Protecting ECC Against Fault Attacks:
The Ring Extension Method Revisited

Marc Joye
OneSpan
Brussels, Belgium
marc.joye@onespan.com

Abstract. Due to its shorter key size, elliptic curve cryptography (ECC) is gaining more and more popularity. However, if not properly implemented, the resulting cryptosystems may be susceptible to fault attacks. Over the past few years, several techniques for secure implementations have been published. This paper revisits the ring extension method and its adaptation to the elliptic curve setting.

Keywords: Elliptic curves; formal groups; degenerate curves, elliptic curve cryptosystems; fault attacks; countermeasures.

1 Introduction

This paper deals with secure implementations [24] for ECC-based cryptosystems [45,50,49,10,11,20] and, more specifically, with the development of efficient detection methods against fault attacks (or errors) [14]. Practical ways to mount fault attacks are surveyed in [4,27]. See also [41, Part III] for a more recent and complete account.

Fault Attacks and Countermeasures. A fault attack disturbs the expected behavior of a security device and makes it work abnormally so as to infer sensitive data. Since their discovery in 1997, several countermeasures were proposed. The key principle consists in computing a sensitive operation in a redundant way or in exploiting some redundancy already present in the calculation.

Shamir’s Countermeasure. Most known countermeasures rely on an elegant method first suggested by Shamir [58] for RSA [55] using Chinese remaindering [53]. These include [2,63,12,18,43,61] to name a few.

We follow the general presentation of [38]. Consider the ring \( \mathbb{Z}/N \mathbb{Z} \) of integers modulo \( N \) where \( N = pq \) is the product of two large primes. On input an element \( x \in \mathbb{Z}/N \mathbb{Z} \) (for example, \( x \) is a ciphertext or the hash value of a message) and a private exponent \( d \), the goal is to compute an RSA exponentiation, \( y = x^d \mod N \), in the presence of faults. In order to prevent fault attacks, the evaluation of \( y = x^d \mod N \) is carried out in three steps as follows.

1. Compute \( \hat{y} = x^d \mod rN \) for a (small) integer \( r \);
2. Compute \( y' = x^d \mod r \);
3. Check whether \( \hat{y} \equiv y' \) (mod \( r \)), and
   - if so, output \( y = \hat{y} \mod N \);
   - if not, return error.

Shamir’s method is an application of the Chinese remainder theorem (CRT). We obviously have \( \hat{y} \equiv y \) (mod \( N \)) and \( \hat{y} \equiv y' \) (mod \( r \)) when the computations are not faulty. In the presence of random faults, the probability that \( \hat{y} \equiv y \) (mod \( r \)) is about \( 1/r \). Larger values for \( r \) imply a higher detection probability, but at the expense of more demanding computations.
Vigilant’s countermeasure. Another method was proposed at CHES 2008 by Vigilant [61]. Again, the goal is to perform a private RSA exponentiation,
\[ y = x^d \mod N, \]
in the presence of faults. The method goes as follows.

1. Form \( X = \text{CRT}(x \mod N, 1 + r \mod r^2) \) for a (small) integer \( r \);
2. Compute \( \hat{y} = X^d \mod r^2 N \);
3. Check whether \( \hat{y} \equiv 1 + dr \mod r^2 \), and
   - if so, output \( y = \hat{y} \mod N \);
   - if not, return \text{error}.

In Step 1, \( \text{CRT}(.,.) \) denotes an application of the Chinese remainder theorem; namely, the so-constructed \( X \) satisfies \( X \equiv x \mod N \) and \( X \equiv 1 + r \mod r^2 \).

Remark 1. When Vigilant’s method is applied to RSA with Chinese remaindering, special care needs to be exercised. A number of potential fault attacks against RSA-CRT are presented in [21]; implementation recommendations are also provided.

Elliptic Curve Cryptography. Elliptic curve cryptography [45,50] is an interesting alternative to RSA because the keys are much shorter for a same conjectured security level. Given a point \( P \) on an elliptic curve \( E \) and a private integer \( d \), the basic operation consists in computing the scalar multiplication \([d] P\), that is,
\[ P \boxplus P \boxplus \cdots \boxplus P \] (\( d \) times) where \( \boxplus \) denotes the group operation on \( E \). The goal of an attacker is to recover the value of \( d \) (or a part thereof) by inducing faults. See [8,1,17,13,57,42,44,51] for examples of fault attacks against elliptic-curve cryptosystems.

Our Contributions. Vigilant’s method presents a couple of advantages over Shamir’s method. In particular, it trades the small exponentiation \( y' = x^d \mod r \) against the multiplication \( 1 + dr \mod r^2 = 1 + r \cdot (d \mod r) \) in the verification step. This latter operation is much faster. We note however that the evaluation of \( y' \) in Shamir’s method can be sped up as \( x^d \mod \varphi(r) \mod r \) (where \( \varphi \) denotes Euler’s totient function), provided that the value of \( \varphi(r) \) is known. The correctness of Vigilant’s countermeasure can be seen as a consequence of the binomial theorem. This latter states that
\[ (1 + r)^d = \sum_{j=0}^{d} \binom{d}{j} 1^{d-j} r^j = \sum_{j=0}^{d} \binom{d}{j} r^j = 1 + dr + \frac{d(d-1)}{2} r^2 + \cdots \]
Reducing this identity modulo \( r^2 \) yields \( (1 + r)^d \equiv 1 + dr \mod r^2 \). Hence, since by construction \( X \equiv 1 + r \mod r^2 \), the following relation holds modulo \( r^2 \):
\[ \hat{y} \equiv X^d \equiv (1 + r)^d \equiv 1 + dr \mod r^2 \].

Shamir’s countermeasure generalizes to the elliptic curve scalar multiplication (cf. Section 2). In contrast, Vigilant’s method does not readily lend itself to a generalization to elliptic curves. The reason is that there is no equivalent of the binomial theorem. We adopt a different approach and rely on the theory of formal groups as put forward in [26] for developing elliptic curve Paillier schemes. Doing so, we obtain a first efficient and versatile method to protect elliptic-curve cryptosystems against fault attacks.

It is well known that the singular elliptic curve over the finite prime field \( \mathbb{F}_r \) given by the Weierstraß equation \( y^2 = x^3 \) is isomorphic to the additive group \( \mathbb{F}_r^+ \); e.g., [34, Theorem 7.2]. Neves–Tibouchi [51] take advantage of this property to propose an efficient protection against fault attacks. They also extend their method to other models (including Edwards curves) with [less efficient] multiplicative isomorphisms. As a second contribution, we exhibit efficiently computable isomorphisms to the additive group \((\mathbb{Z}/r\mathbb{Z})^+ \) for all elliptic curve models commonly used in cryptographic applications. This results in a second efficient and versatile method to protect against fault attacks.

Organization. The rest of this paper is organized as follows. In the next section, we review variants of Shamir’s countermeasure applied to ECC systems. Section 3 describes our general methodology for detecting faults with two possible realizations. Next, in Section 4, we apply it to a variety of elliptic curve models. Finally, we conclude the paper in Section 5.
2 Overcoming Fault Attacks

Shamir’s method generalizes to the elliptic curve scalar multiplication. We review hereafter two different implementations. The first countermeasure is due to Blömer–Otto–Seifert and known as the BOS countermeasure [13] while the second one is due to Baek–Vasyltsov [3].

BOS countermeasure. As aforementioned, the main operation for elliptic curve cryptography is the scalar multiplication. Specifically, the usual setting is the computation of $Q = [d]P$ on an elliptic curve $E$ defined over the prime field $\mathbb{F}_p$, which is given by the Weierstraß equation $E$: $y^2 = x^3 + ax + b$. The BOS countermeasure proceeds in five steps:

1. For a (small) prime $r$, define an elliptic curve $E’$ over $\mathbb{F}_r$ and a point $P’$ on $E’$;
2. Form the combined curve $\tilde{E} = \text{CRT}(E, E’)$ over $\mathbb{Z}/pr\mathbb{Z}$ and the combined point $\tilde{P} = \text{CRT}(P, P’)$;
3. Compute $Q = [d]\tilde{P}$ on $\tilde{E}$;
4. Compute $Q’ = [d]P’$ on $E’$;
5. Check whether $\tilde{Q} \equiv Q’ \pmod{r}$, and
   - if so, output $Q = \tilde{Q} \pmod{p}$;
   - if not, return error.

Remark 2. If $y^2 = x^3 + ax + b$ is the equation defining the elliptic curve $E’$ over $\mathbb{F}_r$, $\text{CRT}(E, E’)$ denotes the elliptic curve over $\mathbb{Z}/pr\mathbb{Z}$ given by the equation $y^2 = x^3 + \hat{a}x + \hat{b}$ where $\hat{a} = \text{CRT}(a \pmod{p}, a’ \pmod{r})$ and $\hat{b} = \text{CRT}(b \pmod{p}, b’ \pmod{r})$; i.e., such $\hat{a} \equiv a \pmod{p}$ and $\hat{a} \equiv a’ \pmod{r}$, and idem for $\hat{b}$. Point $\tilde{P}$ is defined similarly from the coordinates of points $P$ and $P’$.

In a concrete implementation, prime $r$, curve $E’$ and point $P’$ are precomputed so that the order of point $P’$ on $E’$, $\text{ord}_{E’}(P’)$, is maximal. The value of $n’ := \text{ord}_{E’}(P’)$ together with $r$, the curve parameters and point $P’$ are stored in non-volatile memory. This presents the further advantage that the computation of $Q’$ in Step 4 can be performed more efficiently as $Q’ = [d \text{ mod } n’]P’$.

Baek–Vasyltsov’s countermeasure. Another variant of Shamir’s countermeasure was subsequently developed in [3]. Compared to the BOS countermeasure, in a practical setting, it does not require pre-computed values and does not assume that the parameter $r$ is prime.

Numerical experiments conducted in [36] however show that a non-negligible proportion of faults is undetected and that larger bit-lengths for $r$ should be used. For example, for a 20-bit randomizer $r$, the average proportion of undetected faults ranges from 23.2% to 37.3%. Moreover, by construction, Baek–Vasyltsov’s countermeasure is restricted to a special Weierstraß model and makes use of less efficient addition formulas.

3 The Ring Extension Method Revisited

In a way similar to Vigilant’s countermeasure for RSA, the adaptation of Shamir’s method to elliptic curves can be improved by finding a shortcut in the evaluation of $Q’ = [d]P’$ on $E’$ by an appropriate choice for $E’$ in the BOS countermeasure. Further, for more versatility and better efficiency, it should work for any randomizer $r$ (i.e., not only prime values) and without the need of pre-computing and pre-storing curve orders.

The core idea is to replace in the BOS countermeasure the combined curve $\tilde{E}$ with

$$E(\mathbb{F}_p) \times G’ \cong E(\mathbb{F}_p) \times (\mathbb{Z}/r\mathbb{Z})^+,$$

that is, a group isomorphic to the cross product of the groups $E(\mathbb{F}_p)$ and $(\mathbb{Z}/r\mathbb{Z})^+$ and where the group $G’$ is represented with elements having a group law that coincides (i.e., is compatible) with the group law used in the representation of $E(\mathbb{F}_p)$. 


We present two such realizations. In the first realization, $G'$ is chosen as the subgroup of points on an elliptic curve over $\mathbb{Z}/r^2\mathbb{Z}$ that reduce to the neutral point modulo $r$ [37]. The second realization modifies a recent countermeasure due to Neves and Tibouchi [51, §5]. The proposed methods are generic and can readily be adapted to any elliptic curve model and corresponding addition formulas. Also, although focusing on protecting elliptic curve computations over prime fields for the sake of concreteness, they can be generalized to elliptic curve computations over arbitrary fields, including over binary fields.

3.1 First Realization

It is useful to introduce some notation. Given a commutative ring $R$ with 1, we let $E(R)$ denote the set of rational points on an elliptic curve $E$ defined over $R$. For the ring $R = \mathbb{Z}/r^2\mathbb{Z}$ (namely, the ring of integers modulo $r^2$), we define the order-$r$ subgroup $G' := E_1(\mathbb{Z}/r^2\mathbb{Z}) = \{P \in E(\mathbb{Z}/r^2\mathbb{Z}) \mid P \text{ modulo } r \text{ reduces to } O\}$ where $O$ denotes the identity element on $E(\mathbb{Z}/r\mathbb{Z})$. The analogue of the combined curve $\hat{E}$ becomes $E(\mathbb{F}_p) \times E_1(\mathbb{Z}/r^2\mathbb{Z}) \subseteq E(\mathbb{Z}/r^2\mathbb{Z})$.

As will be made explicit in Section 4, the so-defined group $G'$ is isomorphic to $(\mathbb{Z}/r\mathbb{Z})^{+}$ and the isomorphisms

\[ \Upsilon_1: (\mathbb{Z}/r\mathbb{Z})^{+} \overset{\sim}{\longrightarrow} E_1(\mathbb{Z}/r^2\mathbb{Z}), \quad \{0 \mapsto \Upsilon_1(0) = O, \quad \vartheta \mapsto \Upsilon_1(\vartheta) = P \} \]

and $\Upsilon_1^{-1}$ are efficiently computable.

3.2 Second Realization

The authors of [51] suggest to choose $G'$ as the group of points on a degenerate curve over $\mathbb{F}_r$. However, most elliptic curve models (the Weierstraß model is a notable exception) do not have an additive degeneration: they either degenerate to the $(r - 1)$-order multiplicative group $\mathbb{F}_r^{\ast}$ or to the $(r + 1)$-order multiplicative subgroup $T_2(\mathbb{F}_r)$ of elements of norm 1 in $\mathbb{F}_r^{\ast}$ [56]. In this case, the shortcut function translates into an exponentiation modulo $r$ (degeneration to $\mathbb{F}_r^{\ast}$) or into the evaluation of Lucas sequences modulo $r$ (degeneration to $T_2(\mathbb{F}_r)$).

Actually, it turns out that we can always identify a group $G'$ isomorphic to $(\mathbb{Z}/r\mathbb{Z})^{+}$ from the group law in $E$ for a particular choice for the curve parameters; we call $E'$ the corresponding curve. We so define the $r$-order group

\[ G' := E'(\mathbb{Z}/r\mathbb{Z})[r] = \{P \text{ satisfying the curve equation } E' \text{ modulo } r \mid [r]P = O\} \]

for the particular curve equation $E'$. Again, this comes with efficiently computable isomorphisms

\[ \Upsilon_2: (\mathbb{Z}/r\mathbb{Z})^{+} \overset{\sim}{\longrightarrow} E'(\mathbb{Z}/r\mathbb{Z})[r], \quad \{0 \mapsto \Upsilon_2(0) = O, \quad \vartheta \mapsto \Upsilon_2(\vartheta) = P \} \]

and $\Upsilon_2^{-1}$. This will be illustrated in Section 4 with several elliptic curve models commonly used in cryptographic applications.

3.3 Implementation

The computation of $Q = [d]P$ on an elliptic curve $E(\mathbb{F}_p)$ in the presence of faults can be carried out as depicted in Algorithms 1 and 2. Algorithm 1 corresponds to the first realization and Algorithm 2 corresponds to the second realization.
The proposed methods apply to many elliptic curve models. This is illustrated below with the (twisted) $G$ implementations. The verification step (i.e., Step 5 in Algorithms 1 and 2) involves an $Q$ and 2) the resulting point $Q$ inducing a fault during the comparison

Implementation notes. It is worth noting that in the “redundancy” step (i.e., Step 4 in Algorithms 1 and 2) the resulting point $Q' = [d \mod r]T_1(\vartheta)$ (resp. $Q' = [d \mod r]T_2(\vartheta)$) is viewed as an element of $G' = E_1(\mathbb{Z}/r^2\mathbb{Z})$ (resp. of $G' = E'(\mathbb{Z}/r\mathbb{Z})[r]$). This is much faster than computing a scalar multiplication in $E(\mathbb{Z}/r^2\mathbb{Z})$ (resp. in $E'(\mathbb{Z}/r\mathbb{Z})$). This also allows the reduction of $d$ modulo $r$, the group order of $G'$.

Furthermore, single points of failure like conditional branchings should be avoided in fault-resistant implementations. The verification step (i.e., Step 5 in Algorithms 1 and 2) involves an if-branching. By inducing a fault during the comparison

$$(\hat{Q} \mod r^2) \not\equiv Q' \quad \text{(resp. } (\hat{Q} \mod r) \not\equiv Q')$$

an attacker may hope to force the comparison bit to 0 (i.e., false) and therefore get the value of $\hat{Q} \mod p$. The if-branching can however be avoided by making use of the so-called “infective computation” technique [63].

For better fault coverage, it is recommended to choose $\vartheta$ in Step 1 of Algorithms 1 and 2 so that $P'$ is of maximal order (i.e., of order $r$). Obtaining a generator for the additive group $(\mathbb{Z}/r\mathbb{Z})^+$ is fairly easy since any non-zero integer co-prime to $r$ generates $(\mathbb{Z}/r\mathbb{Z})^+$. Two possible strategies are:

1. Take 1 as a generator or fix a priori a prime $\vartheta$ larger than the maximum value for $r$. Then $(\mathbb{Z}/r\mathbb{Z})^+ = \langle 1 \rangle$ or $(\mathbb{Z}/r\mathbb{Z})^+ = \langle \vartheta \rangle$.
2. Select $r$ as a prime number. Then any non-zero integer $0 < \vartheta < r$ is a generator of $(\mathbb{Z}/r\mathbb{Z})^+$.

The first strategy is preferred as it does not impose conditions on $r$.

4 Illustration

The proposed methods apply to many elliptic curve models. This is illustrated below with the (twisted) Edwards model and the Weierstraß model. Applications to further models can be found in Appendix A.
4.1 Edwards Model

In [23], Edwards proposed a normal form for elliptic curves. It was later extended in [7] and subsequently in [5] (see also [30]). The latter form, referred to as the twisted Edwards form, is given by the equation

$$E_{E_a,d} : ax^2 + y^2 = 1 + dx^2 y^2 .$$

(1)

The neutral element is $O = (0, 1)$. The addition law is unified. Given two points $(x_1, y_1)$ and $(x_2, y_2)$, their sum $(x_3, y_3) = (x_1, y_1) \oplus (x_2, y_2)$ is given by

$$(x_3, y_3) = \left( \frac{x_1 y_2 + x_2 y_1 - ax_1 x_2}{1 + dx_1 x_2 y_1 y_2}, \frac{y_1 y_2 - ax_1 x_2}{1 - dx_1 x_2 y_1 y_2} \right).$$

(2)

First Realization. We define:

$$E_{E_a,d,1}(\mathbb{Z}/r^2\mathbb{Z}) = \{ Y_1(\vartheta) = (\vartheta \cdot r, 1) \mid \vartheta \in \mathbb{Z}/r\mathbb{Z} \} \cong (\mathbb{Z}/r\mathbb{Z})^+ .$$

(3)

In words, the group $G' = E_{E_a,d,1}(\mathbb{Z}/r^2\mathbb{Z})$ is the set of points $(x, 1) = (\vartheta \cdot r, 1)$ on an Edwards curve (1) over the ring $\mathbb{Z}/r^2\mathbb{Z}$, equipped with the addition law (2). It is easily verified that:

1. $Y_1(\vartheta) \equiv (\vartheta \cdot r, 1) \equiv (0, 1) \equiv O \pmod{r}$, and
2. $Y_1(\vartheta_1) \oplus Y_1(\vartheta_2) = (\vartheta_1 \cdot r, 1) \oplus (\vartheta_2 \cdot r, 1) = \left( \frac{\vartheta_1 + \vartheta_2 - r}{1}, \frac{1}{1} \right) = ((\vartheta_1 + \vartheta_2) \cdot r, 1)$

as desired. We also have $E_{E_a,d,1}(\mathbb{Z}/r^2\mathbb{Z}) = \langle (r, 1) \rangle$.

Second Realization. We have:

$$(\mathbb{Z}/r\mathbb{Z})^+ \cong E'_{e_{o,0}}(\mathbb{Z}/r\mathbb{Z})[r] = \{ Y_2(\vartheta) = (\vartheta, 1) \mid \vartheta \in \mathbb{Z}/r\mathbb{Z} \} \subseteq \{ (x, y) \in E'_{e_{o,0}}(\mathbb{Z}/r\mathbb{Z}) \}.$$

(4)

In more detail, the group $G' = E'_{e_{o,0}}(\mathbb{Z}/r\mathbb{Z})[r]$ is the set of points $(x, 1)$ on an Edwards curve $E'$ given by Eq. (1) with parameters $a = d = 0$, over the ring $\mathbb{Z}/r\mathbb{Z}$, equipped with the addition law (2). When $a = d = 0$, it immediately follows that:

1. $Y_2(0) = (0, 1) = O$, and
2. $Y_2(\vartheta_1) \oplus Y_2(\vartheta_2) = (\vartheta_1, 1) \oplus (\vartheta_2, 1) = \left( \frac{\vartheta_1 + \vartheta_2 - 1}{1}, \frac{1}{1} \right) = ((\vartheta_1 + \vartheta_2), 1) = Y_2(\vartheta_1 + \vartheta_2)$;

and $E'_{e_{o,0}}(\mathbb{Z}/r\mathbb{Z})[r] = \langle (1, 1) \rangle$.

4.2 Weierstraß Model

The Weierstraß model (e.g., [59, Chapter III]) is the most common way to represent an elliptic curve. It is given by the equation $E_{W_{a,b}} : y^2 = x^3 + ax + b$ or, using projective coordinates,

$$E_{W_{a,b}} : Y^2 Z = X^3 + aXZ^2 + bZ^3 .$$

(5)

The neutral element is the point at infinity $O = (0 : 1 : 0)$. A unified addition formula [46, Section 3] (see also [47,15,35,54]) for adding two projective points $(X_1 : Y_1 : Z_1)$ and $(X_2 : Y_2 : Z_2)$ is given by

$$X_3 = (Y_1Z_2 + Y_2Z_1) A + (X_1Y_2 + X_2Y_1) B$$

$$Y_3 = (X_1Z_2 + X_2Z_1) M + (Y_1Y_2 + 3bZ_1Z_2)(Y_1Y_2 - 3bZ_1Z_2) - aN$$

$$Z_3 = (X_1Y_2 + X_2Y_1)(aZ_1Z_2 + 3X_1X_2) + (Y_1Z_2 + Y_2Z_1)V$$

with $A = a(X_1Z_2 - X_1X_2) - 3b(X_1Z_2 + X_2Z_1), B = Y_1Y_2 - a(X_1Z_2 + X_2Z_1) - 3bZ_1Z_2, M = 3b(3X_1X_2 - aZ_1Z_2) - a^3(X_1Z_2 + X_2Z_1), N = (aZ_1Z_2 + 3X_1X_2)(aZ_1Z_2 - X_1X_2), and V = Y_1Y_2 + 3bZ_1Z_2 + a(X_1Z_2 + X_2Z_1)$. As detailed in [54, Algorithm 1], this can be evaluated with only 12 general multiplications plus 5 multiplications by constants (namely, $a$ and $3b$).
First Realization. We define:

\[ E_{W_{a,b,1}}(\mathbb{Z}/r^2\mathbb{Z}) = \{ Y_1(\vartheta) = (\vartheta \cdot r : 1 : 0) \mid \vartheta \in \mathbb{Z}/r\mathbb{Z} \} \cong (\mathbb{Z}/r\mathbb{Z})^+. \]  

(7)

Here again, it can be verified that \( Y_1(\vartheta_1) \equiv (\vartheta \cdot r : 1 : 0) \equiv (0 : 1 : 0) \equiv O \) (mod \( r \)) and that the addition formula (6) yields \( Y_1(\vartheta_1) \oplus Y_1(\vartheta_2) = (\vartheta_1 \cdot r : 1 : 0) \oplus (\vartheta_2 \cdot r : 1 : 0) = ((\vartheta_1 + \vartheta_2) \cdot r : 1 : 0) = Y_1(\vartheta_1 + \vartheta_2) \) by observing that we then have \( A = 0, B = 1, M = N = 0, V = 1 \) and thus \( (X_1 : Y_3 : Z_3) = ((\vartheta_1 \cdot r \cdot 1 + \vartheta_2 \cdot r \cdot 1) \cdot 1 : 1 : 1 : (\vartheta_1 \cdot r \cdot 1 + \vartheta_2 \cdot r \cdot 1) \cdot 0 + 0 \cdot 1) = ((\vartheta_1 + \vartheta_2) \cdot r : 1 : 0) \). We also have \( E_{W_{a,b,1}}(\mathbb{Z}/r^2\mathbb{Z}) = \langle (r : 1 : 0) \rangle \).

Second Realization. We have:

\[ (\mathbb{Z}/r\mathbb{Z})^+ \cong E'_{W_{0,0}}(\mathbb{Z}/r\mathbb{Z})[r] = \{ Y_2(\vartheta) = (\vartheta : 1 : \vartheta^3) \mid \vartheta \in \mathbb{Z}/r\mathbb{Z} \} \subseteq \{(X : Y : Z) \in E'_{W_{0,0}}(\mathbb{Z}/r\mathbb{Z}) \}. \]  

(8)

Similarly to the first realization, it can be verified that \( Y_2(0) = (0 : 1 : 0) = O \) and, when \( a = b = 0 \), that the addition formula (6) yields \( Y_2(\vartheta_1) \oplus Y_2(\vartheta_2) = (\vartheta_1 : 1 : \vartheta_1^3) \oplus (\vartheta_2 : 1 : \vartheta_2^3) = (\vartheta_1 + \vartheta_2 : 1 : (\vartheta_1 + \vartheta_2) \cdot 1 \cdot \vartheta_1 + \vartheta_1^3) = (\vartheta_1 + \vartheta_2 : 1 : (\vartheta_1 + \vartheta_2)^3) = Y_2(\vartheta_1 + \vartheta_2) \); and \( E'_{W_{0,0}}(\mathbb{Z}/r\mathbb{Z})[r] = \langle (1 : 1 : 1) \rangle \).

4.3 Comparison

The proposed methods share the advantages (but not the weaknesses!) of the Baek–Vasyltsov’s countermeasure: they do not require pre-computed values in some non-volatile memory and do not suppose randomizer \( r \) to be prime. Furthermore, they are more general as they are not restricted to a special type of Weierstrass parametrization.

Another advantage of the proposed methods is that they carry the completeness of the addition law, whatever the choice of the parameters. For example, for twisted Edwards curves, completeness is guaranteed provided that curve parameter \( a \) is a square and curve parameter \( d \) is a non-square. Further, twisted Edwards curves as given by Eq. (1) do not hold in characteristic 2. There are no such restrictions on \( G' = E'_{\mathbb{Z},a,1}(\mathbb{Z}/r^2\mathbb{Z}) \) (cf. (3)) or on \( G' = E'_{\mathbb{Z},a,0}(\mathbb{Z}/r\mathbb{Z})[r] \) (cf. (4)). Indeed, for any points \( P_1 = (\vartheta_1 \cdot r, 1) \) and \( P_2 = (\vartheta_2 \cdot r, 1) \) in \( E'_{\mathbb{Z},a,1}(\mathbb{Z}/r^2\mathbb{Z}) \) (resp. \( P_1 = (\vartheta_1, 1) \) and \( P_2 = (\vartheta_2, 1) \) in \( E'_{\mathbb{Z},a,0}(\mathbb{Z}/r\mathbb{Z})[r] \)), the addition formula given by Eq. (2) remains always valid since the denominators always are equal to 1 and thus are invertible modulo \( r^2 \) (resp. modulo \( r \)), including for even values for \( r \). The same conclusion holds true for the completeness of the Weierstrass model as described in §4.2 and the other models given in appendix.

Furthermore, unlike the BOS countermeasure, the order of the small curve is known in advance: by construction, we have \#\( G' \equiv (\mathbb{Z}/r\mathbb{Z})^+ \). Scalar \( d \) in the computation of \( Q' \) in \( E_1(\mathbb{Z}/r^2\mathbb{Z}) \) (resp. \( E'(\mathbb{Z}/r\mathbb{Z}) \)) can therefore be reduced modulo \( r \). Because the BOS countermeasure makes use of general groups of points on an elliptic curve, the group order is not so easily obtained: this is addressed by fixing randomizer \( r \) once and for all and by pre-computing (and storing) the group order for the curve modulo \( r \). In our case, randomizer \( r \) can be freely selected on the fly, with a fresh value for each execution. In addition to better efficiency and easier implementation, this offers better security guarantees and fault coverage.

Finally, the verification step essentially boils down to a mere modular multiplication modulo \( r \) rather than a full scalar multiplication on an elliptic curve.

5 Conclusion

This paper revisited the ring extension method over elliptic curves as presented in [13,3]. The proposed approaches apply to a variety of elliptic models and provide more practical countermeasures against fault attacks.
References


A Further Models

A.1 Jacobi Quartic Model

The (extended) Jacobi quartic model is presented in [9] (see also [16,22,29,31]). Its curve equation is given by

\[ E_{a,d}: y^2 = dx^4 + 2ax^2 + 1 \]
with \( O = (0, 1) \) as the neutral element. The unified addition of two points \((x_1, y_1)\) and \((x_2, y_2)\), \((x_3, y_3) = (x_1, y_1) \boxplus (x_2, y_2)\), is given by

\[
(x_3, y_3) = \left( \frac{x_1 y_2 + x_2 y_1}{1 - dx_1^2 x_2^2}, \frac{1 + dx_1^2 x_2^2}{1 - dx_1^2 x_2^2} (y_1 y_2 + 2ax_1 x_2) + 2dx_1 x_2 (x_1^2 + x_2^2) \right)
\]

[The original Jacobi quartics correspond to the case \( d = k^2 \) and \(-2a = 1 + k^2\) for some parameter \( k \).]

**First Realization.** We define:

\[
E_{d,a,1}(\mathbb{Z}/r^2\mathbb{Z}) = \{ Y_1(\vartheta) = (\vartheta \cdot r, 1) \mid \vartheta \in \mathbb{Z}/r\mathbb{Z} \} \cong (\mathbb{Z}/r\mathbb{Z})^+.\]

Analogously to the Edwards model (cf. §4.1), it is easily verified that \( Y_1(0) \equiv (0, 1) \equiv (0, 1) \equiv O \pmod{r} \) and that \( Y_1(1) \boxplus Y_1(2) = (1 \cdot 1, 1) \boxplus (1, 1) = \left( \frac{2r^2 - 1}{1 - r^2}, \frac{1}{1 - r^2} \right) = ((1 + 0) \cdot r, 1) = Y_1(1 + 0).\)

**Second Realization.** We have:

\[
(\mathbb{Z}/r\mathbb{Z})^+ \cong E'_{d,a,o}(\mathbb{Z}/r\mathbb{Z})[r] = \{ Y_2(\vartheta) = (1, \vartheta) \mid \vartheta \in \mathbb{Z}/r\mathbb{Z} \} \subseteq \{ (x, y) \in E'_{d,a,o}(\mathbb{Z}/r\mathbb{Z}) \}.\]

As for the Edwards model, we have \( Y_2(0) = (0, 1) = O \) and, when \( a = d = 0 \), \( Y_2(1) \boxplus Y_2(2) = (1, 1) \boxplus (2, 1) = (2, 1) \boxplus (2, 1) = (2, 1) \).

### A.2 Jacobi Quadrics Intersection Model

Another way to represent an elliptic curve is as the intersection of two quadrics in \( \mathbb{P}^3 \) (see, e.g., [16]). Applications to cryptography are discussed in [16,29,48]. The most general form [32] reads as

\[
E_{Q,a,b}: \begin{cases} ax^2 + y^2 = 1 \\ bx^2 + z^2 = 1 \end{cases}.
\]

The neutral element is \( O = (0, 1, 1) \). The unified sum of two points \((x_1, y_1, z_1)\) and \((x_2, y_2, z_2)\) is given by \((x_3, y_3, z_3) = (x_1, y_1, z_1) \boxplus (x_2, y_2, z_2)\) where

\[
(x_3, y_3, z_3) = \left( \frac{x_1 y_2 z_2 + x_2 y_1 z_1}{1 - abx_1^2 x_2^2}, \frac{y_1 y_2 - ax_1 z_1 x_2 z_2}{1 - abx_1^2 x_2^2}, \frac{z_1 z_2 - bx_1 y_1 x_2 y_2}{1 - abx_1^2 x_2^2} \right).
\]

**First Realization.** We define:

\[
E_{Q,a,b}(\mathbb{Z}/r^2\mathbb{Z}) = \{ Y_1(\vartheta) = (\vartheta \cdot r, 1, 1) \mid \vartheta \in \mathbb{Z}/r\mathbb{Z} \} \cong (\mathbb{Z}/r\mathbb{Z})^+.\]

A straightforward calculation shows that \( Y_1(0) \equiv (0, 1, 1) \equiv (0, 1, 1) \equiv O \pmod{r} \) and that \( Y_1(1) \boxplus Y_1(2) = (1 \cdot 1, 1, 1) \boxplus (1, 1, 1) = \left( \frac{2r^2 - 1}{1 - r^2}, \frac{1}{1 - r^2}, \frac{1}{1 - r^2} \right) = ((1 + 0) \cdot r, 1, 1) = Y_1(1 + 0).\)

**Second Realization.** We have:

\[
(\mathbb{Z}/r\mathbb{Z})^+ \cong E'_{Q,a,o}(\mathbb{Z}/r\mathbb{Z})[r] = \{ Y(\vartheta) = (1, \vartheta, 1) \mid \vartheta \in \mathbb{Z}/r\mathbb{Z} \} \subseteq \{ (x, y, z) \in E'_{Q,a,o}(\mathbb{Z}/r\mathbb{Z}) \}.
\]

It can be checked that \( Y_2(0) = (0, 1, 1) = O \) and, when \( a = b = 0 \), \( Y_2(1) \boxplus Y_2(2) = (1, 1, 1) \boxplus (2, 1, 1) = (2, 1, 1) \).
A.3 Hessian Model

Hessian curves [28] were generalized, modified, and extended for cryptographic applications in several works, including [39,60,6,25]. We follow the presentation of [6] where the neutral element is \(O = (0, -1)\). The curve equation is

\[
E_{\vartheta,a,d} : ax^3 + y^3 + 1 = dxy.
\]

The unified sum \((x_3, y_3) = (x_1, y_1) \oplus (x_2, y_2)\) of two points \((x_1, y_1)\) and \((x_2, y_2)\) is given by

\[
(x_3, y_3) = \left( \frac{x_1 - y_1^2x_2y_2}{ax_1y_1x_2^2 - y_2}, \frac{y_1y_2^2 - ax_1^2x_2}{ax_1y_1x_2^2 - y_2} \right).
\]

First Realization. We define:

\[
E_{\vartheta,a,d,1}(\mathbb{Z}/r\mathbb{Z}) = \{ \mathcal{T}_1(\vartheta) = (3\vartheta \cdot r, -1 - d\vartheta \cdot r) \mid \vartheta \in \mathbb{Z}/r\mathbb{Z} \} \cong (\mathbb{Z}/r\mathbb{Z})^+.
\]

Again, it can be verified that \(\mathcal{T}_1(\vartheta) \equiv (3\vartheta \cdot r, -1 - d\vartheta \cdot r) \equiv (0, -1) \equiv \mathcal{T}_1(0) \equiv O \) (mod \(r\)). A quick inspection shows that the above addition law for computing \(\mathcal{T}_1(\vartheta_1) \oplus \mathcal{T}_1(\vartheta_2) = (3\vartheta_1 \cdot r, -1 - d\vartheta_1 \cdot r) \oplus (3\vartheta_2 \cdot r, -1 - d\vartheta_2 \cdot r)\) incurs the value of \((-1 - d\vartheta_2 \cdot r) = 1 + d\vartheta_2 \cdot r\) in the denominator. We therefore must have \(d\vartheta_2 \cdot r \neq -1\) (mod \(r^2\)). This is always satisfied since \(d\vartheta_2 \cdot r \equiv -1\) (mod \(r^2\)) would imply \(0 \equiv -1\) (mod \(r\)). Hence, the sum is always defined and is given by as \(\mathcal{T}_1(\vartheta_1) \oplus \mathcal{T}_1(\vartheta_2) = \left(\frac{3\vartheta_1 \cdot r + 3\vartheta_2 \cdot r}{1 + d\vartheta_2 \cdot r}, \frac{-1 - d\vartheta_1 \cdot r - d\vartheta_2 \cdot r}{-1 - d\vartheta_2 \cdot r}\right) = (3(\vartheta_1 + \vartheta_2) \cdot r, -1 - d(\vartheta_1 + \vartheta_2) \cdot r) = \mathcal{T}_1(\vartheta_1 + \vartheta_2),\)

noting that \((1 + d\vartheta_2 \cdot r)^{-1} = 1 - d\vartheta_2 \cdot r\) and that \((3\vartheta_1 \cdot r + 3\vartheta_2 \cdot r)(1 - d\vartheta_2 \cdot r) = 3(\vartheta_1 + \vartheta_2) \cdot r\).

Second Realization. We have:

\[
(\mathbb{Z}/r\mathbb{Z})^+ \cong E'_{\vartheta,a,o}(\mathbb{Z}/r\mathbb{Z})[r] = \{ \mathcal{T}_2(\vartheta) = (\vartheta, -1) \mid \vartheta \in \mathbb{Z}/r\mathbb{Z} \} \subseteq \{ (x, y) \in E'_{\vartheta,a,o}(\mathbb{Z}/r\mathbb{Z}) \}.
\]

Likewise, we have \(\mathcal{T}_2(0) = (0, -1) = O\) and the addition law when \(a = d = 0\) yields \(\mathcal{T}_2(\vartheta_1) \oplus \mathcal{T}_2(\vartheta_2) = (\vartheta_1, -1) \oplus (\vartheta_2, -1) = \left(\frac{\vartheta_1 - (1)^2\vartheta_2(-1)}{-1}, \frac{(1)(-1)^2}{-1}\right) = (\vartheta_1 + \vartheta_2, -1) = \mathcal{T}_2(\vartheta_1 + \vartheta_2).

A.4 Huff’s Model

Huff curves, after [33], were introduced for cryptographic applications in [40]. The most general form as presented in [52] (see also [19,62]) is given by the equation

\[
E_{H,a,c,d} : y(ax^2 + 1) = cx(dy^2 + 1)
\]

with neutral element \(O = (0, 0)\). The unified addition formula of points \((x_1, y_1)\) and \((x_2, y_2)\) is given by

\[
(x_3, y_3) = \left( \frac{(x_1 + x_2)(1 - dy_1y_2)}{(1 - ax_1x_2)(1 + dy_1y_2)}, \frac{(y_1 + y_2)(1 - ax_1x_2)}{(1 + ax_1x_2)(1 + dy_1y_2)} \right).
\]

First Realization. We define:

\[
E_{H,a,c,d,1}(\mathbb{Z}/r^2\mathbb{Z}) = \{ \mathcal{T}_1(\vartheta) = (\vartheta \cdot r, c \vartheta \cdot r) \mid \vartheta \in \mathbb{Z}/r\mathbb{Z} \} \cong (\mathbb{Z}/r\mathbb{Z})^+.
\]

The correctness follows by observing that \(\mathcal{T}_1(\vartheta) \equiv (\vartheta \cdot r, c \vartheta \cdot r) \equiv (0, 0) \equiv \mathcal{T}_1(0) \equiv O \) (mod \(r\)) and that the addition law leads to \(\mathcal{T}_1(\vartheta_1) \oplus \mathcal{T}_1(\vartheta_2) = (\vartheta_1 \cdot r, c \vartheta_1 \cdot r) \oplus (\vartheta_2 \cdot r, c \vartheta_2 \cdot r) = \left(\frac{(\vartheta_1 \cdot r + \vartheta_2 \cdot r)}{1}, \frac{(c \vartheta_1 \cdot r + c \vartheta_2 \cdot r)}{1}\right) = (\vartheta_1 + \vartheta_2 \cdot r, c(\vartheta_1 + \vartheta_2) \cdot r) = \mathcal{T}_1(\vartheta_1 + \vartheta_2).

Second Realization. Fix \(\bar{c} \in \mathbb{Z}/r\mathbb{Z}\). We have:

\[
(\mathbb{Z}/r\mathbb{Z})^+ \cong E'_{H,a,c,d}(\mathbb{Z}/r\mathbb{Z})[r] = \{ \mathcal{T}_2(\vartheta) = (\vartheta, \bar{c} \cdot \vartheta) \mid \vartheta \in \mathbb{Z}/r\mathbb{Z} \} \subseteq \{ (x, y) \in E'_{H,a,c,d}(\mathbb{Z}/r\mathbb{Z}) \}.
\]

We observe that \(\mathcal{T}_2(0) = (0, 0) = O\) and, when \((a, c, d) = (0, \bar{c}, 0)\), the addition law gives \(\mathcal{T}_2(\vartheta_1) \oplus \mathcal{T}_2(\vartheta_2) = (\vartheta_1, \bar{c} \cdot \vartheta_1) \oplus (\vartheta_2, \bar{c} \cdot \vartheta_2) = (\vartheta_1 + \vartheta_2, \bar{c} \cdot \vartheta_1 + \bar{c} \cdot \vartheta_2) = \mathcal{T}_2(\vartheta_1 + \vartheta_2).\)