Transactions on Machine Intelligence 4(1) (2021) 21–28

ISSN Online: 2821-1693

Transactions on Machine Intelligence

Journal Homepage: https://tmachineintelligence.ir/index.php/TMI

Extended Access Control on Electronic Passport with the Aim of Overcoming Limited Computing Resources

Sh. Ghanbari[1], M.R Salehnamadi[2,*]

[1] Department of Computer-Software Engineering, Faculty of Engineering, Islamic Azad University, South Tehran Branch, Tehran, IRAN

[2] Assistant Professor, Department of Software Engineering, Software Engineering, Faculty of Engineering, South Tehran Branch, Islamic Azad University, Tehran, Iran

ARTICLE INFO

Article History:
Received 20 December 2020
Received in revised form
14 January 2021
Accepted 11 March 2021
Available online 12 March 2021

Keywords:
Authentication, Biometrics, Fingerprint, Diffie-Hellman method, Fast Exponential, Extended Access Control

ABSTRACT

In this project, Extended Access Control on the electronic passport was designed to overcome limited computing resources. Today, experts are looking for safer ways to identify and authenticate authenticity. One of the most successful of these ways is the use of biometrics. In this project, in order to reduce the volume of computing, the Fast Exponential method has also been added to Diffie- Hellman, as well as to enhance the security of the proposed research protocol and reduce the success rate of attacks such as a man-in-the-middle attack to steal information, from fingerprint to extract some of the required parameters of the Diffie-Hellman method (parameters q and g) is used. To this end, three different scenarios were raised. The results of the simulation showed that the proposed method reduces the computational load of the classical Diffie-Hellman method and, therefore, reduces the run-time. Also, the results showed that the first scenario is better than the other two scenarios in terms of both runtime and computational load.

1. INTRODUCTION

It has been a long-standing recognition of authenticity for human beings. Today, with the advancement of technology, attempts have been made to mechanize identification or identification systems. These improvements are due to the need of society and the world. Advances in which these needs have reduced violations, increased security, accelerated routines, and so on. Authentication is the process of attributing an identifier to a particular person. Acknowledging the authenticity of the process is to ensure that the user is properly identified. For example, to ensure authenticity, people are issued cards that have a photo and are made by comparing a person's face with a photo on a authenticity card. Biometrics refers to technology for measuring and analyzing the body's characteristics to identify a person. In a biometric, a person's automatic identification is performed using specific features such as physiological

* Corresponding Author: mrezanamadi@yahoo.com
Assistant Professor, Department of Software Engineering, Software Engineering, Faculty of Engineering, South Tehran Branch, Islamic Azad University, Tehran, Iran

http://dx.doi.org/10.47176/TMI.2021.21

© 2021 by the authors. Licensee T.M.I, Tehran, Iran. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) license (http://creativecommons.org/licenses/by/4.0/).

or behavioral characteristics. Fingerprint recognition, retinal diagnosis, iris diagnosis, face, DNA, speech and signature including these specifications. Among all these methods, the use of fingerprint recognition is more common. Biometric science, given its many benefits, has become a global focus on smart cards, including electronic passport. This method does not have other disadvantages (token and method of knowledge) and greatly increases security and accuracy.

To handling the challenges of biometric passports, including lack of direct input and display support, the Extended Access Control (EAC) mechanism was provided by experts. Reducing the computational load of the EAC protocol reduces the time it takes to authenticate and identify. In addition, the hardware costs of the protocol are also reduced. So far, references to the EAC protocol have not raised the issue of minimum requirements for computational resources. Therefore, in this research, we are presenting a methodology that, by focusing on the EAC protocol with less volume of computing, issues the certification on an electronic passport.

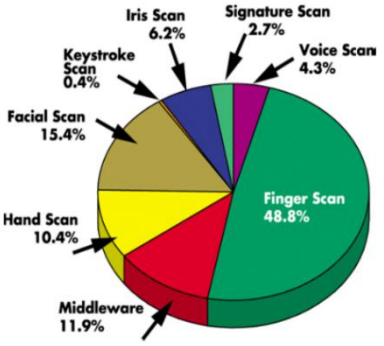


Fig. 1. Frequency of different Biometry methods in determining identity [1].

The first part of this article relates to the biometric passport and its challenges. In the second part, the EAC protocol and its types are reviewed and the steps and challenges of the advancement of this protocol are introduced. In the following, some of the EAC-based protocols are introduced to handling the challenges presented. The third part of this article contains a brief overview of related resources. In the fourth section, we first introduce the Diffie-Hellman algorithm and then the improved model of this fingerprint algorithm is presented and three suggested research scenarios are introduced to reduce the computation load and the time required for authentication. In the fifth part, we also present the results of the proposed method. Finally, Section 6 relates to the conclusions of the research.

2. BIOMETRIC PASSPORT AND EAC PROTOCOL

A biometric passport is a combination of traditional and electronic passports that have a chip containing biometric information that is embedded in the back cover and includes the name, date and place of birth, gender, digital photo of the traveler, issuance date and passport number And used to authenticate passengers. One of the most important challenges and problems encountered in the electronic passport is security issues related to the authentication of electronic passport holders and how to do it. So if the person using the passport is the same as the holder of the passport? Confronting the types of attacks on electronic passports is another challenge that electronic passport development may face. [3]

The On-line Secure E-Passport Protocol (OSEP) protocol and the PACE and BioPACE security mechanisms are examples of electronic passport protocols. In all existing technologies, the issue of unauthorized access to the biometric information of the passport holder is an important issue. To this end, the EAC protocol emerged to control the access. The purpose of this protocol is to provide a tool for protecting biometric content and overcoming unauthorized use. The EAC mechanism restricts access to specific details of the content of the electronic passport to only authorized sections such as border control [4].

The EAC protocol itself includes a variety of designs and architectures. Using the infrastructure of this protocol, countries will be able to perform EAC-based authentication with fingerprints and iris images under bilateral

agreements. The EAC E-Passport characteristic is based on the authentication techniques proposed by Dr. Kluger from the German Federal Office for Information Security (BSI) and has three consecutive steps:

- ✓ PACE
- ✓ Chip authentication
- ✓ Terminal authentication

The PACE protocol for reading and using information requires the physical link between the eMRTD and Terminal [5]. This protocol is a Diffie-Hellman-based password-based protocol, in which a random amount (s) is selected and encrypted by the embedded eMRTD chip, and then transmitted to the terminal, the terminal receives and decrypts it. The eMRTD chips and the terminal simultaneously create a pair of temporary-life keys and a secure message exchange with validation.

The TA protocol has the ultimate endorsement and the attack is "sensitive information theft" [6]. Terminal authentication (TA) is used to determine whether the inspection system (IS) is allowed to read sensitive data from the e-passport.The purpose of the CA protocol is to verify the chip. The proposed attack is "simulation of the electronic passport chip". At the CA stage, the chip also answers itself through the challenge-response step, but using the key received, it validates a message authentication code instead of a signature. The present research deals with the approach to reduce the computational load for this stage.

The architecture of the EAC protocol is shown in Figure 2. Naturally, many countries, and not all of them, will appear in both the role of the issuer and the receiver of electronic passports, hence the presumed architecture include two states of the exporter and the accepting state. Contains entities including a national identification authority, a CAS validation document, personalization systems, and inspection systems. [7]

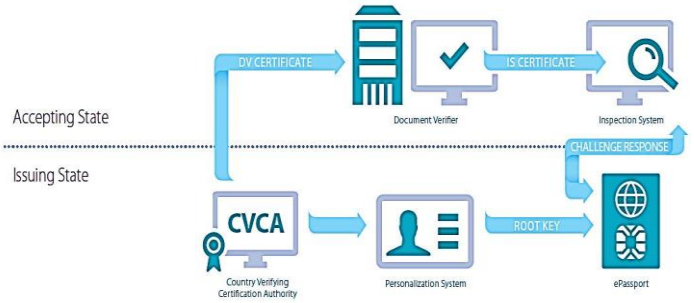


Fig. 2. EAC protocol architecture [7].

The following is a review of internal and external investigations on biometric passports and EAC protocols.

3. A RESOURCE OVERVIEW

Because electronic interactions are not faced, the issue of authentication is considered as one of the issues of electronic security. If one can surely prove that the business parties are the same as those claiming, one of the challenges in electronic interactions will surely be resolved. In [8], a new model for identity authentication has been presented alongside the biometric index of individuals, RFID identification and image processing. The proposed system is designed in two phases of the production of identity card and authentication process. Personal biometric images are placed on an RFID tagged contactless card, and for each identity verification, information on the card is compared with its online biometric image. If the identity of the person is established, personal information entry and his birth certificate is not required, but his information is called by an Electronic Personal Code (EPLC) from a centralized database.

The main purpose of reference [9] is to improve authentication protocols and key agreement. Thus, in this research, the security of the two authentication protocols and the key agreement recently presented for the Session start protocol and remote medical information systems have been analyzed. In this research, it has been shown that the authentication protocol and the key agreement provided for the start-up protocol are based on the user's identity tampering protocol and the protocol provided for remote medical information systems against repeat and denial-of-

service attacks are Vulnerable. Then, using the elliptical curve encryption, two authentication protocols and a new key agreement for the session start protocol and remote medical information systems are presented. Security and performance analysis shows that the proposed protocols not only increase security but also improve performance.

Given that the proposed method of research is based on the Diffie-Hellman algorithm and fingerprint minutiae, we will further describe this algorithm and then the fingerprint.

4. DIFFIE-HELLMAN ALGORITHM

The Diffie-Hellman key exchange protocol is a cryptography protocol in which two person or two organizations can create a common password key without any prior knowledge and exchange it through a non-secure communication path. The protocol was designed in 1976 by two scientists named Wimbledon, Whitfield D. and Martin Hellman, and published in a scientific paper[10]. The introduction of this protocol is an important step in the introduction and development of asymmetric key cryptography. According to [11] and [12], this protocol consists of the following four algorithms:

4.1. Algorithm for generating domain parameters

The parameters (p, q, g) are called domain parameters.

Input: Required Lengths for p Modulus and Density First q

Output: Parameters (p, q, g)

4.2. Domain parameter authentication algorithm

Input: Parameters (p, q, g)

Output: "Confirmation of Parameters" or "Failure to Accept Parameters"

4.3. The key pair production algorithm

Input: Parameters (p, q, g)

Output: private / public key pair A, (a, A) and side B, (b, B)

4.4. Common Counter Calculator Algorithm

Side A:

Input: Parameters (p, q, g), B and a

Output: Common password Z

Side B

Input: Parameters (p, q, g), A and b

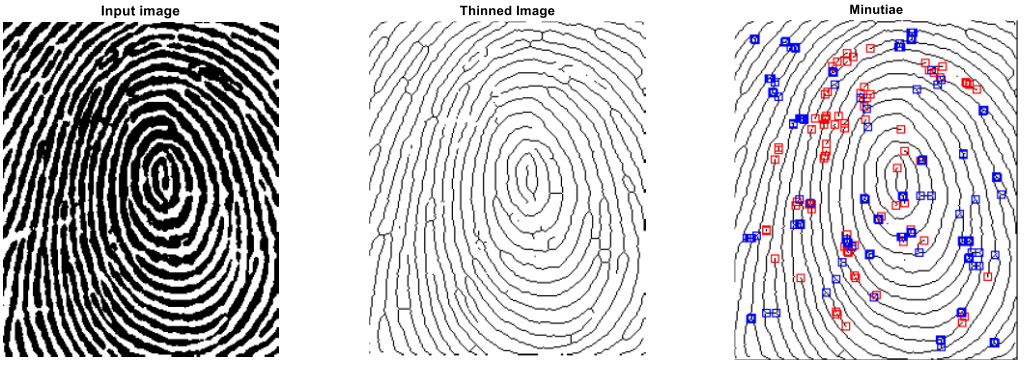
Output: Common password Z

5. MINUTIAE FINGERPRINTS

The process of extracting fingerprints from the three stages is as follows:

1. Take binary image
2. Undo binary image and convert to skeletal image
3. Minutiae extraction

Figure (3a) shows the binary image of a person's fingerprint. After thinning, the skeletal image is obtained according to Fig. 3 (b). Eventually, minutiae mining operations are carried out by performing two processes for finding Ridge and Bifurcation.



(a) (b) (c)

Fig. 3. Minimized fingerprint extraction.

6. SUGGESTED METHOD

In the Diffie-Hellman protocol, we deal with numbers in terms of $c = a^n$ to modulus of m. Given that the numbers a and b are large, calculating the number c requires a n-1 Modular multiplication that can be long and slow Computational load. To solve this problem, you can use the fast exponential method. If we can write n as a power of 2 or a sum of multiple numbers with power 2, then the number of multiplications will decrease from n-1 number to $\lfloor \log n \rfloor$ number or $2^{\lfloor \log n \rfloor}$. This reduces the predicted load significantly, which speeds up the Diffie-Hellman key exchange procedure. This method is known as fast exponential. According to the fast exponential method, if $n = (\beta_k \beta_{k-1} ... \beta_.)_2$ and $\beta_k \neq 0$ Unless $k = 0$, in this case $2^k < n < 2^{k+1}$ and $k = \lfloor \log n \rfloor$. In the Diffie-Hellman algorithm, the parameters q and g are also chosen at random in the field of generating domain parameters.

In the present study, these parameters are obtained from the fingerprint, in order to increase the security and prevent data theft through attacks such as the man-in-the-middle attack, instead of randomly generating the parameters q and g. How to extract these numbers from a fingerprint is as follows:

By extracting a person's fingerprint binary image of a person, we obtain its bifurcation information. Bifurcation is in two directions x and y. By combining these two large numbers, one number is obtained as follows:

S = [bifurcation_x', bifurcation_y']

Now, by specifying the number between the required parameters q and g (lq and lg), we act as follows:

Select a lq bit and lg from S. This can be done randomly, ie, by mixing the number S or non-random. Here, in order to find a unique number, we choose lq and lg of the first bit of the S number.

Calculate the remainder of the division of numbers q and g into 2.

- If this remainder is equal to 1 then q = q+1 and g = g+1.
- If this remainder is equal to 1 then q = q+2 and g = g+2.

1- Step 2 We go forward to get the numbers q and g of the prime number.

Therefore, in this research, the first stage of the Diffie-Hellman algorithm presented in Section 5 is stated as follows:

Algorithm for generating domain parameters

Input: Parameters q, g and required length of p

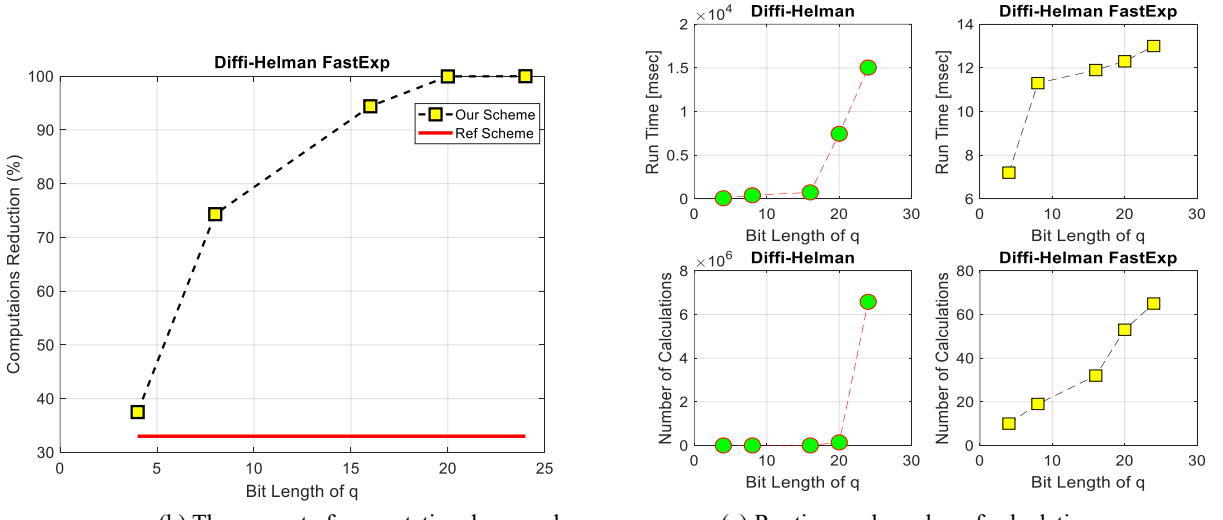
Output: Parameter (p)

1- Extraction of the prime number q and g with the required length of fingerprint.
2- Choosing a random number j of bit length bitlen (p) - bitlen (q); (bitlen: bit length)
3- Calculate p = jq + 1. If p is not the prime, go to step 2.
4- Calculate g modulus to p. If g = 1 go to step 4.
5- Obtain (p).

Of course, it is worth mentioning that in addition to the above, with both q and g of fingerprints extracted, two other scenarios, in which only q or g of fingerprints are extracted, will also be considered. Therefore, in the series, three scenarios are investigated in the following study: First scenario: q and g extraction of fingerprints, second scenario: q extraction of fingerprints and g randomly, third scenario: g extraction of fingerprints and q randomly.

7. THE RESULTS OF THE RESEARCH

In this section, the results of the simulation of the classical Diffie-Hellman method and the Diffie-Hellmann method with rapid power over the length of the various bits of the q parameter, which are randomly selected, are compared. This comparison is based on the parameters of the run-time and the number of calculations. Figure (4a) shows the execution time of the algorithms and the number of calculations of the two algorithms for the various bit lengths q. As can be seen, with increasing bit length, runtime and number of computations of the classical Diffie-Hellman method, the rapid expansion is much lower. Reference [13] has introduced an algorithm that reduces by about 33%, according to the number of calculations, compared to the classical Diffie-Hellman method. Figure (4b) shows the reduction in the calculation of the proposed method of rapid strength compared to the classical Diffie-Hellman.



(b) The amount of computation decreased

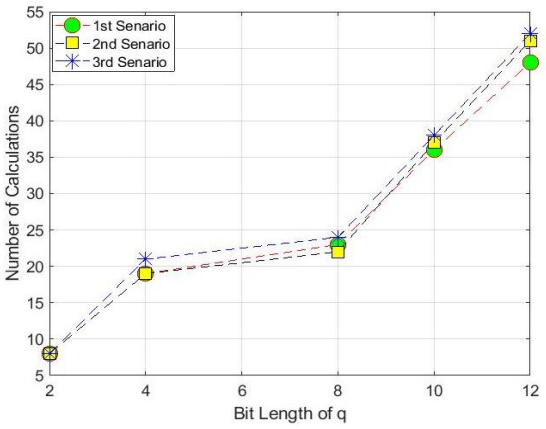
(a) Runtime and number of calculations

Fig. 4. Runtime, number of calculations, and the amount of computation of the proposed method and reference method [12]. Two differential Diffie-Hellman algorithms and fast exponential for different bit length q.

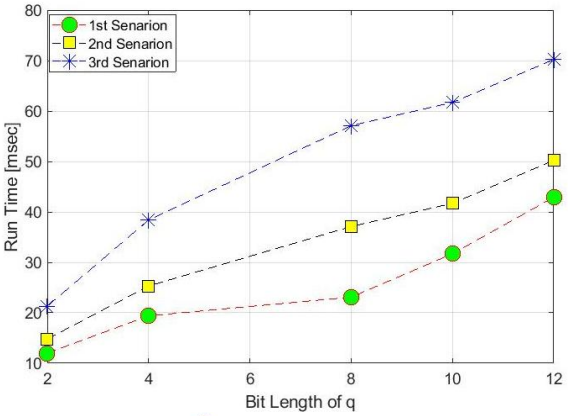
In the following, we will look at the outcomes of the three scenarios described in the previous section.

Figure (5a) shows the implementation time required for the three proposed research scenarios. According to this diagram, it is clear that the first scenario has the least time for the other two scenarios, and the third scenario has the highest execution time. Therefore, in terms of run time, the best scenarios can be arranged in the first scenario, second scenario, third scenario. Figure (5b) also shows the number of calculations required for the three scenarios. According to this diagram, it is also clear that all three scenarios have a close number of calculations, and the first scenario has the lowest computations and the third scenario has the highest number of computations.

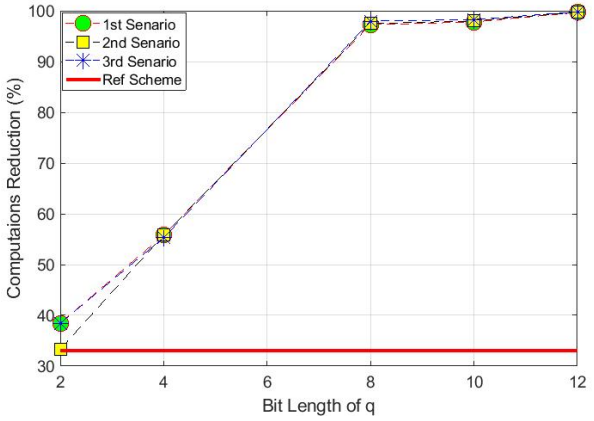
Fig. 5 (c) also shows a reduction in the calculations of the three scenarios compared to the classical Diffie-Hellman method. According to this chart, all three scenarios are successful in reducing the amount of computations and their reduction is approximately the same.



(b) Required number of calculations



(a) *Running time*



(c) The amount of computation decreased

Fig. 5. Runtime, number of calculations, and the amount of computation of the three proposed research scenarios for different bits.

8. CONCLUSION

In the present study, the Diffie-Hellmann method was used to identify identity. To reduce the computational volume, the Rapid Enhancement Method was also added to the Diffie-Hellmann method, and as a result, a rapid diffusion-Hellman method was improved. Also, to enhance the security of the proposed protocol and reduce the success rate of attacks such as an intermediate man strike to steal information, fingerprints were used to extract some of the parameters required by the Diffie-Hellman method (parameters q and g).

Classical Diffie-Hellman method is one of the high computational load methods for identifying the number of heavy calculations required at each stage. So, in order to reduce the computational burden, a quick power-up method was introduced, in which a far fewer amount of computations is required for computational calculus. The results of

the simulation show that the load volume of the calculations decreases from 30 to more than 98 percent using the fast-strength method, depending on the length of the bit of the parameter q, which is a significant reduction, compared with the result of a reduction of 33 percent comes [12]. Also, the time of execution of the two-Diffie-Hellman classical and Diffie-Hellman quick algorithms showed that the implementation time of the Diffie-Hellman method increases with a significant increase in the length of the bit q, but the Diffie-Hellman method is rapidly increasing slightly. This result is associated with a reduction in the calculation load of the Diffie-Hellman method in comparison with the classical Diffie-Hellman.

In addition, simulation results show that in all three proposed research scenarios, the load of calculations is significant and the rate of this reduction is almost the same in each scenario. In all three scenarios, the implementation time is far less than the classical Diffie-Hellman method. In this regard, scenario 1 is the best scenario and the third scenario is the worst scenario. In all three scenarios, the calculation is far less than the classical Diffie-Hellman method, and the number of calculations for each of the three scenarios is close. However, the first scenario has the lowest computational load, and the third scenario has the highest computational burden. According to the results of the research, the first scenario is presented as the best scenario for reducing the run-time and load of identification calculations with increasing security.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFRENCES

[1] Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: A tool for information security. IEEE Transactions on Information Forensics and Security, 1(2), 125–143. https://doi.org/10.1109/TIFS.2006.873653

[2] Jain, A. K., Ross, A. A., & Nandakumar, K. (2011). Introduction to biometrics. Springer. https://doi.org/10.1007/978-0-387-77326-1

[3] Sinha, A. (2011). A survey of system security in contactless electronic passports. Journal of Computer Security, 19(1), 203–226. https://doi.org/10.3233/JCS-2010-0414

[4] Dagdelen, Ö., & Fischlin, M. (2010, October). Security analysis of the extended access control protocol for machine readable travel documents. In International Conference on Information Security (pp. 54–68). Springer. https://doi.org/10.1007/978-3-642-18178-8_6

[5] Buchmann, N., Peeters, R., Baier, H., & Pashalidis, A. (2013, September). Security considerations on extending PACE to a biometric-based connection establishment. In 2013 International Conference of the BIOSIG Special Interest Group (BIOSIG) (pp. 1–13). IEEE.

[6] Calderoni, L., & Maio, D. (2014). Cloning and tampering threats in e-passports. Expert Systems with Applications, 41(11), 5066–5070. https://doi.org/10.1016/j.eswa.2014.02.044

[7] Mbithi, M. (2010). East African Community (EAC) Protocol on Common Market: implications for Kenya Private Sector in Kenya.

[8] Victory, N. (2009). Integrated system design for radio frequency identification (RFID) based identification and biometric indicators in e-commerce interactions [Master's thesis, Shiraz University].

[9] Abbasinezhad-Mood, D., Nikooghadam, M., Mazinani, S. M., Babamohammadi, A., & Ostad-Sharif, A. (2019). More efficient key establishment protocol for smart grid communications: Design and experimental evaluation on ARM-based hardware. Ad Hoc Networks, 88, 194–202. https://doi.org/10.1016/j.adhoc.2019.03.005

[10] Cervantes-Vázquez, D., Ochoa-Jiménez, E., & Rodríguez-Henríquez, F. (2021). Extended supersingular isogeny Diffie–Hellman key exchange protocol: Revenge of the SIDH. IET Information Security, 15(5), 364–374. https://doi.org/10.1049/ise2.12027

[11] Rescorla, E. (1999). Diffie–Hellman key agreement method (RFC 2631). Internet Engineering Task Force. https://doi.org/10.17487/rfc2631

[12] Law, L., Menezes, A., Qu, M., Solinas, J., & Vanstone, S. (2003). An efficient protocol for authenticated key agreement. Designs, Codes and Cryptography, 28(2), 119–134. https://doi.org/10.1023/A:1022595222606

[13] Tsaban, B. (2006). Fast generators for the Diffie–Hellman key agreement protocol and malicious standards. Information Processing Letters, 99(4), 145–148. https://doi.org/10.1016/j.ipl.2005.11.025