EC and Lattice Key Exchange performance study based Public-Key Cryptographic Protocols

Mohammad Ahmad Alia
Al Zaytoonah University of Jordan
dr.m.alia@zuj.edu.jo

Abstract

With the rapid evolution of the internet of Things, key exchange protocols become one of today's hottest research areas due to its ability to verify things together, which reduce costs associated with computing. This paper summarizes the development in Elliptic Curve (EC) and Lattice key exchange protocols which are actually based on mathematical hard problems. In general, most of the currently used public-key exchange protocols are computationally expensive with relatively lengthy key requirement due to the dependency on the number theory. Therefore, it's essential to show the relationships and differences between EC and lattice protocols. In the surveyed protocols, we present exemplified region of some public-key exchange protocols. Every public-key cryptosystem is normally based on a mathematical problem that is, in some sense, difficult to solve. Nevertheless, the EC and Lattice of the key size become crucial to prevent a brute force attack. Lattice problem offers the possibility of faster cryptographic protocols.

Keywords: *Cryptography, Elliptic Curve, Lattice, and Key Exchange.*

1. Introduction

In general, a security protocol uses public-key cryptosystem to exchange the secret key between communicating nodes. However, public key cryptosystem is employed to exchange the secret key and then uses faster secret key algorithms to ensure confidentiality of the data stream [1, 2]. In public key algorithm, there are two keys, which are generated by one of the communication party, either the sender or the recipient. Whereby, each key is used to accomplish the rest tasks of the other key.

The key exchange is an essential method in public-key Cryptography. Keys are exchanged between the users according to Cryptography protocols, which are based on different mathematical hard problems. The first cryptosystem was created to utilize public-key or asymmetric cryptography keys by Diffie-Hellman [3]. Asymmetric key systems use two keys – one called the private key that the user keeps private and one called the public key that can be shared [3, 4, 5].

This paper shows the relationships and deference between EC and Lattice public-key primitives based key exchange protocols (refer to Figure 1). The article discusses the security performance on public-key schemes, which include EC and Lattice key exchange.

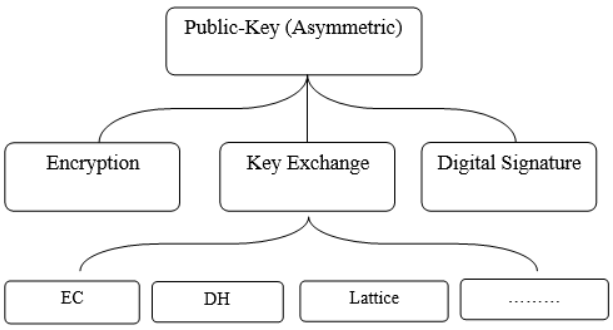

Figure 1: public-key exchange scheme

2. Public-Key Cryptography

The most important branches of an asymmetric cryptosystem (public-key) are shown in Figure 1 as classified into three techniques: key exchange, encryption, and digital signature. Based on mathematical hard problems, each technique is categorised into many subcategories (discrete logarithm, integer factorization, Elliptic Curve, lattice, etc.).

2.1 Key Exchange

As mentioned earlier, the key exchange protocol is defined by Whitfield Diffie and Martin Hellman [3] as the first method in public-key Cryptography. Keys are exchanged between the users according to Cryptography protocols. Diffie and Hellman highlighted the most important method of exchanging the keys over insecure medium by using the discrete logarithm hard problem as the trap-door function (refer to Figure 2).

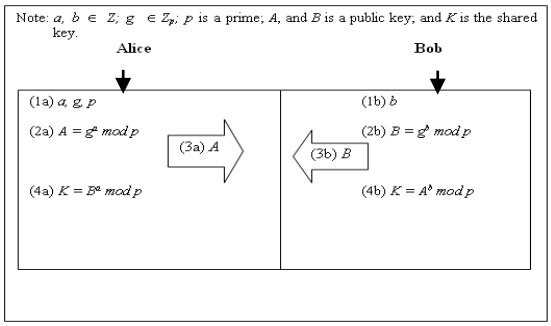

Figure 2: Whitfield Diffie and Martin Hellman protocol [1]

2.2 ECC Cryptography

Elliptic Curve Cryptography (ECC) was developed by Koblitz and Miller [6]. It is normally using small key size for key exchange, encryption/decryption and digital signature. Meanwhile, The ECC security mechanism is based on the Elliptic Curve Discrete Logarithmic math Problem (ECDLP) [8], since it can reach the RSA security level with small key size and high performance speed. Recently, EC is being used intensively through the internet of things to provide confidentially, integrity and non-repudiation for messages. However, Elliptic Curve (refer to Figure 3) is defined over a prime finite fields and generated by Equations 1 and 2.

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

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

.

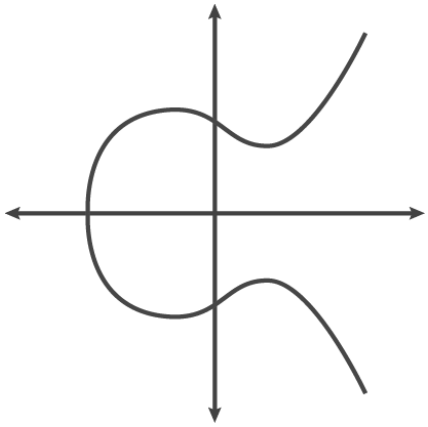

Figure 5 Elliptic curve $y^2 = x^3 - 3x + 5$

In ECC, The parameters set is dependent on the underlying finite field. So that if the field is GF(p), then the parameters set defines the curve as (p,a,b,G,n,h). Whereas, if the finite field is GF(2^m) then parameters defines the curve as (m,f(x),a,b,G,n,h). The meaning of each element in both sets is the following [9]:

- p: is the prime number that characterizes the finite field GF(p).
- m: is the integer number specifying the finite field GF(2^m).
- f(x): is the irreducible polynomial of grade m defining GF(2^m).
- a and b: are the elements of the finite field GF(q) taking part in the equation (1).
- G=(Gx,Gy): is the point of the curve that will be used as a generator of the points representing public keys.
- n: is the prime number whose value represents the order of the point G (i.e. n·G=O).
- h: is the cofactor of the curve, computed as h=#E/n, where n is the order of the generator G.

Therfore, the public key is computed as a point on the curve and the private key is selected as curve random number.

2.3 Key Exchange Based on Elliptic Curve: Elliptic Curve Diffie-Hellman (ECDH) Key Exchange

The Elliptic Curve Diffie-Hellman is a key exchange protocol. It is used to exchange a secret key between two users over an insecure medium without any prior communication between them. Elliptic Curve

Diffie-Hellman protocol is based on the additive Elliptic Curve group G_p or GF(2^k) [10]. The exchanged secret is then used as the secret key for subsequent communication (refer to Figure 3).

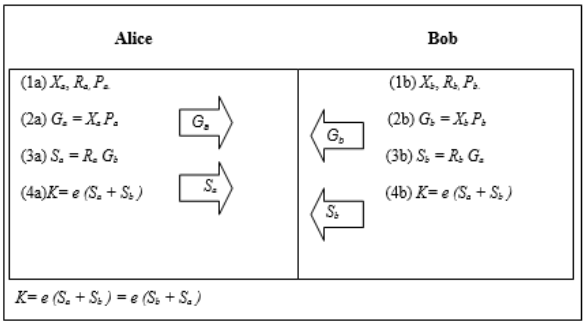

Figure 3: Elliptic Curve Diffie-Hellman (ECDH) key exchange protocol

Elliptic Curve Diffie-Hellman Protocol

This protocol assumes that only the curve E and F_q are public (refer to Figure 3) and assumes the point P as a secret key [10].

Elliptic Curve Diffie-Hellman Algorithm

Algorithm for key exchange

Alice must do the following (refer to Steps 1a to 4a in Figure 3):

1a. Alice must choose the following:
- X_a: Alice's first ephemeral key, random number in F_n.
- R_a: Alice's second ephemeral key, random number in F_n.
- P_a: Elliptic Curve point.

2a. Alice will compute the point: $G_a = X_a P_a$ and send it to Bob.

3a. Alice receives G_b from Bob and compute the point: $S_a = R_a G_b$, and send it to Bob.

4a. Alice receives S_b from Bob and then he will compute the secret key: $K = e(S_a + S_b)$.

Bob must do the following (refer to Steps 1b to 4b in Figure 3):

1b. Bob must choose the following:
- X_b: Bob's first ephemeral key, random number in F_n.
- R_b: Bob's second ephemeral key, random number in F_n.
- P_b: Elliptic Curve point.

2b. Bob will compute the point: $G_b = X_b P_b$ and send it to Alice.

3b. Bob receives G_a and computes the point: $S_b = R_b G_a$ and send it to Alice.

4b. Bob receives S_a from Alice and then he will compute the secret key: $K = e(S_b + S_a)$.

The security of the Elliptic Curve Diffie-Hellman key exchange protocol is based on the strength of the Elliptic Curve discrete logarithm hard problem and the size of the key used. However, the Elliptic Curve Diffie-Hellman protocol is considered secure against brute force attack because the private key is not disclosed and no party can get the private key of the other [10].

2.4 Lattice Cryptography

Lattice is a high-performance mathematical object (refer to Eq. 3) that have been used to solve several serious problems efficiently in computer security. Computationally, Lattices have been used in Cryptography by applying lattice hard problems to design robust cryptographic utilities. Lattice Cryptography implements the key exchange protocol that was proposed by Alkim, Ducas, Pöppelmann and Schwabe [11], [12]. However, the implementation of key exchange based lattice has been successfully computed on the Number Theoretic Transform to achieve higher performance. Lattice Cryptography is fully protected against timing and cache attacks (Its security prevents hardness assumptions) and is significantly faster than previous cryptographic protocols in term of the same security level [12]. Moreover, Lattices have classified its mathematical background based problems to; Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP). Whereby, SVP and CVP usually are considered hard to solve. Also, Lattices have been efficiently designed to implement public key exchange, encryption and digital signatures [13] (refer to Figure 4).

$$l(b_1, \ldots, b_n) = \left\{ \sum_{i=1}^{n} x_i b_i : x_i \in Z \right\} \qquad (3)$$

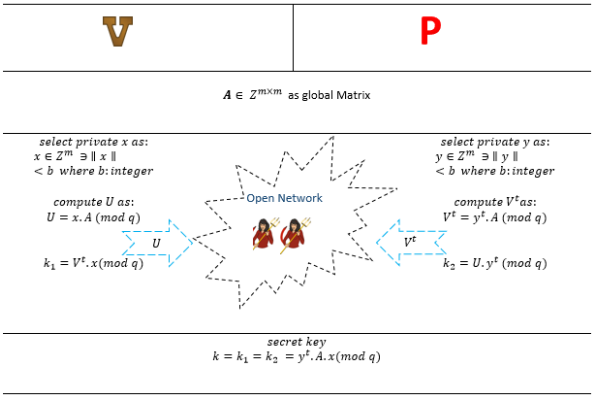

Figure 4: key exchange protocol based Lattice

3. Performance Evaluation Based on Equivalent Key Sizes for Lattice, EC, and other Public-Key cryptography Protocols

In this study, Authors show the security performance for Lattice and Elliptic Curve Cryptography comparing with other public-key exchange based primes protocols. So the comparison results show that the Lattice and EC public key cryptosystem perform better than other public key based prime's cryptosystem. In general, Lattice and EC public key cryptosystem provide a higher level of security with much lower cost. Although, Table 1 shows the key size for prime based public key protocols such as DH [3], Lattice protocols [12], and EC (refer to Figure 5), regarding the resistance to brute force attacks [14].

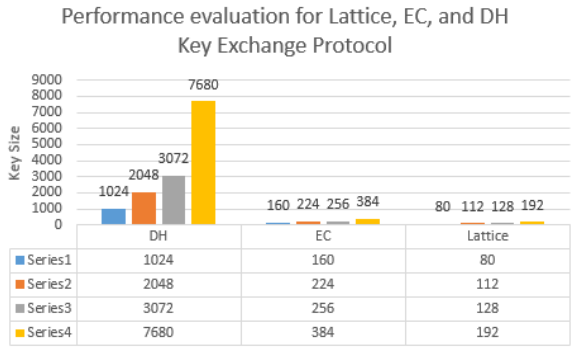

Figure 5: Performance for Lattice, EC, and DH based on key size evaluation

Table 1: Performance evaluation for Lattice, EC, and DH

key exchange Protocols		
Mathematical Hard Problem / Protocol	**Efficiency**	**Typical Key Size for High Performance**
Discrete Logarithm (DH)	DH speed is slow	(1024-bit)
EC	EC is faster than DH	(160-bit)
Lattice	Lattices are more complicated than DH. The lattice based public-key cryptosystem provides Key generation 300 times speed advantage compared to DH.	(128-bit)

The performance of the Lattice and EC public-key cryptosystem algorithms had been compared against the well-known public key protocols such as DH. The comparisons show that the Lattice based public-key exchange protocol provides a higher level of security at a much lower cost, both in terms of key size and execution time.

7. Conclusion

This paper has shown the possibility of applying Lattice and EC cryptographic systems for key exchanging over insecure networks. Lattice key exchange is more complicated than EC and DH. As the discussion, this summarization is proposed to replace the traditional previous key exchange protocol based cryptography, since the authentication, confidentiality, and accessibility cryptographic services are truly provided by Lattice with small key size, as well as it considered as faster cryptographic protocol.

Acknowledgments

The authors would like to thank AL-Zaytoonah University of Jordan for supporting this study.

10. References

[1] M. Alia and A. Samsudin, "New Key Exchange Protocol Based on Mandelbrot and Julia Fractal Sets", *International Journal of Computer Science and Network Security*, 7(2), pp. 302-307, 2007.

[2] Menezes, A., P. Van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, pp.4-15, 516, 1996.

[3] W. Diffie, and M. E. Hellman, "New Directions in Cryptography", *IEEE Transactions on Information Theory*, IT-22, pp. 644-654, 1976.

[4] T. ElGamal, "A Public-Key Cryptosystem and a Signature *Scheme Based on Discrete Logarithms", IEEE Transactions on Information Theory, IT-31(4), pp. 469–472, 1985.*

[5] *R. A. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, 21(2), pp.120-126, 1978*.

[6] N. Koblitz, "Elliptic Curve Cryptosystems", *Mathematics of Computation*, pp. 203–209, 1987.

[7] V. Miller , "Use of elliptic curves in Cryptography," Springer-Verlag, vol. CRYPT0 '85, no. LNCS 218, pp. 417-426, 1986.

[8] D. S. Kumar, C. Suneetha and A. ChandrasekhAR , "Encryption of data using elliptic curve over finite fields," International Journal of Distributed and Parallel systems, vol. 3, no. 1, pp. 301-308, 2012.

[9] V. G. Martinez, L. H. Encinas and C. San, "A survey of the elliptic curve inegrated encryption scheme," Journal of Computing Science and Engineering, vol. 2, no. 2, pp. 7-13, 2010.

[10] Kaabneh, k., and Al-Bdour, H. (2005) Key Exchange Protocol in Elliptic Curve Cryptography with No Public Point. American Journal of Applied Sciences, 2(8), pp. 1232-1235.

[11] J. Bos, C. Costello, M. Naehrig, D. Stebila, "Post-quantum key exchange for the TLS protocol from the ring learning with errors problem", in Proceedings of the IEEE Symposium on Security and Privacy, 2015.

[12] E. Alkim, L. Ducas, T. Pöppelmann and P. Schwabe, "Post-quantum key exchange – a new hope", IACR Cryptology ePrint Archive, Report 2015/1092, 2015.

[13] Luca De Feo 2017, "Mathematics of Isogeny Based Cryptography". CoRR, abs/1711.04062

[14] B. Elaine, W. Barker, W. Burr, W. Polk, and M. Smid, "Recommendation for Key Management – Part 1: General", NIST Special Publication 800-57, 2006.