A systematic literature review on high speed elliptic curve cryptography

Daniele Canavese

1 Introduction

Cryptography is one of the central founding pillars of modern information security. In the last decades, this field has seen numerous radical evolutions such as the introduction of public key algorithms. In this very area, elliptic curves are starting to emerge as a powerful technique capable to provide high levels of secrecy while maintaining small the key size. Elliptic curves were initially introduced as a way to solve elliptic integrals, and so they were largely used in physics since the middle of the XIX century. A pivotal discovery however was made in 1985 by Miller and Koblitz which, independently, proposed their use in public key algorithms. Since then, their usage in cryptography started to take place due to their security features. In order to increase the encryption throughput, an efficient implementation (in hardware, software or both) of such systems is highly desirable, especially on gateways and servers which may have to cipher huge quantity of bytes in a short amount of time.

This documents contains a systematic literature review (SLR) on the subject of high speed elliptic curve cryptography, which was conducted between October and November 2014. In order to restrict the number of papers to a manageable amount, several exclusion criteria where applied. In the end, 181 documents where found, but only 21 papers where selected as relevant for this study's purpose.

This document is structured as follows. Section 2 is a short background on elliptic curve cryptography (ECC). Section 3 describes the planning of the systematic literature review, while Section 4 contains a description of how the SLR was conducted. Section 5 is an analysis of the collected papers and it includes several statistics and plots. Section 6 is a discussion about the obtained results and finally Section 7 lists all the papers which were reviewed.

2 Background

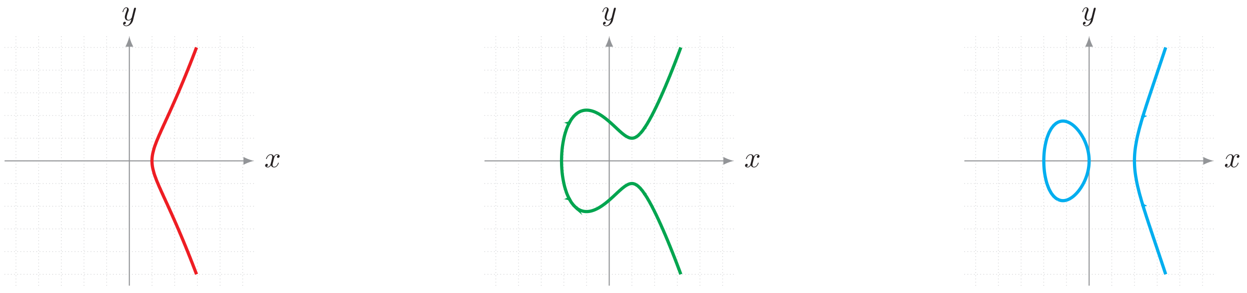
Given a field $\mathbb{F}$, an elliptic curve $\mathcal{E}$ over $\mathbb{F}$ is a non-singular planar curve with at least one $\mathbb{F}$-rational point which satisfies the *Weierstraß equation*

$$\mathcal{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Figure 1 depicts the plots of three elliptic curves over the field of the real numbers $\mathbb{R}$.

It can be shown that given two points $P(x_P, y_P)$ and $Q(x_Q, y_Q)$ on an elliptic curve, there exists a point addition operation $P + Q = R$ where $R(x_R, y_R)$ can be computed as

$$\begin{aligned} \lambda &= \begin{cases} \dfrac{y_P - y_Q}{x_P - x_Q} & \text{if } P \neq \pm Q \\ \dfrac{3x_P^2 + 2a_2x_P + a_4 - a_1y_P}{2y_P + a_1x_P + a_3} & \text{if } P = Q \end{cases} \\ x_R &= \lambda^2 + a_1\lambda - a_2 - x_P \\ y_R &= \lambda(x_P - x_R) - y_P - a_1x_R - a_3. \end{aligned}$$



(a) Plot of $y^2 = x^3 - 1$.

(b) Plot of $y^2 = x^3 - 3x + 3$.

(c) Plot of $y^2 = x^3 - 4x$.

Figure 1: Plots of three elliptic curves over $\mathbb{R}$.

In other words, the set of all the points on an elliptic curve forms a group with respect to the point addition operation. Figure 2 depicts a graphical representation of the point addition, that is to compute $R = P + Q$ in a 'geometrical' fashion we can

- draw the line passing through P and Q;
- denote the third intersection point between the elliptic curve and the line as $-R$;
- compute R as the point specular of $-R$ with respect to the x axis.

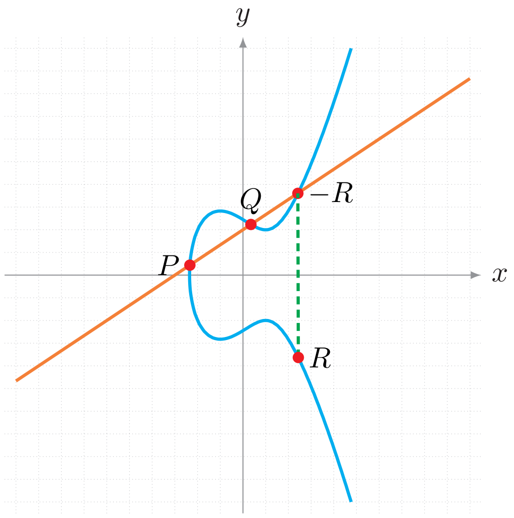


Figure 2: Graphical representation of the point addition on an elliptic curve.

If we sum a point P to itself, we say that we are *doubling* the point P, and we will write

$$R = 2P = P + P.$$

By extension, we can perform a point tripling $3P$ and so on. In general we can define a *scalar multiplication* operation

$$R = nP$$

Where R and P are two points on an elliptic curve and $n \in \mathbb{N}$.

Computing the scalar multiplication is a 'fast' operation, that is it can be executed using algorithm that have a polynomial running time. However, the inverse operation (the division) is a 'slow' operation, that is the only known algorithms are completely exponential. This means that

- given an integer n and a point P, it is fast to compute $nP = R$;

- given two points P and R, it is slow to compute n such that $nP = R$.

In cryptography the problem to efficiently compute the point 'division' is known as the *ECDLP*, the elliptic curve discrete logarithm problem[1]. This problem is the basis of the ECC, since to encrypt or decrypt data a scalar multiplication is needed, however to break the algorithm it is needed to perform a point division.

3 Planning

The planning phase in a SLR includes the definition of the research questions and the criteria for including or excluding a document in the review process.

The research questions which are the basis for this SLR are:

RQ1. What is the state-of-the-art of high speed elliptic curve cryptography?
Motivation: Discover the different type of algorithms and approaches used to speed-up the ECC computations and where most of the research interests lies.

RQ2. Are the performances of elliptic curve cryptography adequately tested?
Motivation: Determine how well ECC is tested in practical and theoretical scenarios.

The search of the related documents was conducted using the Internet and using only on-line electronic libraries via an ad-hoc constructed query. The following major terms were identified:

- cryptography;
- elliptic curve;
- efficient.

For each term a set of alternatives were found in order to build the final search string:

(*Cryptography* `OR` Encrypt `OR` Encryption `OR` Cipher)
`AND`
(*Elliptic curve* `OR` EC `OR` ECC)
`AND`
(*Efficient* `OR` Efficiency `OR` Efficiently `OR` Fast `OR` Speed)

In order to limit the research results to a manageable number, only the journal papers available from the IEEE Xplore Digital Library (`http://ieeexplore.ieee.org`) were selected. In particular, the documents included in the review process were papers:

- available through the IEEE Xplore Digital Library;
- published in international journals or as book chapters;
- which deal with elliptic curve cryptography as a main argument;
- which provide some result on the efficiency, in a theoretical or experimental way;
- completely in English;
- published from 1990 to 2014.

On the other hand, the papers excluded from the SLR were the documents:

- which have a quality score less than 2 (see Section 5 for a description of the metrics);

[1] The acronym ECDLP is misleading since we are computing a division and not a logarithm. The name was chosen for the similarity of the ECDLP to another problem known as the DLP (discrete logarithm problem).

- which are surveys or SLRs;
- which are slides or technical reports;
- which are duplicates of other papers;
- solely based on discussions and opinions;
- with only speculations with no theoretical and no experimental results;
- discussing only implementations based on web programming languages (JavaScript, PHP, ...) or scripting languages (Perl, Python, ...);
- discussing only hardware implementations (FPGAs, ASICs, ...).

4 Conducting the review

The SLR was planned and conducted between October and November 2014 and the time-line is showed in Table 1.

Date	Phase	Outcome
October 21–22	Protocol development	Initial review protocol
November 10	Protocol improvement	Refined review protocol
November 10	Retrieval of the files	Initial paper repository (181 papers)
November 10–11	Paper selection	Refined paper repository (21 papers)
November 11	Data extraction	Data extraction forms
November 11–12	Data synthesis	Document statistics
November 12	Report of the SLR	Pilot report

Table 1: Timeline of the review process.

The initial planning started in October and the SLR process was concluded in November.

During the initial retrieval of the files from the Internet a total of 181 research results (documents) were obtained. By applying the inclusion and exclusion criteria described in Section 3, the number of relevant papers were reduced to 21. Table 2 shows results of the exclusion process.

Type	Documents
Hardware-related	70 (37%)
Off-topic	88 (49%)
Not in English	1 (0%)
Not available	1 (0%)
Relevant	21(12%)
Total	181 (100%)

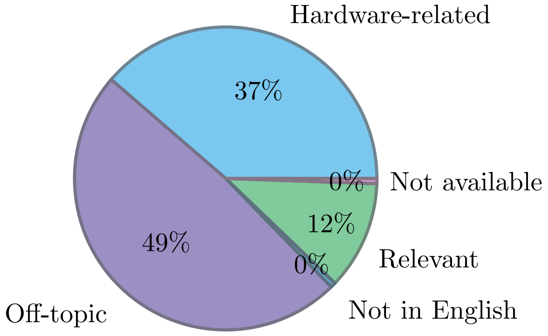


Table 2: Paper exclusion results.

In the end 160 documents were excluded, in particular:

- 1 paper was not downloadable from the Internet (broken URL);
- 1 paper was not in English (it was in Spanish);
- 70 papers were treating only hardware implementations;

- 88 papers were off-topic, treating only ECC as a secondary argument (they were mainly discussing security protocols or only finite field algebra).

The complete list of the 21 selected papers is available in Section 7.
The 'surviving' documents were then registered on a form containing:

- demographic information, as the paper title, the publication year, the journal and so on;
- technical information, as the applicability of the approach proposed and the type of tests conducted.

The technical information part was constructed in order to provide a mean of answering the research questions presented in Section 3.

5 Data synthesis and results

In order to address the research questions previously described, several analysis were performed on the 21 candidate papers. The results of the studies is listed in the following paragraphs.

5.1 Quality

One of the first analysis performed was aimed to asses the quality of the selected papers in order to exclude the documents with the lowest scores. The score is a numerical (integer) value ranging from 0 to 7 which was assigned to each paper, where 0 indicates the lowest quality and 7 the highest one. Table 3 shows the papers per quality score.

Score	Papers
0	0 (0%)
1	0 (0%)
2	0 (0%)
3	5 (24%)
4	4 (19%)
5	7 (33%)
6	3 (29%)
7	2 (10%)
Mean	4.7

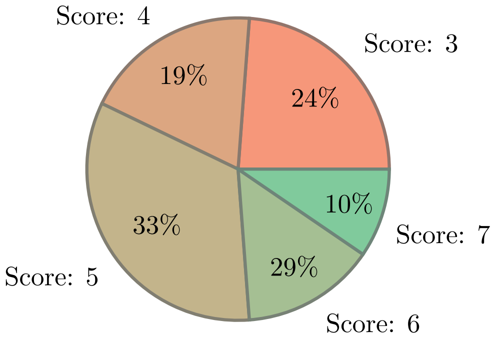


Table 3: Number of papers per quality score.

The results show that the weighted arithmetic mean score is 4.7 and the lowest score attained is 3. The overall paper quality is quite good, as expected, since only journal papers were chosen for the review. No low-quality paper were found, so all the 21 papers were selected to participate in the following analysis.

In the ECC field there are usually two kind of results on the efficiency that can be given:

- theoretical results, that is formulas stating the expected complexity of the calculations;
- experimental results, that is timings which were measured by executing a software implementing the proposed approach.

Keeping that in mind, the quality scores were computed using the following simple rules:

1. a paper starts with a quality score of 0;

2. a value between 0 and 2 is added based on the paper findings *credibility* (0 means that the paper results are totally not credible, 1 means that they seems quite reasonable and 2 that are completely credible);
3. a 1 is added to the score if the paper performs some kind of *comparison* with respect to other approaches;
4. a 1 is added to the score if the paper discusses the *security* of the proposed approach;
5. a 1 is added to the score if the paper performs some kind of *experimental* results (0 means that they are purely theoretical);
6. a value between 0 and 2 is added based on how many elliptic *curves* are tested (0 means that no curve was tested, 1 means that only one curve was tested and 2 means that two or more curves were tested).

Table 4 lists in detail the results of the features that were tested for the quality assessment.

Feature	Value	Papers
Credibility	0	0 (0%)
	1	3 (14%)
	2	18 (86%)
Comparison	0	5 (24%)
	1	16 (76%)
Security	0	16 (76%)
	1	5 (24%)
Experimental	0	13 (62%)
	1	8 (38%)
Curves	0	3 (14%)
	1	6 (29%)
	2	12 (57%)

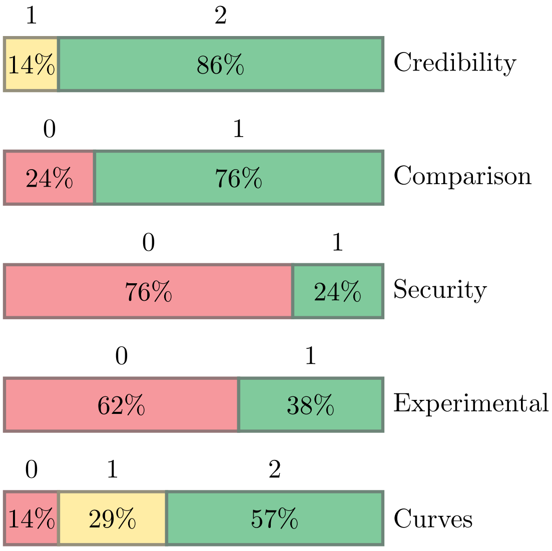


Table 4: Number of papers per quality feature.

Most of the papers offer quite credible findings and usually report some comparisons with other techniques. However, several documents give only theoretical proofs with no tests on real-world implementations and rarely the security of the proposed approaches is discussed.

5.2 State-of-the-art (RQ1)

The first research question regards the current state-of-the-art of ECC.

Elliptic curve cryptography has started to attract several researchers in the last decades as shown in Table 5, which lists the number of publications per year.

The data clearly shows that the research interest in this field is remarkable increased in the 2000s. Until 1993 there was only 1 paper published on the matter, while all the other documents are dated after the year 2000. After 2011 there was not a single year without a journal publication on this subject.

Elliptic curves are built on top of a field, so it is natural to investigate what are the most used fields in the current state-of-the-art. We can then classify the ECC algorithms in three main categories:

- approaches suitable only for binary fields, that is (extension) fields with characteristic 2;
- approaches suitable only for prime fields, that is (base) fields with any prime characteristic;
- approaches suitable for any field.

Year	Papers
1993	1 (5%)
2001	1 (5%)
2002	2 (10%)
2004	1 (5%)
2005	2 (10%)
2006	2 (10%)
2007	2 (10%)
2008	3 (14%)
2009	1 (5%)
2011	1 (5%)
2012	1 (5%)
2013	1 (5%)
2014	3 (14%)

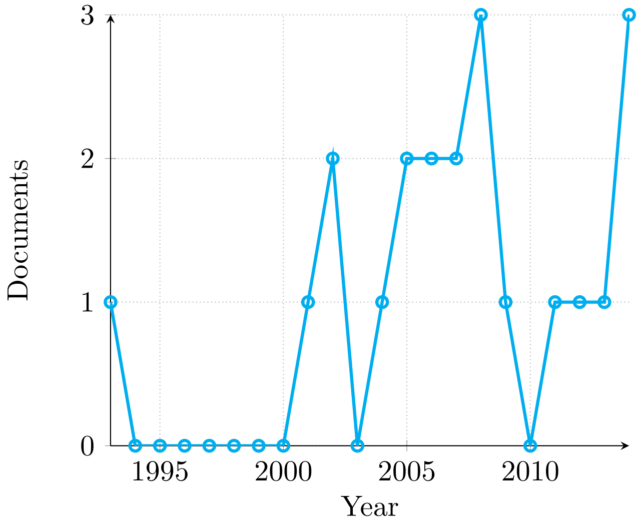


Table 5: Number of papers per year.

Field	Papers
Prime	5 (24%)
Binary	9 (43%)
Any	7 (33%)

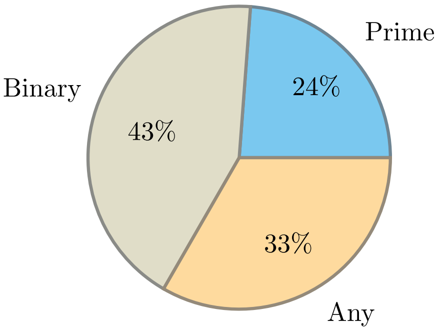


Table 6: Paper per field type.

Table 6 lists the results of such classification in the selected papers.

The vast majority (43% + 33%) of the documents propose a technique that can be applied to a binary field, while only 57% (24% + 33%) of the documents focus their attention on prime fields.

On the other hand, also the kind of elliptic curve studied in a paper is an interesting statistic. We can therefore classify the approaches also in:

- approaches suitable only for prime curves, if they work on prime fields;
- approaches suitable only for binary curves, if they work on binary fields;
- approaches suitable only for Koblitz curves, that is a peculiar family of binary curves;
- approaches suitable only for Edwards curves, that are curves that can be defined on any non-binary field;
- approaches suitable only for Montgomery curves, that are curves that can be defined on any non-binary field;
- approaches suitable for any elliptic curve.

Table 7 shows the results of the classification.

Most of the work is focused on binary elliptic curves, while there is a small, but non insignificant, number of papers (4) which are oriented toward some specific kind of curves (Koblitz, Edwards and Montgomery).

Curve	Papers
Prime	3 (14%)
Binary	8 (38%)
Koblitz	2 (10%)
Edwards	1 (5%)
Montgomery	1 (5%)
Any	6 (29%)

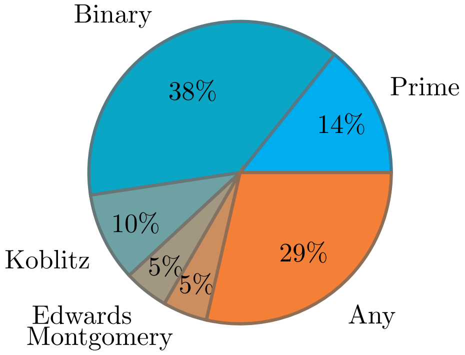


Table 7: Papers per elliptic curve type.

5.3 Testing and performances (RQ2)

The second research question regards the efficiency of ECC and how well the performances are tested.

Table 8 shows the programming languages used to implement the algorithms proposed in the reviewed papers.

Language	Papers
C	7 (33%)
C++	1 (5%)
None	13 (62%)

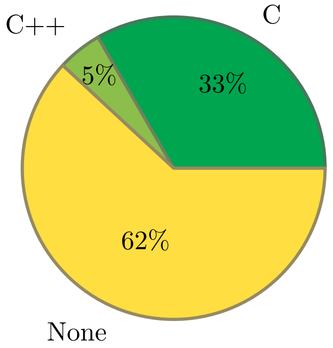


Table 8: Papers per programming language.

This statistic show two interesting results. The first one is that most of the papers (62%) propose only theoretical results and do not report any kind of experimental result. The second one is that the C/C++ programming languages are essentially the de-facto standard programming languages in this area.

Furthermore, it is also interesting to know the main CPU architectures which are the target of the implementations. Table 9 shows such results.

CPU family	Papers
x86	3 (14%)
x86-64	2 (10%)
ARM	2 (10%)
H8	1 (5%)
None	13 (62%)

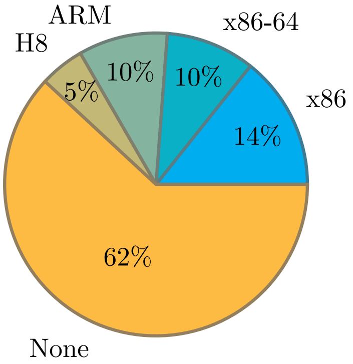


Table 9: Papers per CPU family.

32-bit processors seems to be the main target of the results, however both processors for PCs (x86 and x86-64 families) and embedded systems (ARM and H8 families) seem to be an interesting platform in this research area.

6 Discussion

The review toke into account 21 papers from an initial selection of 181 documents that were excluded by using the criteria listed in Section 3.

With respect to the RQ1: 'What is the state-of-the-art of high speed elliptic curve cryptography?', several facts have been found:

- the interest in ECC has significantly increased in the last few years, especially from the year 2000;
- most of the state-of-the-art is focused on approaches for binary fields and binary elliptic curves;
- Koblitz curves (a kind of binary elliptic curve) seems also to have gained some (minor) degree of popularity.

With respect to the RQ2: 'Are the performances of elliptic curve cryptography adequately tested?', the results showed that:

- most of the papers do not provide any kind of practical implementation results and prefer to rely only on theoretical complexity calculations to prove the effectiveness of their findings;
- most of the papers have tested (theoretically or experimentally) their approaches on at least 2 elliptic curves;
- the C and C++ languages are clearly the favorite choice of all the ECC implementations;
- there exists software implementations for both PCs and embedded systems processors.

7 References

[1] Gordon B. Agnew, R. C. Mullin, and Scott A. Vanstone. An implementation of elliptic curve cryptosystems over F_2^{155}. *IEEE Journal on Selected Areas in Communications*, 11(5):804–813, June 1993.

[2] Essame Al-daoud, Ramlan Mahmod, Mohammad Rushdan, and Adem Kilicman. A New Addition Formula for Elliptic Curves over $GF(2^n)$. *IEEE Transactions on Computers*, 51(8):972–975, 2002.

[3] M. Aydos, Tugrul Yanik, and C. K. Koc. High-speed implementation of an ECC-based wireless authentication protocol on an ARM microprocessor. *IEEE Proceedings-Communications*, 148(5):273–279, 2002.

[4] Reza Azarderakhsh and Koray Karabina. A new double point multiplication algorithm and its application to binary elliptic curves with endomorphisms. *IEEE Transactions on Computers*, 63(10):2614–2619, October 2013.

[5] Sandro Bartolini, Irina Branovic, Roberto Giorgi, and Enrico Martinelli. Effects of Instruction-Set Extensions on an Embedded Processor: A Case Study on Elliptic-Curve Cryptography over $GF(2^m)$. *IEEE Transactions on Computers*, 57(5):672–685, 2008.

[6] Jung Hee Cheon, Stanislaw Jarecki, Taekyoung Kwon, and Mun-Kyu Lee. Fast Exponentiation Using Split Exponents. *IEEE Transactions on Information Theory*, 57(3):1816–1826, March 2011.

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

[8] Christophe Doche and Daniel Sutantyo. New and Improved Methods to Analyze and Compute Double-Scalar Multiplications. *IEEE Transactions on Computers*, 63(1):230–242, January 2014.

[9] Kenny Fong, Darrel Hankerson, Julio Lopez, and Alfred Menezes. Field inversion and point halving revisited. *IEEE Transactions on Computers*, 53(8):1047–1059, August 2004.

[10] Darrel Hankerson, Koray Karabina, and Alfred Menezes. Analyzing the Galbraith-Lin-Scott Point Multiplication Method for Elliptic Curves over Binary Fields. *IEEE Transactions on Computers*, 58(10):1411–1420, October 2009.

[11] Jing-Shyang Hwu, Rong-Jaye Chen, and Yi-Bing Lin. An efficient identity-based cryptosystem for end-to-end mobile security. *IEEE Transactions on Wireless Communications*, 5(9):2586–2593, September 2006.

[12] Majid Khabbazian, T. Aaron Gulliver, and Vijay K. Bhargava. A New Minimal Average Weight Representation for Left-to-Right Point Multiplication Methods. *IEEE Transactions on Computers*, 54(11):1454–1459, 2005.

[13] Majid Khabbazian, T. Aaron Gulliver, and Vijay K. Bhargava. Double Point Compression with Applications to Speeding Up Random Point Multiplication. *IEEE TR*, 56(3):305–313, 2007.

[14] Duc-phong Le and Chik How Tan. Improved Miller's Algorithm for Computing Pairings on Edwards Curves. *IEEE Transactions on Computers*, 63(10):2626–2632, October 2014.

[15] Mun-Kyu Lee. Comments on "Provably Sublinear Point Multiplication on Koblitz Curves and Its Hardware Implementation". *IEEE Transactions on Computers*, 61(4):591–592, April 2012.

[16] Duo Liu, Tao Song, and Yiqi Dai. Isomorphism and generation of montgomery-form elliptic curves suitable for cryptosystems. *Tsinghua Science and Technology*, 10(2):145–151, April 2005.

[17] Patrick Longa and Ali Miri. Fast and Flexible Elliptic Curve Point Arithmetic over Prime Fields. *IEEE Transactions on Computers*, 57(3):289–302, 2008.

[18] Chia-yu Lu, Shang-ming Jen, and Chi-sung Laih. A General Framework of Side-Channel Atomicity for Elliptic Curve Scalar Multiplication. *IEEE Transactions on Computers*, 62(3):428–438, 2013.

[19] Moad Mowafi, Lo'ai Tawalbeh, and Walid Aljoby. Use of elliptic curve cryptography for multimedia encryption. *IET Information Security*, 7(2):67–74, June 2013.

[20] Katja Schmidt-Samoa, Olivier Semay, and Tsuyoshi Takagi. Analysis of fractional window recoding methods and their application to elliptic curve cryptosystems. *IEEE Transactions on Computers*, 55(1):48–57, January 2006.

[21] Camille Vuillaume, Katsuyuki Okeya, and Tsuyoshi Takagi. Short-Memory Scalar Multiplication for Koblitz Curves. *IEEE Transactions on Computers*, 57(4):481–489, April 2008.