The ISC Int'l Journal of Information Security

July 2015, Volume 7, Number 2 (pp. 127–134)

http://www.isecure-journal.org

Cryptanalysis of Some First Round CAESAR Candidates

Javad Alizadeh [1,*], Mohammad Reza Aref [2], Nasour Bagheri [3,4], Alireza Rahimi [1], and Hassan Sadeghi [5]

[1] *Faculty and Research Center of Communication and Information Technology, Imam Hossein University, Tehran, Iran.*
[2] *Information Systems and Security Lab (ISSL), Sharif University of Technology, Tehran, Iran.*
[3] *The Electrical Engineering Department of Shahid Rajaee Teachers Training University, Tehran, Iran.*
[4] *School of Computer Science of Institute for Research in Fundamental Sciences (IPM), Tehran, Iran.*
[5] *Department of Mathematics, Faculty of Science, University of Qom, Qom, Iran.*

ARTICLE INFO.

Article history:
Received: 11 April 2015
First Revised: 22 September 2015
Last Revised: 2 November 2015
Accepted: 11 November 2015
Published Online: 16 November 2015

Keywords:
Authenticated Encryption, CAESAR, AES – CMCCv1, AVALANCHEv1, CLOCv1, SILCv1, Distinguishing Attack, Forgery Attack.

ABSTRACT

AES – CMCCv1, AVALANCHEv1, CLOCv1, and SILCv1 are four candidates of the first round of CAESAR. CLOCv1 is presented in FSE 2014 and SILCv1 is designed upon it with the aim of optimizing the hardware implementation cost. In this paper, structural weaknesses of these candidates are studied. We present distinguishing attacks against AES – CMCCv1 with the complexity of two queries and the success probability of almost 1, and distinguishing attacks on CLOCv1 and SILCv1 with the complexity of $\mathcal{O}(2^{n/2})$ queries and the success probability of 0.63, in which n is bit length of message blocks. In addition, a forgery attack is presented against AVALANCHEv1 which requires only one query and has the success probability of 1. The attacks reveal weaknesses in the structure of these first round candidates and inaccuracy of their security claims.

1 Introduction

Privacy and authentication are two main goals in information security. In many applications, these security parameters are required, simultaneously. For example, in the transport layer security (TLS) the MAC-then-Encrypt approach [1], which is a generic approach, is used. A cryptographic scheme that provides both privacy and authentication is called authenticated encryption (AE) scheme.

An AE scheme takes message M and optional associated data A and generates a ciphertext C and an authentication tag T as output. Most of AE schemes use nonces as a part of the input, denoted by N, and it has an important impact on their security. An AE scheme has two main components: an iterative structure and a primitive that is iterated in the structure. A flaw in the structure or primitive of an AE scheme can lead to a flaw in the scheme. Therefore, attacks on AE schemes can be divided in to two categories: the structural attacks, and the attacks that use the weaknesses of the AE schemes primitives. For a structural attack on the AE scheme, it is supposed that the primitive of the scheme is an ideal primitive.

Authenticated encryption has received considerable research interest in the recent years [2], especially with the NIST-funded CAESAR [3] which is an ongoing competition in this field. In March 2014, 57 candidates were submitted to the CAESAR as the first round candidates. An overview and a classification of the candidates is presented by Abed *et al.* in [4].

AES – CMCCv1 [5], AVALANCHEv1 [6, 7], CLOCv1 [8],

* Corresponding author.
Email addresses: jaalizadeh@ihu.ac.ir (J. Alizadeh), aref@sharif.edu (M. R. Aref), nbagheri@srttu.edu (N. Bagheri), arahimi@ihu.ac.ir (A. Rahimi), sadeghihassan64@gmail.com (H. Sadeghi)
ISSN: 2008-2045

and SILCv1 [9] are four CAESAR candidates, which are published for public comments in the first round of the competition. All these schemes are block cipher-based modes that can be instantiated with any block cipher. The prefix AES in AES − CMCC means that the submission use AES [10] as the internal block cipher. In this paper, we study the security of AES − CMCCv1, AVALANCHEv1, CLOCv1, and SILCv1 and we show that the claimed security for the confidentiality of AES − CMCCv1, CLOCv1 and SILCv1, and also for the integrity and confidentiality of AVALANCHEv1 are not satisfied.

1.1 Related Work

1.1.1 AES − CMCCv1.

A cryptanalysis of AES − CMCCv1 is published in [11], in which a forgery attack is presented on the stateless version of AES − CMCCv1 by only one query and it is shown that the existence of a forgery for the stateless version of AES − CMCCv1 leads directly to a two-query distinguisher in the nonce-reuse setting. The success probability of this attack is almost 1, for the short messages, and 2^{-7} for longer messages [11].

1.1.2 AVALANCHEv1.

The only published attack on AVALANCHEv1 is a key recovery attack with the complexity of $2^{l/2}$, in which l is the length of the secret key [12].

1.2 Our contribution

1.2.1 AES − CMCCv1.

In the stateless version of AES − CMCCv1, the security goal for the confidentiality of plaintext is claimed to be 128-bit [5]. In this paper, an efficient distinguishing attack on the scheme is presented, which requires only two queries to the algorithm and has the success probability of almost 1. This attack disproves the claimed security for the stateless version of AES − CMCCv1.

1.2.2 AVALANCHEv1.

In this paper, a very efficient forgery attack is presented on AVALANCHEv1, which requires only one query to the algorithm and has the success probability of 1. This attack disproves the security goal for the integrity of plaintext, which is claimed to be 127-bit [7]. In addition, the attack is exploited as a distinguishing attack against AVALANCHEv1, demonstrating that the claimed security goal for the confidentiality of plaintext (n-bit, where n is the block length of the underlying block cipher) [7] is not correct.

1.2.3 CLOCv1 and SILCv1.

The claimed security for the confidentiality in CLOCv1 and SILCv1 has time complexity of 2^n, where n is the block length of the underlying block cipher [8, 9]. In this paper, a distinguishing attack is presented on the schemes with the success probability of $(q^2-3q+2)/2^n$, where q is the total number of queried message blocks. This attack shows that the confidentiality of CLOCv1 and SILCv1 is upper bounded by $\mathcal{O}(2^{n/2})$.

1.2.4 Organization

In the rest of the paper, related concepts and preliminaries are defined in Section 2. A brief description of the stateless version of AES − CMCCv1 and a distinguishing attack on the scheme are presented in Section 3. AVALANCHEv1 and a forgery attack on the scheme are explained in Section 4. In this section, the forgery is exploited as a distinguisher for AVALANCHEv1, too. In Section 5, CLOCv1 and SILCv1 are introduced and a distinguishing attack is shown on these two schemes. Finally, the paper is concluded in Section 6.

2 Preliminaries

In this paper the plaintext is denoted by M and the ciphertext is denoted by C, a short string of bits, which is used to authenticate the decrypted message M, and provides integrity of message and authenticity of the sender is tag and denoted by T. In some applications, an auxiliary data which is denoted by Associated Data A is used, that should be authenticated, but left unencrypted. In addition, through the paper we use the following terms:

Confidentiality: Property to assure that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Integrity: Data integrity means maintaining and assuring the accuracy and completeness of data over its entire life-cycle.

Authenticity: Property that ensures the identity of a subject or resource is the claimed identity.

Authenticated Encryption Scheme: An authenticated encryption scheme takes message M and provides confidentiality, integrity, and authenticity of it, all together.

Authenticated Encryption Scheme with Associated Data: An authenticated encryption scheme which beside confidentiality, integrity, and authenticity of the message M, provides the integrity and authenticity of the associated data A.

Secure Authenticated Encryption Scheme:

An authenticated encryption scheme is secure if one cannot violate the property of confidentiality, integrity, and authenticity of the scheme except using brute force methods.

Distinguishing Attack: An attack which can be used to distinguish a scheme (or algorithm) from a random oracle.

Random Oracle: An oracle (black box) that responds to any new query with a (truly) random response chosen uniformly from its output's domain.

Forgery Attack: An attack which can be used to find a forgery authentication tag for a message.

3 AES – CMCCv1

3.1 Specification

AES – CMCCv1 [5] is an authenticated encryption scheme which has two main stateless and stateful versions. Since the given attack is on the stateless version of the scheme, this version is described here. The scheme gets message M, key K, nonce N, and optional associated data A and produces ciphertext C and an authentication tag T. The procedure is as follows:

First, the scheme uses a key generation algorithm and produces the keys $\overline{K}$, L_1, L_2, $\overline{L}_2$, and L_3 [5]. Then, it gets the $16 - |N|$ most significant bytes of constant

`0xb6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6`

and prepends them to N to obtain N'. It computes $W = E_{\overline{K}}(N')$ and $Q = M \parallel Z$, where $E_{\overline{K}}$ is the block cipher (e.g. AES) that is used in the CMCC mode and Z is a bit string with τ zero bits (τ is the length of the authentication tag). Using the parameters, AES – CMCCv1 acts as follows to produce the ciphertext and tag.

$$Q = P_1 \parallel P_2$$

$$X = \mathrm{CBC}(W, P_1, L_3) \oplus P_2,$$

where $\mathrm{CBC}(x, y, z)$ is CBC encryption with initialization vector x, plaintext y, and key z.

$$Y = X \parallel A$$

Suppose that B is the block length of $E_{\overline{K}}$. If $|Y| \leq B$ and $|P_1| \leq B$, then:

$$X_2 = E_{L_2}(Y \parallel \textit{zero padding}) \oplus P_1$$

else

$$P_1 = P_{1,1} \parallel \ldots \parallel P_{1,i} \parallel P_{1,i+1}$$

where $i \geq 0$, $P_{1,1} \ldots P_{1,i}$ are the full blocks and $P_{1,i+1}$ is a partial block,

$$V = \mathrm{MAC}(W, Y, L_2)$$

where $\mathrm{MAC}(x, y, z)$ is MAC algorithm with initialization vector x, plaintext y, and key z.

$$X_2 = V \oplus P_{1,1} \parallel E_{\overline{L}_2}(V+1) \oplus P_{1,2} \parallel \ldots \parallel E_{\overline{L}_2}(V+i) \oplus P_{1,i+1}$$

$$X_1 = \mathrm{CBC}(W, X_2, L_1)$$

The output of the algorithm is X_1, X_2, and N'. The stateless version of AES-CMCC v1 when $|Y| > B$ is depicted in Fig 1.

3.2 Distinguishing Attack

In this section, a distinguishing attack is presented on AES – CMCCv1. In AES – CMCCv1, there is a public message number N. Given constant `0xb6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6` and nonce N, the scheme gets $16 - |N|$ most significant bytes of the constant, and prepends them to N to obtain N'. Now, N' is used through the message encryption. If the adversary, for any arbitrary M and A, queries $\{A, N_1, M\}$, where $N_1 =$ `0xb6`, and he receives $\{A, C, N_1, T\}$, then he can generate the following pairs as the forgery:

- $\{A, C, N_2, T\}$ where $N_2 =$ `0xb6b6`.
- $\{A, C, N_3, T\}$ where $N_3 =$ `0xb6b6b6`.

  ⋮
- $\{A, C, N_{16}, T\}$ where $N_{16} =$ `0xb6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6`.

Although the transferred value to the receiver is $\{A, C, M, T\}$, the above observation can be used to distinguish the AES-CMCC v1 from a random oracle as follows:

(1) Choose any arbitrary M and A.
(2) Set $N_1 =$ `0xb6`, query the tuple (N_1, M, A) to AES-CMCC v1, and receive (C, N_1', A, T).
(3) Set $N_2 =$ `0xb6b6`, query the tuple (N_2, M, A) to the given AE, and receive (C', N_2', A', T').
(4) Output 1 if $(C', N_2', A', T') = (C, N_1', A, T)$; otherwise, output 0.

Note that an adversary which queries AES – CMCCv1 will output 1 with the probability of 1, while an adversary which queries an ideal AE will output 1 with a negligible probability.

4 AVALANCHEv1

4.1 Specification

AVALANCHEv1 gets message M of m blocks, optional associated data A of arbitrary length, and nonce N and produces ciphertext C of $m+1$ blocks and authentication tag T. The scheme is based on two algorithms: i.e. PCMAC to process the message, and RMAC to process the associated data. Key of AVALANCHEv1 is $K = (K_P, K_A)$ where K_P is the secret key to be used in PCMAC, and K_A is the secret key to be used

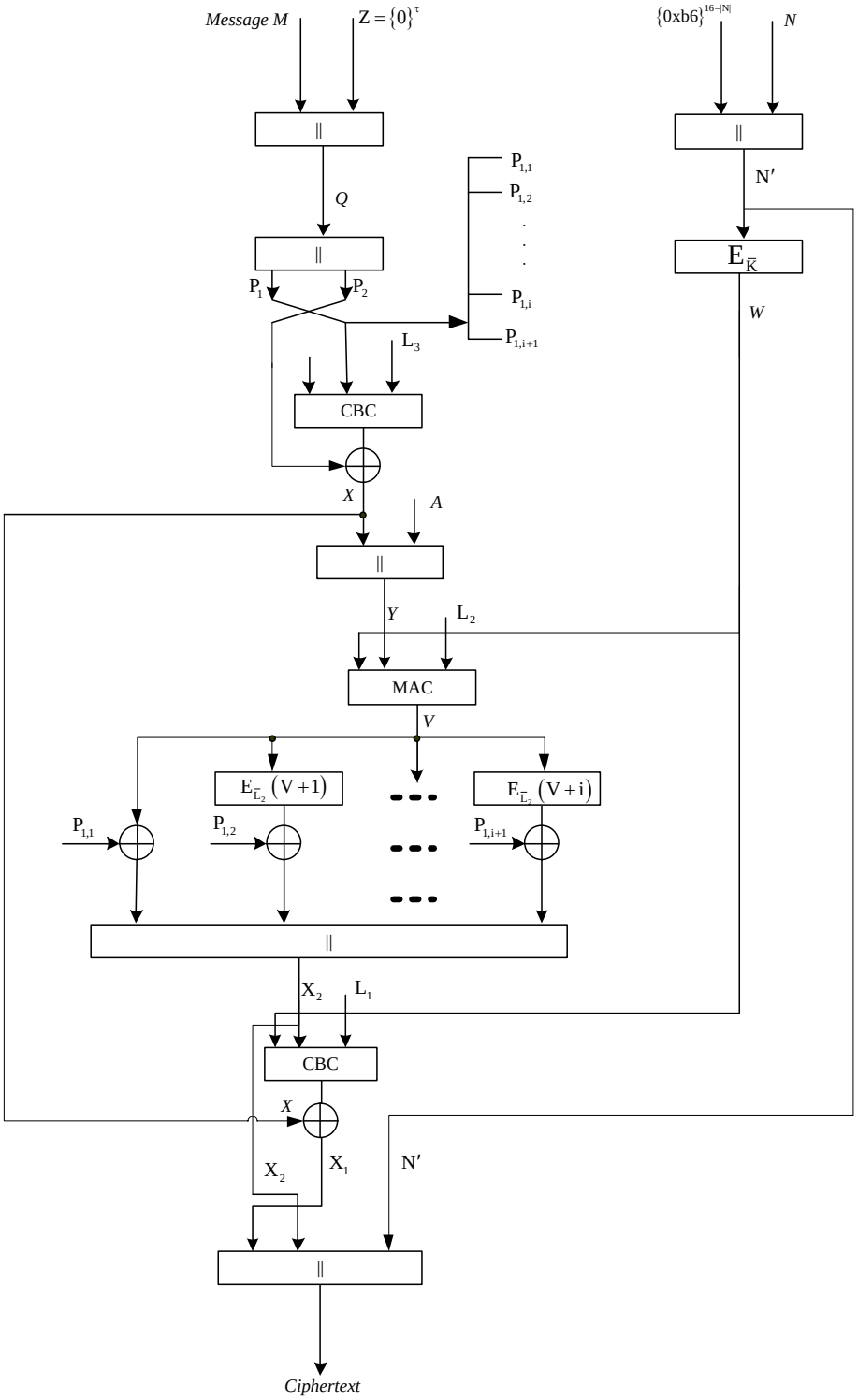

Figure 1. Stateless version of AES – CMCCv1 when $|Y| > B$

in RMAC. Assume that $M = M[1]\| \dots \|M[m]$ is the message, where $M[i]$ is the i^{th} block of the message, $C = C[0]\| \dots \|C[m]$ is the cipher, where $C[i]$ is the i^{th} block of C, n is the bit length of the blocks, and T is the final authentication tag. To produce (N, A, C, T) given (M, A), AVALANCHEv1 does as follows:

$$(N, C, \tau_P) = \text{PCMAC}(M)$$

$$\tau_A = \text{RMAC}(A),$$

where τ_P is an interface for PCMAC and τ_A is another interface for RMAC. τ_P is computed as:

$$\tau_p = r \oplus \sigma,$$

where r is a random number generated by PCMAC and σ is:

$$\sigma = \sum_{i=1}^{m} M[i] \ (mod\ 2^n).$$

The final tag T is computed as:

$$T = \tau_P \oplus \tau_A.$$

The illustration of the encryption mode of AVALANCHEv1 is depicted in Figure 2. In this figure, E is a block cipher such as AES and *ctr* represents a counter. It is clear that the length of the ciphertext is one block longer than that of the plaintext. The additional block corresponds to the encryption of random number r.

4.2 Forgery Attack

In this section, an efficient forgery attack on AVALANCHEv1 is presented, which requires only one query to the scheme. The attack can be used as a distinguisher of AVALANCHEv1. In the main reference of AVALANCHEv1 [6, 7], it is stated that *there is no secret message number* in this scheme. Given this property, a valid forgery attack on AVALANCHEv1 can be presented as follows:

(1) Query (M, A) and receive (N, A, C, T), where $M = M[1]\|M[2]\| \dots \|M[m-1]\|M[m]$, $C = C[0]\|C[1]\| \dots \|C[m-1]\|C[m]$ and $T = \text{RMAC}(A) \oplus r \oplus (\sum_{i=1}^{m} M[i] \ (mod\ 2^n))$.
(2) Output (N, A, C', T') as the forgery tuple, where $C' = C[0]\|C[1]\| \dots \|C[m-1]$ and $T' = T - M[m] \ (mod\ 2^n)$.

To verify the given tuple, receiver recovers $M' = M[1]\|M[2]\| \dots \|M[m-1]$ and the same r from the given C' and N. Now, the receiver verifies whether $T' \stackrel{?}{=} \text{RMAC}(A) \oplus r \oplus (\sum_{i=1}^{m-1} M[i] \ (mod\ 2^n))$ or not, where:

$$\text{RMAC}(A) \oplus r \oplus (\sum_{i=1}^{m-1} M[i] \ (mod\ 2^n)) =$$
$$\text{RMAC}(A) \oplus r \oplus (\sum_{i=1}^{m-1} M[i] + M[m] - M[m] \ (mod\ 2^n)) =$$
$$\text{RMAC}(A) \oplus r \oplus (\sum_{i=1}^{m} M[i] - M[m] \ (mod\ 2^n)) =$$
$$T - M[m] \ (mod\ 2^n) = T'$$

Hence, the forgery tuple is authenticated with probability 1.

Remark 1. Designer of AVALANCHEv1 states "*Append a unique End-of-Message character to the end of M*" and divide the message into blocks with length n. However, it is not clear from the text what that character is. Anyway, given that any character has a binary representation and assuming $M1 = M[1]\| \dots \|M[m-1]$ is a valid padded message, then the adversary can query for $M2 = M1\|M[m]$ as its query to do the forgery. Then the given attack works in that case as well.

4.3 Using the Forgery as a Distinguisher

The forgery attack on AVALANCHEv1 can be used to distinguish the scheme from a random oracle as follows:

(1) Query (M, A) and receive (N, A, C, T).
(2) Using (N, A, C, T), generate (N, A, C', T') as the forgery tuple corresponding to the forgery attack scenario.
(3) Output 1, if (N, A, C', T') is authenticated; otherwise output 0.

Note that an adversary which queries AVALANCHEv1 will output 1 with probability 1, while an adversary which queries an ideal AE will output 1 with negligible probability.

5 CLOCv1 and SILCv1

5.1 Specification

The AE scheme, CLOCv1 [8] submitted to the CAESAR, is presented in [13]. The main difference of the CAESAR submission from [13] is that the minimum data unit is defined to be a byte (8-bit) string and CLOC v1 is instated based on AES for 16-byte block length and TWINE [14] for 8-byte block length [8]. SILCv1 [9] is another candidate for the CAESAR, which is designed upon CLOCv1 with the aim of optimizing the hardware implementation cost of CLOCv1 [9]. Because of the similarity of the two schemes, they are specified together.

CLOCv1 and SILCv1 get message M, optional associated data A, and nonce N and generate ciphertext C

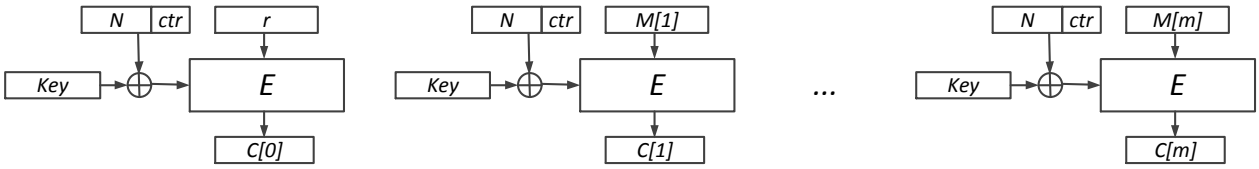

Figure 2. Counter-based parallelizable mode of encryption used in AVALANCHEv1 [6]

and the authentication tag T. Thus, the schemes using three subroutines based on the key K, are as follows:

- HASH_K for the authentication of the associated data A,
- ENC_K for the encryption of the massage M, and
- PRF_K for the authentication of the ciphertext C.

The presented attack on CLOCv1 and SILCv1 is based on the relation between the message and ciphertext in the subroutine ENC_K. Hence, ENC_K will be explained in the following subsection. For the details of other subroutines of the schemes, one can refer to [8, 9].

5.1.1 Encryption by CLOCv1 and SILCv1.

Suppose that V is a value which is computed in the authentication procedure of the associated data, A, using the subroutine HASH_K, E as a block cipher and K as the key of block cipher. The pseudo-code of the encryption procedure of CLOCv1 and SILCv1 (*i.e.* the subroutine ENC_K) is depicted in Table 1 [8, 9]. In this table, ε is an empty string and $M[i]$ and $C[i]$ are n-bit blocks of the message M and ciphertext C, respectively, $msb_l(X)$ is the most significant (the leftmost) l bits of X, $|X|$ denotes the bit length of the string X, and $fix1$ is a bit-fixing function to fix the most significant bit of an input string to " 1" . For a given string X, the bit-fixing function is defined as $fix1(X) = X \vee 10^{X-1}$, where $\vee$ is the bit-wise OR operation.

Algorithm 1 Encryption pseudo-code of CLOCv1 and SILCv1 [8, 9].

Input: K, V, M
Output: $\text{ENC}_\text{K}(V, M)$

if $|M| = 0$ **then**
  $C \leftarrow \varepsilon$
  return C
end if
$(M[1], \ldots, M[m]) \leftarrow M$
$S_E(1) \leftarrow E_k(V)$
for $i \leftarrow 1$ to $m-1$ **do**
  $C[i] \leftarrow S_E(i) \oplus M[i]$
  $S_E[i+1] \leftarrow E_K(fix1(C[i]))$
end for
$C[m] \leftarrow msb_{|M[m]|}(S_E[m]) \oplus M[m]$
$C \leftarrow (C[1], \ldots, C[m])$
return C

5.2 Distinguishing Attack

In this section, an observation on CLOCv1 and SILCv1 is presented and it is extended to a distinguishing attack on the schemes.

Theorem 1. *Suppose that* $M = M[1]\|M[2]\|...\|M[m]$ *is a message, where* $M[i]$ *is an* n*-bit block, and* $C = C[1]\|C[2]\|...\|C[m]$ *is the ciphertext of* M *encrypted by* CLOCv1 *or* SILCv1. *For* $1 \leqslant i, j \leqslant m-1$,

$$C[i] = C[j] \text{ or } C[i] \oplus C[j] = 10^{n-1}$$

iff

$$C[i+1] \oplus C[j+1] = M[i+1] \oplus M[j+1].$$

Proof. Suppose that, for $1 \leqslant i, j \leqslant m-1$, $C[i] = C[j]$ or $C[i] \oplus C[j] = 10^{n-1}$. Then,

$$\begin{aligned}
&fix1(C[i]) = fix1(C[j]) \\
&\Rightarrow E_K(fix1(C[i]) = E_K(fix1(C[j]) \\
&\Rightarrow E_K(fix1(C[i]) \oplus M[i+1] \oplus M[j+1] \\
&= E_K(fix1(C[j]) \oplus M[i+1] \oplus M[j+1] \\
&\Rightarrow C[i+1] \oplus M[j+1] = C[j+1] \oplus M[i+1] \\
&\Rightarrow C[i+1] \oplus C[j+1] = M[i+1] \oplus M[j+1].
\end{aligned}$$

Conversely, suppose that, for $1 \leqslant i, j \leqslant m-1$, $C[i+1] \oplus C[j+1] = M[i+1] \oplus M[j+1]$. Then,

$E_K(fix1(C[i]) \oplus M[i+1] \oplus [E_K(fix1(C[j]) \oplus M[j+1]$
$= M[i+1] \oplus M[j+1]$
$\Rightarrow E_K(fix1(C[i]) = E_K(fix1(C[j])$
$\Rightarrow C[i] = C[j]$ *or* $C[i] \oplus C[j] = 10^{n-1}$.

□

Theorem 1 is extended to a distinguishing attack on CLOCv1 and SILCv1 as follows:

(1) Choose message $M = M[1]\|M[2]\|\dots\|M[q]$, where $M[i]$ is an n-bit block.
(2) Query the ciphertext of M encrypted by CLOC v1 or SILCv1 and find $C = C[1]\|C[2]\|\dots\|C[q]$.
(3) If, for $1 \leqslant i, j \leqslant q-1$, the equation $C[i] = C[j]$ or $C[i] \oplus C[j] = 10^{n-1}$ yields the equation $C[i+1] \oplus C[j+1] = M[i+1] \oplus M[j+1]$, output 1, otherwise output 0.

Note that, according to Theorem 2 below, an adversary will output 1 with $\mathcal{O}(2^{n/2})$ queries to CLOCv1 or SILCv1, while the adversary needs $\mathcal{O}(2^n)$ queries to an ideal AE to output 1.

Theorem 2. *The distinguishing attack on* CLOCv1 *or* SILCv1*, which is explained above, has the success probability of* $(q^2 - 3q + 2)/2^n$*, where* q *is the total number of queried message blocks.*

Proof. Suppose that an adversary chooses message $M = M[1]\|M[2]\|\dots\|M[q]$, where $M[i]$ is an n-bit block, and queries the ciphertext of M encrypted by CLOCv1 or SILCv1 to find $C = C[1]\|C[2]\|\dots\|C[q]$. For $1 \leqslant i, j \leqslant q-1$, the probability of $C[i] = C[j]$ is $\mathbf{C}(q-1, 2) \times 2^{-n}$, where $\mathbf{C}$ is the notation of mathematical combination. Also, the probability of $C[i] \oplus C[j] = 10^{n-1}$ is $\mathbf{C}(q-1, 2) \times 2^{-n}$. Then, the success probability of the adversary to find $C[i]$ and $C[j]$, such that $C[i] = C[j]$ or $C[i] \oplus C[j] = 10^{n-1}$, is:

$$1 - (1 - 2^{-n})^{2 \times \mathbf{C}(q-1,2)} = 1 - (1 - 2^{-n})^{(q^2-3q+2)} \approx 1 - e^{-\frac{q^2-3q+2}{2^n}}$$

□

where for $q = 2^{n/2}$, the success probability would be almost $1 - e^{-1} = 0.63$.

6 Conclusion

In this paper, several distinguishing attacks were presented on AES − CMCCv1, CLOCv1, and SILCv1, and it is shown that the claimed security for the confidentiality of these CAESAR candidates were not accurate. In addition, a simple and efficient forgery attack against AVALANCHEv1 was shown and exploited as a distinguishing attack on the scheme. This attack demonstrates that the claimed security for the integrity and confidentiality of AVALANCHEv1 were not accurate.

The given attack on AES − CMCCv1 exploits a flaw on the padding rule of the nonce in the scheme. However, the given flaw is minor and can be fixed by padding any short nonce with appending 0 to its MSB and putting some restriction on the nonce-misusing.

The attack on AVALANCHEv1 exploited a flaw on the padding of this AE scheme, which do not include the length of the secret message in the padding. However, even including the length of the message in the last block will not fix the problem and with a clever selection of the queried message, it would be possible to apply a forgery attack on such variant of AVALANCHEv1. The suggestion would be to change the way that the tag is generated. In the current version, the tag-generation mainly exploited XoR or modular addition which is very efficient for implementation; but, it allows the adversary to do the given forgery attack on the scheme.

Acknowledgment

This work was partially supported by Iran-NSF under grant no. 92.32575.

References

[1] Mihir Bellare and Chanathip Namprempre. Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm. *J. Cryptology*, 21(4):469–491, 2008.
[2] Shengbao Wu, Hongjun Wu, Tao Huang, Mingsheng Wang, and Wenling Wu. Leaked-State-Forgery Attack Against The Authenticated Encryption Algorithm ALE. ASIACRYPT 2013, 2013.
[3] CAESAR. CAESAR: Competition for Authenticated Encryption: Security, Applicability,and Robustness, 2013. http://competitions.cr.yp.to/caesar.html.
[4] Farzaneh Abed, Christian Forler, and Stefan Lucks. Classification of the CAESAR Candidates. IACR Cryptology ePrint Archive, 2014.
[5] Jonathan Trostle. AES-CMCC v1. CEASAR Cryptographic Competitions, 2014. http://http://competitions.cr.yp.to/round1/aescobrav1.pdf.
[6] Basel Alomair. AVALANCHEv1. CEASAR Cryptographic Competitions, 2014. http://competitions.cr.yp.to/round1/avalanchev1.pdf.
[7] Basel Alomair. AVALANCHEv1. CAESAR mailing list, 2014.
[8] Tetsu Iwata, Kazuhiko Minematsu, Jian Guo, and Sumio Morioka. CLOC: Compact Low-

Overhead CFB. CEASAR Cryptographic Competitions, 2014. http://competitions.cr.yp.to/caesar-submissions.html.

[9] Tetsu Iwata, Kazuhiko Minematsu, Jian Guo, Sumio Morioka, and Eita Kobayashi. SILC: SImple Lightweight CFB. CEASAR Cryptographic Competitions, 2014. http://competitions.cr.yp.to/caesar-submissions.html.

[10] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Information Security and Cryptography. Springer, 2002.

[11] Guy Barwell. FORGERY ON STATELESS CMCC WITH A SINGLE QUERY. CEASAR Cryptographic Competitions mailing list, 2014.

[12] Andrey Bogdanov, Martin M. Lauridsen, and Elmar Tischhauser. Cryptanalysis of AVALANCHEv1. CEASAR Cryptographic Competitions mailing list, 2014. http://martinlauridsen.info/pub/avalanchev1.pdf.

[13] Tetsu Iwata, Kazuhiko Minematsu, Jian Guo, and Sumio Morioka. CLOC: Compact Low-Overhead CFB. FSE 2014, 2014.

[14] Tomoyasu Suzaki, Kazuhiko Minematsu, Sumio Morioka, and Eita Kobayashi. TWINE: A Lightweight Block Cipher for Multiple Platforms. In *Selected Areas in Cryptography*, pages 339–354, 2012.

Javad Alizadeh received M.S. degree in Telecommunication in the field of Cryptography from Imam Hoseein University, Tehran, Iran, in 2010. He serves as a member of Information Systems and Security Lab (ISSL) at the Electrical Engineering Department of Sharif University of Technology. He is currently working toward the Ph.D. degree in Cryptography at Imam Hoseein University. His research interest include symmetric cryptology, with an emphasis on block cipher and authenticated encryption.

Mohammad Reza Aref received B.S. degree in 1975 from University of Tehran, Iran, and M.S. and Ph.D. degrees in 1976 and 1980, respectively, from Stanford University, Stanford, CA, USA, all in Electrical Engineering. He returned to Iran in 1980 and was actively engaged in academic affairs. He was a Faculty member of Isfahan University of Technology from 1982 to 1995. He has been a Professor of electrical engineering at Sharif University of Technology, Tehran, since 1995, and has published more than 230 technical papers in communication and information theory and cryptography in international journals and conferences proceedings. His current research interests include areas of communication theory, information theory, and cryptography.

Nasour Bagheri is an assistant professor at Electrical Engineering Department, Shahid Rajaee Teacher Training University, Tehran, Iran. He is the author of over 50 articles in information security and cryptology.

Alireza Rahimi received the B.S. degree in 1988 from the Kharazmi University, Tehran, Iran, the M.S. degree in 1993 from the Shahid Bahonar University, Kerman, Iran, and the Ph.D. degree in 2012 from the Kharazmi University, Tehran, Iran, all in mathematics. He is an assistant professor at Faculty of Communication and Information Technology, Imam Hossein University, Tehran, Iran. His interesting is the mathematics of cryptography. He is the author of some articles in mathematics and cryptography.

Hassan Sadeghi holds a Ph.D. in the area of Differential Geometry from University of Qom. The title of his dissertation is Finsler Geometry. He has published several articles and report about the curvature of (α, β)-metrics. Since 2011, he has collaborated closely with Iranian Mathematical Society in Math education. In 2014, he began his graduate studies in Cryptography. Different aspects of authenticated encryption are Sadeghi's research interests.