

Enhanced and authenticated cipher block chaining mode

Yasmeen Shaher Alslman¹, Ashraf Ahmad¹, Yousef AbuHour²

¹Department of Computer Science, King Hussein School of Computing Sciences, Princess Summaya University, Amman, Jordan

²Department of Basic Sciences, King Abdullah II School of Engineering, Princess Summaya University, Amman, Jordan

Article Info

Article history:

Received Dec 21, 2022

Revised Jan 8, 2023

Accepted Jan 27, 2023

Keywords:

Authenticated modes

Chain block cipher

Cyber security

Encryption modes

Integrity

ABSTRACT

Due to the increased attacks on different applications, data security has become crucial. Many modes can be used to operate the advanced encryption standard (AES), some of which provide integrity, and some outperform other modes in security and simplicity. In this paper, the chain block cipher (CBC) mode has been modified to provide more security to the encrypted data by making it robust against the bit-flipping attack and adding an integrity approach using the keyed-hash function. In addition, using the keyed-hash function increases the number of keys needed in CBC-AES to two keys, and this can make the proposed model more secure against bruteforce attacks and Grover's quantum search algorithm.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Yousef AbuHour

Department of Basic Sciences, King Abdullah II School of Engineering, Princess Summaya University

Amman, 11941, Jordan

Email: y.abuhour@psut.edu.jo

1. INTRODUCTION

In recent years, cryptography has become a necessity in each organization to protect their information and achieve the three main security standards: confidentiality, integrity, and authenticity (CIA), which are considered essential in every organization in the internet era [1]–[3]. Encryption techniques are varied between symmetric and asymmetric encryption. Asymmetric encryption is more secure than symmetric. However, symmetric encryption is much faster than asymmetric, which is why many applications tend to use symmetric key encryption for achieving data confidentiality [4], [5]. Researchers [6]–[8] have recently developed and surveyed medical image cryptography algorithms to enhance the security of medical image transfer and manipulation. Although these algorithms have proposed novel methods to enhance the security of medical image usage they did not address the mode of operation of these algorithms. According to Ibrahim *et al.* [9], new technology to prevent distributed denial of service (DDoS) attacks using a crypto-based algorithm was presented yet the cryptographic mode was primitive. The use of our proposed mode of operation would result in a high rate of prevention due to its reliability as will be proven in the discussion section. Generally speaking, there are no fully secure encryption techniques because the security of any encryption algorithm depends on two main criteria; the encryption algorithm itself, and the methods used to implement the algorithm. Thus, the encryption algorithm being robust is not enough to achieve good security in any system. Therefore, many modes are used in implementing AES; electronic code book (ECB) mode, cipher block chaining (CBC) mode, cipher feedback (CFB) mode, output feedback mode (OFB), and counter (CTR) mode [10]. There is no mode used in advanced encryption standard (AES) that can fulfill the CIA. CBC, for example, only meets confidentiality. On the other hand, CTR achieves both integrity and confidentiality. It is noteworthy that increasing the security of any AES mode can affect the system's performance and complexity. CBC mode is preferable over ECB because in CBC, if the same block of data is repeated through the plaintext, the resulting cipher will not be the same, unlike ECB.

Nevertheless, there is a significant attack-bit flipping attack-on the CBC [11], [12], that's why some applications try to use other mods that are robust against such attacks. Therefore, this paper proposed enhancements over CBC mode, making it secure against bit-flipping attacks, adding an authentication tag for data integrity, and increasing the key size, increasing the AES's security. These enhancements can make use of CBC mode in much broader applications. The rest of this paper is organized as follows; section 2 represents the related work. The proposed enhancements are described in section 3. Section 4 discusses the result. Finally, the conclusion of this paper is presented in section 5.

2. RELATED WORK

In the late twentieth century, Bellare *et al.* [13] proposed the CBC message authentication code (MAC). Meaning that the ability to achieve message integrity and authenticity has been achieved using CBC mode by setting the initial vector (IV) to zero, and the output of the last block in the original CBC mode will be the MAC for the message. Sihite and Salman [14] have used the CBC MAC in their proposed e-voting and e-recap system. Pirzada *et al.* [15] use the AES-CTR mod for achieving a message authentication tag. Many researchers tend to enhance the AES algorithm itself to increase security and other impotent factors like time and power consumption [16], [17]. In contrast, others proposed an enhancement on the AES mode [18]–[22]. Assafli and Hashim [18] proposed an enhancement on AES-CBC using the avalanche effects in reference one. Their main contribution was to generate a different IV each time where the value of the IV will be conducted from the unix timestamp. Unix timestamp consists of ten bytes, and only the first 8 bytes will be used in Initializing the IV. Their approach generates two different ciphertexts for the exact plaintext. It has been shown that their enhancement maintains strict avalanche criteria for 53%. Lee and Sim [19] also enhanced the security of the AES-CBC algorithm for IoT devices by changing the IV and by changing the secret key periodically. Two cipher keys were combined to generate a new key used in the AES encryption. Changing keys depends on a predefined time, meaning if the time is the same as the predefined time, the key will not be changed. Updating the cipher key consists of three main steps; shift operation, XOR, and changing the key's time. Research by Pillai *et al.* [23] provided a time analysis of the ransomware that uses the AES-CBC encryption algorithm. Their results show that the encryption time depends on two main factors; the key size and the size of the data to be encrypted. According to An and Seo [24] a new parallel optimization in implementing the XTS-AES has been proposed to enhance the speed of the encryption process by modifying the XTS form to be implemented to the GPU. Their model performance exceeds the implementation of the Openssl.

3. PROPOSED MODEL

As mentioned before, AES has many modes, every mode implements all AES operations, substitution byte, shift row, mix-column, and add-round key. However, each mode has its algorithm. For example in ECB mode, the simplest way of implementing AES, each data block will be encrypted and placed in its corresponding place in cipher text. In CBC, the first plaintext block will be XORed with the IV and then encrypted. The resulting cipher block is XORed again with the next plaintext block and then encrypted again. Making the final cipher text depends on all plaintext blocks. Figure 1 illustrates how CBC mode works. It can be noted that CBC provides data confidentiality nevertheless, CBC is vulnerable against bit flipping attack if $token = ciphertext(block_1, block_2, X)$ where x is the targeted block then: $x = block_2 \oplus Oblock \oplus Nblock$; where O-block is the original block before corruption and N-block is the new block that the attacker wants to replace. In addition, CBC doesn't provide any data authentication. As a result, an extra step is performed if data authentication is needed, especially in case of a bit-flipping attack. Data authentication can be achieved using HMAC, MAC, and many other data authentication algorithms. Therefore, the proposed model enhances CBC mode to make it robust against bit-flipping attacks. In the proposed enhancement, the XOR operation will be between the plaintext and the ciphertext hash. As a result, the attackers will not be able to determine which bit of the hashed ciphertext will affect the plaintext. Inspired by CTR (AES-GSM) mode, all the hashes will be XORed to get the authentication tag. The hash function used in the proposed is key hash meaning that an extra key is needed. Using two keys in AES encryption isn't new. In the XTS mode, two key has been used. Figures 2 and 3 show the new CBC encryption, decryption structure. Starting with the encryption process, encrypting the first plaintext block will be the same as the original CBC mode. However, the next plaintext block will be XORed with the key hash of the previous ciphertext block. The ciphertext can be computed using: $c_i = E_{k_1}(Hash(c_{i-1}, k_2) \oplus p_i)$.

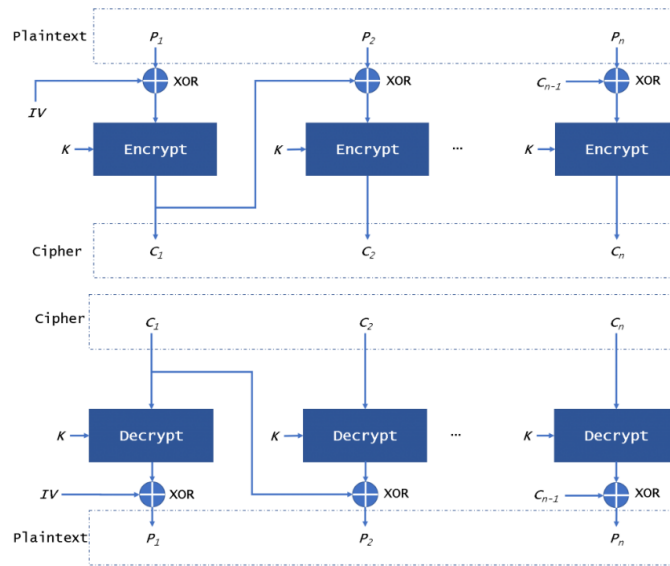


Figure 1. CBC mode [25]

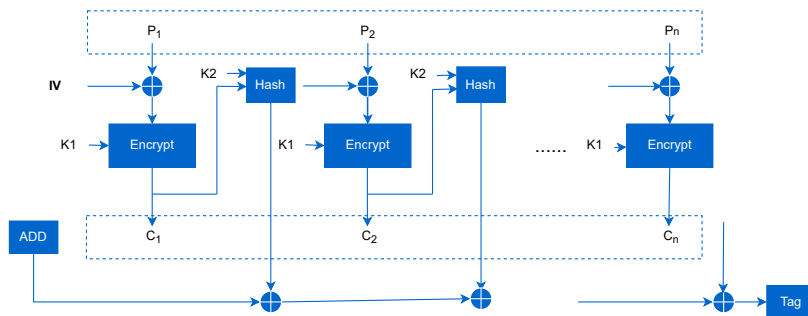


Figure 2. The enhanced CBC encryption

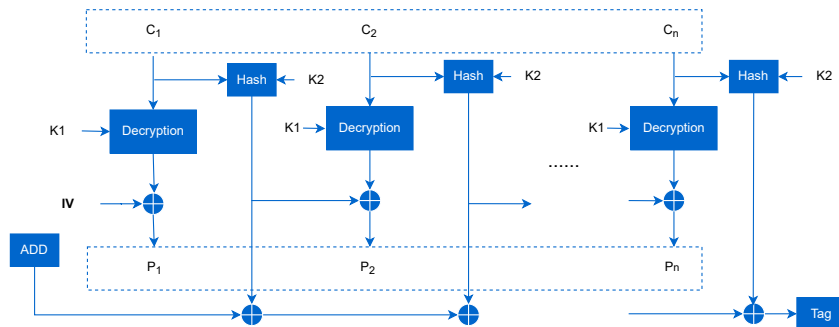


Figure 3. The enhanced CBC decryption

The authentication tag can be calculated using the (add), which is authentication data, XORed with the hashes of the ciphertext. Thus the sender will end up sending the encrypted message along with the authentication tag and IV. Figure 4 shows the protocol between the sender and receiver. On the other side, the

receiver will perform the decryption process shown in Figure 3. The process starts by decrypting the first ciphertext block, with the received IV obtaining the first plaintext block. The second ciphertext block is decrypted and XORed with the hash of the previous ciphertext block. The decryption process can be written: $p_i = D_{k_1}(c_i) \oplus Hash(c_{i-1}, k_2)$.

The integrity can be assured using the authentication tag. The receiver can calculate the tag from the received ciphertext. Starting from the (add) authentication data and XORed it with the Hash of the first ciphertext and XORed the result with the hash of the next ciphertext. If the calculated tag equals the received tag then the data integrity is guaranteed. Grover's quantum search algorithm [26] will speed up the brute-force attack. Therefore, the AES security level will be decreased by half [27].

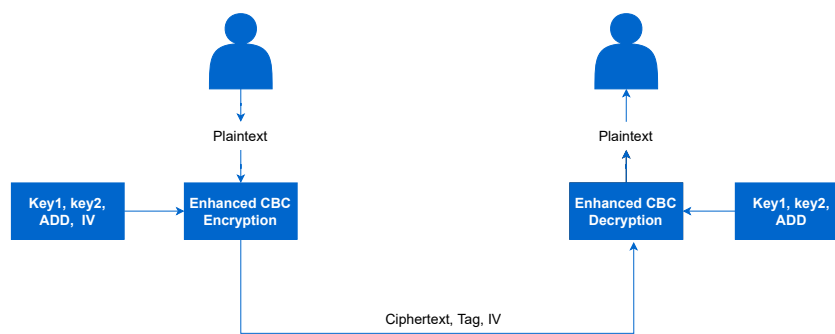


Figure 4. The proposed enhanced CBC mode protocol

4. EXPERIMENTS AND RESULTS

In this section, the proposed model has been implemented and tested on different data types (text, images of various sizes, pdf). Colab, which provides 12 GB RAM and 128 GB disk, has been used for implementing the proposed model using python3. As in any AES mode encryption, the first thing is padding the data if needed so that it can be divided into equal sizes of data blocks. Thus the public key cryptography standard (PKCS) 7 has been used for padding the data. The data block size in the experiment has been set to 16 bytes. As mentioned earlier, two keys have been used in the proposed model, each with 256 bits. The first key is used to encrypt each block with AES, while the second is used for the keyed hash (blake2). Time analysis was obtained on the proposed model and compared with the original CBC. The proposed model can be used on all types of data. Therefore, the proposed model has been tested on three data types: text, images, and pdfs. Table 1 represents the time analysis when using the proposed model and the original CBC, considering the size of each data type in bytes.

From Table 1, it can be noticed that adding security (using more than one key, adding a message authentication tag, preventing bit-flipping attack) layers to the original CBC can affect the time. However, additional time is considered to be negligible. It is worth mentioning that parallelism hasn't been taken into consideration during the implementation. A brief comparison between the original CBC mode, the enhanced model, and CBC-MAC can be represented in Table 2. CBC can provide decryption parallelization, while CBC-mac is used only for providing data authentication rather than data encryption. The proposed model has advantages over the aforementioned modes; it provides authenticity with a parallelization technique for decryption. Moreover, the number of keys required has doubled.

Table 1. Time analysis

Data type	Text	Image	PDF
Size (types)	3020	512×512	756823
Enhanced CBC encryption (sec)	0.019	0.52	1.42
CBC encryption (sec)	0.0098	0.37	1.03
Enhanced CBC decryption (sec)	0.014	0.53	0.37
CBC decryption (sec)	1.03	1.42	1.07

Table 2. Comparison

	CBC	Enhanced CBC	CBC-MAC
Decryption parallelization	✓	✓	-
Integrity	×	✓	✓
Robust against bit flipping attack	×	✓	✓
Encryption parallelization	×	×	-
Number of key needed	1-key	2-key	1-key

5. CONCLUSION

This paper proposes a modification to AES-CBC mode to make it robust against bit-flipping attacks since the xor operation becomes between the plaintext and the hash of the previous ciphertext, making it almost impossible to determine from the hash which bit will affect the plaintext. In addition, an authentication tag has been added to the proposed enhancement, achieving two necessary security standards: confidentiality and integrity. Moreover, by using keyed hash, the number of keys has increased to two, which adds a security layer to the original AES-CBC. In other words, using two keys increases the executive search space, keeping the security level at 128, against Grover's quantum research. It has been concluded from the implementation that the proposed model can be used in various applications, and the extra steps (keyed-hash, calculating the hash) can affect the time. However, the additional time is considered negligible when compared with the original CBC. It can be noticed that the proposed mode is not considered a lightweight crypto design for IoT since the number of time needed to apply encryption and hashing are equal to the number of blocks. In addition, the proposed mode's error propagation (if one-bit changes) affects all bits in the following two successive blocks. Finally, two independent keys need two key-exchange protocols. For future work, hardware design for the proposed mode by FPGA, with parallelization technique, can be considered.




REFERENCES

- [1] S. Samonas and D. Coss, "The cia strikes back: redefining confidentiality, integrity and availability in security," *Journal of Information System Security*, vol. 10, no. 3, pp. 21–38, 2021.
- [2] S. Nasiri, F. Sadoughi, M. Tadayon, and A. Dehnad, "Security requirements of internet of things-based healthcare system: a survey study," *Acta Informatica Medica*, vol. 27, no. 4, pp. 253–258, 2019, doi: 10.5455/aim.2019.27.253-258.
- [3] R. v. Solms and J. v. Niekerk, "From information security to cyber security," *Computers & Security*, vol. 38, pp. 97–102, 2013, doi: 10.1016/j.cose.2013.04.004.
- [4] A. Praveena and S. Smys, "Efficient cryptographic approach for data security in wireless sensor networks using MES V-U," in *2016 10th International Conference on Intelligent Systems and Control (ISCO)*, 2016, pp. 1–6, doi: 10.1109/ISCO.2016.7726911.
- [5] A. J. Elbirt and C. Paar, "An instruction-level distributed processor for symmetric-key cryptography," *IEEE Transactions on Parallel and Distributed Systems*, vol. 16, no. 5, pp. 468–480, 2005, doi: 10.1109/TPDS.2005.51.
- [6] M. A. A. -Fayoumi, A. Odeh, I. Keshta, and A. Ahmad, "Techniques of medical image encryption taxonomy," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 4, pp. 1990–1997, 2022, doi: 10.11591/eei.v11i4.3850.
- [7] A. Ahmad, Y. AbuHour, R. Younis, Y. Alsman, E. Alnagi, and Q. A. A. -Haija, "MID-crypt: a cryptographic algorithm for advanced medical images protection," *Journal of Sensor and Actuator Networks*, vol. 11, no. 2, pp. 1–17, 2022, doi: 10.3390/jsan11020024.
- [8] S. Kumar, B. Panna, and R. K. Jha, "Medical image encryption using fractional discrete cosine transform with chaotic function," *Medical & Biological Engineering & Computing*, vol. 57, no. 11, pp. 2517–2533, 2019, doi: 10.1007/s11517-019-02037-3.
- [9] R. F. Ibrahim, Q. A. A. -Haija, and A. Ahmad, "DDoS attack prevention for internet of thing devices using ethereum blockchain technology," *Sensors*, vol. 22, no. 18, pp. 1–21, 2022, doi: 10.3390/s22186806.
- [10] M. Dworkin, "Recommendation for block cipher modes of operation methods and techniques," *Gaithersburg*, 2001.
- [11] M. R. Albrecht and K. G. Paterson, "Lucky microseconds: a timing attack on Amazon's s2n implementation of TLS," in *Advances in Cryptology—EUROCRYPT 2016*, Berlin, Heidelberg: Springer, 2016, pp. 622–643, doi: 10.1007/978-3-662-49890-3_24.
- [12] S. Yao, J. Chen, R. Du, L. Deng, and C. Wang, "A survey of security network coding toward various attacks," in *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, 2014, pp. 252–259, doi: 10.1109/Trust-Com.2014.35.
- [13] M. Bellare, J. Kilian, and P. Rogaway, "The security of the cipher block chaining message authentication code," *Journal of Computer and System Sciences*, vol. 61, no. 3, pp. 362–399, 2000, doi: 10.1006/jcss.1999.1694.
- [14] A. B. Sihite and M. Salman, "E-voting and e-recap verification and validation schemes for indonesia utilizing cryptographic hash function message authentication codes (MAC) and public key infrastructure (PKI)," in *2019 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)*, 2019, pp. 29–34, doi: 10.1109/ICIMCIS48181.2019.8985212.
- [15] S. J. H. Pirzada, A. Murtaza, J. Liu, and T. Xu, "The parallel CMAC authentication algorithm," in *2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN)*, 2019, pp. 800–804, doi: 10.1109/ICCSN.2019.8905326.
- [16] I. A. Awan, M. Shiraz, M. U. Hashmi, Q. Shaheen, R. Akhtar, and A. Ditta, "Secure framework enhancing AES algorithm in cloud computing," *Security and Communication Networks*, vol. 2020, pp. 1–16, 2020, doi: 10.1155/2020/8863345.
- [17] C. Adams and S. Lloyd, *Understanding PKI: concepts, standards, and deployment considerations*. Boston, MA: Addison-Wesley Professional, 2003.




- [18] H. T. Assaffi and I. A. Hashim, "Security enhancement of AES-CBC and its performance evaluation using the avalanche effect," in *2020 3rd International Conference on Engineering Technology and its Applications (IICETA)*, 2020, pp. 7–11, doi: 10.1109/IICETA50496.2020.9318803.
- [19] S.-W. Lee and K.-B. Sim, "Design and hardware implementation of a simplified DAG-based blockchain and new AES-CBC algorithm for IoT security," *Electronics*, vol. 10, no. 9, pp. 1–20, 2021, doi: 10.3390/electronics10091127.
- [20] A. S. W. Man, E. S. Zhang, V. K. N. Lau, C. Y. Tsui, and H. C. Luong, "Low power VLSI design for a RFID passive tag baseband system enhanced with an AES cryptography engine," in *2007 1st Annual RFID Eurasia*, 2007, pp. 1–6, doi: 10.1109/RFIDEURASIA.2007.4368097.
- [21] S. Sahnoud, W. Elmasry, and S. Abudalfa, "Enhancement the security of AES against modern attacks by using variable key block cipher," *International Arab Journal of e-Technology*, vol. 3, no. 1, pp. 17–26, 2013.
- [22] S. M. Wadi and N. Zainal, "Rapid encryption method based on AES algorithm for grey scale HD image encryption," *Procedia Technology*, vol. 11, pp. 51–56, 2013, doi: 10.1016/j.protcy.2013.12.161.
- [23] A. Pillai, R. Kadikar, M. S. Vasanthi, and B. Amutha, "Analysis of AES-CBC encryption for interpreting crypto-wall ransomware," in *2018 International Conference on Communication and Signal Processing (ICCCSP)*, 2018, pp. 599–604, doi: 10.1109/ICCCSP.2018.8524494.
- [24] S. An and S. C. Seo, "Designing a new XTS-AES parallel optimization implementation technique for fast file encryption," *IEEE Access*, vol. 10, pp. 25349–25357, 2022, doi: 10.1109/ACCESS.2022.3155810.
- [25] S. Wang, "The difference in five modes in the AES encryption algorithm," *High Go*, 2019. <https://www.highgo.ca/2019/08/08/the-difference-in-five-modes-in-the-aes-encryption-algorithm/> (accessed Dec. 17, 2022).
- [26] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing-STOC '96*, 1996, pp. 212–219, doi: 10.1145/237814.237866.
- [27] L. Chang, Y. Wei, X. Wang, and X. Pan, "Collision forgery attack on the AES-OTR algorithm under quantum computing," *Symmetry*, vol. 14, no. 7, pp. 1–16, 2022, doi: 10.3390/sym14071434.

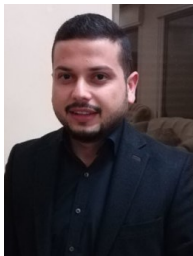
BIOGRAPHIES OF AUTHORS






Yasmeen Shaher Alsman    is currently a second-year Ph.D. and a former Masters's student in Computer Science at Princess Summaya University. Her research is focused on cryptography and finding new techniques for encrypting data. Another major research interest is integrating machine learning algorithms in security fields. Currently, she is working as a Teaching Assistant in the department. She can be contacted at email: yasmeenalsman1996@gmail.com.



Dr. Ashraf Ahmad    is currently an Associate Professor at Princess Summaya University for Technology (PSUT). Having obtained his B.Sc. from PSUT. He went on to obtain his Ph.D. degree in Computer Science and Engineering from National Chiao Tung University (NCTU) in Taiwan, graduating with distinction. He has formerly served as Head of the Department of Computer Graphics and Animation at PSUT for four years. His areas of research interest include security application development and computer programming, mobile application, video transcoding, secure multimedia, and interoperability. He has authored several scientific publications including journal papers, conference papers, book chapters, and books. He can be contacted at email: a.ahmad@psut.edu.jo.



Yousef AbuHour    is currently a full-time lecturer at Princess Summaya University of Technology. He received BSc degree in Mathematics from Hashemite University in 2013. In 2016, he was awarded his MSc degree in Applied Mathematics from Jordan University of Science and Technology (JUST). In 2019, he was certified in cryptography at "The Military University of Technology" from Warsaw (WAT). During 2017-2022, he was a mathematician in the Encryption Center of Jordan Design and Development Bureau. His research interests are in the fields: of applied mathematics, and cryptography. He can be contacted at email: y.abuhour@psut.edu.jo.