Lightweight Security Algorithm for Low Power IoT Devices

Tarun Kumar Goyal
Electronics and Communication Engineering
Malaviya National Institute of Technology
Jaipur, India 302017
Email: tarunkgoyal11@gmail.com

Vineet Sahula
Electronics and Communication Engineering
Malaviya National Institute of Technology
Jaipur, India 302017
Email: sahula@ieee.org

***Abstract*—In today's technology, ever increasing number of electronics applications require secure communication, for example the Internet of things devices. Elliptic Curve Diffie Hellman (EC-DH) Algorithm has emerged as an attractive and effective public-key cryptosystem. Elliptic curves are widely used in various key exchange techniques that include the Diffie-Hellman Key agreement scheme. When contrasted with conventional cryptosystems like RSA, ECC offers equivalent security with smaller key sizes, which results in lower power consumption, speedier calculations, and also lower memory and transmission capacity (bandwidth) reserve. This is particularly valid and helpful for applications like IoT gadgets, which are regularly constrained regarding their CPU processing speed, power, and area. This work includes the software and hardware implementation of Diffie-Hellman, Elliptic Curve Diffie-Hellman (ECDH) Key agreement algorithm, and RSA algorithm. The proposed work also involves analysis of power, performance, area, and their comparisons thereof. The comparison is based on metrics obtained, after implementing the algorithms in synopsys using 90 nm UMC Faraday library. The ECDH algorithm is found to be better than others as far as power and area are concerned.**

***Index Terms*—Cryptography, crypt-analysis, ECC, ECDH, internet of things (IoT).**

I. Introduction

Internet has facilitated a comprehensive and global view to connect "everything" in literal sense. Today, a computer is much less useful without a connection; tomorrow, that will be the case with appliances like washing machine and refrigerator. In short, these appliances should communicate to each other; and do so in one or few common languages that others would be able to understand. That is impossible without global fraternity working together to create those languages. The new developments and IoT in particular, are making the twain meet. That means, we will get abnormal accuracy, speed, and efficiency of the digital world in our physical world, not just make it better in quantitative means, but also in some qualitative ways as well by taking things to those who do not have access to a lot of those because of "physical" constraints e.g. -shopping, banking, education, healthcare etc. Authors in [1] emphasize that security, protection, and trust should be considered as major configuration parameters (e.g. security by-configuration) of sensor frameworks, in light of the fact that genuine and multi-dimensional issues related with these ranges are natural to the IoT paradigm. One vision of the future is that IoT turns into a utility with expanded modernity in detection [2]. This will bring about subjectively diverse ways of life from today. As indicated by authors in [3], the future is unpredictable and they claim not to have predicted the Internet, social networking, Facebook, Twitter, millions of apps for smart phones, etc. Furthermore, these have all subjectively changed social orders' way of life. Vast size of devices have given birth to new issues, the association between the physical and digital universes, the openness of the frameworks, and proceeding with issues of protection and security. The Internet of Things is an idea that envelopes an assortment of innovations and exploration territories that intend to extend the current Internet to genuine objects like health, smart cities, and digital India. According to Pike Research on Smart Cities, the Smart City business sector is evaluated at several billion dollars by 2020, with a yearly spending coming to about 16 billion [4]. The exploratory remote sensor system testbed, with more than 300 hubs, conveyed at the University of Padova has been outlined by rules, and effectively used to acknowledge verification of idea exhibitions of the keen framework and medicinal services administrations. The essential objective of Padova Smart City is to advance the early selection of open information and ICT arrangements in general society organization. The objective application comprises of a framework for gathering natural information and checking general society road lighting by method for remote hubs, outfitted with various types of sensors, set on road light posts and associated with the Internet through an gateway unit [5]. Available IoT solutions in the market is smart wearable, Smart home, smart city, and many more[6].

On the other hand, all the vulnerabilities of the digital world, despite evolving protection mechanisms at one go, come to the physical world. There's no choice to retreat; no hiding place - our electricity, our car, our library, our water, our refrigerator, our city's transport systems - all are vulnerable to attack. The moment we imagine an attack on a smart city centralized servers, we realize the challenges and and urgency to move ahead with the new revolution.

A. Proposed work

This paper's primary focus is on lightweight yet robust & low power algorithm for encryption and decryption using key

978-1-5090-2029-4/16/$31.00 @2016 IEEE

exchange algorithm. While exploring several algorithms for the purpose, we focused on Diffie-Hellman, Rivest-Shamir-Adleman (RSA), and Elliptic curve cryptography. We have proposed an improvement in computation of modulus of fractional numbers used in ECC methodology. We performed crypt-analysis alongside comprehensive power/performance analysis. The comparison is based on various metrics obtained, after implementing the algorithms in hardware using Synopsys CAD suite using 90 nm UMC Faraday library. The ECDH algorithm is found to be better than others as far as power and area are concerned.

The rest of the paper is organized as follows. We discuss Elliptical Curve Cryptography method in details in Section II, presenting affine point based multiplication & crypt-analysis. In Section III, we present methodology and algorithms- (i) for efficient computation of modulus of fractional number for use in ECDH, (ii) standard RSA algorithm for comparison benchmark, as it is asymmetric block cipher. Section IV, illustrates detailed results and comparison thereof of software & hardware implementation of RSA, DH and proposed efficient ECDH. The power consumption and security provided by each of the three is compared. We conclude in Section V .

II. Public-key algorithms

Two keys are involved in this type of crypto system through which a secure communication can be established between communicating user over an insecure channel. Since two different keys are applied here so this technique is termed asymmetric encryption. During this procedure, each party generates two keys. First is the private key that is the secret key and can not be disclosed and another is the public key, which is shared among all communicating users. If user A wants to send a message to user B, then user B generates and provides her/his public key and shares it with user A. Then user A encrypts the message using public key of B and own private key [7].

A. Encryption Scheme

The main purpose of message encryption is that unauthorized users do not get knowledge of original message. Therefore it seems reasonable to demand robustness of encryption schemes, so that it becomes hard to decrypt cipher text by unauthorized users. as an illustration, Elliptic Curve Cryptography (ECC) is applied to an image that is the transformation of an image into affine points (obtained by performing the multiplication operation) lie on the elliptic curve. Let a be the pixel value of an image then $P_{ML} = a * P_M$ yields a coordinate value that is transformation of scalar value into an affine point, and it is evaluated by performing multiplication on affine point P_M with a pixel value. After that P_{ML} is added with $K * PUB_B$ where K is a random number and PUB_B is a public key of user B. Upon completion of encryption a cipher text gets generated $CF = \{KG, P_{ML} + PUB_B\}$. Here, the first part KG forms a coordinate from mean (x_1, y_1), and second part of the cipher text $P_{ML} + PUB_B$ also forms a coordinate (x_2, y_2). Finally cipher text generated is $CF = \{(x_1, y_1), (x_2, y_2)\}$. This is an encrypted data yielded by encryption procedure.

B. Crypt-analysis

The general purpose of cryptography is to secure the plain text or key or both from cyber thieves called viz. foes, assailants, interceptors. Cyber terrorists are assumed to have complete access to the correspondences between the sender and beneficiary. Crypt-analysis is the process of recovery of the plain text of a message without availability of the key. It may likewise discover shortcomings in a cryptosystem that inevitably prompt the past results. In this section, we attempt to illustrate, how hard it is even with today's methods and computing power. The two most productive calculations for registering discrete logarithms on elliptic curve the baby step, giant step method, and Pollard's rho method has been tabulated in Table I [8].

TABLE I
CRYPT-ANALYSIS FOR ECC(PRIME V1 192 BIT)

Algorithm	*Time Complexity*	*Space Complexity*
Brute-Force	O(n) =O(2^{192})	O(l)
Baby-Step, Giant-Step	O(l)	O($\sqrt{n}$)=O($2^{\frac{192}{2}}$)
Pollard's Rho	O($\sqrt{n}$)=O($2^{\frac{192}{2}}$)	O(l)

C. Elliptic Curve Cryptography

The majority of the items and norms that utilize public key cryptography for encryption and Digital Signature use RSA. It is being observed that secure RSA needs lengthier key, which has been expanding over late years, and this has put a heavier overhead on applications utilizing RSA. This weight has consequences, particularly for e-commerce sites that direct huge quantity of secure transactions. Recently, elliptic curve cryptography (ECC) has started to challenge RSA. The main fascination of ECC, contrasted with RSA, is that it seems to offer equivalent security for a far smaller key size, and in this manner decreasing handling overhead. ECC is hard to clarify than either RSA or Diffie-Hellman. This section and the following one provide an understanding of elliptic curve and EC-DH. We present computations for elliptic curve characterized by the real numbers. This is trailed by a gander at elliptic curve characterized over prime fields. The curves is reproduced in Figure 1 for value of $a = 1$ and $b = 1$.

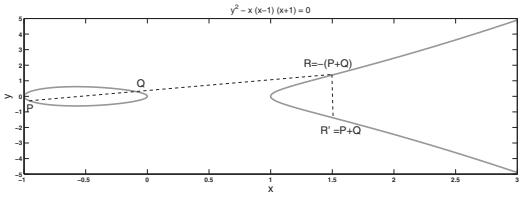


Fig. 1. Example of Elliptic Curves

D. Algebraic Description of Addition

In this subsection, we show some outcomes that empower computation of increments over an elliptic curve. For two

Algorithm 1 Modulus of a Fractional Number

1) For $i = 1, 2, 3, \ldots, (P-1)$, obtain smallest i for which $D * i > P > D * (i-1)$;
2) Update the values N and D; $N = N * i \,\%\, P$; $D = D * i \,\%\, P = D * i - P$
3) Repeat through STEP. 1), if $D \neq 1$;
4) Modulus of Fractional number is N

different points, $P = (x_P,\ y_P)$ and $Q = (x_Q,\ y_Q)$ slope of the line is $S = (y_Q - y_P)/(x_Q - x_P)$. Sum of two point $R = P + Q$ is computed as follows [9] .

$$x_R = S^2 - x_P - x_Q \tag{1}$$

$$y_R = -y_P + S * (x_P - x_R) \tag{2}$$

Doubling: $P + P = 2P = R$, when $y_p \neq 0$, the expressions would be as following.

$$x_R = (\frac{3 * x_P^2 + a}{2 * y_p})^2 - 2 * x_P \tag{3}$$

$$y_R = (\frac{3 * x_P^2 + a}{2 * y_p}) * (x_p - x_R) - y_P \tag{4}$$

III. Methodology

A. Modulus of a Fractional Number

Modulus of integers is simpler to compute. However, it is little hard to calculate modulus of a fractional number. Some scholars has proposed methods to calculate modulus of fractional numbers, but they are quite complex and heavy for presently considered application. We propose a method described in Algorithm 1. It is quite simpler and easier. In the method, numerator is denoted by N and denominator has been denoted by D. The modulus of this fractional number with respect to prime number P is expressed as $(N/D)\ \%\ P$.

B. Elliptic Curve Diffie-Hellman Key Exchange

Key exchange [10] utilizing elliptic curves should be possible in an accompanying way. To start with, let's pick (i) an extensive whole number q, which is either a prime number or a number of the structure 2^m and (ii) elliptic curve parameters a and b. This defines the value of $E_q(a, b)$. Next, select a base point $G = (x_1, y_1)$ in $E_q(a, b)$, whose order n is a large value. The order n is defined as smallest positive integer such that $nG = 0$. Here, n and G are parameters of the cryptosystem known to all participants.

A key exchange between users Alice and Bob can be accomplished as illustrated in Figure 2.

Algorithm 2 Elliptic Curve Diffie-Hellman Key Exchange

1) Alice pick a secret integer n_A as her private key such that $n_A < n$; Alice then produces her public key $P_A = n_A * G$ using equations 1 , 2 & 3, 4; The base point is $E_q(a, b)$;
2) Bob likely pick a secret integer n_B as his private key less than $n_B < n$; Bob then produce his public key $P_B = n_B * G$; The base point is $E_q(a, b)$;
3) Alice calculates the secret key $K = n_A * P_B$; Bob calculates the secret key $K = n_B * P_A$;

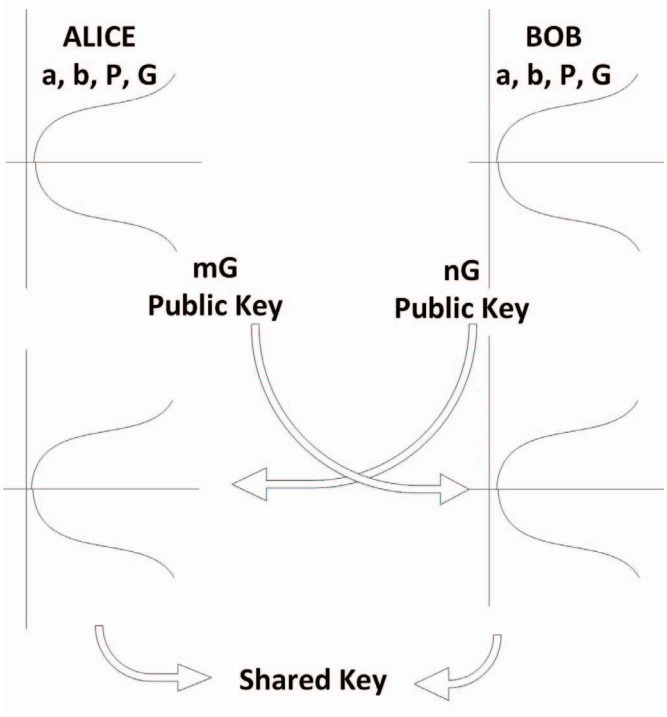


Fig. 2. Elliptic Curve Diffie-Hellman Key Exchange

The two generated key in Algorithm 2 produce the same result because $K = n_A * P_B = n_A * (n_B * G) = n_B * (n_A * G)$.

C. Rivest-Shamir-Adleman (RSA)

The Rivest-Shamir-Adleman (RSA) scheme is a block cipher in which the plain text and cipher text are integer values between 0 and $L - 1$ illustrated in Algorithm 3. A typical key size is 1024 bits. That is, $L < 2^{1024}$ [11].

IV. Results

Elliptic Curve Diffie-Hellman (ECDH)

A general elliptic curve is taken that is represented by the following equation: $Y^2 = (X^3 + aX + b) mod P$ where X and Y are elements of $GF(P)$ and a, b are the integers modulo P satisfying: $4a^3 + 27b^2 \neq 0 (mod\, P)$. Then, elliptic curve values are generated for which $a = 2$, $b = 0$ and $P = 37$. The generated private and public key pairs for user A and B are shown in Table II

Algorithm 3 Rivest-Shamir-Adleman (RSA)

1) Alice and Bob pick secret prime numbers, i.e. $p = 13$ and $q = 19$; both p and q are less than n and $p \neq q$;
2) Calculate a public parameter $n = p * q$; Compute a private parameter $\phi(n) = (p-1)(q-1) = 216$.
3) Alice picks an integer e as $1 < e < \phi(n)$ such that $gcd(\phi(n),\ e) = 1$;
4) Bob calculates a secret key using $(e,\ \phi(n))$ i.e. $d \equiv e^{-1}(mod\ \phi(n))$; e.g. for $e = 31$ computation yields $d = 7$;
5) Public key is $P_U = e,\ n = 31,\ 247$; Private key is $P_R = \{d,\ n\} = 7,\ 216$;

TABLE II
KEY EXCHANGE BETWEEN ALICE AND BOB

User	*Private Key*	*Base Point*	*Public Key*	*Share Key*
Alice	13	(5,1)	(5,36)	(24,14)
Bob	11	(5,1)	(24,23)	(24,14)

A. Encryption

During encryption of a sample image, each of its pixel value is read and transformed into a ciphertext by XORing it with the shared key. Message is shown in Figure 3(a). Values of pixel (M) will vary between 0 to 255 (Black to White). Encryption operation will be as follows- For plain text $(M_i) = 144$, Cipher text is $(C_i) = M_i \oplus (K_aX * K_aY)$. Encrypted image is shown in Figure 3(b).

B. Decryption

Now Bob will receive (C_i) and calculate the plain text (M_i) using his private key K_b. Decryption process will be as follows- $(M_i) = C_i \oplus (K_bX * K_bY)$. Decrypted image is shown in Figure 3(c).

C. Power Comparison

Diffie-Hellman key exchange algorithm, Rivest-Shamir-Adleman (RSA) algorithm, and Elliptic curve Diffie-Hellman (ECDH) algorithm were realized in hardware. Dynamic power is calculated using PrimeTime tool of Synopsys CAD suite. The results are shown in Figure 4. The dynamic power dissipated is sum of the internal power and switching power.

Table III summarizes the dynamic power comparison for various algorithms computed using PrimeTime (Synopsys) and Xilinx Xpower.

TABLE III
POWER COMPARISON FOR VARIOUS ALGORITHMS

CAD Tool	*Diffie-Hellman*	*RSA*	*ECDH*
PrimeTime (Synopsys)	0.832 mW	1.512 mW	0.570 mW
Xilinx XPower	6.0 mW	11.0 mW	5.0 mW

D. Area Comparison

Table IV summarizes the power comparison for various algorithm .

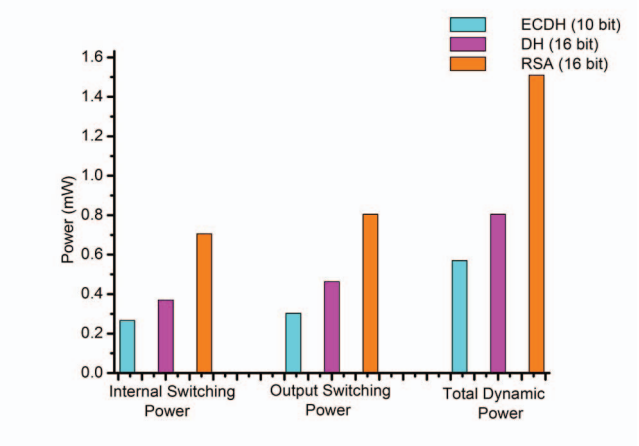


Fig. 4. Comparing dynamic power consumption for RSA, DH, and ECDH Algorithms

TABLE IV
AREA COMPARISON FOR VARIOUS ALGORITHMS

Design	*Diffie-Hellman*	*RSA*	*ECDH*
Design Area(90 nm)	0.058 mm^2	0.386 mm^2	0.032 mm^2

E. Performance Comparison

Table V summarizes the delay time comparison for various algorithm .

TABLE V
DELAY TIME COMPARISON FOR VARIOUS ALGORITHM

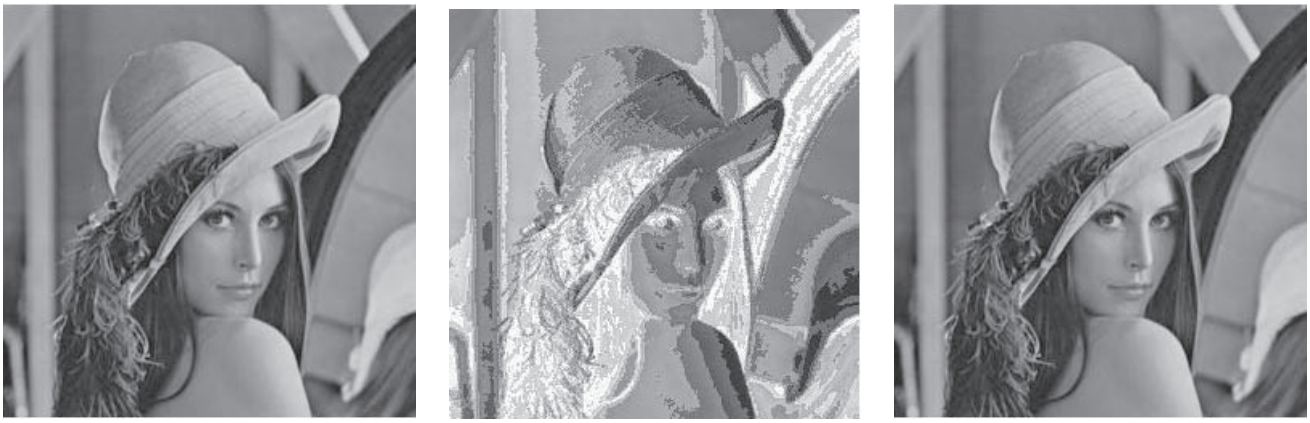
Delay Time (ms)	*Diffie-Hellman*	*RSA*	*ECDH*
Software (run time)	06.9	08.3	06.1
Critical path delay	49.6	90.7	22.4
Latency	49.6	90.7	22.4

F. Security Comparison

Security of a cryptography algorithm depends on the key size used. Difficulty in AES algorithms is exponential 2^n. Difficulty in ECDH is sub exponential $\sqrt{2^n}$. Difficulty is defined in RSA by n, where n is shown in equation 5 and L is the number of bits in key.

$$n = \frac{1.923 * \sqrt[3]{L * ln(2)} * \sqrt[3]{ln(L * ln(2))^2} - 4.69}{ln(2)} \quad (5)$$

Table VI summarizes the equivalent number of bits for each of the algorithms required to provide identical security; for considered algorithm, it is equivalent number of bits, for which key can be reverse-computed in equal amount of time for all algorithms considered. Here, the base algorithm is AES.



(a) Plain text image (b) Encrypted image (c) Decrypted image

Fig. 3. Encryption/Decryption of an image

TABLE VI
SECURITY COMPARISON FOR VARIOUS ALGORITHM

Key Size (No. of Bits)(L)	*AES*	*DH*	*RSA*	*ECDH*
5	5	16	16	10
27	27	128	128	54
57	57	512	512	114
80	80	1024	1024	160
110	110	2048	2048	220

V. CONCLUSION

In today's era of the omnipresent computing, the Internet has turned into the primary method of information correspondence. In such a domain, giving security to gadgets, Elliptic Curve Diffie Hellman(EC-DH) Algorithm has received achieved significance in view of its features like low power, lightweight & robustness, which is reasonable for IoT gadgets. We have performed comparisons with respect to power, area, and timing etc. for various algorithms like Diffie-Hellman, Rivest-Shamir-Adleman and ECDH. The Diffie-Hellman plan is one of the exchanging key cryptosystems. Messages are not included in this plan and hence we exploit this plan by utilizing the key being exchanged as a secret key; we utilize Elliptic curve cryptography with Diffie- Hellman for generating a key. We have implemented the EC-DH, DH, and RSA in software as well as in hardware. We synthesized and realized IC layout in $90nm$ FARADAY low power library and compared performance parameters like power, area and performance based on post-layout simulations. Results lead us to conclude that ECDH is superior to other considered algorithms in terms of power and area.

ACKNOWLEDGMENTS

The authors gratefully acknowledge the support received from project SMDP-C2SD funded by Ministry of Communication & IT, Government of India.

REFERENCES

[1] A. Skarmeta and M. V. Moreno, *Secure Data Management: 10th VLDB Workshop, SDM 2013, Trento, Italy, August 30, 2013, Proceedings*. Cham: Springer International Publishing, 2014, ch. Internet of Things, pp. 48–53.

[2] J. A. Stankovic, "Research directions for the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3–9, Feb 2014.

[3] K. Akpinar, K. A. Hua, and K. Li, "Thingstore: A platform for internet-of-things application development and deployment," in *Proceedings of the 9th ACM International Conference on Distributed Event-Based Systems*, ser. DEBS '15. New York, NY, USA: ACM, 2015, pp. 162–173. [Online]. Available: http://doi.acm.org/10.1145/2675743.2771833

[4] D. Bonino, M. T. D. Alizo, A. Alapetite, T. Gilbert, M. Axling, H. U. andJose Angel Carvajal Soto, and M. Spirito, "Almanac: Internet of things for smart cities," in *Future Internet of Things and Cloud (FiCloud), 2015 3rd International Conference on*, Aug 2015, pp. 309–316.

[5] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, Feb 2014.

[6] C. Perera, C. H. Liu, S. Jayawardena, and M. Chen, "A survey on internet of things from industrial market perspective," *IEEE Access*, vol. 2, pp. 1660–1679, 2014.

[7] S. M. C. Vigila and K. Muneeswaran, "Implementation of text based cryptosystem using elliptic curve cryptography," in *2009 First International Conference on Advanced Computing*, Dec 2009, pp. 82–85.

[8] J. M. Pollard, "Monte carlo methods for index computation," *Mathematics of Computation*, vol. 32, pp. 918–924, 1978.

[9] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, Nov 1976.

[10] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 5th ed. Upper Saddle River, NJ, USA: Prentice Hall Press, 2010.

[11] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978. [Online]. Available: http://doi.acm.org/10.1145/359340.359342