

# Implementation and Analysis of an Elliptic Curve Cryptography System

Student Name: T. Butterfield

Supervisor Name: M. Bordewich

Submitted as part of the degree of BSc Computer Science to the  
Board of Examiners in the Department of Computer Sciences, Durham University  
March 18, 2021

**Abstract** — Do not cite references in the abstract.

This section should not be longer than half of a page, and having no more than one or two sentences under each heading is advised.

**Background** - Diffie-Hellman, RSA, ...

**Aims** - The aim of this project was to create a working Elliptic Curve Cryptography system and to analyse that system in terms of security and efficiency.

**Method** - Euclid's extended algorithm, point addition, point multiplication, ...

**Results** - Cannot discover information about private key, enables secure communication

**Conclusions** - Strength of ECC, smaller key size than RSA, much more suitable for mobile devices

**Keywords** — Elliptic Curve Cryptography (ECC), Elliptic Curve Diffie-Hellman (ECDH), Elliptic Curve Digital Signature Algorithm (ECDSA), Safe Curves, User Interface (UI)

## I INTRODUCTION

The whole report, including references, should not be longer than 20 pages in length. It should be noted that not all the details of the work carried out in the project can be represented in 20 pages. It is therefore vital that the Project Log book be kept up to date as this will be used as supplementary material when the project paper is marked. There should be between 10 and 20 referenced papers—references to Web based pages should be less than 10%.

This section briefly introduces the general project background, the research question you are addressing, and the project objectives. It should be between 2 to 3 pages in length.

- Abstract & Introduction make 5% of paper
- Adequacy of Abstract
- Description of background - Diffie-Hellman, RSA, ECC
- Discussion of aims and achievements - Aimed to create system which implemented safe curves

There were a total of nine objectives for this project, split equally into three sections: basic, intermediate, and advanced.

The first basic objective was to create a basic working ECC system which computed the essential functions required. The second and third basic objectives were to create a client application that can conduct ECDH over a network connection, and to create a UI allowing a user to easily make use of the system and to decide what level of complexity is revealed to them.

The intermediate objectives revolved around improving the functionality and security of the system, with the first objective being to add secure random private key generation to the system. The other intermediate objectives were to implement the ECDSA and to enable the exchange of secure signed files via the UI.

The first advanced objective was to make improvements to the UI and to reveal the workings of the system. The penultimate objective was to analyse the code for efficiency, including how the time required scales with the curve and key size, making any necessary changes to the system to improve the efficiency. The final objective was to analyse the code for vulnerabilities, such as side-channel attacks, and to fix any such weaknesses.

## II RELATED WORK

This section presents a survey of existing work on the problems that this project addresses. it should be between 2 to 4 pages in length.

- 15% of paper
- Adequacy of literature surveyed
- Critical analysis

Cryptography is the study of mathematical systems for solving two kinds of security problems: privacy and authentication (Diffie & Hellman 1976). A privacy system prevents the extraction of information by unauthorised parties from messages transmitted over a public channel, assuring it is read only by the intended recipient. An authentication system prevents the unauthorised injection of messages into a public channel, assuring the legitimacy of the sender. (Diffie & Hellman 1976) proposed that it was possible to develop systems in which two parties communicating solely over a public channel and using only publicly known techniques could create a secure connection. This was the first public discovery of public-key cryptography.

Diffie and Hellman presented the concept of a public-key cryptosystem but not any practical implementation of such a system. So in 1978, Rivest, Shamir, and Adleman presented a new encryption method which did just that, it was the first public implementation of public-key cryptography. This method had the novel property that publicly revealing an encryption key did not thereby reveal the corresponding decryption key (Rivest et al. 1978). This is known as RSA public-key cryptography.

(Miller 1986) and (Koblitz 1987) discussed an analogue of the Diffie-Hellman key exchange protocol based on elliptic curves over finite fields which used the multiplicative group of a finite field. The advantage of this system was that it appeared to be immune from attacks of the style of (Miller 1986, Adleman 1979). This was the invention of Elliptic Curve Cryptography.

Whilst the *Elliptic Curve Discrete Logarithm Problem* is difficult to solve on classical computers (Hankerson et al. 2003), there is a gap between ECDLP difficulty and ECC security (Bernstein & Lange 2013). In 2010, it was discovered that Sony had made a basic and critical mistake in the implementation of their Elliptic Curve Cryptosystem. As discussed in section B.6, as part of the Signature Generation stage of the ECDSA, a random integer  $k$  is generated and used, it is imperative that  $k$  is truly random and not predictable in any way. However, Sony

wrote their own software which used a constant number for each signature. This allowed the computation of their private key, from the public key, using simple algebra (Hotz 2010).

### III SOLUTION

This section presents the solutions to the problems in detail. Included here are details of the specification and design (Section A), an outline of the implementation issues faced (Section D), a description of the tools used (Section C), as well as the verification and validation of the components (Section E), and finally a discussion of the testing of the system (Section F).

#### A Architecture and Design

At a high level, my system is a client-server network designed to allow multiple instances of a client program to connect to a single server program. The clients can communicate with each other, via the server, using end-to-end ECC encryption. In the description and explanation of my system I will personalise the participants; Alice and Bob want to communicate while Eve, the eavesdropper, intercepts and tries to read their messages. The diagram below illustrates the protocol for Alice to send a message to Bob:

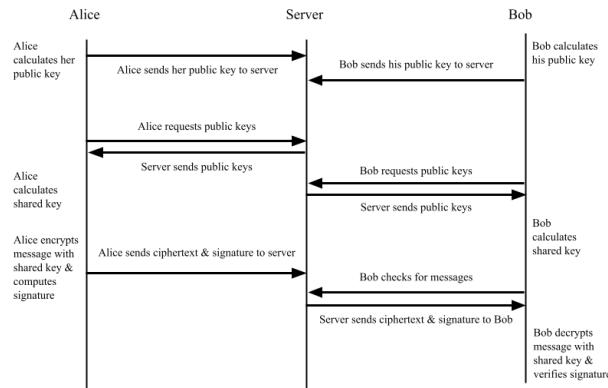


Figure 1: Message Exchange Diagram

A message here can be either a text message or a file from Alice's device. The server stores a list of the public keys of every client who is connected, and will send this to any client who requests it in order for them to establish a shared key with other clients. The server also holds the encrypted data and the accompanying signature for messages which have yet to be requested by the recipient. After the recipient has asked the server if there are any messages waiting for them, the server has sent the relevant message(s), and the recipient has decrypted and verified the message(s), the server then deletes the message(s). The only data stored by the client is a list of their shared keys with other clients. As shown in Figure 1, all of the computation is done by the client and the server does not perform any calculations; it only receives, stores, and sends client data. There are two ECC specific algorithms performed by each client in the exchange shown in Figure 1, namely the Elliptic Curve Diffie-Hellman (ECDH) key exchange algorithm and the Elliptic Curve Digital Signature Algorithm (ECDSA).

## B Algorithms

This section outlines the algorithms which are used by my system and how I implemented them. The two ECC specific algorithms mentioned previously (ECDH and ECDSA) differ from their RSA counterparts (DH and DSA) only in that the operation of exponentiation of an integer is instead replaced by the operation of multiplying a point on an elliptic curve. The naive approach to this of repeatedly adding a point  $G$  to itself  $k$  times in order to calculate  $kG$  would take prohibitively long. Therefore I had to implement an adapted version of the repeated squares method (squaring and multiplying integers) used by RSA to calculate large exponents efficiently. This adapted method I implement is to use doubling and adding of points on an elliptic curve in order to achieve multiplication of a point. While the naive approach would take  $O(k)$  time to calculate  $kG$ , this approach takes  $O(\log(k))$  time, making it practical for my system since  $k$  will be a very large number (of the order  $2^{250}$ ). An elliptic curve, along with the operations of adding and doubling points on the curve, are formally defined below:

### B.1 Elliptic Curve

Let  $p$  be a prime number, and let  $F_p$  denote the field of integers modulo  $p$ . An elliptic curve  $E$  over  $F_p$  is defined by an equation of the form

$$y^2 = x^3 + ax + b, \quad (1)$$

where  $a, b \in F_p$  satisfy  $4a^3 + 27b^2 \neq 0 \pmod{p}$ .

### B.2 Point Addition

Let  $P = (x_1, y_1) \in E(F_p)$  and  $Q = (x_2, y_2) \in E(F_p)$ , where  $P \neq Q$ . Then  $P + Q = (x_3, y_3)$ , where

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1, \quad \text{and} \quad \lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad (2)$$

### B.3 Point Doubling

Let  $P = (x_1, y_1) \in E(F_p)$ . Then  $P + P = 2P = (x_3, y_3)$ , where

$$x_3 = \lambda^2 - 2x_1, \quad y_3 = \lambda(x_1 - x_3) - y_1, \quad \text{and} \quad \lambda = \frac{3x_1^2 + a}{2y_1} \quad (3)$$

(Hankerson et al. 2003, López & Dahab 2000).

In my system when I want to multiply a point  $G$  by an integer  $k$ , I take the point  $G$  and double it  $\lfloor \log_2(k) \rfloor$  times, storing each new point in an array where index  $i$  holds  $2^i * G$ . The final value is then calculated by adding the points in the array whose index corresponds to a 1 in the binary expansion of  $k$ . My system actually implements this using bitwise operations on  $k$  for efficiency, however it is more intuitive to imagine it as a binary expansion and an array of equal length as described. That is how I implement point multiplication using point addition and point doubling. Things are complicated further however due to the fact that an elliptic curve is defined over a field of integers modulo  $p$  (B.1), meaning that these operations are all carried out

in modulo  $p$  and can only involve integers. Since the equations for both point addition (B.2) and point doubling (B.3) involve division, it is clear that a naive implementation of division cannot be used here since it would produce non-integer results. Therefore I had to implement the Extended Euclidean algorithm (EEA) in order to ensure integer results of these division calculations. For example, in order to calculate the gradient  $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$  in point addition (B.2), I use the EEA to calculate  $(x_2 - x_1)^{-1} \bmod p$  and then multiply this by  $(y_2 - y_1)$ . This ensures that  $\lambda$  is an integer, and therefore that the coordinates  $(x_3, y_3)$  as defined in B.2 are also integers.

Once I had a function for efficiently computing point multiplication, I was able to move on to the functions of ECDH and ECDSA.

## B.4 ECDH

The *Elliptic Curve Diffie-Hellman* key agreement protocol allows Alice and Bob to securely agree upon the value of a point on an elliptic curve, although neither of them initially knows the value of the point. This point becomes their shared key, and the algorithm for generating it is formally defined below:

Alice and Bob must agree on a finite field  $F_q$ , an elliptic curve  $E/F_q$ , and a generator point  $G \in E(F_q)$  of (prime) order  $n$ . Both Alice and Bob have a key pair  $(d, Q)$  consisting of a private key  $d$  (a randomly selected integer less than  $n$ ) and a public key  $Q = d * G$ .

Let  $(d_A, Q_A)$  be the key pair of Alice and  $(d_B, Q_B)$  be the key pair of Bob.

1. Alice computes  $K = (x_K, y_K) = d_A * Q_B$
2. Bob computes  $L = (x_L, y_L) = d_B * Q_A$
3. Since  $d_A Q_B = d_A d_B G = d_B d_A G = d_B Q_A$ . Therefore  $K = L$  and hence  $x_K = x_L$
4. Hence the shared secret is  $x_K$

Since it is practically impossible to find the private key  $d_A$  or  $d_B$  from the public key  $K$  or  $L$ , it is not possible for Eve to obtain the shared secret (Jurišić & Menezes 1997, Anoop 2007, Silverman 2009, Brown 2009).

In my implementation of this algorithm, all clients are automatically using the same generator point which lies on the same elliptic curve, defined over the same finite field, since every client is an instance of the same program and this is hard-coded. I generate the random private key for each client, using Python's "secrets" module, right when the client instance is started, and the public key is then calculated immediately after using the point multiplication function mentioned previously. This public key is then sent to the server along with the user's name (e.g. Alice) which they have entered via the command line, such that any other user (e.g. Bob) can then get Alice's public key from the server and establish a secret shared key with her. In my system, Bob (or any other client) calculates their shared key with Alice by asking the server for any available public keys, and using the point multiplication function to multiply Alice's public key by their private key. The shared keys that each client has established with their contacts is stored locally and then used to encrypt future messages with symmetric AES.

## B.5 ECDSA

The *Elliptic Curve Digital Signature Algorithm* allows Alice to sign a message or file in such a way that Bob is able to then verify that Alice must have been the sender and that the message/file has not been altered. Alice does this by generating a signature using the hash of the message and her private key. She then sends this to Bob alongside her message. Bob then uses Alice's

public key and the hash of the message to check that the signature must have been generated on the same message and by Alice. The two parts of this algorithm are formally defined below.

## B.6 Signature Generation

For signing a message  $m$  sent by Alice, using Alice's private key  $d_A$ .

1. Calculate  $e = HASH(m)$ , where  $HASH$  is a cryptographic hash function, such as SHA
2. Select a random integer  $k$  from  $[1, n - 1]$
3. Calculate  $r = x_1$ , where  $(x_1, y_1) = k * G \pmod{n}$
4. Calculate  $s = k^{-1}(e + d_A r) \pmod{n}$
5. The signature is the pair  $(r, s)$

## B.7 Signature Verification

For Bob to authenticate Alice's signature, Bob must have Alice's public key  $Q_A$ .

1. Calculate  $e = HASH(m)$
2. Calculate  $w = s^{-1} \pmod{n}$
3. Calculate  $u_1 = ew \pmod{n}$  and  $u_2 = rw \pmod{n}$
4. Calculate  $(x_1, y_1) = u_1 G + u_2 Q_A$
5. The signature is valid if  $x_1 = r \pmod{n}$ , invalid otherwise

(Jurišić & Menezes 1997, Koblitz et al. 2000, Hankerson et al. 2003, Anoop 2007, Silverman 2009, Brown 2009).

In my implementation of this algorithm, Alice and Bob first agree upon all of the same initial setup things mentioned in Section B.4 by default since again they are all hard-coded in to every client. When Alice wants to send a signed message or a file to Bob, she enters the message or the name of the file via the command line, and generates a hash of the message/file using SHA-512 from Python's "hashlib" module. This hash is converted to an integer and truncated to be smaller than  $n$ . A random number  $k$  is then generated using the same "secrets" module previously mentioned and the point  $G$  is multiplied by  $k$  using the point multiplication function, with the x-coordinate taken as  $r$  and the y-coordinate discarded. The integer  $r$  is multiplied by Alice's private key (also an integer) and added to the truncated hash of the message (another integer), finally this is divided by  $k$  to generate  $s$ . This division is done by multiplying by the inverse of  $k$  modulo  $n$ , calculated with the EEA function mentioned earlier. Alice sends both  $r$  and  $s$  to the server, along with her AES encrypted message.

On the receiving end of my implementation, after Bob receives all of this data from the server, he first decrypts the message itself using the shared key he has already established with Alice. He uses the plaintext message and the same hashing algorithm to generate a hash of the message, which he converts to an integer and truncates in the same way that Alice did, calling it  $e$ . The multiplicative inverse of  $s$  modulo  $n$  is then calculated using the EEA function and called  $w$ . Bob then does two integer multiplications, the first is the  $e * w \pmod{n}$ , and the second is  $r * w \pmod{n}$ , these new integers are called  $u_1$  and  $u_2$  respectively. Next, two lots of point multiplication are carried out and their results are summed by point addition. The first point multiplication is  $u_1 * G$  where  $G$  is the generator point mentioned previously, and the second is  $u_2 * Q_A$  where the point  $Q_A$  is Alice's public key. After adding these two points together using the point addition function to create a new point, Bob takes just the x-coordinate of this new point and compares it to the  $r$  from Alice's signature. If these are equal  $\pmod{n}$  then the signature is valid and was

definitely generated by Alice using the same message which Bob received. So now Bob has the plaintext message and is assured that it is authentic.

### ***C Tools used***

The system was created entirely in Python, I chose this language because of both its ability to handle large integers with ease, and its large number of well-established modules for computing generic cryptographic functions. Since my system carries out operations involving huge integers, other less abstracted languages would have required much more involvement at the lower level which would only detract from my progress with the actual aims of the project. The specific Python modules that I used in my system are: "Pyro4", "AES" from "PyCryptodome", "base64", "hashlib", "secrets", and "os". "Pyro4" is used for remote object invocation I only used long standing and well used libraries because of (Ducklin 2021). I chose to use secrets because after my initial implementation using "random", I realised that this wasn't cryptographically secure.

The system can be started and interacted with via a command line interface, this was chosen since it allowed me to focus more on the protocols and back-end of the system rather than on designing a visually appealing graphical user interface, which was not relevant to the mathematical-based aims of this project.

### ***D Implementation Issues***

After I successfully implemented client-client communication with separate instances of the client program running on the same machine, I then attempted to adapt the system for use with the client instances on separate machines on the same network. However, I encountered issues with this due to the security protocols in place on networks and I decided against attempting to circumvent these protocols due to both the potentially time-consuming nature of the problem and fact that my project is not aiming to recreate Signal or WhatsApp, network communication is not necessary.

### ***E Verification and Validation***

#### **E.1 Safe Curves**

There are several different standards covering selection of curves for use in elliptic-curve cryptography, most recently NSA Suite B (2005) and ANSSI FRP256V1 (2011). Each of these standards tries to ensure that the ECDLP (finding a user's private key, given their public key) is difficult. Unfortunately, there is a gap between ECDLP difficulty and ECC security. None of these standards do a good job of ensuring ECC security, secure implementations of the standard curves are theoretically possible but very hard. There are many attacks that break real-world ECC without solving ECDLP (Bernstein & Lange 2013). MORE DETAIL ABOUT WHAT MAKES A CURVE SAFE/UNSAFE

In 2006, Daniel Bernstein designed a new high-security ECDH function which achieved record setting speeds (twice as fast as any other function), with several side benefits including state-of-the-art timing-attack protection. This function, known as Curve25519, is suitable for a wide variety of cryptographic applications. The Curve25519 function is  $F_p$ -restricted x-coordinate scalar multiplication on  $E(F_{p^2})$ , where  $p$  is the prime number  $2^{255} - 19$  and  $E$  is the elliptic curve  $y^2 = x^3 + 486662x^2 + x$  (Bernstein 2006). Curve25519 is regarded as a safe curve,

since it satisfies the basic parameter requirements, the ECDLP security requirements, and the ECC security requirements beyond ECDLP security (Bernstein & Lange 2013).

## E.2 Exhaustive Search

The elliptic curve parameters for cryptographic schemes should be carefully chosen in order to resist all known attacks on the ECDLP. The most naïve algorithm for solving the ECDLP is exhaustive search whereby one computes the sequence of points  $P, 2P, 3P, 4P, \dots$  until  $Q$  is encountered. The running time is approximately  $n$  steps in the worst case and  $n/2$  steps on average. Therefore, exhaustive search can be circumvented by selecting elliptic curve parameters with  $n$  sufficiently large to represent an infeasible amount of computation (e.g.,  $n \geq 2^{80}$ ) (Hankerson et al. 2003).

## E.3 Pohlig-Hellman and Pollard's rho algorithm

The best general-purpose attack known on the ECDLP is the combination of the Pohlig-Hellman algorithm and Pollard's rho algorithm, which has a fully-exponential running time of  $O(\sqrt{p})$  where  $p$  is the largest prime divisor of  $n$ . To resist this attack, the elliptic curve parameters should be chosen so that  $n$  is divisible by a prime number  $p$  sufficiently large so that  $\sqrt{p}$  steps is an infeasible amount of computation (e.g.,  $p > 2^{160}$ ). If, in addition, the elliptic curve parameters are carefully chosen to defeat all other known attacks (e.g. Isomorphism attacks), then the ECDLP is believed to be infeasible given the state of today's computer technology (Hankerson et al. 2003).

## F Testing

Graphs from testing of security and efficiency of system: number of 1 bits vs time, log key value vs time, various curves vs time.

I analysed the time taken to compute  $kG$  here and Figure 2 shows the results

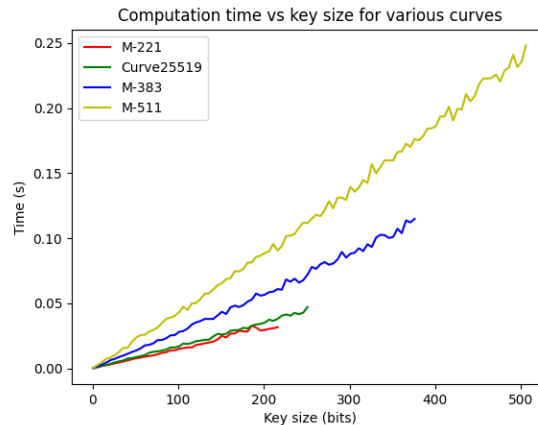


Figure 2: Comparison of various safe curves

I also looked at whether my implementation leaks any information through timing attacks, for example, is it possible to determine how many 1s are in the binary expansion of the key by analysing the time taken to compute results in Figure 3.



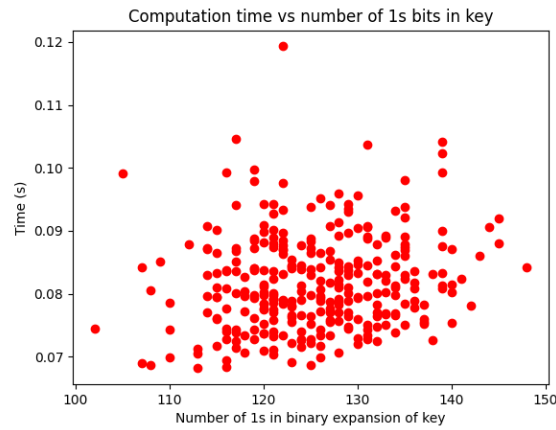


Figure 3: Analysis of information leaked through timing attacks

I then investigated timing attacks with regards to the size of the binary expansion of the key in Figure 4

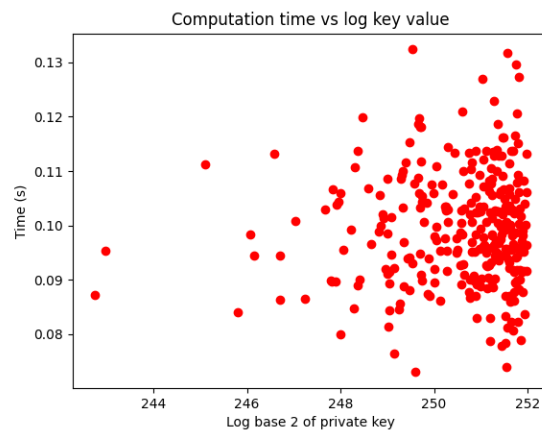


Figure 4: Timing attacks analysis

## IV RESULTS

This section presents the results of the solutions. It should include information on experimental settings. The results should demonstrate the claimed benefits/disadvantages of the proposed solutions.

This section should be between 2 to 3 pages in length.

- 25% of paper
- Description of the evaluation method adopted - evaluated by trying to break the encryption and demonstrating that it would take an infeasible amount of time
- Clarity of results

## V EVALUATION

This section should be between 1 to 2 pages in length.

- 20% of paper
- Suitability of approach
- Discussion of strengths and limitations of the system - limitations with communicating over networks, works well with multiple client instances on a local machine
- Discussion of algorithms used - ECDH, ECDSA, point addition and point multiplication
- Appraisal of project organisation

## VI CONCLUSIONS

This section summarises the main points of this paper. Do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions. This section should be no more than 1 page in length.

- 5% of paper
- Description of the main findings
- Clarity of conclusions
- Discussion of further work

Much research has been done into Elliptic Curve Cryptography since its discovery in 1985 (Miller 1986, Koblitz 1987). The security of ECC is based on the hardness of the ECDLP, and currently the best algorithms known to solve the ECDLP have fully exponential running time. In contrast to the subexponential-time algorithms known for the integer factorisation problem, on which the security of RSA is based. This means that, for example, a 160-bit EC key provides the same level of security as a 1024-bit RSA key (Hankerson et al. 2003, Silverman 2009). ECC is a very strong encryption method, but only when implemented properly, using a safe curve (Bernstein & Lange 2013, Bernstein 2006) and a good random number generator (Hotz 2010).

## References

- Adleman, L. (1979), A subexponential algorithm for the discrete logarithm problem with applications to cryptography, *in* '20th Annual Symposium on Foundations of Computer Science (sfcs 1979)', pp. 55–60.
- Anoop, M. (2007), 'Elliptic curve cryptography, an implementation guide', *online Implementation Tutorial, Tata Elxsi, India* **5**.
- Bernstein, D. J. (2006), Curve25519: New diffie-hellman speed records, *in* M. Yung, Y. Dodis, A. Kiayias & T. Malkin, eds, 'Public Key Cryptography - PKC 2006', Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 207–228.
- Bernstein, D. J. & Lange, T. (2013), 'Safecurves: choosing safe curves for elliptic-curve cryptography. <https://safecurves.cr.yp.to>, accessed 25 october 2020'.
- URL:** <https://safecurves.cr.yp.to>
- Brown, D. (2009), 'Standards for efficient cryptography 1 (sec-1)', *Standards for Efficient Cryptography, 2009*.

- Diffie, W. & Hellman, M. (1976), 'New directions in cryptography', *IEEE Transactions on Information Theory* **22**(6), 644–654.
- Ducklin, P. (2021), 'Poison packages - "supply chain risks" user hits python community with 4000 fake modules'.  
**URL:** <https://nakedsecurity.sophos.com/2021/03/07/poison-packages-supply-chain-risks-user-hits-python-community-with-4000-fake-modules>
- Hankerson, D., Menezes, A. J. & Vanstone, S. (2003), *Guide to elliptic curve cryptography*, Springer Science & Business Media.
- Hotz, G. (2010), Console hacking 2010-ps3 epic fail, in '27th Chaos Communications Congress'.  
**URL:** <https://fahrplan.events.ccc.de/congress/2010/Fahrplan/events/4087.en.html>
- Jurišić, A. & Menezes, A. (1997), 'Elliptic curves and cryptography', *Dr. Dobb's Journal* pp. 26–36.
- Koblitz, N. (1987), 'Elliptic curve cryptosystems', *Mathematics of computation* **48**(177), 203–209.
- Koblitz, N., Menezes, A. & Vanstone, S. (2000), 'The state of elliptic curve cryptography', *Designs, codes and cryptography* **19**(2-3), 173–193.
- López, J. & Dahab, R. (2000), 'An overview of elliptic curve cryptography'.
- Miller, V. S. (1986), Use of elliptic curves in cryptography, in H. C. Williams, ed., 'Advances in Cryptology — CRYPTO '85 Proceedings', Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 417–426.
- Rivest, R. L., Shamir, A. & Adleman, L. (1978), 'A method for obtaining digital signatures and public-key cryptosystems', *Commun. ACM* **21**(2), 120–126.  
**URL:** <https://doi.org/10.1145/359340.359342>
- Silverman, J. H. (2009), *The arithmetic of elliptic curves*, Vol. 106, Springer Science & Business Media.