8%	49.2	–4.4%	42.8%	–6.5%

4 On the security of the used curves

As mentioned before, the elliptic curves defined over composite fields may be vulnerable to the GHS attack (Gaudry et al., 2002). In this section, we will show that we can find sufficiently of such curves which are recommended by several standards that are resistant to the GHS attack.

The GHS attack on elliptic curves over composite binary fields was fully analysed by Mauer et al. (2001). They have concluded that some elliptic curves over $\mathbb{F}_{2^m}$, where $m \in [100, 600]$ succumb to the GHS attack. Such curves include some ones over $\mathbb{F}_{2^{155}}$, $\mathbb{F}_{2^{161}}$, $\mathbb{F}_{2^{180}}$, $\mathbb{F}_{2^{186}}$, $\mathbb{F}_{2^{217}}$, $\mathbb{F}_{2^{284}}$, which are recommended by the ANSI X9.62 standard. On the other hand, they have stated that the GHS attack fail on all curves defined over $\mathbb{F}_{2^{185}}$, $\mathbb{F}_{2^{215}}$, $\mathbb{F}_{2^{265}}$, $\mathbb{F}_{2^{176}}$, $\mathbb{F}_{2^{208}}$, $\mathbb{F}_{2^{304}}$, $\mathbb{F}_{2^{368}}$, which are also specified by the ANSI X9.62 standard. Furthermore, they have established that for the most composite binary fields $\mathbb{F}_{2^m}$, the proportion of elliptic curves over $\mathbb{F}_{2^m}$ that succumb to GHS attack is very small. For example, the proportion of such curves over $\mathbb{F}_{2^{155}}$, which are proposed for key agreement, is only $1/2^{52}$.

The elliptic curves over optimal extension fields $E(\mathbb{F}_{q^m})$ are not really concerned by the GHS attack. Indeed, according to Diem (2003), the GHS attack fail in such curves even if he claimed that this attack may succeed for some elliptic curves when $m = 5$ or $m = 7$. Further researches are however necessary to confirm the success of this attack.

On the other hand, the elliptic curves defined over small fields of odd characteristics have never been proposed for commercial applications. Their security against the attacks based on the Weil descent attacks has not plainly explored, consequently we have to be careful about their use in cryptography.

Consequently, we can conclude that there are sufficiently curves over composite extension fields or optimal extension fields on which the GHS attack fail. However, the curves parameters should be carefully selected, in order to avoid potential security weaknesses.

5 Conclusions

In this paper we have presented two methods that allow to improve the efficiency of the τ-based scalar multiplication methods. The first one improves both the running time and the size of the used space memory of the generalised τ-adic method especially when the trace of used elliptic curves is small. The second technique allows to reduce by about 50% the size of the space memory required by the τ-base method introduced by Sarkar et al. (2004).

References

Aranha, D., Faz-Hernández, A., López, J. and Rodríguez-Henriquez, F. (2012) *Faster Implementation of Scalar Multiplication on Koblitz Curves*, Cryptology eprint Archives, Report 519.

Blake, I., Seroussi, G. and Smart, N. (1999) *Elliptic Curves in Cryptography*, Cambridge University Press.

Chung, B., Kim, H. and Yoon, H. (2007) 'Improved base-ϕ expansion method for Koblitz curves over optimal extension fields', *Information Security IET*, Vol. 1, pp.19–26.

Diem, C. (2003) *The GHS Attack in Odd Characteristics* [online] http://www.exp-math.uni.essen.de/∼diem/english.html.

Gaudry, P., Hess, F. and Smart, N. (2002) 'Constructive and destructive facets of Weil descent on elliptic curves', in *Journal of Cryptology*, Vol. 15, No. 1, pp19–46.

Hedabou, M., Pinel, P. and Bénéteau, L. (2005) 'Countermeasures for preventing comb method against SCA attacks', in *ISPEC 2005, LNCS*, Vol. 3439, pp.85–96.

Kobayashi, T., Morita, H., Kobayashi, K. and Hoshino, F. (1999) 'Fast elliptic curve algorithm combining Frobenius map and table reference to adapt to higher characteristic', in *Eurocrypt '99, LNCS*, Vol. 1592, pp.176–189.

Koblitz, N. (1991) 'CM-curves with good cryptographic properties', in J. Feigenbaum (Ed.): *Advances in Cryptology-CRYPTO '91, LNCS*, Vol. 576, pp.279–287.

Kocher, P., Jaffe, J. and Jun, B. (1999) 'Differential power analysis', in *CRYPTO 1999, LNCS*, Vol. 1666, pp.388–397, Springer-Verlag.

Müller, V. (1998) 'Fast multiplication on elliptic curves over small fields of characteristic two', *Journal of Cryptology*, January, Vol. 11, pp.219–234.

Mauer, M., Menezes, A. and Tesk, E. (2001) 'Analysis of the GHS Weil descent attack on the ECDLP over characteristic two finite fields of composite degree' [online] http://eprint.iacr.org/2001/084.

Meier, W. and Staffelbach, O. (1992) 'Efficient multiplication on certain nonsupersingular elliptic curves', in *Advances in Cryptology-CRYPTO '92, LNCS*, Vol. 740, pp.333–344.

Menezes, A. (1992) *Elliptic Curve Public Key Cryptosystems*, Vol. 234, pp.333–344, The Kluwer Academic Publishers.

Roy, S., Rebeiro, C., Mukhopadhyay, D., Takahashi, J. and Fukunaga, T. (2011) *Scalar Multiplication on Koblitz Curves using* $\tau^2 - NAF$, Cryptology eprint Archives, Report 318.

Sarkar, P. Mishra, P. and Baruna, R. (2004) 'New table look-up Frobenius map based scalar multiplication over $\mathbb{F}_{p^m}$', in *ACNS 2004, LNCS*, Vol. 3089, pp.479–493.

Smart, N.P. (1997) *Elliptic Curve over Small Fields of Odd Characteristics*, HP Labs, Technical report, pp.97–126.