Peertechz

Trends in Computer Science and Information Technology
submitpaper@peertechz.com

ENGINEERING GROUP

TRENDS IN Computer Science and Information Technology

OPEN ACCESS JOURNAL

ISSN: 2641-3086 DOI: https://dx.doi.org/10.17352/tcsit

Review Article

Enhancing cryptographic robustness with dual key chaining

Muhammad Faisal Nawaz[1] and Yasir Nawaz[2]*

[1]University of Lahore, Pakistan

[2]Shanghai Jiao Tong University, China

Received: 19 February, 2024
Accepted: 13 March, 2024
Published: 14 March, 2024

***Corresponding author**: Yasir Nawaz, Shanghai Jiao Tong University, China, E-mail: my_nawaz@alumni.sjtu.edu.cn, my_nawaz@sjtu.edu.cn

ORCiD: https://orcid.org/0009-0001-3093-4475

Keywords: Dual key chaining mode; Cryptographic security; IND-CPA security; Chosen plaintext attack; Block cipher modes

Abstract

In this paper, we introduce an advanced mode of operation for block ciphers, named Dual Key Chaining Mode (DKC), aimed at bolstering cryptographic security for safeguarding sensitive information. Building upon the foundations laid by established modes while adhering to guidelines set by the National Institute of Standards and Technology (NIST), DKC innovates through a dual-key mechanism and the generation of highly unpredictable values. This novel approach markedly enhances security, particularly against chosen plaintext attacks, a common vulnerability in traditional modes. Through rigorous mathematical analysis, we demonstrate DKC's superiority, proving its indistinguishability under chosen plaintext attacks (IND-CPA) and showing that an adversary cannot practically distinguish DKC-encrypted ciphertexts from those produced by a random permutation. Our security proof employs a structured approach, contrasting DKC with conventional modes to highlight its robust defense mechanisms and its capacity to mitigate error propagation, reduce chain dependency, and resist pattern recognition attacks. The DKC mode not only surpasses existing standards in cryptographic security but also offers significant improvements in efficiency and security complexity, making it particularly suited for environments demanding stringent data protection. This study's findings underscore DKC's potential as a leading candidate for securing communication channels, financial transactions, and cloud storage services against an array of cryptographic attacks.

Introduction

Block ciphers are scrutinized cryptographic primitives for secure encryption and decryption that ensures confidentiality, authenticity, and authenticated encryption [1], where particular plaintext blocks are treated as a single block and always produce ciphertext blocks with the same size [2]. In the last few years, researchers conducted a lot of research on block cipher, and it is believed that building an efficient and secure block cipher is now a big problem [3]. Currently, some block cipher algorithms developed like DES, 3DES, Blowfish, AES, RC4, RC5, and RC6 [4-7]. In particular, each block cipher algorithm allowed to prove efficiency and security against attacks like chosen plaintext attacks and chosen ciphertext attacks [8-11]. The more secure block cipher algorithm that has been incorporated into the current main worldwide standard for encryption is AES by NIST [12]. The size of AES is 128-bit block, and the key size of AES can be 128-bit, 196-bit, or 256-bit. The security of the block cipher is based on the four functions, permutation, substitution, arithmetic operation, and XOR operation when fixed with the secret key. The size of the block of AES provides sufficient security and efficiency, particularly the key size of 128-bit provides resistance to brute force attacks [13].

Block cipher algorithms are unenabled to encrypt plaintext with a size that is different from the defined size of one block as well. There are two ways to solve this issue one is the padding technique present in [14] and another way is operation modes. Block cipher operation modes may also provide security, and efficiency, strengthen the effect of the encryption algorithm as well as convert block cipher into stream cipher. To meet this requirement NIST recommends five modes of operation that apply to AES, these operation modes are Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB),

Citation: Nawaz MF, Nawaz Y (2024) Enhancing cryptographic robustness with dual key chaining. Trends Comput Sci Inf Technol 9(1): 026-033.
DOI: https://dx.doi.org/10.17352/tcsit.000077

Output Feedback (OFB), Counter mode (CTR) and standardized in 2001 [15]. Generally, the ECB mode encrypts the same plaintext into the same ciphertext under a given key, so in critical applications, ECB mode is practically undesirable that's why it's not widely used [16]. In CBC mode each block of plaintext depends on the outcome of the previous block (ciphertext) and the first plaintext block requires an initialization vector (IV) that's XORed with the first block of plaintext. The IV must be unpredictable and need not be secret [17]. In CFB mode each input block of the encryption algorithm feeds successive ciphertext blocks of the previous block, the output XORed with the block of plaintext to produce the ciphertext block. So, error propagation can be occurred in CFB mode [18]. In OFB mode, the output of the encryption block is independently XORed with plaintext to produce ciphertext [19]. In CTR mode, each encryption block produces output independently from the set of input blocks called counter, XORed with the plaintext block provides ciphertext blocks. Each mode of operation has its own parameter that provides necessary security to the encryption algorithm. Currently, there are different types of attack on these operation modes have been developed [20,21]. So, these operations modes have their own security risk.

The development and analysis of more secure and efficient authenticated encryption modes have gained considerable attention. Research efforts have been directed toward creating algorithms that not only encrypt data but also authenticate it, thereby ensuring data integrity and confidentiality simultaneously. Authenticated encryption modes like OCB (Offset Codebook Mode) and AEAD (Authenticated Encryption with Associated Data) have been highlighted for their capability to provide high security and performance, particularly in protocols where both encryption and authentication are paramount [22]. Moreover, the advent of lightweight cryptography has been instrumental in addressing the challenges posed by the Internet of Things (IoT) and other resource-constrained environments. The design of lightweight block cipher modes aims to achieve optimal security with minimal resource utilization, ensuring the widespread applicability of cryptographic solutions across various platforms [23]. Another significant area of research has been the focus on enhancing resistance to side-channel attacks, which exploit physical implementations of cryptographic algorithms. Innovations in block cipher modes are increasingly incorporating countermeasures against such attacks, ensuring that security is maintained not only at the algorithmic level but also in practical implementations [24].

The integration of quantum-resistant cryptographic algorithms into block cipher modes represents a forward-looking approach to cryptography, anticipating the potential impact of quantum computing on current cryptographic standards. This research area is crucial for future-proofing cryptographic protocols against the capabilities of quantum computers [25]. Lastly, the ongoing efforts by standardization bodies like NIST to evaluate and recommend block cipher modes of operation underscore the global commitment to securing digital information. These efforts aim to establish a set of standardized, secure, and efficient cryptographic protocols that can be universally adopted [26].

Our research introduces a new block cipher mode of operation named DKC, designed to enhance the security measures of existing modes. DKC is predicated on generating highly unpredictable values, offering advanced cryptographic protection for sensitive information. Traditional block cipher modes rely on a singular key to encrypt sequential blocks of plaintext, whereas DKC utilizes a dual-key system to elevate the security and intricacy of encryption.

In practical application scenarios, the DKC offers enhanced security features that are particularly beneficial in environments requiring stringent data protection. For instance, DKC can be applied in secure communication channels, such as those used for governmental or military communication, where the integrity and confidentiality of the transmitted information are paramount. Additionally, DKC's robustness against various cryptographic attacks makes it an ideal candidate for securing financial transactions in the banking sector, ensuring the safety of sensitive customer data. Furthermore, its application in cloud storage services can provide an added layer of security, protecting users' personal and corporate data from unauthorized access and breaches.

The forthcoming sections of this paper are structured as follows: Section 2 delves into the NIST-recommended operation modes of block ciphers; Section 3 elucidates our proposed DKC mode; Section 4 presents a detailed security analysis comparing DKC against these operation modes, particularly focusing on resistance to chosen plaintext attacks; and Section 5 concludes the paper with our findings and implications of the study.

Block cipher mode of operation

In this section, we describe existing operation modes of block cipher that are recommended by NIST. Now first we define the parameter that's used in these operation modes, particularly in CBC mode, CFB mode, OFB mode, and CTR mode.

P_1: The 1st plaintext block to be encrypted.

P_i: The ith plaintext block to be encrypted, for i = 2 … n.

C_1: The 1st ciphertext block to be encrypted.

C_i: The ith ciphertext block to be encrypted, for i = 2 … n.

O_1: The 1st output after encryption of IV in OFB mode

O_i: The ith output after encryption of O_{i-1} in OFB mode, for i = 2 … n.

O_{i-1}: The output of previous block

IV: Initialization Vector (a random number for CBC, CFB, and OFB).

K: key for encryption algorithm

ctr: The counter is an input of the encryption algorithm in CTR mode.

⊕: Add XOR

The Cipher Block Chaining (CBC) Mode

The CBC mode is a confidential mode in which a chain appears between the successive encryption/decryption blocks. The CBC mode can be formulated as follows.

$$C_1 = E_k\left(P_1 \oplus IV\right);\ \text{(Encryption)} \tag{1}$$

$$C_i = E_k\left(P_i \oplus C_{i-1}\right) \text{for } 2 \le i \le n. \tag{2}$$

$$P_1 = D_k(C_1) \oplus \mathrm{IV}\text{(Decryption)} \tag{3}$$

$$P_i = D_k(C_i) \oplus C_{i-1} \text{for } 2 \le i \le n. \tag{4}$$

In the encryption process plaintext P_i XORed with ciphertext block of the previous block C_{i-1}, then encrypt under the block cipher encryption algorithm in the usual way. Every encryption algorithm depends on the previous block cipher. The first plaintext P_1 XORed to a random IV. The IV has the same size as a plaintext block. During the decrypting of a ciphertext block, every ciphertext block is decrypted under a key k, and the outcome is XORed with the previous block ciphertext C_{i-1} whereas in the first decryption block the ciphertext decrypted under a key k the result XORed with the IV.

The Cipher Feedback (CFB) mode

The CFB mode is a confidential mode that requires an initialization input IV and it must be unpredictable like CBC mode and need not be secret. The CFB mode can be formulated as follows.

$$C_1 = (E_k\left(IV\right) \oplus P_1)\ \text{(Encryption)} \tag{5}$$

$$C_i = (E_k\left(C_{i-1}\right) \oplus P_i)\ \text{for } 2 \le i \le n. \tag{6}$$

$$P_1 = (D_k(IV) \oplus C_1)\ \text{(Decryption)} \tag{7}$$

$$P_i = (D_k(C_{i-1}) \oplus C_i)\ \text{for} 2 \le i \le n. \tag{8}$$

The encryption process of CFB depends on the ciphertext of the previous block C_{i-1} then it encrypts under a key k and XORed with P_i and produce ciphertext C_i but in the first encryption block, IV encrypts under key k instead of C_{i-1}. Whereas in the decryption process, each block takes the ciphertext of the previous block C_{i-1} decrypt under key k then XORed with ciphertext C_i and give P_i. Nonetheless, like the encryption process of the first block, the decryption process also takes IV as input in the first block.

The Output Feedback (OFB) mode

The OFB mode is a confidential mode that is quite similar to the CFB mode and runs a block cipher as a stream cipher. The OFB mode can be formulated as follows.

$$O_1 = E_k\left(IV\right); C_1 = (O_1 \oplus P_1)\ \text{(Encryption)} \tag{9}$$

$$O_i = E_k\left(O_{i-1}\right); C_i = (O_i \oplus P_i)\ \text{for } 2 \le i \le n. \tag{10}$$

$$O_1 = E_k\left(IV\right); P_1 = (O_1 \oplus C_1)\ \text{(Decryption)} \tag{11}$$

$$O_i = E_k\left(O_{i-1}\right); P_i = (O_i \oplus C_i)\ \text{for } 2 \le i \le n. \tag{12}$$

The encryption process of each plaintext block takes O_{i-1} as input and encrypt under key k give output O_i and then XORed with plaintext P_i produce ciphertext C_i, but the first encryption block takes IV as input instead of O_{i-1}. Whereas the decryption process takes O_{i-1} as input (like encryption process) and encrypt under a key k then XORed with ciphertext C_i to produce plaintext P_i, On the other hand, the first block takes IV as input instead of O_{i-1} like the encryption process.

The Counter (CTR) Mode

The CTR mode is a confidential mode that uses a block cipher as its stream generator, whose input is a counter value. The value of the counter changes every time a new key stream is generated and the counters for a given message are divided into chunks of counters. The CTR mode can be formulated as follows.

$$C_i = E_k(ctr_i) \oplus P_i\ \text{(Encryption)} \tag{13}$$

$$P_i = E_k(ctr_i) \oplus C_i\ \text{(Decryption)} \tag{14}$$

The value of the counters is independent of the previous block output. In CTR encryption each encryption block is invoked on each counter the resulting is XORed with the corresponding block of plaintext P_i to produce a block of ciphertext C_i. In CTR decryption each encryption block is invoked on each counter and the outcome is XORed with the corresponding ciphertext C_i to produce plaintext P_i.

Dual key chaining mode

In this section, we describe how our proposed DKC structures encrypt the plaintext blocks as well as decrypt ciphertext blocks. First, we will define those functions and parameters invoked by the DKC mode. The definitions of P_i, C_i and IV are the same as defined in section 2. New parameters for DKC mode are defined below.

k_1: The block cipher encryption key, the same role as key K defined in section 2.

k_2: It is used to encrypt IV to get unpredictable output, same length as IV.

O_1: The unpredictable output from encryption of IV under k_2

The DKC mode overcomes the parallelization of ECB mode and CTR mode as well as overcomes the chaining dependency of CBC, CFB, and OFB mode. The DKC mode takes advantage of these five operation modes that are recommended by NIST and overcomes the deficiency of these operation modes. The DKC mode improves efficiency and provides chaining dependency as well as high security. The DKC mode divided block of plaintext into the sequence of plaintext blocks: $P_i = \{P_1, P_2, P_3, \ldots, P_n\}$, the length of each block of plaintext $\left|P_i\right|$ is equal to the length of the encryption algorithm. The length of $\left|P_i\right|$ depend on the encryption algorithm, if the encryption algorithm is DES then the size of each block is 64-bit and if the encryption algorithm is AES then the size of each block is 128-bit [27], respectively. The DKC provides partial parallelization as well as chaining encryption because each encryption block takes output directly from the previous block before encryption. So, error propagation cannot occur.

On the other hand, existing operation modes like CBC, CFB, and OFB mode provide chaining encryption but they have some drawbacks and security deficiencies [28,29]. In these modes of operation, each block depends on the output/ciphertext of the previous block. The error propagation can occur in these modes. Moreover, the CTR mode has parallel encryption but bit-flipping attacks are easy and reusing of key as well as nonce/counter is dangerous [28-30].

In the DKC encryption process, each encryption block partially depends on the previous encryption block O_{i-1} then XORed with the plaintext P_i give output O_i and encryption block encrypt P_i under the key k_1 and outcome XORed with the output O_1 produce ciphertext C_i. Whereas the first encryption block takes the output O_1 instead of output O_{i-1}. The output O_1 is the highly unpredictable value produced by the encryption of k_2 and *IV*. The DKC encryption can be formulated as follows.

$$O_1 = E_{k_2}\left(IV\right) \tag{15}$$

$$O_i = O_1 \oplus P_1 \text{ for } 2 \le i \le n \tag{16}$$

$$C_1 = E_{k_1}\left(O_1 \oplus P_1\right) \oplus O_1 \tag{17}$$

$$C_i = E_{k_1}\left(O_{i-1} \oplus P_i\right) \oplus O_1 \text{for } 2 \le i \le n \tag{18}$$

The encryption process of DKC mode is shown in Figure 1. The general rule is that O_{i-1}, $k_1$and P_i are input to the encryption algorithm that's XORed with O_1 to produce C_1.

Figure 1 illustrates the encryption process of the DKC. The components and flow are represented as follows:

IV (Initialization Vector): This is a random or pseudorandom value that is used only once per encryption session. It ensures that the encryption of the same plaintext results in different ciphertexts each time.

Block cipher encryption with k_2: The *IV* is encrypted using the second key k_2, to generate O_1, an unpredictable value. This step is crucial for achieving cryptographic security, as O_1 is used to ensure that each block of plaintext encrypts to a different ciphertext block, even if the same plaintext block is encrypted multiple times throughout the encryption process.

Plaintext blocks $(P_1, P_2, P_3, \ldots, P_n)$: These are the sequential plaintext blocks that need to be encrypted. Each block is of a fixed size determined by the block cipher's design (e.g., 128 bits for AES).

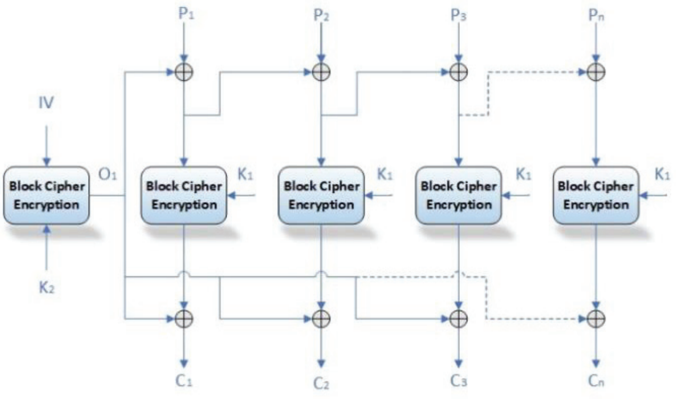

Figure 1: DKC Encryption.

XOR operation: Each plaintext block P_i is XORed with the output from the previous encryption step. For the first plaintext block P_1, the XOR operation is performed with O_1.

Block cipher encryption with k_2: After the XOR operation, the resulting value is then encrypted using the first key, k_1. This encryption step generates an intermediate value, which is then XORed with O_1 to produce the final ciphertext block C_i.

Ciphertext blocks $(C_1, C_2, C_3, \ldots, C_n)$: These are the resulting blocks of encrypted data. Each ciphertext block C_i is produced by the XOR operation between O_1 and the encrypted intermediate value from the previous step.

Chaining dependency: The output of each encryption block (O_{i-1}) is used as an input for the encryption of the next block (O_i). This creates a dependency chain that ensures the ciphertext is influenced by the previous ciphertext blocks, enhancing security.

This DKC mode encryption diagram shows that the encryption process for each block partially depends on the output of the previous block, which is a design intended to mitigate error propagation while still providing the security benefits of chaining. The dual-key approach (using both k_1 and k_2) and the use of the unpredictable O_1 generated from the *IV* increase the encryption complexity and security level of the system, making it resistant to certain types of cryptographic attacks like chosen plaintext attacks.

In the DKC decryption process, each encryption block depends on the output O_1 then XORed with the ciphertext C_i and the outcome value is encrypted under the key k_1 give output O_i and then output O_i XORed with previous block output O_{i-1} produce plaintext P_i. The DKC decryption is defined as follows:

$$O_1 = D_{k_2}\left(IV\right) \tag{19}$$

$$O_i = D_{k_1}(O_1 \oplus C_1) \text{ for } 2 \le i \le n \tag{20}$$

$$P_1 = D_{k_1}\left(O_1 \oplus C_1\right) \oplus O_1 \qquad (21)$$

$$P_i = D_{k_1}\left(O_1 \oplus C_i\right) \oplus O_{i-1} \text{ for i } = \text{ 2 … n.} \qquad (22)$$

Figure 2 depicts the decryption process for the DKC, which is essentially the reverse of the encryption process. Here's a condensed version of the DKC decryption process:

Reversing initialization: The IV is decrypted with k_1 to produce O_1, the initial output which was used during the encryption phase.

Sequential decryption: For each ciphertext block C_i, XOR it with O_1 and then decrypt with k_1 to produce an intermediate output O_i. To obtain the original plaintext P_i, XOR O_i with the intermediate output from the previous block O_{i-1}. For the first block, O_1 is used instead o O_{i-1}.

Chaining effect: The decryption of each block is dependent on the successful decryption of the previous block, mirroring the encryption chaining mechanism.

Figure 2 shows how DKC mode maintains the inter-block dependencies during decryption, ensuring that the original plaintext is reconstructed correctly from the ciphertext blocks.

Security analysis

The mode of operations for block cipher described above in section 2, including the CBC, CFB, OFB, and CTR, have their own security risk because the security level of these operation modes does not effectively improve. So, this section analyses the security of these existing block cipher modes of operation as well as our proposed DKC mode when each of them faces the chosen plaintext attacks.

The CBC mode security

The CBC mode is vulnerable to chosen plaintext attacks if intruders predict IV, then encryption cannot be resistant to chosen plaintext attacks. Whereas the intruder inputs large plaintext $P_i = \{P_1, P_2, P_3, \ldots, P_n\}$ to block cipher encryption algorithm to acquire the corresponding ciphertext $C_i = \{C_1, C_2, C_3, \ldots, C_n\}$, after that intruder obtained IV, P_i, C_i and C_{i-1}, in such a way intruders with the help of these components analyse the key K of the block cipher encryption algorithm.

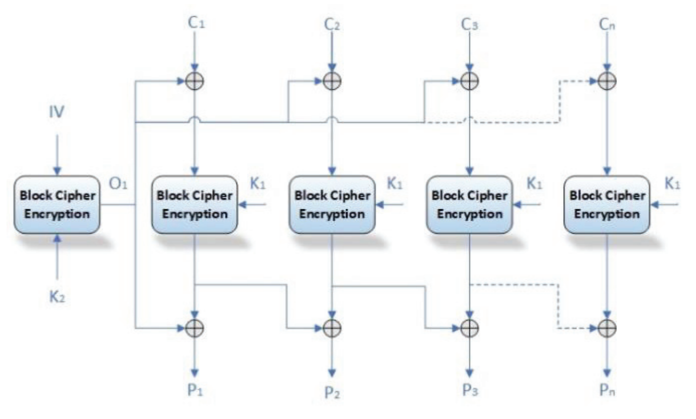

Figure 2: DKC Decryption.

The CFB mode security

In the CFB mode, O_i is only derived from IV/C_{i-1} and key K of the encryption algorithm. If the intruder successfully predicts the IV then they input a large plaintext $P_i = \{P_1, P_2, P_3, \ldots, P_n\}$ to block cipher encryption algorithm to obtain the corresponding ciphertext $C_i = \{C_1, C_2, C_3, \ldots, C_n\}$. Nonetheless, when intruders acquire C_{i-1} and O_i then they can surely analyse the key k of the encryption algorithm. So, the CFB mode is vulnerable to chosen plaintext attacks.

The OFB mode security

The OFB mode is also vulnerable to chosen plaintext attacks. If intruders predict IV, then they can get the advantage of inputting an IV into the encryption algorithm to acquire O_1 and corresponding $O_i = \{O_2, O_3, \ldots, O_n\}$ (the output O_i only be acquired by output O_{i-1} where 1 ≤ i ≤ n and key k, then the intruder inputs a long plaintext $P_i = \{P_1, P_2, P_3, \ldots, P_n\}$ that's XORed with the corresponding O_i and obtain ciphertext $C_i = \{C_1, C_2, C_3, \ldots, C_n\}$. Now intruders know the O_i and corresponding O_{i-1}, so they can analyse the key k of the encryption algorithm. So, OFB mode is vulnerable to chosen plaintext attacks.

The CTR mode security

In CTR mode, the output value O_i only determined by incremental integer ctr and fixed key k. If the intruder has an advantage on ctr, then they can obtain the set of output $O_i = \{O_1, O_2, O_3, \ldots, O_n\}$ from $E_{k,ctr}$. On the other hand, intruders input the large plaintext $P_i = \{P_1 = \{P_1, P_2, P_3, \ldots, P_n\}$ that's XORed with O_i and produce the corresponding ciphertext $C_i = \{C_1, C_2, C_3, \ldots, C_n\}$. In this way when intruders obtain O_i corresponding to ctr they can analyse the key k.

The DKC mode security

The security goal for DKC is achieving indistinguishability under chosen plaintext attacks (IND-CPA), implying an adversary cannot practically distinguish ciphertexts produced by DKC from those produced by a random permutation.

Let us consider two games:

- **Game 0 (real game):** An adversary interacts with a real encryption oracle of DKC, where for a chosen plaintext P, the oracle returns a ciphertext C from encrypting P using DKC mode.

Citation: Nawaz MF, Nawaz Y (2024) Enhancing cryptographic robustness with dual key chaining. Trends Comput Sci Inf Technol 9(1): 026-033. DOI: https://dx.doi.org/10.17352/tcsit.000077

- **Game 1 (random game):** The adversary interacts with a simulated oracle returning a random string C of identical length to the encryption of P, regardless of P.

An adversary A selects plaintexts $P_1, P_2, P_3, \ldots, P_n$ and queries the oracle to receive corresponding ciphertexts. The advantage of A in distinguishing between the two games is:

$$Adv_A = | \; Pr[A \text{ wins } Game\, 0] - Pr[A \text{ wins } Game\, 1] \; |$$

For DKC mode,encrypting a plaintext block P_i under keys k_1 and k_2 is defined as: $C_i = E_{k_1}(O_{i-1} \oplus P_i \oplus O_1$ where $O_1 = E_{k_1}(\mathrm{IV})$ and O_i is the output for block i, determined by the encryption process. The decryption is the inverse: $P_i = D_{k_1}(C_i \oplus O_1) \oplus O_{i-1}$

Assuming an adversary A has a non-negligible advantage ε in distinguishing Game 0 from Game 1 implies A can distinguish DKC's encryption from a random permutation, contradicting DKC's IND-CPA security definition. Given DKC's structure, where k_1 and k_2 layer security and O_1 is unpredictable due to its derivation from E_{k1}(IV), it argues that without knowledge of k_1, k_2, or IV, distinguishing Ci from random output is computationally infeasible. Thus, if Adv_A is non-negligible, it contradicts the assumption that DKC is secure under the IND-CPA model, implying no such adversary A exists, and thereby DKC mode is secure against chosen plaintext attacks under the IND-CPA model.

The DKC presents significant security improvements over traditional block cipher modes like ECB, CBC, CFB, OFB, and CTR. Unlike ECB, which suffers from pattern recognition vulnerabilities due to identical plaintext blocks producing identical ciphertext blocks, DKC's dual-key mechanism and generation of unpredictable values ensure that similar patterns are not discernible in the ciphertext. This enhances its resistance to pattern analysis and chosen plaintext attacks. In contrast to CBC and CFB, which are susceptible to error propagation and chosen plaintext attacks due to their chaining dependencies, DKC minimizes these risks with its unique encryption process that avoids direct dependency on previous blocks. Furthermore, OFB's vulnerability to IV reuse attacks is mitigated in DKC through its sophisticated IV encryption process, providing a robust defense mechanism against such exploits. Additionally, unlike CTR, which depends on the uniqueness of counters, DKC's approach avoids potential vulnerabilities associated with counter-reuse, offering enhanced security. Overall, DKC's advanced design principles, including the dual key strategy and unpredictable value generation, position it as a superior mode of operation, providing stronger security guarantees against a wider range of cryptographic attacks compared to traditional modes.

Discussion

Our research presents the DKC mode as an innovative block cipher operation mode. We assess DKC against conventional modes across various criteria detailed in Table 1. These criteria span the type of encryption algorithm used, error propagation potential, dependency on previous encryption blocks (chain dependency), confidentiality assurance, support for parallel processing (parallelism), adaptability to plaintext of varying sizes, resilience to chosen plaintext attacks (indicating security level), and the rate at which the process can be executed (processing speed).

The DKC mode integrates a dual-key system to bolster security and reduce error propagation, a common issue in modes that rely heavily on the outcome of preceding blocks. While it maintains chain dependency, this does not impede parallel processing as much as in some other modes, striking a balance between security and efficiency. DKC's handling of variable-sized plaintext and its defense against chosen plaintext attacks demonstrate its robustness and adaptability, potentially rendering it a superior option for secure cryptographic applications.

The DKC mode is a block cipher encryption method like AES or DES, designed for fixed-size input to generate ciphertext. DKC stands out because it can handle variable-sized plaintext; if a plaintext block exceeds the fixed size, DKC simply moves the overflow to the next block. One of the key features of DKC is that while it incorporates a chaining mechanism, it does not solely rely on the previous block's encryption, thus preventing error propagation—a common issue in traditional chaining modes.

Unlike other modes, which often create a linear chain where each block's encryption depends on the previous one, DKC allows for a form of partial parallelism. This characteristic improves the processing speed, making it faster than most other modes, though not as fast as CTR mode, which encrypts plaintext blocks in parallel.

In terms of security, especially regarding chosen plaintext attacks, DKC offers enhanced protection. While existing modes like CTR are susceptible to such attacks, DKC's design, which involves encrypting each plaintext block with an unpredictable value, provides a strong defense, making it secure against chosen plaintext attacks.

Table 1 offers a comparative evaluation of various block cipher operation modes, including the novel DKC mode, across several cryptographic parameters.

Table 1: Evaluation of DKC mode with existing modes of operation.

Evaluation Criteria	CBC	CFB	OFB	CTR	DKC
Encryption Algorithm	Any	Any	Any	Any	Any
Chain Dependency	Yes	Yes	Yes	No	Yes
Error Propagation	Yes	Yes	Yes	No	No
Confidentiality	Yes	Yes	Yes	Yes	Yes
Parallelism	No	No	No	Yes	No
CPA Security	No	No	No	Partially	Yes
Plaintext Size	Any	Any	Any	Any	Any
Processing Speed	Low	Low	Low	High	Medium

Citation: Nawaz MF, Nawaz Y (2024) Enhancing cryptographic robustness with dual key chaining. Trends Comput Sci Inf Technol 9(1): 026-033.
DOI: https://dx.doi.org/10.17352/tcsit.000077

Encryption algorithm: This criterion signifies compatibility with any encryption algorithm. All modes, including DKC, show versatility by supporting various encryption algorithms without restrictions.

Chain dependency: Chain dependency refers to the reliance of a block's encryption on the previous block's output. DKC, CBC, CFB, and OFB modes demonstrate a 'Yes' for chain dependency, indicating a sequential encryption process where the encryption of each block depends on the preceding one. CTR mode, however, is independent, as indicated by a 'No,' allowing for each block to be processed in isolation.

Error propagation: DKC and CTR modes excel by preventing error propagation ('No'), meaning that an error in one ciphertext block does not affect subsequent blocks, thereby localizing any potential issues. In contrast, CBC, CFB, and OFB modes are susceptible to error propagation ('Yes'), where a single block error can affect the decryption of subsequent blocks.

Confidentiality: All modes provide confidentiality ('Yes'), ensuring that encrypted data remains inaccessible to unauthorized entities.

Parallelism: Only the CTR mode supports parallel processing ('Yes'), enabling faster encryption and decryption by processing multiple blocks simultaneously. DKC, alongside CBC, CFB, and OFB, does not support this feature ('No'), implying a sequential processing of blocks.

CPA security: CPA security assesses the mode's resilience against chosen plaintext attacks. DKC asserts full security ('Yes'), purporting robustness against such attacks. The CTR mode is 'Partially' secure, implying some susceptibility, whereas CBC, CFB, and OFB modes are deemed insecure ('No') against CPA.

Plaintext size: The table indicates all modes, including DKC, can manage plaintext of any size ('Any'). This typically involves padding the plaintext to fit the block cipher's block size requirements.

Processing speed: Figure 3 shows a comparison of encryption times for various modes against the proposed DKC mode over increasing block sizes. DKC's performance is in line with conventional modes, displaying only a marginal increase in encryption time despite its enhanced security features. This suggests that DKC provides a significant security advantage, particularly against chosen plaintext attacks, without sacrificing efficiency. Its dual-key mechanism is designed to mitigate vulnerabilities inherent in single-key modes, making it a compelling choice for applications where security is paramount.

In essence, the DKC mode offers a trade-off between the highly parallelizable yet partially CPA-vulnerable CTR mode and the more traditional, sequentially dependent modes (CBC, CFB, OFB) that are prone to error propagation. DKC's 'Medium' speed is justified by its significant security benefits, particularly in preventing error propagation and ensuring CPA security.

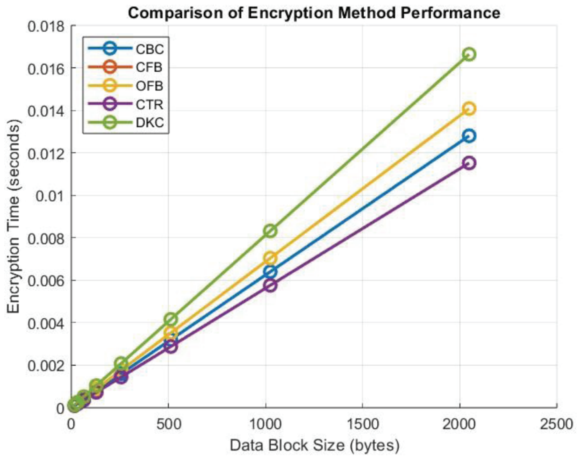

Figure 3: Performance Analysis (i.e. Processing Speed).

Conclusion

This study introduces the DKC, a novel block cipher mode of operation designed to address the security limitations of existing modes while integrating the advantages of both chaining and parallelization techniques recommended by NIST. Through our comprehensive analysis, DKC has demonstrated its superior capability to withstand chosen plaintext attacks, thereby offering a robust cryptographic solution for securing sensitive information across various applications. In comparison with traditional modes, DKC's unique dual key mechanism and the generation of unpredictable values significantly elevate its security posture. This innovative approach ensures that DKC is not only resistant to common vulnerabilities but also excels in maintaining the confidentiality and integrity of data without compromising on efficiency.

The practical implications of DKC are profound. By effectively mitigating risks such as error propagation, chain dependency, and susceptibility to pattern recognition and chosen plaintext attacks, DKC presents a compelling case for adoption in high-security environments. Whether for securing communication channels, financial transactions, or cloud storage services, DKC offers a versatile and reliable solution that stands out in the face of evolving cryptographic challenges. Our findings affirm the potential of DKC as a leading cryptographic standard for future implementation. As the digital landscape continues to grow in complexity, the importance of innovative and secure encryption modes like DKC cannot be overstated. We encourage further research and application of DKC to explore its full capabilities and integration into global security frameworks.

References

1. Rogaway P. Evaluation of some blockcipher modes of operation. 2011.

2. Buchmann JA. Discrete Logarithms. Introduction to Cryptography: Springer. 2001; 185-204.

3. Thabit F, Can O, Aljahdali AO, Al-Gaphari GH, Alkhzaimi HAJIoT. A Comprehensive Literature Survey of Cryptography Algorithms for Improving the IoT Security. 2023; 100759.

4. Nadeem A, Javed MY. A performance comparison of data encryption

algorithms. Information and communication technologies, 2005 ICICT 2005 First international conference on; 2005: IEEE.

5. Singh G. A study of encryption algorithms (RSA, DES, 3DES, and AES) for information security. International Journal of Computer Applications. 2013; 67(19).

6. Bhanot R, Hans R. Applications I. A review and comparative analysis of various encryption algorithms. International Journal of Security and Its Applications. 2015; 9(4):289-306.

7. Barker E. NIST SP 800-67 Rev. 2, Recommendation for Triple Data Encryption Algorithm (TDEA) Block Cipher. 2017; 800; 67.

8. Matsui M. Linear cryptanalysis method for DES cipher. Workshop on the Theory and Application of Cryptographic Techniques; 1993: Springer.

9. Bleichenbacher D. Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS# 1. Annual International Cryptology Conference; 1998: Springer.

10. Canetti R, Halevi S, Katz J. Chosen-ciphertext security from identity-based encryption. International Conference on the Theory and Applications of Cryptographic Techniques; 2004: Springer.

11. Peng X, Zhang P, Wei H, Yu B. Known-plaintext attack on optical encryption based on double random phase keys. Opt Lett. 2006 Apr 15;31(8):1044-6. doi: 10.1364/ol.31.001044. PMID: 16625897.

12. Standard A. Federal information processing standards publication. 197. 2001:46-3.

13. Stallings W. Cryptography and Network Security, 4/E: Pearson Education India; 2006.

14. Van Tilborg HC, Jajodia S. Encyclopedia of cryptography and security: Springer Science & Business Media; 2014.

15. Dworkin M. Recommendation for block cipher modes of operation. Methods and techniques. National Inst of Standard and technology Gaithersburg MD Computer Security DIV, 2001.

16. Daemen J. JhcngearRp. AES proposal. Rijndael, Document Version 2, 1999.

17. Stallings W. Cryptography and network security: principles and practice: Pearson Upper Saddle River, NJ; 2017.

18. Heys HM. Analysis of the statistical cipher feedback mode of block ciphers. IEEE Transactions on Computers. 2003; 52: 77-92.

19. Smid ME, Branstad D. Data encryption standard: past and future. Information Technology Laboratory Computer Security Resource Center. 1988; 76(5):550-9.

20. Wang D, Lin D, Wu WJINS. Related-Mode Attacks on CTR Encryption Mode. Computer Science 2007; 4(3):282-7.

21. Hudde HC. Building stream ciphers from block ciphers and their security. 2009.

22. Jimale MA, Z'aba MR, Kiah MLBM, Idris MYI, Jamil N, Mohamad MS. Authenticated encryption schemes: A systematic review. IEEE Access. 2022; 10:14739-66.

23. Hassan A, editor Lightweight cryptography for the Internet of Things. Proceedings of the Future Technologies Conference (FTC) 2020, Volume 3; 2021: Springer.

24. Bow I, Bete N, Saqib F, Che W, Patel C, Robucci R. Side-channel power resistance for encryption algorithms using implementation diversity. Cryptography. 2020; 4(2):13.

25. Mashatan A, Heintzman DJQ. The complex path to quantum resistance: is your organization prepared? 2021; 19(2):65-92.

26. Mammeri ZZ. Cryptography: Algorithms, Protocols, and Standards for Computer Security: John Wiley & Sons; 2024.

27. Stallings W, Brown L, Bauer MD, Bhattacharjee AK. Computer security: principles and practice: Pearson Education; 2012.

28. Wobst R. Adventure Cryptology: Methods, risks and benefits of data encryption: Pearson Deutschland GmbH; 2001.

29. Lindell Y, Katz J. Introduction to modern cryptography: Chapman and Hall/CRC; 2014.

30. De Canniere C, Biryukov A, Preneel BJPotI. An introduction to block cipher cryptanalysis. 2006; 94(2):346-56.