A Frobenius Map Approach for An Efficient and Secure Multiplication on Koblitz Curves

Mustapha Hedabou

INSA de Toulouse, LESIA
135, avenue de Rangueil, 31077 Toulouse cedex 4, France. (Email: hedabou@insa-toulouse.fr)

(Received Sept. 20, 2005; revised and accepted Oct. 27, 2005)

Abstract

The most efficient technique for protecting the using Frobenius algorithms for scalar multiplication on Koblitz curves against the Side Channel Attacks seems to be the multiplier randomization technique proposed by Joye and Tymen. In this paper, an heuristic analysis on the security of the Joye and Tymen's technique is given. A new method improving this technique is proposed. Analysis shows that the proposed method reduce the cost of the Joye and Tymen's technique by about 50%.

Keywords: Elliptic curve, Frobenius map, public key cryptography, side Channel Attacks, τ-NAF method

1 Introduction

The scalar multiplication methods based on the use of the Frobenius map allow to speed up the scalar multiplication on certain categories of elliptic curves (Koblitz curves) defined over a field with a small characteristic [7, 12]. However, on devices with small resources they are, as the usual double-and-add algorithms, vulnerable to Side Channel Attacks (SCA) [1, 3, 8].

Many countermeasures have been proposed to prevent the SCA attacks on the Frobenius based methods for scalar multiplication. Hasan [4] has proposed three countermeasures. The Key Masking with Localized Operations (KMLO) technique, The Random Rotation of Key (RRK) technique and the Random Insertion of Redundant Symbols (RIRS) technique. Another countermeasure was proposed by Smith [13], but the most efficient one seems to be the randomization technique proposed by Joye and Tymen [6] which consist of reducing the secret scalar k modulo ρ $(\tau^m - 1)$, where ρ is a random element of $\mathbb{Z}[\tau]$, instead of $\tau^m - 1$.

This communication will focus on the increasing the efficiency the Joye and Tymen's countermeasure for preventing the SCA attacks on the Frobenius based methods. A further discussion on the security of this technique is given, and another method, which is an improvement of the Joye and Tymen's technique, is introduced. The proposed technique reduce the cost of the Joye and Tymen's countermeasure by about 50%.

The paper is organized as follows: Section 2 briefly reviews the properties of the Frobenius map in the setting of ECC and describes the Frobenius-based scalar multiplication. In Section 3, we introduce the Side Channel Attacks and their countermeasures. In Section 4, we give an heuristic estimation on the number of the elements $\rho \in \mathbb{Z}(\tau)$ such that $N(\rho) \leq N$ where N is a positive integer. Our proposed method will be introduced in Section 5, and we conclude in Section 6.

2 The τ-NAF Method

Koblitz curves [7] are defined over $\mathbb{F}_2$ by the following equations:

$$y^2 + xy = x^3 + ax^2 + 1, \text{ where } a \in \{-1, 1\}.$$

In this section we introduce briefly the Frobenius map. The reader can refer to [11] for details. Let $E(\mathbb{F}_q)$ an elliptic curve defined over a finite field $\mathbb{F}_q$.

We define the q-th power Frobenius map τ on $E(\mathbb{F}_q)$ as follows:

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

The Frobenius map satisfies the equation $\tau^2 - t\tau + q = 0$, where t is the trace of the curve $E(\mathbb{F}_q)$ $(\#E(\mathbb{F}_q) = q + 1 - t)$. For Koblitz curves the characteristic equation of the Frobenius map is $\tau^2 - (-1)^{1-a}\tau + 2 = 0$

Since $\tau^m(x, y) = (x^{q^m}, y^{q^m}) = (x, y)$ for all $(x, y) \in \mathbf{F}_{q^m}$ x $\mathbf{F}_{q^m}$, it is clear that the Frobenius map on $E(\mathbb{F}_q)$ verifies:

$$\tau^m(R) = R \text{ for all points } R \in E(\mathbb{F}_{q^m}).$$

Let τ denote the Frobenius endomorphism of a Koblitz curve. In this section, we will describe the Frobenius-based τ-NAF method. The results about the τ-NAF representation in $\mathbb{Z}[\tau]$ are presented without proof; more details can be found in [7, 10, 12].

In [7], Koblitz showed that the use of the Frobenius map τ can speed up the multiplication of a point P of the curve by a scalar k on certain categories of elliptic curves defined over fields with a characteristic $q = 2$ (Koblitz curves), as k may be written in the form $k = \sum_{i=0}^{l-1} k_i \tau^i$ with $k_i \in \{-1, 0, 1\}$, after what the computation of kP may be performed by applying the usual left-to-right point multiplication scheme. The representation $(k_{l-1}, \cdots, k_0)$ such that $k = \sum_{i=0}^{l-1} k_i \tau^i$, with $k_i \in \{-1, 0, 1\}$ for $i = 0, \cdots, l-2$, is called the τ-adic representation of k. In the same manner as the NAF representation of the secret scalar k gives improvement over the binary representation in the case of the integers, we can reduce the number of the non-zero digits in the representation of scalar k by using the $\tau - NAF$ representation of k (Algorithm 4 in [14]).

The length of the τ-NAF representation of the scalar k is about twice the length of its binary representation. To reduce the computation time of kP, Solinas [14] has proposed an efficient algorithm (Algorithm 5 in his paper) based on a previous work by Meier-Staffelbach [10].

Since $\tau^m(R) = R$ for all points $R \in E(\mathbb{F}_{2^m})$, it follows that, if α and β are elements of $\mathbb{Z}[\tau]$ with $\alpha \equiv \beta \bmod (\tau^m - 1)$, then $\alpha R = \beta R$ for all R; this means that rather than computing kP, we compute αP where α is the remainder obtained from dividing k by $\tau^m - 1$. From [10], we know that $\mathbb{Z}[\tau]$ is an euclidean domain, thus the norm of the remainder α is smaller than the norm of $\tau^m - 1$. Since the norm of $\tau^m - 1$ is precisely the order of the curve $E(\mathbb{F}_{2^m})$, the τ-NAF expansion of the remainder α has a length $\backsim m$. For a better efficiency, the $\tau - NAF$ expansion of the scalar (Algorithm 4 in [14]) will be used. The algorithm below implements in detail the τ-NAF method.

Algorithm 1 : τ-NAF method

Input : an integer k, and a point $P \in E(\mathbb{F}_{2^m})$.

Output : kP.

```
1. Computation of the τ-NAF representation: $k = \sum_{i=0}^{m-1} k_i \tau^i$, with $k_i \in \{-1, 0, 1\}$, with $k_i k_{i+1} = 0$ for $i = 0, \cdots, m-2$.
2. $Q \leftarrow P$.
3. for $i = m-2$ down to $0$ do
3.1 $Q \leftarrow \tau(Q)$.
3.2 if $k_i = 1$ then $Q \leftarrow Q + P$.
3.3 if $k_i = -1$ then $Q \leftarrow Q - P$.
4. Return $Q$.
```

3 The SCA Attacks and Their Countermeasures

Side Channel Attacks exploit some data leaking information such as power consumption and computing time to detect a part or the whole of the bits of the secret key. We can distinguish two types of SCA attacks:

- The Simple Power Analysis (SPA) attacks which analyzes the information leaking from a single execution of the algorithm. The $\tau - adic$ method computes a Frobenius map and an adding of points if $k_i \neq 0$, and only a Frobenius map if $k_i = 0$. By observing the power consumption, an SPA attacker can detect whether the secret digits k_i are zero or not. To prevent SPA attacks, many countermeasures have been proposed; the standard approach is to use fixed pattern algorithms.

- The Differential Power Analysis (DPA) attacks which collect informations from several executions of the algorithm and interpret them with statistical tools. To prevent DPA attacks, randomization of parameters seems to be an efficient technique [2, 6]. The usual approach is to randomize the base point P. Coron proposes to transform the affine point $P = (x, y)$ into randomized Jacobian projective coordinates $P = (r^2x, r^3y, r)$ for a random non-zero integer r. Joye and Tymen use a random curve belonging to the isomorphism class of the elliptic curve. A point $P = (x, y)$ of an elliptic curve E is transformed into $P' = (r^2x, r^3y)$ which is a point of the corresponding isomorphic curve E' of E.

- The RPA attack proposed by Goubin [3] belongs to a new generation of DPA attacks that use special points to deduce the bits of the secret key. The fundamental remark of Goubin is that randomizing points with a 0-coordinate ($(x, 0)$ or $(0, y)$) yields points that possess still a 0-coordinate. Supposing that the bits $k_{l-1}, \cdots, k_{j+1}$ of the secret scalar k are known by the attacker, and that he wants to guess the value of the next bit k_j, he just needs to choose the point $P = (c^{-1} mod \# E)(0, y)$ with $c = 2^j + \sum_{i=j+1}^{l-1} 2^i k_i$. If, in the process of the computation of kP, the scalar multiplication computes the point $cP = (0, y)$, the power consumption for the next step is significantly distinct. Thus, the attacker can know whether cP has been computed or not, and hence if k_j was 1 or 0. Iterating this process, all bits of the secret key can be determined. Akishita-Takagi [1] generalize Goubin's idea to elliptic curves without points with a 0-coordinate. Their attack focuses on the auxiliary registers which might contain a zero value, when the adding and doubling operations a re performed by the scalar multiplication. The ZPA attack is in particular efficient on several standard curves with no 0-coordinate point. To prevent the RPA and ZPA attacks, the authors in [5, 9] have proposed the Randomized Linearly-transformed coordinates (RLC) technique.

- To prevent the SCA attacks on the $\tau - adic$ method, Joye and Tymen [6] have proposed to randomize the secret scalar k. The scalar k is reduced modulo ρ $(\tau^m - 1)$, where ρ is a random element of $\mathbb{Z}[\tau]$. For the same purpose, Hasan [4] proposed previously three countermeasures. In the Key Masking with Localized Operations (KMLO) technique, the symbols of the $\tau-adic$ representation can be replaced in more than one way on a window of three and more symbols, since we have $2 = \tau - \tau^2 = -\tau^3 - \tau$ which is derived from the equation $\tau^2 - \tau + 2 = 0$ (assuming that $t = 1$). The Random Rotation of Key (RRK) technique proposes to compute the scalar multiplication kP as $k'P'$ where $P' = \tau^r P$, and r is a random integer such as $r \leq m - 1$. Finally, the Random Insertion of Redundant Symbols (RIRS) technique proposes to insert in the $\tau - adic$ representation of the secret scalar k a number of redundant symbols such as they collectively neutralize their own effects. Another countermeasure was proposed by Smith [13]; it consists in decomposing the $\tau-adic$ representation of k into r groups of g coefficients, r being a random element such as $r \leq m$ and $g = \lceil \frac{m}{r} \rceil$. The point multiplication between each group and the base point P is performed in a random order. The countermeasure of Joye and Tymen seems to be more efficient in thwarting the SCA attacks, since it randomizes the entire digits of the secret scalar k.

4 Heuristic Estimation

As mentioned previously, the Joye and Tymen's technique for preventing the τ-NAF method against the SCA attacks proposes to randomize the secret scalar k by reducing it modulo $\rho(\tau^m - 1))$ instead of $\tau^m - 1$, where ρ is a random element of $\mathbb{Z}[\tau]$. The length of the obtained τ-NAF representation is approximately $m + log_2(N(\rho))$, where $N(\rho)$ denotes the norm of ρ in $\mathbb{Z}[\tau]$. The efficiency of this technique depends on the number of the random elements ρ of $\mathbb{Z}[\tau]$, where $N(\rho) \leq N$ and N is positif integer N. The length of the integer N allows to control the trade-off between the computation time and the required security.

The following theorem gives an heuristic estimation on the number of the randomized scalars obtained by the Joye and Tymen's technique.

Theorem 1 *Let N be a positive integer, the number of element ρ of $\mathbb{Z}(\tau)$ with $N(\rho) \leq N$ is approximately αN, where $\frac{4}{\sqrt{7}} \leq \alpha \leq \frac{8\sqrt{2}}{\sqrt{21}}$.*

To prove this theorem we have first to prove the following lemma.

Lemma 1 *$\#\{a + b\tau \in \mathbb{Z}(\tau) \;/\; N(a + b\tau) = a^2 + ab + 2b^2 \leq N\} = 2\sum_{i=0}^{\lfloor \frac{2}{\sqrt{(7)}}\sqrt{N}\rfloor} \lfloor\sqrt{4N - 7i^2}\rfloor$, where $\lfloor . \rfloor$ denotes the function which returns the entire part.*

Proof. Let b be a fixed integer, and let us estimate the number of the integers a such that $N(a+b\tau) = a^2 + ab + 2b^2 \leq N$ for a given positive integer N.

The inequality $a^2+ab+2b^2-N \leq 0$ admits a solutions if the discriminan $b^2 - 4(2b^2 - N) = 4N - 7b^2$ is a positif integer, which means that $\mid b \mid \leq \frac{2}{\sqrt{7}}\sqrt{N}$.

For a fixed positive integer $b \leq \frac{2}{\sqrt{7}}\sqrt{N}$, the solutions of the inequality $a^2 + ab + 2b^2 - N \leq 0$ are the integers $a \in \lbrack \frac{-b-\sqrt{4N-7b^2}}{2}, \frac{-b+\sqrt{4N-7b^2}}{2} \rbrack$, which means that, for a fixed b, the number of the integer a such that $N(a + b\tau) \leq N$ is $\lfloor\sqrt{4N - 7b^2}\rfloor$. Consequently, the number of the elements $a + b\tau$ of $\mathbb{Z}(\tau)$ such that $N(a + b\tau) \leq N$ is $2\sum_{i=0}^{\lfloor\frac{2}{\sqrt{7}}\sqrt{N}\rfloor} \lfloor\sqrt{4N - 7i^2}\rfloor$. □

By using the above lemma we will prove the Theorem 1. By applying the following inequality: for every positif integers $x,\ y$, with $x \geq y$, we have $\sqrt{x-y} \geq \sqrt{x} - \sqrt{y}$, then we can write

$$\sum_{i=0}^{\lfloor\frac{2}{\sqrt{7}}\sqrt{N}\rfloor} \sqrt{4N - 7i^2} \geq \sum_{i=0}^{\lfloor\frac{2}{\sqrt{7}}\sqrt{N}\rfloor} \sqrt{4N} - \sum_{i=0}^{\lfloor\frac{2}{\sqrt{7}}\sqrt{N}\rfloor} \sqrt{7i^2}. \quad (1)$$

since

$$sum_{i=0}^{\lfloor\frac{2}{\sqrt{7}}\sqrt{N}\rfloor} \sqrt{4N} = 2(\lfloor \frac{2}{\sqrt{7}}\sqrt{N}\rfloor + 1)\sqrt{N} \approx \frac{4}{\sqrt{7}}N$$

and

$$\begin{aligned} \sum_{i=0}^{\lfloor\frac{2}{\sqrt{7}}\sqrt{N}\rfloor} \sqrt{7i^2} &= \sqrt{7}\sum_{i=0}^{\lfloor\frac{2}{\sqrt{7}}\sqrt{N}\rfloor} i \\ &= \sqrt{7}(\frac{\lfloor\frac{2}{\sqrt{7}}\sqrt{N}\rfloor(\lfloor\frac{2}{\sqrt{7}}\sqrt{N}\rfloor + 1)}{2}) \\ &\approx \frac{2}{\sqrt{7}}N. \end{aligned}$$

then

$$\sum_{i=0}^{\lfloor\frac{2}{\sqrt{7}}\sqrt{N}\rfloor} \sqrt{4N} - \sum_{i=0}^{\lfloor\frac{2}{\sqrt{7}}\sqrt{N}\rfloor} \sqrt{7i^2} \approx \frac{2}{\sqrt{7}}N$$

and thus from Equation (1) we can write

$$2\sum_{i=0}^{\lfloor\frac{2}{\sqrt{7}}\sqrt{N}\rfloor} \sqrt{4N - 7i^2} \geq \frac{4}{\sqrt{7}}N.$$

On the other hand, by using the inequality of Cauchy-Schwartz we can write

$$\sum_{i=0}^{\lfloor\frac{2}{\sqrt{7}}\sqrt{N}\rfloor} \sqrt{4N - 7i^2} \leq (\sum_{i=0}^{\lfloor\frac{2}{\sqrt{7}}\sqrt{N}\rfloor} 1)^{\frac{1}{2}} (\sum_{i=0}^{\lfloor\frac{2}{\sqrt{7}}\sqrt{N}\rfloor} (4N - 7i^2))^{\frac{1}{2}}. \quad (2)$$

since

$$\begin{aligned} \sum_{i=0}^{\lfloor\frac{2}{\sqrt{7}}\sqrt{N}\rfloor} 7i^2 &= 7(\frac{\lfloor\frac{2}{\sqrt{7}}\sqrt{N}\rfloor(\lfloor\frac{2}{\sqrt{7}}\sqrt{N}\rfloor + 1)(2\lfloor\frac{2}{\sqrt{7}}\sqrt{N}\rfloor + 1)}{6}) \\ &\approx \frac{8}{3\sqrt{7}}N^{\frac{3}{2}} \end{aligned}$$

then we can write

$$(\sum_{i=0}^{\lfloor\frac{2}{\sqrt{7}}\sqrt{N}\rfloor} (4N - 7i^2))^{\frac{1}{2}} \approx (\frac{16}{3\sqrt{7}}N^{\frac{3}{2}})^{\frac{1}{2}}$$

On the other hand we have

$$(\sum_{i=0}^{\lfloor\frac{2}{\sqrt{7}}\sqrt{N}\rfloor} 1)^{\frac{1}{2}} \approx (\frac{2}{\sqrt{7}}\sqrt{N})^{\frac{1}{2}}$$

Thus

$$(\sum_{i=0}^{\lfloor\frac{2}{\sqrt{7}}\sqrt{N}\rfloor} 1)^{\frac{1}{2}}(\sum_{i=0}^{\lfloor\frac{2}{\sqrt{7}}\sqrt{N}\rfloor} (4N-7i^2))^{\frac{1}{2}} \approx \frac{4\sqrt{2}}{\sqrt{21}}N.$$

and thus from Equation (2), we can write

$$2\sum_{i=0}^{\lfloor\frac{2}{\sqrt{7}}\sqrt{N}\rfloor} \sqrt{4N-7i^2} \leq \frac{8\sqrt{2}}{\sqrt{21}}N.$$

Which complete the proof of the theorem.

Without loss of generalities, let us suppose that the number of the elements ρ with $N(\rho) \leq N$ is approximately αN, for some fixed α, where $\frac{4}{\sqrt{7}} \leq \alpha \leq \frac{8\sqrt{2}}{\sqrt{21}}$. The result stated by the following lemma will be used in the next section to evaluate the security of our proposed method.

Lemma 2 *The number of the random elements* (r, ρ) *where* r, ρ *are a random elements of* $\mathbb{Z}[\tau]$ *with* $N(\rho) \leq N$ *and* $N(r) \leq N(\rho)$, *is approximately* $\alpha N^2/2$.

Proof. By the theorem 1 we know that the number of the elements ρ of the $\mathbb{Z}[\tau]$ with $N(\rho) \leq N$ is approximately αN. Thus, for each $\rho \in \mathbb{Z}[\tau]$, there exist about $\alpha N(\rho)$ elements r of $\mathbb{Z}[\tau]$ with $N(r) \leq N(\rho)$.

Consequently, the number of the random elements (r, ρ) where r, ρ are a random elements of $\mathbb{Z}[\tau]$ with $N(\rho) \leq N$ and $N(r) \leq N(\rho)$ is : $\sum_{i=0}^{i=N} \alpha i = \alpha\frac{N(N+1)}{2} \approx \alpha N^2/2$, which complete the proof of the lemma. □

5 The Proposed Technique

Let $E(\mathbb{F}_{2^m})$ be an elliptic curve, and let τ the Frobenius map on $E(\mathbb{F}_2)$, i.e $\tau((x,y)) = (x^2, y^2)$.

It is clear that τ verifies $\tau^m = 1$ in End_E. Thus

$$\tau^m - 1 = (\tau - 1)\sum_{i=0}^{m-1} \tau^i = 0.$$

Then for all points $R \in E(\mathbb{F}_{2^m}) \setminus E(\mathbb{F}_2)$ (i.e $\tau(R) \neq R$) we have

$$\sum_{i=0}^{m-1} \tau^i(R) = \frac{\tau^m - 1}{\tau - 1}(R) = 0. \qquad (3)$$

To reduce the cost of the Joye-Tymen's technique, we propose to exploit the Equation (3), and replace the secret scalar k by the random element $k' = k + r\frac{\tau^m-1}{\tau-1}\ mod\ (\rho(\tau^m - 1))$, where r, ρ are a random elements of $\mathbb{Z}[\tau]$, with $N(r) \leq N(\rho)$ and $N(\rho) \leq N$ for some positif integer N. From the Equation (3), it is clear that $kP = k'P$ for every base point P (points with high orders).

Now we will evaluate the security of the proposed method, which means estimate the number of the random scalars k'. From the Lemma 2, we know that the number of the random elements (r, ρ), where r, ρ are a random elements of $\mathbb{Z}[\tau]$ with $N(\rho) \leq N$ and $N(r) \leq N(\rho)$, is approximately $\alpha N^2/2$. Thus the number of the randomized scalars $k' = k + r\frac{\tau^m-1}{\tau-1}\ mod\ (\rho(\tau^m - 1))$ is $\alpha\frac{N^2}{2} - c$, where c is the number of the collisions.

Definition 1 *We said that we have a collision if there exist two couple of elements* (r_1, ρ_1) *and* (r_2, ρ_2) *such that*

$$\begin{aligned} k &+ r_1\frac{\tau^m - 1}{\tau - 1}\ mod\ (\rho_1(\tau^m - 1)) \\ = k &+ r_2\frac{\tau^m - 1}{\tau - 1}\ mod\ (\rho_2(\tau^m - 1)). \end{aligned}$$

Lemma 3 *The number of collisions is at most* $\alpha\frac{N^2}{4}$

Proof. Let us suppose that the random elements (r_1, ρ_1) and (r_2, ρ_2) give rise to a collision, which mean that the following equation yields

$$\begin{aligned} k &+ r_1\frac{\tau^m - 1}{\tau - 1}\ mod\ (\rho_1(\tau^m - 1)) \\ = k &+ r_2\frac{\tau^m - 1}{\tau - 1}\ mod\ (\rho_2(\tau^m - 1)). \end{aligned} \qquad (4)$$

The Equation (4) implies that there exist $\lambda_1, \lambda_2 \in \mathbb{Z}[\tau]$ such as

$$\begin{aligned} k &+ r_1\frac{\tau^m - 1}{\tau - 1} - \lambda_1(\rho_1(\tau^m - 1)) \\ = k &+ r_2\frac{\tau^m - 1}{\tau - 1} - \lambda_2(\rho_2(\tau^m - 1)) \end{aligned} \qquad (5)$$

(5) implies that there exist $\lambda_1, \lambda_2 \in \mathbb{Z}[\tau]$ such as

$$\frac{r_1 - r_2}{\tau - 1} = \lambda_1\rho_1 - \lambda_2\rho_2 \qquad (6)$$

The Equation (6) implies that $\tau - 1/r_1 - r_2$ and that the $gcd(\rho_1, \rho_2)$ is a multiple of $\frac{r_1 - r_2}{\tau - 1}$. Thus, to give an upper bound for the number of collisions we can only evaluate the number of (r_1, r_2) such as $r_1 - r_2$ is divisible by $\tau - 1$.

It is easy to see that an element $a + b\tau$ of $\mathbb{Z}[\tau]$ is divisible by $\tau - 1$ if and only if $a + b$ is an even integer. Thus, for a random elements r_1, r_2 of $\mathbb{Z}[\tau]$ the probability that $r_1 - r_2$ is divisible by $\tau - 1$ is $\frac{1}{2}$. Consequently the number of collisions is at most

$$\frac{\#\{(r, \rho)\ /\ N(\rho) \leq\ N \text{ and } N(r)\ \leq\ N(\rho)\}}{2} \approx \alpha\frac{N^2}{4},$$

which complete the proof of the lemma. □

From Lemmas 2 and 3, we can conclude that the number of the randomized scalars obtained by our proposed method is approximately at least $\alpha\frac{N^2}{4}$.

Now suppose that for some required level of security, we may impose that $N(\rho) \approx N$ for the technique of Joye and Tymen. The length of the obtained τ-adic representation by the Joye and Tymen's technique is approximately $m + log_2(N(\rho))$, which penalizes the computation time by about $log_2(N(\rho))$ additional steps. To get the same level of security with our proposed technique, we will impose that norm of the random element ρ is only about $2\sqrt{N}$. Indeed, from the Lemma 2 and 3 the number of the obtained randomized scalars by our proposed technique is approximately $\alpha(\frac{(2\sqrt{N})^2}{4}) = \alpha N$, which is the the same one as that obtained by the Joye and Tymen's technique for $N(\rho) \approx N$ (Theorem 1).

On the other hand, the length of the obtained τ-NAF representation by our proposed method will be only $m + log_2(2\sqrt{N}) \approx m + \frac{log_2(N(\rho))}{2} + 1$, hence it penalizes the computation time by about $\frac{log_2(N(\rho))}{2} + 1$ additional steps, which is about the half of number of the additional steps caused by the Joye and Tymen technique. Thus, we can conclude that our proposed technique reduce the cost of the Joye and Tymen's one by about 50%.

6 Conclusion

In this paper, we have proposed an heuristic analysis on the security of the Joye and Tymen's countermeasure that aim to prevent the SCA attacks on the τ-NAF method for scalar multiplication on elliptic curve. We have also proposed an new method that improve this technique. Indeed our proposed method reduce the cost of Joye and Tymen's technique by about 50%.

References

[1] T. Akishita and T. Takagi, "Zero-value point attacks on elliptic curve crytosystems," in *ISC 2003* , LNCS 2851, pp. 218-233, Springer-Verlag, 2003.

[2] J. S. Coron, "Resistance against differential power analysis for elliptic curve cryptosystems," in *Cryptography Hardware and Embedded Systems-CHES'99*, LNCS 1717, pp. 292-302, Springer-Verlag, 1999.

[3] L. Goubin, "A refined power-analysis attack on elliptic curve cryptosystems," in *Public Key Cryptography International Workshop-PKC 2003*, LNCS 2567, pp. 199-210, Springer-Verlag, 2003.

[4] M. A. Hasan, "Power analysis attacks and algorithmic approaches to their countermeasures for Koblitz curve cryptosystems," in *Cryptography Hardware and Embedded Systems-CHES'00*, LNCS 1965, pp. 93-108, Springer-Verlag, 2000.

[5] K. Itoh, T. Izu, and M. Takenaka, "Efficient countermeasures against power analysis for elliptic curve cryptosystems," in *Proceedings of CARDIS-WCC 2004*, pp. 99-114, 2004.

[6] M. Joye and C. Tymen, "Protections against differential analysis for elliptic curve cryptography: An algebraic approach," in *Cryptography Hardware and Embedded Systems-CHES'01*, LNCS 2162, pp. 386-400, Springer-Verlag, 2001.

[7] N. Koblitz, "CM-curves with good cryptographic properties," in *CRYPTO'91*, J. Feigenbaum, editor, LNCS. 576, pp. 279-287, Springer-Verlag, 1991.

[8] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *CRYPTO'99*, LNCS 1666, pp. 388-397, Springer-Verlag, 1999.

[9] H. Mamiya, A. Miyaji, and H. Morimoto, "Efficient Countermeasures against RPA, DPA, and SPA," in *Cryptography Hardware and Embedded Systems-CHES'04*, LNCS 3156, pp. 343-356, Springer-Verlag, 2004.

[10] W. Meier and O. Staffelbach, "Efficient multiplication on certain nonsupersingular elliptic curves," in *CRYPTO'92*, LNCS 740, pp. 333-344, Springer-Verlag, 1992.

[11] A. Menezes, "Elliptic curve public key cryptosystems," *The Kluwer Academic publishers*, vol. 234, pp. 333-344, 1992.

[12] V. Müller, "Fast multiplication on elliptic curves over small fields of characteristic two," *Journal of Cryptology*, vol. 11, pp. 219-234, Jan. 1998.

[13] E. W. Smith, *The Implementation and Analysis of the ECDSA on the Motorola StarCore SC*140 *DSP Primarily Targeting Portable Devices* Master thesis, University of Waterloo, Ontario, Canada, 2002.

[14] J. A. Solinas, "An improved algorithm for arithmetic on a family of elliptic curves," in *Crypto 1997*, LNCS 1294, pp. 357-371, Springer-Verlag, 1997.

Mustapha Hedaboou received his M. Sc degree in Mathematics from the university of Paul Sabatier, Toulouse, France, in 2002. Currently, he is pursuing his Ph.D. degree in computer science at INSA de Toulouse, France. His area interest is Information Security and Public Key Cryptography based on Elliptic Curves.