Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI)
Vol. 7, No. 3, December 2021, pp. 380-387
ISSN: 2338-3070, DOI: 10.26555/jiteki.v7i3.22210

Secure Key Exchange Against Man-in-the-Middle Attack: Modified Diffie-Hellman Protocol

Mostefa Kara [1], Abdelkader Laouid [1], Muath AlShaikh [2], Ahcène Bounceur [3], Mohammad Hammoudeh [4]
[1] LIAP Laboratory, El Oued University, PO Box 789, El Oued 39000, El Oued, Algeria
[2] Computer Science Department, College of Computing and Informatics, Saudi Electronic University, 11673 Riyadh, KSA
[3] Lab-STICC UMR CNRS, University of Western Brittany UBO, Brest 6285, France
[4] School of Computing, Mathematics and Digital Technology, Manchester Metropolitan University, Manchester, M1 5GD, UK

ARTICLE INFO

Article history:

Received November 10, 2021
Revised December 10, 2021
Accepted December 12, 2021

Keywords:

Key exchange;
Diffie-Hellman protocol;
Cryptography;
Security;
Secure communication

ABSTRACT

One of the most famous key exchange protocols is Diffie-Hellman Protocol (DHP) which is a widely used technique on which key exchange systems around the world depend. This protocol is simple and uncomplicated, and its robustness is based on the Discrete Logarithm Problem (DLP). Despite this, he is considered weak against the man-in-the-middle attack. This article presents a completely different version of the DHP protocol. The proposed version is based on two verification stages. In the first step, we check if the pseudo-random value α that Alice sends to Bob has been manipulated! In the second step, we make sure that the random value β that Bob sends to Alice is not manipulated. The man-in-the-middle attacker, Eve, can impersonate neither Alice nor Bob, manipulate their exchanged values, or discover the secret encryption key.

Corresponding Author:

Mostefa Kara, LIAP Laboratory, El Oued University, PO Box 789, El Oued 39000, El Oued, Algeria
Email: karamostefa@univ-eloued.dz

1. INTRODUCTION

In cryptology, a key exchange mechanism (Fig. 1) is a method that allows several elements to agree on an encryption key. Thanks to asymmetric cryptography in the 1970s, the first key exchange protocol appeared, and it can be secure and with the use of an insecure communication channel, where a trusted third party is not used. Before the appearance of asymmetric (public key) encryption, there were no mathematical methods to perform a key exchange. Only it was completely based on operational security where the key must be passed through an already secure channel; in other words, one must involve the physical transport of diplomatic bags containing the keys.

The first key exchange technique is described in [1]. The idea is to put a public list of problems (the puzzles), which require some effort to find the solutions, and which reveal two secrets once solved. To get a key, we randomly choose one of these problems and solve it. The first secret should be passed on to the puzzled owner and let them know which puzzle was solved, and the second secret serves as a key. The attacker listening to the conversation does not know, a priori, which puzzle was selected. To find the key chosen by both participants, the attacker must, in the worst-case solve all the puzzles offered. It, therefore, faces a problem of quadratic complexity. On the one hand, coming up with a set of puzzles each time is not a practical method. On the other hand, in the random oracle model, the safety of this technique is shown to be effectively quadratic in the number of puzzles. This level of complexity is not sufficient in modern cryptography, so in [2], this technique is shown that it is not possible to improve the technique of [1].

The Diffie-Hellman technique only provides security against a passive opponent. That opponent can overhear the conversation but cannot interfere with it. If the opponent is able to intercept the messages, then one speaks to a man-in-the-middle attack. Where it is enough for the adversary to impersonate one to the other,

and vice versa, in the end, the adversary will establish with each a key, and consequently, he will be able to decipher the data sent by one to the other.

In Fig. 1, f denotes the function which calculates the output; not necessarily that f_i equals f_{i+1}. After n iterations, the system gives the secret key.

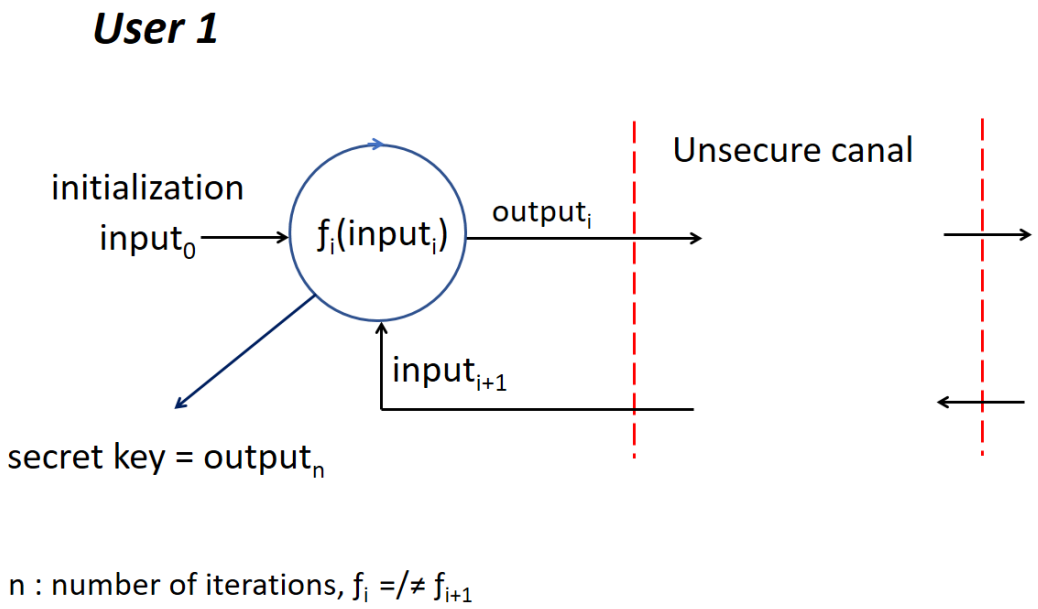


Fig. 1. General diagram of key exchange protocol

In 2002, the work of [3] showed the use of Weil couplings on elliptical curves to make a three-party key exchange. If the Diffie-Hellman mechanism is used, it requires the establishment of a secure channel between each pair. In 2003, the authors in [4] presented a generalization of [3] in order to guarantee the exchange of keys between an arbitrary number of entities using a cryptographic multilinear application.

Quantum key exchange protocols have been proposed to exploit the properties of physics to ensure the security of the key exchange instead of using mathematics and computer science. More particularly, based on the statistical properties of a flow of entangled particles linked to the non-cloning theorem, it is possible to discover an attacker who is listening and discarding a set of the bits thus revealed by correcting the noise. Many of these protocols have been presented and implemented over distances covering a few hundred kilometers [5].

On the other hand, this type of key exchange poses a number of technological and operational challenges. These challenges limit its deployment. In particular, a specific communication channel must be established between the participants. For the BB84, B92 [6], or SARG04 [7] protocols, it must guarantee the transport of low-energy photons with the conservation of their polarization despite decoherence phenomena over the entire length of the channel.

In this article, we define a new key exchange mechanism. This technique is the modification of the Diffie-Hellman protocol in a very simple way and very robust. We have focused especially on avoiding the man-in-the-middle attack as the Diffie-Hellman protocol is widely used around the world, except that it is vulnerable to this type of attack. The remainder of the manuscript is organized as follows. Section Related Work provides an overview of the key exchange protocols. In Section Diffie-Hellman Protocol, we describe the Diffie-Hellman mechanism. In Section Proposed Protocol, we show the proposed protocol. Section Proposal Analysis analyses our technique. Finally, we conclude with Section Conclusion.

2. RELATED WORK

In this section, various related works are discussed. Mainly, we have two genders of information encryption, the first is symmetric key encryption, and the second is asymmetric key encryption [8-9]. In the first type, participants use the same secret key to encrypt and decrypt data. The second type is used in many fields, such as blockchain [10]. Also, we have two genders of keys; the public key that is used in the encryption operation and the private key for the decryption operation.

There are several techniques based on asymmetric encryption like RSA cryptosystem, scheme of Diffie-Hellman key exchange (DH), scheme of Elliptic Curve Cryptography (ECC), the specific Elliptic Curve Diffie-Hellman (ECDH), and ElGamal cryptosystem [11]. In [12], the authors presented a hybrid encryption technique

using the Diffie-Hellman mechanism and a technique called DHTTIE for a Text-to-Image encryption scheme. In this proposition, the message is transformed as an image. The key of encryption will not be sent over the channel but is constructed on both sides based on Diffie-Hellman protocol. Plain text is encrypted, exploiting two levels of encryption. The first is Cipher Text Plan (CIP), and the second Correction Plan (COP). The ECDH is a public key-based agreement technique that allows two entities to share the secret key for use in symmetric encryption [13-14]. ECDH is more robust than other traditional algorithms like RSA regarding key size, compute, also network bandwidth.

There is two class of two-party authenticated key agreement schemes, such as Password Authenticated Key Exchange Protocol (PAKE), the second is Authenticated Key Exchange Protocol (AKE) [15-16]. The AKA (Authenticated Key Agreement) mechanism is used to establish a common session key for two communicators. This key is exploited for the purpose of the following cryptography. Most protocols of key agreement (such as the MQV family) use one key per session. MQV is one of the Memoranda of Understanding of the Diffie - Hellman family [17]. On the one hand, this protocol offers key authentication and transmission confidentiality. On the other hand, MQV is vulnerable to the attack of unknown key sharing [18].

The HMQV protocol is the improvement of MQV [15] based on provable safety. HMQV removes some verification steps done by MQV, such as proof of possession (PoP) verification during certification authority registration and ephemeral public key primary order validation verification [19]. Based on ECDH, the authors in [20] proposed a multi-session key. This protocol exploits the idea of hashed MQV. In [21], the authors proposed a protocol based on Bilateral Generalization Inhomogeneous Short Integer Solution (Bi-GISIS) for post-quantum IoT security. This protocol reduces the time consumption in the key generation. To ensure a reusable key, the authors defined modified bilateral pasteurization in the random oracle model. So, the same key becomes available in several executions. The authors of [22] proposed a lightweight key exchange (LKE) architecture to the honest IoT nodes and interdict uncertified mistreats. This scheme uses lightweight Elliptic Curve Qu-Vanstone (ECQV) that exploits implicit certificates for trust-building and generating keys between parties. In [23], a Diffie-Hellman key exchange implementation using stéganographied images has been presented. The authors used the Least Significant Bit (LSB) method [24]. In which, participant A calculates $x = y^a$, then hidden by the LSB steganography algorithm and transmitted to the other participant B. The problem with this protocol is that an attacker spoofs the entity of B.

In [25], the authors proposed an end-to-end password-based model key exchange protocol for privacy-preserving. This protocol is used for multi-server architecture in the environment of edge computing. In [26], a Lightweight Authenticated Key Exchange (AKE) scheme for the Internet of the Drone (IoD) environment (LAKE-IoD) has been presented. This protocol offers the session key establishment model between MU and drone using a server. LAKE-IoD uses the authenticated encryption technique AEGIS [27], hash function, and XOR compute. The authors of [28] presented an authenticated key exchange technique for fog computing and demonstrated that the [29] model for fog computing is vulnerable to ephemeral secret leakage attacks. Based on elliptic curve cryptography, the authors in [30] presented an authentication and key exchange protocol between the smart meter and the Advanced Metering Infrastructure (AMI) HeadEnd in the smart grid.

3. DIFFIE-HELLMAN PROTOCOL

In 1976, building on Merkle's construction, Whitfield Diffie and Martin Hellman [31] proposed to use the discrete logarithm problem in a finite field, a computational problem considered difficult, as a basis for constructing a key exchange mechanism. It is now the most widely used on the Internet through the TLS protocol.

The publication of Whitfield Diffie and Martin Hellman initiated a revolution in cryptography [32]. The theoretical conceptions of the public key encryption and the digital signature were presented and realized two years after Diffie and Hellman in the RSA cryptosystem by authors Rivest, Shamir, and Adleman [33-39]. However, Diffie and Hellman proposed the first system to take into account public key properties. A previous protocol Merkle, called the Merkle Riddles, served the same purposes, but the DH protocol has the best relationship between safety and efficacy. The DHP allows two users Alice and Bob, who are communicated by an authenticated channel but at the same time not secure, to create a secret cryptographic key. This key is hard to find by an attacker Eve hearing the communication of Alice and Bob. The system works as follows. Let G be a finite cyclic group of order |G| generated by a given number *g*. In order to generate a cryptographic key, Alice and Bob secretly choose the integers α and β, respectively, at random where α and β are less than G. Then, Alice and Bob secretly calculate $A = g^{\alpha} \bmod p$ and $B = g^{\beta} \bmod p$, respectively, and exchange these group items over the unsecured public channel. Finally, Alice and Bob calculate respectively $B^{\alpha} = (g^{\beta})^{\alpha} = g^{\beta\alpha}$ and $A^{\beta} = (g^{\alpha})^{\beta} = g^{\beta\alpha}$. This value is used as a secret key shared by Alice and Bob. Fig. 2 shows a mechanical analog of the Diffie-Hellman protocol. Although this protocol is widely used, it is easily attacked by the man-in-the-middle attack.

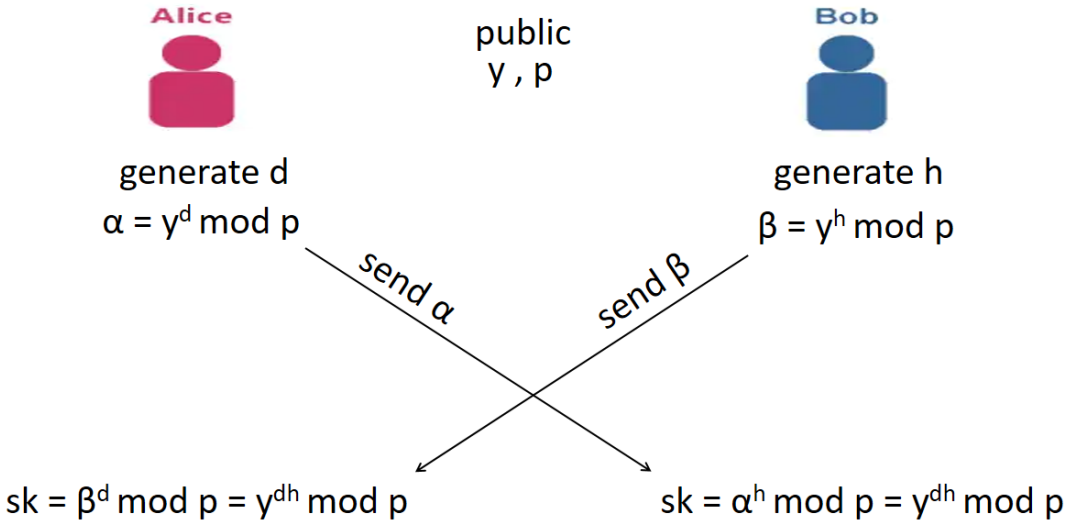


Fig. 2. Diffie-Hellman protocol illustration

3.1. MAN-IN-THE-MIDDLE ATTACK

This attack can be described as follows: Alice generates a one-time private key α, calculates Y_a ($Y_a = y^{\alpha}$), and sends it to Bob. The adversary Eve intercepts Alice's message, saves it and generates a one-time private key *e*, calculates Y_e ($Y_e = y^e$), and sends it to Bob. This message to Bob has Alice's User ID but Eve's public key. This message is sent in such a way that it appears as though it was sent from Alice's host system. Similarly, Bob generates a one-time private key β, calculates Y_b ($Y_b = y^{\beta}$), and sends it to Alice. Eve sends a message to Alice with Eve's public key $Y_{e'}$ ($Y_{e'} = y^{e'}$), purporting to come from Bob. Alice calculates a secret key $k_1 = (Y_{e'})^{\alpha}$ mod p; Bob calculates a secret key $k_2 = (Y_e)^{\beta}$ mod p. So, $k_1 = y^{\alpha e'}$ and $k_2 = y^{\beta e}$; we see that Eve can calculate k_1 and k_2 (Eve have: *e'* and y^{α}; *e* and y^{β}).

4. PROPOSED PROTOCOL

The proposed protocol does not depend on a number given beforehand *g* like the case of DHP, to store the generated value. In our protocol, Alice generates a pseudo-random value α and then sends it to Bob. After generating the random value α, Alice calculates its inverse α^- using (1), where $(x^{\alpha})^{\alpha-} \bmod p = 1$. Bob generates a random value β which will be the encryption key later. After receiving α, Bob calculates the $v_1 = (\beta^{\alpha}, \beta^{\beta})$. The first value ($\beta^{\alpha}$) is for masking β, the second (β^{β}) is for checking that β is not manipulated, then v_1 is sent to Alice. Upon receipt of v_1, Alice calculates β using α^-, which for her is β_1 until it is verified by Bob. After that, Alice performs the first validation process ($\beta_1^{\beta 1}$! β^{β}), which is not sufficient. Alice calculates the value $v_2 = \beta_1^{\alpha}$ and sends it to Bob to finally ensure its validation. After receiving v_2, Bob compares it to β^{α}. If this is correct, the secret key β is valid and secure, and now Alice and Bob can encrypt messages with it. Fig. 3 shows the general diagram of the proposed protocol.

To transport the secret key β, Alice generates a pseudo-random value α and computes α^- where $\beta = (\beta^{\alpha})^{\alpha}$, we don't want to use the public key "*e*" of RSA, i.e., $(m^e)^d \bmod n = m$, because *d*, in this case, is unique. On the other hand, we will calculate the pair (α, α^-) by the following equation:

Calculate the pair (α, α-)
$$a^- = \frac{p + i\ x\ (p-1)}{a} \quad (1)$$

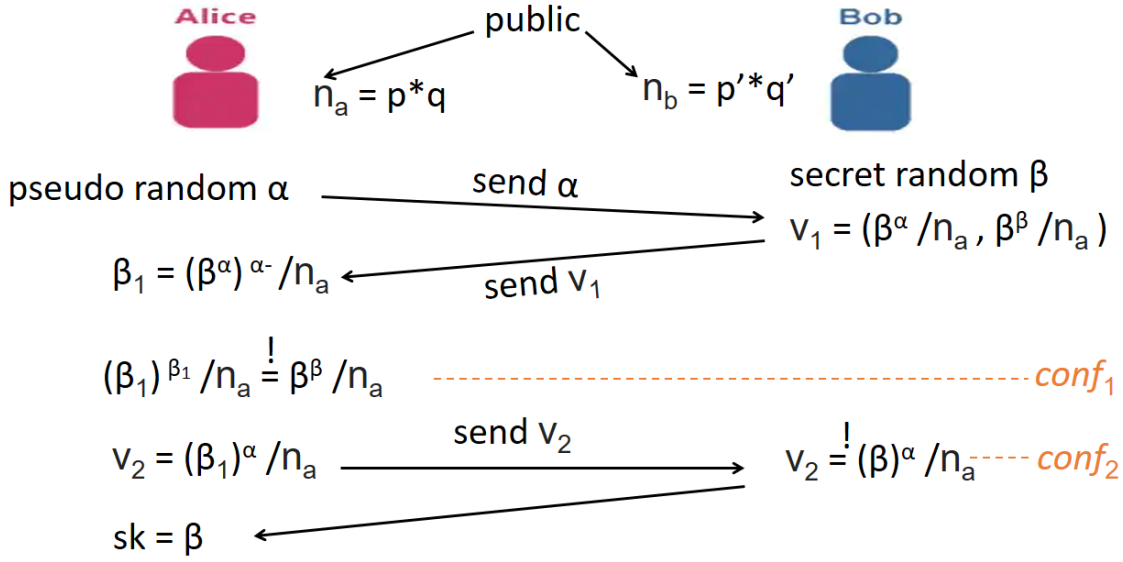
where p denotes the private trapdoor (n = pq), i is an integer, and:

Relation between α and i
$$(p + i\ x\ (p-1)) mod\ a = 0 \quad (2)$$

Equation (1) equivalent to: (α x α^-) = (p + i x (p-1)). Noting here that there is an infinite number of α^- for the same α, so that these values of α^- are easy to find.

Demonstration

According to (1), $\alpha * \alpha- = p + i * (p-1)$, $(m^{\alpha})^{\alpha-} \bmod p = m^{\alpha\,\alpha-} = m^{(p + i * (p-1))} \bmod p = (m^p * m^{i * (p-1)}) \bmod p$, we have $m^p \bmod p = m$, $m^{i * (p-1)} \bmod p = (m^{(p-1)})^i \bmod p$, we have $m^{(p-1)} \bmod p = 1$, so $(m^{\alpha})^{\alpha-} \bmod p = m$.



$(x^{\alpha})^{\alpha-} /p = x$, sk : shared secret key between Alice and Bob, /: modulo, conf: confirmation

Fig. 3. Proposed protocol

5. PROPOSAL ANALYSIS

One of the most important principles in this type of protocol (key exchange) is the assumption that the channel is insecure. In the first scenario of the proposed technique, we assume that the adversary Eve spies on the channel and can manipulate the value of α and impersonate Alice (see Fig. 3). Eve will produce a new value α' and send it to Bob as Alice. Bob calculates the pair $v_1 = (\beta^{\alpha'}, \beta^{\beta})$. When Alice receives v_1, she extracts β_1 using α^- then calculates $\beta_1^{\beta 1}$. Of course, $\beta_1^{\beta 1}$ is different from β^{β} because $\beta_1 \neq \beta$ (see $conf_1$ in Fig. 3).

The second scenario is the most dangerous when Eve does not manipulate the value of α but will produce a new value β', intercepts v_1, and creates a new pair v'_1 using the value real of α, $v'_1 = (\beta'^{\alpha}, \beta'^{\beta'})$. Eve sends v'_1 to Alice as Bob. After receiving v'_1, Alice extracts β'_1, calculates $\beta'^{\beta' 1}_1$, and compares it with $\beta'^{\beta'}$. Now, the $conf_1$ is validated because $\beta'_1 = \beta'$. That's why we added $conf_2$ to the protocol (see Fig. 3). After the first confirmation, Alice calculates $v'_2 = (\beta'_1)^{\alpha}$ and sends it to Bob. Even after Eve intercepts v'_2, there is nothing he can do because it does not have the real value of β. When Bob receives v'_2, he will compare it to β^{α}. Of course, the result does not match because $\beta'_1 \neq \beta$ (β' is generated by Eve). Alice and Bob will easily discover that the values have been manipulated. Finally, we can see that our protocol is secure against a man-in-the-middle attack.

The effective protocol must be robust to passive attacks (if an attacker tries to prevent communication by simply observing honest elements running the protocol) and also to active attacks (if an attacker subverts communications by injection, deletion, etc., modification or replay of messages). There are security attributes that our protocol achieves. We consider that A and B are two honest entities.

- Known key security: Each execution of our protocol between two elements A and B, produces a unique secret key; the keys produced are called session keys. The proposed scheme is always carried out in the presence of an attacker who has learned other session keys.
- Forward secrecy: In the proposal, if the secret keys of the current session of one or more entities are compromised, the secret keys of previous sessions established by these honest entities are not affected.
- Key compromise impersonation resilience: Now suppose that A's long-term secret key is leaked. So, the attacker who knows this key can now pretend to be entity A. However, this scenario does not allow the attacker to pretend to be entities other than A because each communicating pair has its own private key.

6. CONCLUSION

In this article, we have presented a KEP, which we consider to be a new version of DHP. The objective of the proposed protocol was to face up to the man-in-the-middle attack that suffered from it the original DHP. In the analysis, we have proved that the proposed technique is very robust against this type of attack. A man-in-the-middle attack cannot be applied in all scenarios where the attacker in the middle cannot deceive both users by impersonating and by manipulating the secret key. Therefore, the proposed technique ensures the

exchange of keys in complete confidentiality and security. Although attacks other than man-in-the-middle in DHP have been studied, in the future, we would like to study the robustness of the proposed protocol against other known attacks. We would also like to find a simpler, faster, and more efficient way to compute α^{-} which will support this protocol with more flexibility.

REFERENCES

[1] R. C. Merkle, "Secure communications over insecure channels, "*Communications of the ACM*., vol. 21, pp. 294-299, 1978. https://doi.org/10.1145/359460.359473
[2] B. Barak, and M. Mahmoody, "Merkle puzzles are optimal-an O(n 2)-query attack on Any Key Agreement from Random oracle," *Journal of Cryptology*, vol. 30, pp. 699-734, 2017. https://doi.org/10.1007/s00145-016-9233-9
[3] A. Joux, "The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems," *Fieker C., Kohel D.R. (eds) Algorithmic Number Theory. ANTS 2002. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg*., vol 2369, pp. 20-32, 2002. https://doi.org/10.1007/3-540-45455-1_3
[4] B. Dan and S. Alice, "Applications of Multilinear Forms to Cryptography," *Contemporary Mathematics*, vol. 324, pp. 71-90, 2003. https://dx.doi.org/10.1090/conm/324/05731
[5] K. Boris, C. W. L. Charles, H. Raphael, and G. Nicolas, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nature Photonics*, vol. 9, pp. 163–168, 2015. https://doi.org/10.1038/nphoton.2014.327
[6] H. B. Charles, "Quantum cryptography using any two nonorthogonal state," *Physical Review Letters*., vol. 68, pp. 3121–3124, 1992. https://doi.org/10.1103/PhysRevLett.68.3121
[7] S. Valerio, A. Antonio, R. Grégoire, and G. Nicolas, "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations," *Physical Review Letters*, vol. 92, p. 057901, 2004. https://doi.org/10.1103/PhysRevLett.92.057901
[8] M. Kara, A. Laouid, R. Euler, M. A. Yagoub, A. Bounceur, M. Hammoudeh, and S. Medileh, "A Homomorphic Digit Fragmentation Encryption Scheme Based on the Polynomial Reconstruction Problem," *The 4th International Conference on Future Networks and Distributed Systems (ICFNDS)*, vol. 1, pp. 1-6, 2020, https://doi.org/10.1145/3440749.3442592
[9] M. Kara, A. Laouid, M. A. Yagoub, R. Euler, S. Medileh, M. Hammoudeh, and A. Bounceur, "A fully homomorphic encryption based on magic number fragmentation and El-Gamal encryption: Smart healthcare use case," *Expert Systems*, vol. 1, pp. e12767, 2021. https://doi.org/10.1111/exsy.12767
[10] M. Kara, A. Laouid, M. AlShaikh, M. Hammoudeh, A. Bounceur, R. Euler, A. Amamra, and B. Laouid, "A Compute and Wait in PoW (CW-PoW) Consensus Algorithm for Preserving Energy Consumption," *Applied Sciences*, vol. 11, pp. 6750, 2021. https://doi.org/10.3390/app11156750
[11] A. Abusukhon, and B. Hawashin, "A Secure Network Communication Protocol Based on Text to Barcode Encryption Algorithm," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 6, pp. 64-70. 2015. https://doi.org/10.14569/IJACSA.2015.061209
[12] A. Abusukhon, M. N. Anwar, Z. Mohammad, and B. Alghannam, "A hybrid network security algorithm based on Diffie Hellman and Text-to-Image Encryption algorithm," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, pp. 65-81, 2019. https://doi.org/10.1080/09720529.2019.1569821
[13] M. Kumar, A. Iqbal, and P. Kumar, "A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography," *Signal Processing*, vol. 125, pp. 187-202, 2016. https://doi.org/10.1016/j.sigpro.2016.01.017
[14] S. Wang, Z. Cao, M. A. Strangio, and L. Wang, "Cryptanalysis and improvement of an elliptic curve Diffie-Hellman key agreement protocol," *IEEE communications letters*, vol. 12, pp. 149-151, 2008. https://doi.org/10.1109/LCOMM.2008.071307
[15] L. Law, A. Menezes, Qu. Minghua, J. Solinas, and S. Vanstone, "An Efficient Protocol For Authenticated Key Agreement," *Designs, Codes and Cryptography*, vol. 28, pp. 119–134, 2003. https://doi.org/10.1023/A:1022595222606
[16] Q. Xie, D. S. Wong, G. Wang, X. Tan, K. Chen, and L. Fang, "Provably secure dynamic ID-based anonymous two-factor authenticated key exchange protocol with extended security model," *IEEE Transactions on Information Forensics and Security.*, vol. 12, pp. 1382-1392, 2017. https://doi.org/10.1109/TIFS.2017.2659640
[17] M. A. Simplicio Jr, M. V. Silva, R. C. Alves, and T. K. Shibata, "Lightweight and escrow-less authenticated key agreement for the internet of things," *Computer Communications*, vol. 98, pp. 43-51, 2017. https://doi.org/10.1016/j.comcom.2016.05.002
[18] N. N. Anandakumar, M. P. L. Das, S. K. Sanadhya, and M. S. Hashmi, "Reconfigurable hardware architecture for authenticated key agreement protocol over binary edwards curve," *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, vol. 11, pp. 1-19, 2018. https://doi.org/10.1145/3231743
[19] W. Fusheng, Z. Huanguo, N. Mingtao, W. Jun and J. Zhaoxu, "A Novel Key Agreement Protocol Based on RET Gadget Chains for Preventing Reused Code Attacks," *IEEE Access*, vol. 6, pp. 70820-70830, 2018. https://doi.org/10.1109/ACCESS.2018.2879852
[20] A. ABUSUKHON, Z. MOHAMMAD, and A. AL-THAHER, "Efficient and secure key exchange protocol based on elliptic curve and security models," *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), IEEE*, vol. 2019, pp. 73-78, 2019. https://doi.org/10.1109/JEEIT.2019.8717496

[21] K. Seyhan, T. N. Nguyen, S. Akleylek, K. Cengiz, and S. H. Islam, "Bi-GISIS KE: Modified key exchange protocol with reusable keys for IoT security," *Journal of Information Security and Applications*, vol. 58, pp. 102788, 2021. https://doi.org/10.1016/j.jisa.2021.102788
[22] G. S. Gaba, G. Kumar, H. Monga, T. -H. Kim, M. Liyanage and P. Kumar, "Robust and Lightweight Key Exchange (LKE) Protocol for Industry 4.0," *IEEE Access*, vol. 8, pp. 132808-132824, 2020. https://doi.org/10.1109/ACCESS.2020.3010302
[23] K. AMINE, "Diffie-Hellman key exchange through Steganographied images," *Brasilia*, vol. 10, pp. 147-160, 2018. https://doi.org/10.6025/pca/2018/7/2/68-78
[24] M. M. Emam, A. A. Aly, and F. A. Omara, "An improved image steganography method based on LSB technique with random pixel selection," *International Journal of Advanced Computer Science and Applications*, vol. 7, pp. 361-366, 2016. https://doi.org/10.14569/issn.2156-5570
[25] C. Hsu, T. Le, C. Lu, T. Lin, and T. Chuang, "A Privacy-Preserved E2E Authenticated Key Exchange Protocol for Multi-Server Architecture in Edge Computing Networks," *IEEE Access*, vol. 8, pp. 40791-40808, 2020, https://doi.org/10.1109/ACCESS.2020.2976431
[26] M. Tanveer, A. H. Zahid, M. Ahmad, A. Baz, and H. Alhakami, "LAKE-IoD: Lightweight Authenticated Key Exchange Protocol for the Internet of Drone Environment," *IEEE Access*, vol. 8, pp. 155645-155659, 2020, https://doi.org/10.1109/ACCESS.2020.3019367
[27] H. Wu and B. Preneel, "AEGIS: A fast authenticated encryption algorithm," *International Conference on Selected Areas in Cryptography, Springer, Berlin, Heidelberg*, vol. 8282, pp. 185-201, 2013. https://doi.org/10.1007/978-3-662-43414-7_10
[28] C. M. Chen, Y. Huang, K. H. Wang, S. Kumari, and M. E. Wu, "A secure authenticated and key exchange scheme for fog computing," *Enterprise Information Systems*, vol. 15, pp. 1200-1215, 2021. https://doi.org/10.1080/17517575.2020.1712746
[29] X. Jia, D. He, N. Kumar, and K. K. R. Choo, "Authenticated key agreement scheme for fog-driven IoT healthcare system," *Wireless Netw.*, vol. 25, pp. 4737–4750, 2019. https://doi.org/10.1007/s11276-018-1759-3
[30] Y. Luo, W. M. Zheng, and Y. C. Chen, "An anonymous authentication and key exchange protocol in smart grid," *Journal of Network Intelligence*, vol. 6, pp. 206-215, 2021. http://bit.kuas.edu.tw/~jni/2021/vol6/s2/05-v6n2-0185_r01.pdf
[31] M. R. Mishra, and J. Kar, "A study on diffie-hellman key exchange protocols," *International Journal of Pure and Applied Mathematics*, vol. 114, pp. 179-189, 2017. https://doi.org/10.12732/ijpam.v114i2.2
[32] K. A. Kumari, G. S. Sadasivam, and L. Rohini, "An Efficient 3D Elliptic Curve Diffie–Hellman (ECDH) Based Two-Server Password-Only Authenticated Key Exchange Protocol with Provable Security," *IETE Journal of Research*, vol. 62, pp. 762-773, 2016. https://doi.org/10.1080/03772063.2016.1176539
[33] H. Yu, and Y. Kim, "New RSA encryption mechanism using one-time encryption keys and unpredictable bio-signal for wireless communication devices," *Electronics*, vol. 9, no. 2, pp. 246, 2020. https://doi.org/10.3390/electronics9020246
[34] J. H. Seo, "Efficient digital signatures from RSA without random oracles," *Information Sciences*, vol. 512, pp. 471-480, 2020. https://doi.org/10.1016/j.ins.2019.09.084
[35] S. Venkatraman, and A. Overmars, "New method of prime factorisation-based attacks on RSA Authentication in IoT," *Cryptography*, vol. 3, pp. 20, 2019. https://doi.org/10.3390/cryptography3030020
[36] R. Thiyagarajan, and B. M. Priya, "An enhancement of EAACK using P2P ACK and RSA public key cryptography," *Measurement*, vol. 136, pp. 116-121, 2019. https://doi.org/10.1016/j.measurement.2018.12.031
[37] M. Mumtaz, and L. Ping, "Forty years of attacks on the RSA cryptosystem: A brief survey," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, pp. 9-29, 2019. https://doi.org/10.1080/09720529.2018.1564201
[38] M. Suárez-Albela, P. Fraga-Lamas, and T. M. Fernández-Caramés, "A practical evaluation on RSA and ECC-based cipher suites for IoT high-security energy-efficient fog and mist computing devices," *Sensors*, vol. 18, pp. 3868, 2018. https://doi.org/10.3390/s18113868
[39] Y. Wang, H. Zhang and H. Wang, "Quantum polynomial-time fixed-point attack for RSA," *China Communications*, vol. 15, pp. 25-32, 2018, https://doi.org/10.1109/CC.2018.8300269

BIOGRAPHY OF AUTHORS

Mostefa Kara received the Eng. degree in computer science from the University of Biskra, Algeria, in 2005. He received a Master's degree in artificial intelligence from the University of Eloued, Algeria, in 2019. He is currently a Ph.D. student at the University of Eloued, Algeria. His research interests include cryptology, information security, and decentralized algorithms. Email: karamostefa@univ-eloued.dz

Abdelkader Laouid received the MSc. degree in computer science from the University of Bejaia, Algeria, in 2011. He is currently a Ph.D. doctor at El-Oued University, Algeria. He is an associate professor at the University of El-Oued. His research interests include distributed algorithms oriented to limited resource networks. Email: abdelkader-laouid@univ-eloued.dz

Muath Alshaikh had been earned a Ph.D. degree in Computer Science at Universit de Bretagne Occidentale, France, in 2016. He received his Master's degree in computer science from Utara University, Malaysia, in 2010 and his BSc in computer science from AlBalga University, Jordan, in 2006. He is affiated to Lab-STICC / UMR CNRS 6283, SFIIS team, at Universit de Bretagne Occidentale, France. Muath is an assistant professor at the college of computing and informatics, Saudi Electronic University, KSA. His research interests include image and video watermarking, cryptology, information security, image processing, Internet of Things (IoT), Cybersecurity, and computer vision. Email: M.ALSHAIKH@seu.edu.sa

Ahc'ene Bounceur is an associate professor of Computer Science at the University of Brest (UBO). He is a member of the Lab-STICC Laboratory (MOCS Group). He received a Ph.D. in Micro and nanoelectronics at Grenoble INP, France, in 2007. He received the M.S. degrees from ENSIMAG, Grenoble, France, in 2003. From April 2007 to August 2008, he was a postdoctoral fellow at TIMA Laboratory. From September 2007 to August 2008, he was with Grenoble INP, France, where he was a temporary professor. His current research activities are focused on: Tools for physical simulation of Wireless Sensor Networks (WSN), parallel models for accelerating simulations and predicting parameters in WSN, sampling methods for data mining, development of CAT (Computer Aided Test) tools for analog, mixed-signal and RF circuits and statistical modeling of analog, mixed-signal and RF circuits. Email: Ahcene.Bounceur@univ-brest.fr

Mohammad Hammoudeh is the Head of the CfACS IoT Laboratory and a Reader in Future Networks and Security with the Department of Computing and Mathematics, Manchester Metropolitan University. He has been a researcher and publisher in the field of big sensory data mining and visualization. He is a highly proficient, experienced, and professionally certified cybersecurity professional specializing in threat analysis and information and network security management. His research interests include highly decentralized algorithms, communication, and cross-layered solutions to the Internet of Things and wireless sensor networks. Email: M.Hammoudeh@mmu.ac.uk