Pol. J. Appl. Sci., **2017**, *3*, 141-145

# ANALYSIS OF THE CERTAIN CRYTOGRAPHIC PROBLEMS IN PROTOCOLS OF CERTYFING THE NODES IN IOT INFRACTRUCURE

Wiesław Maleszewski

*Faculty of Computer Science and Food Science*
*Lomza State University of Applied Sciences, Lomza, Poland*

E-mail: wmaleszewski@pwsip.edu.pl

**Abstract:** Beginning with the basic issues of number theory and cryptographic theory, selected factorization algorithms and problems associated with cryptographic algorithms based on elliptic curve isogenies are presented in this paper.

**Key words:** elliptic curves cryptography, Edwards curve, fast operations, factoring algorithms, isogeny.

## Introduction

For some time now, we have observed the dynamic development of solutions offered by the Internet of Things. These solutions are dedicated to the various areas of human activity, beginning with tools that monitor our life functions, optimize the performance of devices in homes, help to protect the environment by reducing energy consumption or optimize the operation of urban traffic control systems, and ending with systems supporting the operation of large companies and factories. This development, on the one hand, makes us optimistic about the fact that our functioning is becoming more and more environmentally friendly and easier. On the other hand, we are aware of the ever-increasing threats to our privacy and security. The increase in the importance and applicability of various methods of information exchange contributes to the expansion of cryptography, which had initially been only the domain of the military and intelligence operatives. A major challenge for today's cryptography is the need to reduce the computational costs of the solutions used, while maintaining adequate security guarantees. This situation contributes to the search for cryptographic algorithms that provide similar, or greater security than the popular RSA, and which will generate lower computational costs. A good example of such algorithms are algorithms based on elliptic curves. These curves are also very helpful in the research into factorization problems on which today's cryptographic systems are based. What is more, if we look closer at elliptic curves and algebraic geometry, we will discover the problem of elliptic curves based on isogenies, which is very important from the perspective of post-quantum cryptography. In our work we focus on the problem of factorization and pay special attention to the tools the use of which may contribute to the development of new solutions to improve the level of security.

## Fermat's little Theorem

If $p$ is a prime number and $a \in \mathbb{N}$, then

$$a^p \equiv a \pmod{p}.$$

Further, if $\gcd(a, p) = 1$

$$a^{p-1} \equiv 1 \pmod{p}.$$

## Elliptic curves

An elliptic curve $E$ over a field $F$ can be given by the Weierstrass equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where the coefficients $a_1, a_2, a_3, a_4, a_6 \in E$. Koblitz [1] and Miller [2] were the first to show that the group of rational points on an elliptic curve $E$ over a finite field $F_q$ could be used for the discrete logarithm problem in a public-key cryptosystem.

The canonical short Weierstrass form of an elliptic curve is given by the equation:

$$y^2 = x^3 + ax + b,$$

together with a point at infinity $\mathcal{O}$ where the constants $a, b$ meet the additional condition:

$$4a^3 + 27b^2 \neq 0.$$

*The algorithm of adding points on the elliptic curve*

Let $E$ be an elliptic curve, and $M_1, M_2 \in E$, where $M_1 = (x_1, y_1)$, $M_2 = (x_2, y_2)$, $M_3 = (x_3, y_3)$ and $M_3 = M_1 + M_2$, [3, 4] then:

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases},$$

where:

$$\lambda = \begin{cases} \frac{y_2-y_1}{x_2-x_1} & if \quad (x_1,y_1) \neq (x_2,\pm y_2) \\ \frac{3x_1^2+a}{2y_1} & if \quad (x_1,y_1) = (x_2,\pm y_2) \end{cases} .$$

## Elliptic Curves Cryptography

ECC is an asymmetric cryptographic algorithm which involves some high-level calculation using mathematical curves to encrypt and decrypt data. It is similar to RSA as it is asymmetric, but it uses a very small length key as compared to RSA. ECC is an asymmetric cryptographic algorithm which involves the following steps [5, 6].

*ECC Encryption*

1. Define a curve.
2. Generate a public private key pair using that curve for sender and receiver.
3. Generate a shared secret key from the key pair.
4. From that shared secret key, generate an encryption key.
5. Using that encryption key and symmetric encryption algorithm, encrypt the data to send.

*ECC Decryption*

The sender will either share the curve with receiver, or the sender and the receiver will have the same use for the same curve type. Also, the sender will share its public key with the receiver.

1. Generate a public private key pair using the same curve for that curve. for the receiver.
2. Regenerate a shared secret key using a private key of the receiver and public key of the sender.
3. From that shared secret key, generate an encryption key.
4. Using that encryption key and symmetric encryption algorithm, decrypt the data.

## Edwards curve

Edwards introduced a normal form for elliptic curves which allowed the addition law to be stated explicitly and completely. Additionally, Bernstein and Lange introduced fast formulas for the group operations on Edwards curves showing that these were in fact faster than those for most of the other models for elliptic curves known at that time. Edwards curves are thus gaining popularity in cryptographic applications.

**Definition 0.1.** Let $K$ be a field with $char(K) \neq 2$. Then an Edwards curve $E$ over $K$ is a curve

$$x^2 + y^2 = 1 + dx^2y^2$$

Where $d \in K \setminus \{0, 1\}$. Bernstein, et. al. in [7] introduced twisted Edwards curves which are curves of the form:

$$ax^2 + y^2 = 1 + dx^2y^2,$$

where $a, d \in K$ are distinct and nonzero [8, 9].

*Edwards addition law*

Let $E$ be an Edwards curve over a finite field $K$ and $char(K) \neq 2$. Let $M_1 = (x_1, y_1)$ and $M_2 = (x_2, y_2)$ be points on $E$. We then define $M_3 = M_1 + M_2$ as [10]:

$$M_3 = \left( \frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

and similarly define $M_4 = 2M_1$ as:

$$M_4 = \left( \frac{2x_1y_1}{1 + dx_1^2y_1^2}, \frac{y_1^2 - x_1^2}{1 - dx_1^2y_1^2} \right)$$

*Result* 0.2. The zero element of the Edwards addition law is $(0; 1)$.

Proof Let $M = (x, y)$ and $O = (0, 1)$. Then, from the addition law,

$$M+O = (x, y)+(0, 1) = \left( \frac{x + 0}{1 + d \cdot 0}, \frac{y - 0}{1 - d \cdot 0} \right) = (x, y) = M$$

*Result* 0.3. Result The inverse of any point $(x_1, y_1)$ is $(-x_1, y_1)$.

## Fast formulas for group operations

Bernstein and Lange studied Edwards curves in the context of cryptographic applications and concluded that the Edwards curve supports faster addition and doubling. They consider projective coordinates for their computations in order to avoid inversions, as it appeared in the original Edwards addition law. The Edwards form in the projective coordinates is given by

$$x^2 + y^2 = c^2(z^4 + dx^2y^2)$$

where the corresponding affine coordinates $(x, y)$ of a projective point $(x, y, z)$ with $z \neq 0$ are given by

$$(x, y) = \left( \frac{x}{z}, \frac{y}{z} \right)$$

This article will only present the operations of addition and doubling. More can be found in the literature [10].

**Addition** Given the points $(x_1, y_1, z_1)$ and $(x_2, y_2, z_2)$, the sum $(x_3, y_3, z_3) = (x_1, y_1, z_1) + (x_2, y_2, z_2)$ is computed using the following sequence of operations:

$$\begin{aligned} A &= z_1 \cdot z_2, \\ B &= A^2, \\ C &= x_1 \cdot x_2, \\ D &= y_1 \cdot y_2, \\ E &= d \cdot C \cdot D, \\ F &= B - E, \\ G &= B + E, \end{aligned}$$

$$\begin{cases} x_3 = A \cdot F \cdot (x_1 + y_1) \cdot (x_2 + y_2) - C - D) \\ y_3 = A \cdot G \cdot (D - C) \\ z_3 = c \cdot F \cdot G \end{cases}.$$

Assuming the notations below
$M$ - cost of general multiplication
$S$ - cost of squaring
$C$ - cost of multiplication by the Edwards parameter $c$
$D$ - cost of multiplication by the Edwards parameter $d$
$a$ - cost of addition/subtraction
it is easy to infer that the cost of an operation is

$$10M + 1S + 1C + 1D + 7a.$$

Doubling refers to the case when $(x_1, y_1, z_1) = (x_2, y_2, z_2)$ We save further operations by computing $2xy$ as

$$(x + y)^2 - x^2 - y^2$$

and using common subexpressions as is done in the case of addition:

$$\begin{aligned} B &= (x_1 + x_2)^2, \\ C &= x_1^2, \\ D &= y_1^2, \\ E &= C + D, \\ H &= Z_1^2, \\ J &= E - 2H, \end{aligned}$$

$$\begin{cases} x_3 = (B - E) \cdot J \\ y_3 = E \cdot (C - D) \\ z_3 = E \cdot J \end{cases}.$$

The cost of doubling operation is $3M + 4S + 6a$.

## Other family of curves

**Hessian curves** The Hessian curves, introduced in [11], by the formula

$$x^3 + y^3 + 1 = 3dxy$$

with $d^3 - 1 \neq 0$ and a point $\mathscr{O} = (1, -1)$ as neutral element. The group law is given by:

$$(x_3, y_3) = \begin{cases} \left(\frac{y_1^2 x_2 - y_2^2 x_1}{x_2 y_2 - x_1 y_1}, \frac{x_1^2 y_2 - x_2^2 y_1}{x_2 y_2 - x_1 y_1}\right) & if \quad (x_1, y_1) \neq (x_2, y_2) \\ \left(\frac{y_1(1 - x_1^3)}{x_1^3 - y_1^3}, \frac{x_1(y_1^3 - 1)}{x_2 y_2 - x_1 y_1}\right) & if \quad (x_1, y_1) = (x_2, y_2) \end{cases}$$

**Twisted Hessian form**

The twisted Hessian curves [12] is defined by equation

$$ax^3 + y^3 + 1 = dxy,$$

with neutral element $\mathscr{O} = (0, -1)$ Twisted Hessian curves have addition formula:

$$(x_3, y_3) = \left(\frac{x_1 - y_1^2 x_2 y_2}{a x_1 y_1 x_2^2 - y_2}, \frac{y_1 y_2^2 - a x_1^2 x_2}{a x_1 y_1 x_2^2 - y_2}\right).$$

**Montgomery curves** The Montgomery curves [13] is defined by equation

$$by^2 = x^3 + ax^2 + x,$$

such that $b(a^2 - 4) \neq 0$. with operation of addition given by formula

$$(x_1, y_1) + (x_2, y_2) =$$
$$= \left(\frac{b(x_2 y_1 - x_1 y_2)^2}{x_1 x_2 (x_2 - x_1)^2}, \frac{(2x_1 + x_2 + a)(y_2 - y_1)}{x_2 - x_1} - \frac{b(y_2 - y_1)^3}{(x_2 - x_1)^3 - y_1}\right).$$

## Integer Factorization Problem (IFP)

Problem definition The general integer factorization problem is defined as follows. Given a positive integern, write

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdot \ldots \cdot p_k^{e_k}$$

where $p_i$ are pairwise distinct primes and each $e_i \geqslant 1$. Typically, in practical cryptographic applications, only two factors are used for modulus $n$. A larger number of factors for n does not seem to offer any additional security in the IFP. The best-known public key cryptosystem that bases its security on the difficulty of the IFP is RSA [14, 15].

## Factoring algorithms

**Polard's $p - 1$ Method**

The method is based on the previously mentioned Fermat's little theorem which, with the assumptions fulfilled, for each $k$ multiple of number $p - 1$ has the property:

$$a^k \equiv 1 \pmod{p}$$

What follows is that $a^k - 1$ is a multiple of number $p$. Thus, every first divisorpof number $n$ is also a divisor of $n$ and $a^k - 1$. If we find such $k$ that number $a^k - 1$ is not divisible by $n$, then the calculation of $a^k - 1$ and $\gcd(a^k - 1; n)$ will lead us to the finding of the right divisor of number $n$.

In addition, if $p - 1$ has only small prime divisors $q_i$, then taking $k$ as a product of sufficiently many initial primes, with sufficiently high powers, we will obtain a product incorporating all of the powers present in the distribution $p - 1 = q_1^{e_1} \cdot \ldots \cdot q_m^{e_m}$, and, thus, we will obtain a multiple of number $p - 1$ without knowing this number. A problem appears in this method if $p - 1$ has a very large prime divisor. In practice, an upper limit of $B$ is introduced and it is assumed that $k$ is the product of the powers of $q_i$ primes for which $q_i^{e_i} \leqslant B$ [16, 17].

**Example** For $B = 17$ we have:

$$2^4 \leqslant 17; 3^2 \leqslant 17; 5^1 \leqslant 17; 7^1 \leqslant 17$$
$$11^1 \leqslant 17; 13^1 \leqslant 17; 17^1 \leqslant 17$$

Thus, $k$ should be assumed as $k = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$. If we take $B$ big enough for all the powers of primes in the distribution of number $p - 1$ to not be bigger than $B$, then $k$ obtained using this method will be a multiple of number $p - 1$. Having $k$, we compute $a^k \equiv 1 \pmod{n}$, and then $\gcd(a^k - 1; n)$ for example for $a = 2$. If we do not find the right divisor of number $n$, then we increase the upper limit of $B$ [18].

*Remark* 0.4. THe number $k$ can be assumed as, for example, $\gcd(1;2;\ldots;B)$ or even use the factorial $B!$.

Let $n = 10001$. Let's start with $a = 2$. Then clearly $\gcd(2; 10001) = 1$, so we proceed into the loop. We first compute $a^{2!} = 2^2 = 4$. Then

$$\gcd(a^{2!} - 1; n) = \gcd(3; 10001) = 1$$

so we continue. Now $a^{3!} = (a^{2!})^3 = 4^3 = 64$, and

$$\gcd(a^{3!} - 1; n) = \gcd(63; 10001) = 1$$

Next $a^{4!} = (a^{3!})^4 = 64^4 \equiv 5539 \pmod{10001}$, and

$$\gcd(a^{4!} - 1; n) = \gcd(5538; 10001) = 1$$

Next $a^{5!} = (a^{4!})^5 = 55395 \equiv 7746 \pmod{10001}$, and

$$\gcd(a^{5!} - 1; n) = \gcd(7745; 10001) = 1$$

Next $a^{6!} = (a^{5!})^6 = 77466 \equiv 1169 \pmod{10001}$, and

$$\gcd(a^{6!} - 1; n) = \gcd(1168; 10001) = 73.$$

We've run into a $\gcd(\cdot)$ that is bigger than 1, and not equal to $n = 10001$, so jackpot! 73 must be a prime factor of $n$. Then we can compute quickly that $10001/73 = 137$.

### Lenstra's Elliptic Curve Method

Given an integer $n$, we use the following steps to find factors of $n$.

1. Check that $n$ isn't divisible by 2 or 3, and that $n$ isn't a perfect power.
2. Choose random integers $a, x, y$ between 1 and $n$.
3. Let $b = y^2 - x^3 - ax \pmod{n}$.
4. Calculate $D = \gcd(4a^3 + 27b^2; n)$.
   - If $1 < D < n$, we are done.
   - If $D = 1$, proceed to Step 5.
   - If $D = n$, go back to Step 2 and choose a different $a$.
5. Let $E$ be the elliptic curve $E : y^2 = x^3 + ax + b$, and let $P = (x, y) \in E$.
6. Choose a number $k$ which is a product of small primes raised to small powers. For example, a good choice is $k = \mathrm{lcm}(2; 3; \ldots; B)$ for some integer $B \approx 100$.
7. Compute $kP \pmod{n}$.
8. If $kP$ lies on $E$, go back to Step 2 and choose different values for $a, x, y$. Otherwise, Step 7 yields a factor of $n$ [19].

**Example** Consider $n = 455839$. Let $E : y^2 = x^3 + 5x - 5$, $P = (1, 1)$, $k = 10!$ We begin by finding

$$2!P = 2P \pmod{n}$$

by using the algorithm of adding points on the elliptic curve

$$2P = (14, -53) \pmod{455839}$$

$$4P = (259851, 116255) \pmod{455839}$$

$$6P = (179685, 28708) \pmod{455839}$$

Similarly, we find that $4!P, 5!P, \ldots 7!P$ all lie on $E$, but computing $8!P$ requires inverting 599 (mod $n$) which isn't possible. This is because 599 is a factor of $n$, and we conclude that $n = 599 \cdot 761$.

### Schoof's Algorithm

This algorithm determines the number of points on an elliptic curve over finite fields which we needed for the Elliptic Curve Primality Test. Schoof's main idea behind this algorithm is based on the Hasse bound

$$|\#E(F_q) - q - 1| \leqslant 2\sqrt{q}$$

which estimates the number of points on an elliptic curve over $F_q$ up to a bound where $q$ is a prime integer. The algorithm also utilizes the Frobenius endomorphism which maps a point to its $q - th$ power:

$$\pi : (x, y) \to (x^q, y^q)$$

The Frobenius map has a characteristic equation

$$\pi^2 - t\pi + q = 0$$

where $t = q+1-|E(F_q)|$; from here we can solve for the number of points, $|E(F_q)|$. This is done by computing several t values modulo a set of prime numbers and then recovering the value of $t$ using the Chinese Remainder [20]. Probabilistic primality tests, such as the Goldwasser-Kilian Elliptic Curve Primality Test, are based on the above logarithms. Currently, pure cryptographic research on elliptic curves often transforms into the search for isogenies between them, which an important step towards post-quantum cryptography.

**Definition 0.5.** (Isogeny). Let $E_1$ and $E_2$ be two elliptic curves. An isogeny from $E_1$ to $E_2$ is a mapping of $\phi : E_1 \to E_2$ satisfying $\phi(O) = O$. Two elliptic curves $E_1$ and $E_2$ are isogenous if there is an isogeny from $E_1$ to $E_2$ with $\phi(E_1) \neq O$.

Currently, interesting issues in this field include [21]

- Find an isogeny between two given elliptic curves.
- Determine the rational maps that define isogeny given its kernel.
- Compute the image of a point through an isogeny specified by its rational maps.
- Enumerate all elliptic curves l-isogenous to a given elliptic curve E, where l is a given prime.

The above article presents a brief outline of existing solutions in the field of factorization. The Lenstra factorization method described in the article is much more efficient than the Pollard method, which works in a finite body. The Lenstra method uses elliptic curves, owing to which, with extremely inaccurate initial selections, it provides a great deal of opportunity to re-select the curve and a point on it [19]. Further work on this issue may be based on the classification of elliptic curves and methods of their selection to improve the performance of the Lenstra method.

The above-mentioned Edwards curves are characterized by relatively high speed of operations, but at present they are already well-researched. The pioneers in this field (apart from Harold Edwards) are primarily Daniel Bernstein and Tanja Lange. They are the authors of most of the literature on the application of Edwards curves. Edwards curves have a very important advantage over Weierstrass elliptic curves, which is the speed of adding and doubling points. A disadvantage of Edwards elliptic curve representation is the fact that not for every elliptic curve written in the Weierstrass form one can find an Edwards curve or a twisted Edwards curve, which would be isomorphic to it. In Daniel Bernstein's and Tanja Lange's works there are still Montgomery curves and Hessian curves [6] which are not yet as well researched in literature as Edwards curves. Brenstein's and Lange's studies under the Horizon 2020 program, whose result is in this year's publication entitled "Montgomery curves and the Montgomery ladder", can attest to the potential of these curves [22].

In the literature of the subject there are titles regarding the use of the Sage system (formerly SAGE *Software for Algebra and Geometry Experimentation*) [23], in the study of elliptic curves and Edwards curves. The application of this software to the study of the other families of curves mentioned above, in order to find curves that provide high security guarantee and, at the same time, have low computational costs, seems interesting. Progress in this field could have a positive impact on the improvement of security of the Internet of Things. In addition, the Sage tool can be used to select elliptic curves to identify optimal families in factorization processes.

## Literature


[1] Koblitz N. *Elliptic curve cryptosystems.* Mathematics of computation, 1987, 48(177), 203-209.

[2] Miller V.S. *Use of elliptic curves in cryptography.* In Conference on the Theory and Application of Cryptographic Techniques, 1985, pp. 417-426. Springer, Berlin, Heidelberg

[3] Liu Z., Großsächdl J., Hu Z., Järvinen K., Wang H., Verbauwhede I. *Elliptic curve cryptography with efficiently computable endomorphisms and its hardware implementations for the internet of things.* IEEE Transactions on Computers, 2017, 66(5), 773-785.

[4] Sughasiny M. *Give-and-take key processing for Cloud-linked IoT.* International Journal on Future Revolution in Computer Science and Communication Engineering (Vol. 3).

[5] Silverman J.H. *The arithmetic of elliptic curves.* Springer Science and Business Media, 2009, Vol. 106.

[6] Neves S., Tibouchi M. *Degenerate Curve Attacks.* In IACR International Workshop on Public Key Cryptography, 2016, pp. 19-35. Springer Berlin Heidelberg.

[7] Bernstein D.J., Lange T. *Inverted Edwards coordinates.* In AAECC, 2007, Vol. 4851, pp. 20-27.

[8] Bernstein D.J., Birkner P., Lange T., Peters C. *ECM using Edwards curves.* Mathematics of Computation, 2013, 82(282), 1139-1179.

[9] Bernstein D.J., Lange T. *Faster addition and doubling on elliptic curves.* In Asiacrypt, 2007 Vol. 4833, pp. 29-50.

[10] Saraf A. *A Study of Edwards Curves in Relation to Elliptic Curve Cryptography*, Doctoral dissertation, Sri Sathya Sai Institute of Higher Learning, 2015.

[11] Bernstein D.J. *Curve25519: new Diffie-Hellman speed records.* In International Workshop on Public Key Cryptography, 2006, pp. 207-228. Springer, Berlin, Heidelberg.

[12] Bernstein D.J., Chuengsatiansup C., Kohel D., Lange T. *Twisted hessian curves*, International Conference on Cryptology and Information Security in Latin America, 2015, pp. 269-294. Springer

[13] Montgomery L.P. *Speeding the Pollard and Elliptic Curve Methods of factorization*, Mathematics of Computation, 1987, 48 (177), 243-264

[14] Chou W., Washington D.L. *Elliptic curve cryptography and its applications to mobile devices.* University of Maryland, College Park, USA, 2003.

[15] MenezeS A.J., Van Oorschot P.C., Vanstone S.A. *Handbook of applied cryptography.* CRC press, 1996.

[16] Lenstra Jr H.W. *Factoring integers with elliptic curves.* Annals of mathematics, 1987, 649-673.

[17] Parker D. *Elliptic curves and Lenstra's factorization algorithm*, 2014.

[18] Chrzeszczyk A. *Algorytmy teorii liczb i kryptografii w przykładach.* Wydawnictwo BTC, 2010.

[19] Koblitz N. *A course in number theory and cryptography*, 1994, Vol. 114. Springer Science and Business Media.

[20] Hiatt R., Micovic D., Patino, B.V., Quah B.T.P. *WXML Final Report: Elliptic Curve Primality Test*, 2017.

[21] Ahmadi, O., Granger R. *On isogeny classes of Edwards curves over finite fields.* Journal of Number Theory, 2012, 132(6), 1337-1358.

[22] Bernstein D.J., Lange T. *Montgomery curves and the Montgomery ladder.* IACR Cryptology ePrint Archive, 2017.

[23] Van Nguyen M. *Exploring Cryptography Using the Sage Computer Algebra System.* Victoria University, 2009.


## Literature

Received: 2017
Accepted: 2017