On the security of AEAD scheme recommended for use in Signal protocol

DOI: https://doi.org/10.54654/isj.v1i21.1028

Nguyen Tuan Anh, Trieu Quang Phong

***Abstract*— In this paper, we provide a security assessment for the authenticated encryption mode used in the recommendation of the Signal protocol. Furthermore, we found how tags are computed in Signal's guidance differs slightly from the cited documentation. Our evaluation suggests how to choose the IV value to reduce the data storage space in the Signal protocol.**

***Tóm tắt*— Trong bài báo này, chúng tôi đưa ra đánh giá độ an toàn cho chế độ mã hóa có xác thực được sử dụng trong khuyến cáo của giao thức Signal. Hơn nữa, chúng tôi phát hiện rằng cách tính nhãn xác thực trong hướng dẫn của Signal có chút khác biệt so với tài liệu được trích dẫn. Đánh giá của chúng tôi gợi ý cách chọn giá trị IV để giảm không gian lưu trữ dữ liệu trong giao thức Signal.**

***Keywords*— AEAD, authenticated encryption, Signal.**

***Từ khóa*— AEAD, mã hóa có xác thực, Signal.**

I. INTRODUCTION

Signal is a free messaging app for instant message exchange for mobile devices and PCs. It is encrypted to ensure user privacy and security. Signal is available on multiple platforms, including IOS, Android, Windows, Mac, and Linux, and is widely used worldwide.

At its core, in Signal, messages are encrypted and authenticated using a fresh symmetric key. This is guaranteed by authenticated encryption modes. Therefore, researching suitable modes is an issue of concern in the world's cryptographic community. In [1], J. Alwen et al. showed that the one-time IND-CCA security is enough for authenticated encryption modes used in Signal. This document also makes a recommendation on the use of the SIV scheme or composition of CBC with HMAC but does not provide any proof.

Related work. The authenticated encryption SIV was proposed in [2] and the composition of CBC with HMAC was proposed in [3]. The security of these modes has also been studied in the above documents. In which, the SIV mode is evaluated based on the DAE advantage [2]. In our opinion, the one-time IND-CCA security of SIV can be deduced from this result. However, the authenticated encryption mode based on the Encrypt-then-Mac method which is the general case composition of CBC with HMAC has been evaluated on PRIV and AUTH advantages [3]. The one-time IND-CCA security of this scheme cannot be inferred from [3]. Additionally, in the Signal protocol's manual description, the authentication label calculation is calculated using $F_{K'}(a\|C)$ instead of $F_{K'}(IV\|a\|C)$ as in [3].

Our contributions. In this paper, we give a detail proof for the one-time IND-CCA security of the authenticated encryption mode which is the general construction of the composition of CBC with HMAC as in [1]. Furthermore, we recommend using IV as a fixed value for all packets to minimize storage space for devices using the Signal protocol.

Outline. This paper is organized as follows: Section II recalls some basic definitions. Section III presents our result regarding the one-time IND-CCA security of the authenticated encryption mode based on the Encrypt-then-

This manuscript is received on March 5, 2024. It is commented on June 10, 2024 and is accepted on June 20, 2024 the first reviewer. It is commented on June 14, 2024 and is accepted on June 26, 2024 by the second reviewer.

MAC method which was proposed for use in Signal. Section IV shows how to choose the IVs based on the evaluation of Section III.

II. PRELIMINARIES

A. Notations and security model

Notations: Let $X\|Y$ be the concatenation of two strings X and Y. The set $\{0,1\}^n$ denotes all strings of length n bit, the set $\{0,1\}^*$ denotes all strings of arbitrary length. Let m is a message, $|m|$ is denoted the length of m. Let $X \xleftarrow{\$} \mathcal{X}$ mean that X is selected randomly from $\mathcal{X}$. By $A^F = b$ we mean the event that the adversary A, running with its oracle F and based on the outputs of F, outputs a bit $b \in \{0,1\}$.

Authenticated Encryption. Definition 1 (Definition 1, [1]). An authenticated encryption with associated data (AEAD) scheme is a pair of algorithms $\mathrm{AE} = (\mathrm{Enc}, \mathrm{Dec})$ with the following syntax:

- Encryption: Enc takes a key K, associated data a, and a message m and produces a ciphertext $e \leftarrow \mathrm{Enc}(K, a, m)$.

- Decryption: Dec takes a key K, associated data a, and a ciphertext e and produces a message $m \leftarrow \mathrm{Dec}(K, a, e)$.

In this paper, the AEAD scheme is assumed to be deterministic, that is, all randomness stems from the key K. Note that, in the above definition, the ciphertext e includes the authentication tag.

Correctness: An AEAD scheme is correct if for all keys K and all pairs (K, a), we have

$$\mathrm{Dec}\big(K, a, \mathrm{Enc}(K, a, m)\big) = m.$$

Pseudorandom function. Let $F: \mathcal{K} \times \mathcal{X} \to \{0,1\}^n$ be a function family. Let $\mathrm{Rand}(\mathcal{X}, n)$ be the set of all functions from $\mathcal{X}$ to $\{0,1\}^n$. Define the advantage of a distinguisher A in distinguishing the function F and a function ρ by:

$$\mathrm{Adv}_F^{\mathrm{prf}}(A) = \left|\Pr\left[K \xleftarrow{\$} \mathcal{K}, A^{F_K(\cdot)} = 0\right] - \Pr[A^{\rho} = 0]\right|,$$

where $\rho \xleftarrow{\$} \mathrm{Rand}(\mathcal{X}, n)$.

Define

$$\mathrm{Adv}_F^{\mathrm{prf}}(q) = \max_A \mathrm{Adv}_F^{\mathrm{prf}}(A)$$

the maximum value is taken over attackers make at most q queries.

Privacy. In this paper, we only consider length-preserving encryption schemes $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, where $\mathcal{K}$ is key space, $\mathcal{E}$ is encryption algorithm and $\mathcal{D}$ is decryption algorithm. Denote $\mathcal{E}_K^{\$}(\cdot)$ be the probabilistic algorithm based on $\mathcal{E}$ that takes inputs a key $K \in \mathcal{K}$, a message $m \in \{0,1\}^*$, and a random $IV \xleftarrow{\$} \{0,1\}^n$, computes $C \leftarrow \mathcal{E}_K^{IV}(m)$ and, returns $IV\|c$. The advantage of adversary A in attacking the privacy of Π is defined by

$$\mathrm{Adv}_{\Pi}^{\mathrm{priv}}(A) = \left|\Pr\left[K \xleftarrow{\$} \mathcal{K}: A^{\mathcal{E}_K^{\$}(\cdot)} = 0\right] - \Pr\left[A^{\$(\cdot)} = 0\right]\right|,$$

where $\$(\cdot)$ is a random oracle that returns a random $n + |m|$-bits string. We assume that the adversary never asks a query m outside the message space $\mathcal{X}$.

Define

$$\mathrm{Adv}_{\Pi}^{\mathrm{priv}}(q) = \max_A \mathrm{Adv}_{\Pi}^{\mathrm{priv}}(A),$$

the maximum value is taken over attackers make at most q queries.

Indistinguishability games: Let the init procedure samples a key $K \in \mathcal{K}$ and a secret bit $b \in \{0,1\}$. The adversary wins if he can return a bit b' such that $b' = b$ by interacting with all available oracles. The advantage of an adversary A against construction C in an indistinguishability game Γ is:

$$\mathrm{Adv}_C^{\Gamma}(A) \coloneqq 2 \cdot \left|\Pr[A \text{ win } \Gamma^C] - \frac{1}{2}\right|.$$

Security. According to [1], AEAD schemes that are used in the Signal need to have one-time IND-CCA security. This property is described by the indistinguishability game. In this game, the init procedure initiates the returned value e^* for the adversary, when he

makes an encryption query, is an empty string λ. The adversary only makes one query (a, m) to the encryption oracle. In the case $b = 1$, a value is chosen uniformly randomly from $\mathcal{C}$ and will be returned to the adversary. Where $\mathcal{C}$ is the set of all ciphertexts that have the size $|\text{Enc}(K, a, m)|$. However, he may query to decryption oracle many times (except on the challenge ciphertext). The oracles for one-time IND-CCA security is described in Figure 1. Note that the decryption oracle always returns $\perp$ if $b = 1$.

The advantage of an adversary A against the one-time IND-CCA property of an AEAD scheme AE is denoted by $\text{Adv}_{\text{AE}}^{\text{ot-cca}}(A)$; the attacker is parametrized by its running time t.

Oracles for one-time IND-CCA security	
encrypt(a, m)	**decrypt**(a, e)
if $b = 0$	**if** $e = e^*$ or $b = 1$
$e^* \leftarrow$ **Enc**(K, a, m)	**return** $\perp$
else	**return Dec**(K, a, e)
$e^* \xleftarrow{\$} \mathcal{C}$	
return e^*	

Figure 1. Oracles for IND-CCA security game for an AEAD scheme (Enc, Dec), where encrypt is a one-time oracle

Note. If an AEAD scheme guarantees authenticity, then an attacker can only provide a ciphertext that can be successfully decrypted, i.e. the decryption algorithm produces a plaintext, with a very small probabilty. So in most cases, the decrytion oracle will return the special character $\perp$.

Definition 2 (Definition 2, [1]). An AEAD scheme AE is (t, ϵ)-one-time-CCA-secure if for all t-attacker A,

$$\text{Adv}_{\text{AE}}^{\text{ot-cca}}(A) \leq \epsilon.$$

Note that the probability that the attacker A wins the game can be rewritten as follows:

$$\Pr[A \text{ win } \Gamma^C] = \Pr[b = b']$$

$$= \Pr[b' = 0 | b = 0] \Pr[b = 0] + \Pr[b' = 1 | b = 1] \Pr[b = 1]$$

$$= \Pr[b' = 0 | b = 0] \cdot \frac{1}{2} + \Pr[b' = 1 | b = 1] \cdot \frac{1}{2}$$

$$= \frac{1}{2} \cdot \Pr[b' = 0 | b = 0] + \frac{1}{2}(1 - \Pr[b' = 0 | b = 1])$$

$$= \frac{1}{2} + \frac{1}{2}(\Pr[b' = 0 | b = 0] - \Pr[b' = 0 | b = 1])$$

$$= \frac{1}{2} + \frac{1}{2}\left(\Pr\left[A_{\text{AE}}^{b=0} = 0\right] - \Pr\left[A_{\text{AE}}^{b=1} = 0\right]\right),$$

where $\Pr\left[A_{\text{AE}}^{b=0} = 0\right]$ and $\Pr\left[A_{\text{AE}}^{b=1} = 0\right]$ are the probabilities that the attacker A returns 0 in the case $b = 0$ and $b = 1$, respectively.

Then

$$\text{Adv}_{\text{AE}}^{\text{ot-cca}}(A) = 2 \cdot \left|\Pr[A \text{ win } \Gamma^C] - \frac{1}{2}\right| = 2 \cdot \left|\Pr[b = b'] - \frac{1}{2}\right| = \left|\Pr\left[A_{\text{AE}}^{b=0} = 0\right] - \Pr\left[A_{\text{AE}}^{b=1} = 0\right]\right|.$$

B. *AEAD is used in the Signal*

As recommended in Section 5.2 of [1], the AEAD scheme used in the Signal is a composition of CBC with HMAC [3] or SIV [2]. For the AEAD scheme based on a composition of CBC with HMAC, according to our research the Double Ratchet algorithm at https://signal.org/docs/specifications/doubleratchet/, this scheme uses the Encrypt – then – Mac which is presented in [3]. We will represent the definition of this scheme.

The AEAD scheme based on a composition of CBC with HMAC. Firstly, we found that the authentication tag is computed by $F_{K'}(a\|C)$ instead of $F_{K'}(IV\|a\|C)$ as in Section 7 of [3]. Next, we will present the AEAD scheme according to the Encrypt – then – MAC method with the above modifications, which we call modified Encrypt – then – MAC.

Let $\Pi = (\mathcal{K}_1, \mathcal{E}, \mathcal{D})$ be an encryption scheme. For simplicity, the message space of Π is $\mathcal{X} = \{0,1\}^*$, the IV space is $\mathcal{IV} = \{0,1\}^n$. Let

$F: \mathcal{K}_2 \times \{0,1\}^* \to \{0,1\}^\tau$ be a function family. Let the associated space be Header $\subseteq \{0,1\}^*$. Defined AEAD scheme $\widetilde{\Pi} = [\Pi, F] = \left(\widetilde{\mathcal{K}}, \tilde{\mathcal{E}}, \widetilde{\mathcal{D}}\right)$ with key space $\widetilde{\mathcal{K}} = \mathcal{K}_1 \times \mathcal{K}_2$ as in Figure 2.

Algorithm $\tilde{\mathcal{E}}^{IV}_{K_1,K_2}(a,m)$	**Algorithm** $\widetilde{\mathcal{D}}^{IV}_{K_1,K_2}(a,e)$
$C = \mathcal{E}^{IV}_{K_1}(m)$ $T = F_{K_2}(a\|\|C)$ **return** $e = C\|\|T$	**if** $\|e\| < \tau$ **then return** $\perp$ $e = C\|\|T$ where $\|T\| = \tau$ $T' \leftarrow F_{K_2}(a\|\|C)$ **if** $T = T'$ **then return** $m = \mathcal{D}^{IV}_{K_1}(C)$ **else return** $\perp$

Figure 2. AEAD scheme based on the modified Encrypt – then – MAC with associated data a, message m, key (K_1, K_2), and ciphertext $e = C\|T$.

In the Signal's case, $\Pi = (\mathcal{K}_1, \mathcal{E}, \mathcal{D})$ is the CBC mode and $F: \mathcal{K}_2 \times \{0,1\}^* \to \{0,1\}^\tau$ is HMAC with SHA hash function.

III. The OT-CCA security of modified Encrypt – then – MAC

We will evaluate for general case.

Proposition 1. The authenticated encryption $\widetilde{\Pi} = \text{AEAD}[\Pi, F] = \left(\widetilde{\mathcal{K}}, \tilde{\mathcal{E}}, \widetilde{\mathcal{D}}\right)$ is based on a encryption scheme $\Pi = (\mathcal{K}_1, \mathcal{E}, \mathcal{D})$ with random IV and an authentication message code $F: \mathcal{K}_2 \times \{0,1\}^* \to \{0,1\}^\tau$ as in Fig 2. Then

$$\text{Adv}^{\text{ot-cca}}_{\widetilde{\Pi}} \le q/2^\tau + \text{Adv}^{\text{priv}}_{\Pi}(1) + \text{Adv}^{\text{prf}}_{F}(q+1).$$

Proof. Consider the game in which an attacker A attacks the OT-CCA security of $\widetilde{\Pi}$. First, the init procedure generates a uniformly random key $K = K_1\|K_2$ from the key space, and choose a random bit $b \in \{0,1\}$. Note that the attacker A only makes 1 encryption query (a, m) and q decryption queries (a_i, e_i) where $i \in \{1, \dots, q\}$. Then he guess bit b, we have:

$$\text{Adv}^{\text{ot-cca}}_{\widetilde{\Pi}} = \epsilon = \left|\Pr\left[A^{b=0}_{\widetilde{\Pi}} = 0\right] - \Pr\left[A^{b=1}_{\widetilde{\Pi}} = 0\right]\right|.$$

Considering the case that F is a random function F^*, we call the new scheme $G = \text{AEAD}[\Pi, F^*]$. and evaluate the advantage of attacker on the OT-CCA security of the scheme G. Then the advantage of attacker on the OT-CCA security the scheme $\widetilde{\Pi} = \text{AEAD}[\Pi, F]$ is bounded by the distinguish probability of random function F^* and a function F.

Note that the values are returned by F^* is random, we have:

$$\begin{aligned}\epsilon_0 &= \left|\Pr[A^{b=0}_G = 0] - \Pr\left[A^{b=1}_{\text{G}} = 0\right]\right| \\ &= \left|\Pr[A^{b=0}_G = 0] - \Pr\left[A^{b=0,\perp}_G = 0\right] + \Pr\left[A^{b=0,\perp}_G = 0\right] - \Pr\left[A^{b=1}_{\text{G}} = 0\right]\right| \\ &\le \left|\Pr[A^{b=0}_G = 0] - \Pr\left[A^{b=0,\perp}_G = 0\right]\right| + \left|\Pr\left[A^{b=0,\perp}_G = 0\right] - \Pr\left[A^{b=1}_{\text{G}} = 0\right]\right|,\end{aligned}$$

where $A^{b=0,\perp}_G$ be an attacker on the OT-CCA security of G with encryption query which is the same as of the case $b = 0$ but decryption queries always return $\perp$.

Next, we will evaluate $\epsilon_1 = \left|\Pr[A^{b=0}_G = 0] - \Pr\left[A^{b=0,\perp}_G = 0\right]\right|$ and $\epsilon_2 = \left|\Pr\left[A^{b=0,\perp}_G = 0\right] - \Pr\left[A^{b=1}_{\text{G}} = 0\right]\right|$.

In the case of ϵ_1. Note that the encryption query in both probabilities is the same which is $C\|T$, where $C = \mathcal{E}^{IV}_{K_1}(m)$ and $T = F^*(a, C)$. The only difference is that the attacker can issue a valid decryption query in the left probability. It means that A finds (a_i, e_i), where $e_i = C_i\|T_i$ and $|T_i| = \tau$ such that $T_i = T_i' \leftarrow F^*(a_i, C_i)$. However, since F^* is a random function, $\Pr[T_i = T_i'] = 1/2^\tau$. Then, the probability that A make a valid decryption query in the left probability is $q/2^\tau$. Thus, $\epsilon_1 = q/2^\tau$.

In the case ϵ_2. All decryption queries are returned as $\perp$. For encryption queries, the returned value will be implemented by the construction Π and the function F^* in the left probability while it will be a random value in the right probability. In order to evaluate ϵ_2, we construct an attacker B on the priv of $\mathcal{E}$. When A queries (a, m) to the oracle, B send m to its oracle and receive IV and C. B chooses T random and returns $C\|T$ to A. Then, if A returns a bit $b \in \{0,1\}$, B also returns b. Thus, we have

$$\epsilon_2 \leq \mathrm{Adv}_{\Pi}^{\mathrm{priv}}(1).$$

Next, we convert the function F^* back to the function F, we have:

$$|\epsilon - \epsilon_0| = \Big|\big|\Pr\big[A_{\widetilde{\Pi}}^{b=0} = 0\big] - \Pr\big[A_{\widetilde{\Pi}}^{b=1} = 0\big]\big| - \big|\Pr[A_G^{b=0} = 0] - \Pr\big[A_{\mathrm{G}}^{b=1} = 0\big]\big|\Big|$$

Using the inequality: $\big||a-b|-|c-d|\big| \leq |a-c|+|b-d|$, we have

$$|\epsilon - \epsilon_0| \leq \big|\Pr\big[A_{\widetilde{\Pi}}^{b=0} = 0\big] - \Pr[A_G^{b=0} = 0]\big| + \big|\Pr\big[A_{\widetilde{\Pi}}^{b=1} = 0\big] - \Pr[A_G^{b=1} = 0]\big|.$$

Next, we estimate $\big|\Pr\big[A_{\widetilde{\Pi}}^{b=0} = 0\big] - \Pr[A_G^{b=0} = 0]\big|$. We construct an attacker B_1 on the PRF security of function F using A as a subroutine. B_1 chooses a random key K_1. When A queries (a, m), B_1 chooses a random IV and computes $C = \mathcal{E}_K^{\mathrm{IV}}(m)$ and sends (a, C) to its oracle and receives T. Then, B_1 gives $C\|T$ to A. When A makes a decryption query (a_i, e_i), if $e_i = C_i\|T_i$ is the previously returned value, then B_1 return $\perp$, otherwise, B_1 separates C_i and T_i from e_i. Then, B_1 queries (a_i, C_i) to its oracle and receives T_i'. If $T_i = T_i'$ B_1 chooses a random IV_i and returns $m_i = \mathcal{D}_K^{\mathrm{IV}_i}(C)$ to A, otherwise returns $\perp$. Thus, B_1 simulates the correct environment for A, we have:

$$\big|\Pr\big[A_{\widetilde{\Pi}}^{b=0} = 0\big] - \Pr[A_G^{b=0} = 0]\big| \leq \mathrm{Adv}_F^{\mathrm{prf}}(q+1).$$

Now, we estimate $\big|\Pr\big[A_{\widetilde{\Pi}}^{b=1} = 0\big] - \Pr[A_G^{b=1} = 0]\big|$. We note that, for the left or right probabilities, the encryption query always returns a random value, and the decryption query always returns $\perp$. Thus,

$$\big|\Pr\big[A_{\widetilde{\Pi}}^{b=1} = 0\big] - \Pr[A_G^{b=1} = 0]\big| = 0.$$

From above arguments, we have:

$$\mathrm{Adv}_{\widetilde{\Pi}}^{\mathrm{ot-cca}} \leq q/2^{\tau} + \mathrm{Adv}_{\Pi}^{\mathrm{priv}}(1) + \mathrm{Adv}_F^{\mathrm{prf}}(q+1).$$

Note. In the Signal case, when the encryption scheme Π is CBC mode and the function F is HMAC, the AEAD scheme built by the above will be OT-CCA security. This is inferred from the fact that the CBC is priv security [4] and HMAC is a pseudorandom function. [5]. However, the use of a hash function in the HMAC is also a point of note. For example, in the case of the hash function SHA1, the construction HMAC is not prf. This is because there have been a series of attacks on the SHA1 hash function such as [6-10]. Therefor, in our opinion, to guarantee the security of the Signal protocol, the hash functions SHA-256, SHA-512 should be used as a recommendation by the developer or other stronger hash functions such as Keccak [11, 12].

IV. EVALUATING THE PRACTICAL SIGNIFICANCE OF OT-CCA SECURITY

For authenticated encryption in common use, the IV is usually required to be non-repeat. This can be guaranteed by choosing a random value as in [2].

In the practical implementation of the Signal protocol with the libSignal-protocol [13], each packet is protected by a 16-byte IV and a 64-byte key (including a 32-byte encryption key and a 32-byte authentication key) which are freshly generated in a pseudorandom way (see Fig 3). Such generating IV can somewhat affect the performance of the protocol. Furthermore, packet exchanged between parties may be delayed or lost in the practical communication environment. Therefore, the Signal protocol must store keys and IVs for delayed and lost messages. This also points out that there is the problem of storing the IV when this value is chosen randomly. In particular, the higher the number of delayed or lost packets, the larger the capacity for storing unnecessary IVs.

Our detailed evaluation results show that the IV does not affect the OT-CCA security of authenticated encryption schemes in general (including CBC-then-HMAC). Therefore, the IVs can be chosen to be constant and maintained to handle the encryption and decryption of all packets in the Signal protocol.

This helps minimize storage space for IVs in case packets are delayed or lost.

V. CONCLUSION

In this paper, we analyzed the authenticated encryption mode based on the Encrypt-then-Mac method used in the Signal protocol. The obtained results guarantee that from any encryption mode based on random IV that satisfies the priv security and any prf function, we can build a secure AEAD scheme used in the Signal protocol.

The above result allows us to use a fixed IV instead of refreshing it each time an encryption or decryption operation is performed. This reduces the amount of space required to store IVs in the Signal protocol, which is especially important on resource-constrained mobile devices.

Moreover, investigating and analyzing effective AEAD modes that allow using one key for both encryption and authentication purposes in the Signal protocol which aims to reduce the storage capacity from 64 bytes to 32 bytes for each key is an open problem.

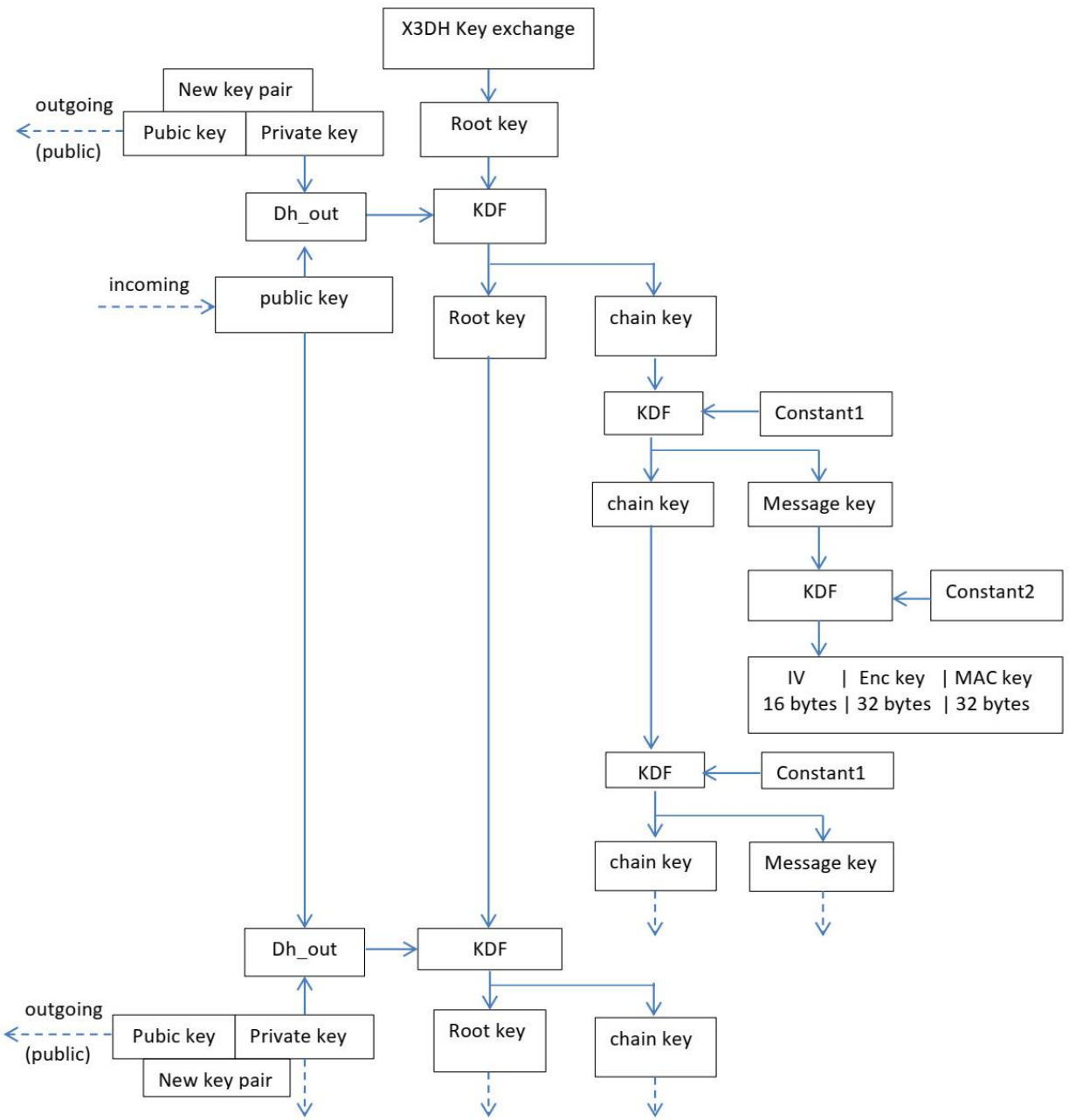

Figure 3. Illustration of key and IV generation in libSignal-protocol library

REFERENCES

[1] Alwen, J., S. Coretti, and Y. Dodis. The double ratchet: security notions, proofs, and modularization for the signal protocol. in Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2019. Springer.

[2] Rogaway, P. and T. Shrimpton. A provable-security treatment of the key-wrap problem. in Annual international conference on the theory and applications of cryptographic techniques. 2006. Springer.

[3] Rogaway, P. Authenticated-encryption with associated-data. in Proceedings of the 9th ACM Conference on Computer and Communications Security. 2002.

[4] Rogaway, P., Evaluation of some blockcipher modes of operation. Cryptography Research and Evaluation Committees (CRYPTREC) for the Government of Japan, 2011. 630.

[5] Bellare, M. New proofs for NMAC and HMAC: Security without collision-resistance. in Annual International Cryptology Conference. 2006. Springer.

[6] Wang, X., Y.L. Yin, and H. Yu, Collision search attacks on SHA1. 2005, Feb.

[7] Rijmen, V. and E. Oswald. Update on SHA-1. in Topics in Cryptology–CT-RSA 2005: The Cryptographers' Track at the RSA Conference 2005, San Francisco, CA, USA, February 14-18, 2005. Proceedings. 2005. Springer.

[8] Manuel, S., Classification and generation of disturbance vectors for collision attacks against SHA-1. Designs, Codes and Cryptography, 2011. 59(1-3): p. 247-263.

[9] Blog, G.S., Announcing the first SHA1 collision. 2017.

[10] Leurent, G. and T. Peyrin. {SHA-1} is a shambles: First {Chosen-Prefix} collision on {SHA-1} and application to the {PGP} web of trust. in 29th USENIX Security Symposium (USENIX Security 20). 2020.

[11] Long, N. V. (2020). Phân tích các thành phần mật mã trong hoán vị Keccak-p. Journal of Science and Technology on Information Security, 8(2), 34-45. https://doi.org/10.54654/isj.v8i2.31.

[12] Nguyen, A.T. and C.B. Nguyen, A new proof for the security of the keyed Sponge construction in the ideal compression function model. Journal of Science and Technology on Information security, 2019. 10(2): p. 18-24.

[13] https://github.com/signalapp/libsignal-protocol-c.

ABOUT THE AUTHOR

Nguyen Tuan Anh

Workplace: Institute of Cryptographic Science and Technology, Vietnam Government Information Security Commission.

Email: tuananhnghixuan@gmail.com

Education: The BS in Department of Mathematics, Hanoi University of Science 2016.

Recent research direction: The provable security for the symmetric schemes.

Tên tác giả: **Nguyễn Tuấn Anh**

Cơ quan công tác: Viện Khoa học - Công nghệ mật mã, Ban Cơ yếu Chính phủ

Email: tuananhnghixuan@gmail.com

Quá trình đào tạo: Cử nhân Toán tại Đại học Khoa học Tự nhiên, Đại học Quốc gia Hà Nội năm 2016.

Hướng nghiên cứu hiện nay: Độ an toàn chứng minh được của các lược đồ đối xứng.

Trieu Quang Phong

Workplace: Institute of Cryptographic Science and Technology, Vietnam Government Information Security Commission

Email: phongtrieu53@gmail.com

Education: The BS in Department of Mathematics, Hanoi University of Science (2014). The PhD in Mathematics at Academy of Military Science and Technology – Ministry Of National Defence.

Recent research direction: The provable security for the signature schemes and the key exchange protocol.

Tên tác giả: **Triệu Quang Phong**

Cơ quan làm việc: Viện Khoa học - Công nghệ mật mã, Ban Cơ yếu Chính phủ

Email: phongtrieu53@gmail.com

Quá trình đào tạo: Cử nhân Khoa Toán, Đại học Khoa học Tự nhiên Hà Nội năm 2014. Tiến sỹ Toán học, Viện Khoa học và Công nghệ quân sự, Bộ Quốc phòng năm 2023.

Hướng nghiên cứu hiện nay: Độ an toàn chứng minh được của các lược đồ chữ ký số và giao thức trao đổi khóa.