Attacking and Fixing the CS Mode

Han Sui[1], Wenling Wu[1], Liting Zhang[1], and Peng Wang[2]

[1] Trusted Computing and Information Assurance Laboratory
Institute of Software, Chinese Academy of Sciences, Beijing 100190, P.R. China
{suihan,wwl,zhangliting}@tca.iscas.ac.cn
[2] Data Assurance and Communication Security
Institute of Information Engineering, Chinese Academy of Sciences,
Beijing 100093, P.R. China
wp@is.ac.cn

Abstract. The security of the Cipher-State (CS) mode was proposed to NIST as an authenticated encryption (AE) scheme in 2004. The usual SPRP blockcipher security for AE schemes may not guarantee its security. By constructing a special SPRP, one can easily make a key-recovery attack with a single block query. The distinguishing attacks and the forgery attacks can also be made with simpler SPRP constructions. The security flaw relies in the method for generating initial whitening values. To fix this shortcoming, we propose a modified version CS* which incorporates a new method for generating initial whitening values, while keeping the main structure of CS unchanged. As we show, CS* is secure when its underlying blockcipher is an SPRP and halves of which are unpredictable.

1 Introduction

Background. An authenticated encryption (AE) scheme is a shared-key encryption scheme whose goal is to provide both privacy and authenticity. There are usually two approaches to build AE schemes from blockciphers.

- A *two-pass* scheme combines essentially separate privacy and authenticity modes together, and has to process data twice; and
- a *one-pass* scheme tightly couples the parts of the mechanism responsible for both privacy and authenticity, and needs only one time to process data.

The latter schemes firstly emerged in 2001, with the work of Jutla [12] and developed by Katz et al. [13], Gilgor et al. [10] and Rogaway et al. [15]. Cipher-State mode is such a one-pass AE scheme.

The CS mode was firstly introduced by Anderson et al. in ACISP 2004 [3] and proposed to National Institute of Standards and Technology (NIST)[4] as submissions for modes development. Besides its advantage for processing data with only one time, it takes a special method for authentication with any round-based blockcipher. That is, it takes the internal states in the middle round of

S. Qing et al. (Eds.): ICICS 2013, LNCS 8233, pp. 318–330, 2013.

encryption for authentication information. This method provides a computationally low cost alternative to CBC mode. Furthermore, it can be fully parallelized, allowing fast execution.

It seems that little attention has been put to CS mode. It has been proposed and put on the NIST's web page for nearly a decade, however, seldom analysis can be found publicly. Švenda provided a brief analysis of CS mode in his comparison of AE modes [16]. Besides this, only an incomplete security analysis can be found in its designers' report [5] without any formal proof.

Our Contribution. Consider the wide requirements for secure AE schemes, especially with the recent motivation of CAESAR competition [1]. We find it necessary to give a formal analysis for such an interesting mode. We study CS mode from the provable-security point of view and discover that CS mode is totally insecure with a special SPRP as its underlying blockcipher. The problem is, $E_K(K \oplus \cdot)$ is used in generating initial whitening values and this may result in non-random internal values, and even the leakage of K. Such a way of XORing the key to a message block has been pointed out to be very dangerous by Furuya and Skurai [9]. By constructing a special permutation $F_K(\cdot)$, we show that one can build a key-recovery attack against CS mode with $F_K(\cdot)$ as its underlying blockcipher. Distinguishing attacks and forgery attacks can also be made using simpler SPRP constructions.

To fix CS mode, we build CS* which retains the main structure of CS and the update method of R_i unchanged, but replaces the method for generating initial whitening values R_0. To simplify the mode, we also take away the LFSR in T_i's updating and unnecessary pre-whiten and post-whiten process in generating a tag from T_m. However, we keep the convenient method that derives internal states from blockciphers to generate the tag. Therefore, CS* inherits the advantages of CS and becomes even simpler.

Due to its special method to compose the tag, we have to handle the detailed proof for CS* more carefully than usual. That is, we have to evaluate the properties of blockcipher internal states, and show how hard for adversaries to get a collision just before the last blockcipher encryption for authentication. To solve this, we introduce *unpredictability* into our proof. We argue that assuming the internal states in the middle of blockcipher encryption are unpredictable is quite suitable here. On the one hand, it is weaker than pseudorandomness, properly simulates the fact that the outputs of half-rounds blockcipher have less randomness than those of full-rounds. On the other hand, unpredictability of blockcipher internal states is sufficient to prevent collisions before the final encryption, allowing random tags for different messages. In the rest of this paper, we say "the internal states in the middle of blockcipher encryption" as "the internal states" for short.

Our fixing mode, CS*, is a secure AE scheme as we prove by assuming that the underlying block E is an SPRP and its internal states are unpredictable. For privacy, the success probability for an adversary to distinguish CS*[Perm(n)] from a random function is upper bounded by

$$\frac{(\sigma+2q+1)^2}{2^n}+1.5(\sigma+q+1)^2\mathbf{Adv}^{\mathrm{up}}_{E_1}(t,q,\sigma).$$

For authenticity, the success probability of making a forgery is upper bounded by

$$\frac{(\sigma+2q+c+5)^2}{2^n}+1.5(\sigma+2q+c+2)^2\mathbf{Adv}^{\mathrm{up}}_{E_1,E_2}(t,q,\sigma),$$

where E_1 and E_2 are two unpredictable permutations satisfying $E=E_2^{-1}\circ E_1$.

2 Preliminaries

2.1 Notation

A *string* is a finite sequence of symbols, each symbol being 0 or 1. The string of length 0 is called *empty string* and is denoted ϵ. Let $\{0,1\}^*$ denote the set of all strings. If $A,B\in\{0,1\}^*$ then AB, or $A\|B$, is their concatenation. 0^i and 1^i denote the strings of i-many 0s and 1s, respectively. Let $\{0,1\}^n$ denote the set of all strings of length n. If $A\in\{0,1\}^*$ then $|A|$ denotes the length of A in bits. If $A,B\in\{0,1\}^*$ are strings of same length then $A\oplus B$ is the bitwise xor of A and B. If A is a set, then $\#A$ denotes the size of set A, and $a\xleftarrow{\$}A$ denotes that a is chosen from set A uniformly at random.

If $M\in\{0,1\}^*$ then the padding rule used in this paper is $\mathrm{pad}(M)=M10^{n-1-(|M| \mod n)}$. Furthermore, we assume that each message M used in this paper has already padded and $|M|$ is a multiple of n. In pseudocodes, "partition M into $M_1\cdots M_m$" means "let m be the length of M in n-bit blocks and let $M_1\cdots M_m$ be string such that $M_1\cdots M_m=\mathrm{pad}(M)$ and $|M_i|=n$ for $1\le i\le n$".

If π is a function on $\{0,1\}^n$, let $\mathrm{Dom}(\pi)$ and $\mathrm{Ran}(\pi)$ be the domain and range of π, respectively. Especially, if we defines the values of $\pi(x)$ point-by-point in game, $\mathrm{Dom}(\pi)$ is the set of values $x\in\{0,1\}^n$ such that $\pi(x)\notin\mathsf{undefined}$. Similarly, $\mathrm{Ran}(\pi)$ is the set of $y\in\{0,1\}^n$ such that there exists an $x\in\{0,1\}^n$ for which $\pi(x)=y$. If π is a fixed function, we use $\mathrm{Dom}(\pi)$ and $\mathrm{Ran}(\pi)$ to describe the sets of queried inputs and outputs, respectively.

2.2 Description of Cipher-State Mode

As illustrated in Fig.1, Cipher-State mode derives internal states from each round-based blockcipher invocations during data encryption for authentication information. It needs one blockcipher key K and one nonce N. An initial whitening value R_0 is created from K and N.

An LFSR is used as a pseudorandom number generator (PRNG) to pre-whiten the plaintext and post-whiten the ciphertext with the same parameter. The polynomial selected for the authentication combiner and the PRNG is the lexicographically least primitive polynomial, $p(x)$ of degree n.

The blockcipher E_K is split into two roughly equal pieces, ${}_{1:r/2}E_K$ and ${}_{(r/2+1):r}E_K$: ${}_{1:r/2}E_K$ returns the internal state after completing $r/2$ rounds of the blockcipher; while ${}_{(r/2+1):r}E_K$ takes the internal state as input and returns the final state after all rounds. If the blockcipher has odd rounds, it will be split into ${}_{1:\lceil r/2 \rceil}E_K$ and ${}_{(\lceil r/2 \rceil+1):r}E_K$.

Let M be a padded data and be split into m n-bit blocks M_i:

$$M = M_1 \| M_2 \| \cdots \| M_m.$$

The initial whitening value R_0 is computed with $R_0 = E_K(N \oplus K) \oplus K$. The plaintext block M_i is pre-whitened using R_i which updates after each step using LFSR with $p(x)$. A pre-authenticator value T_i is computed with internal states of the underlying blockcipher and updates in the same way.

$$R_i = R_{i-1} \times x \pmod{p(x)}, \quad i = 1, 2, \cdots, m.$$
$$T_m = \Sigma_{i=1}^{m} E_K(M_i \oplus R_{i-1}) \times x^{m-i}.$$

To prevent possible information leakages from using the internal cipher state, a final authenticator T is computed using an extra blockcipher invocation:

$$T = E_K(T_m \oplus R_m) \oplus T_m.$$

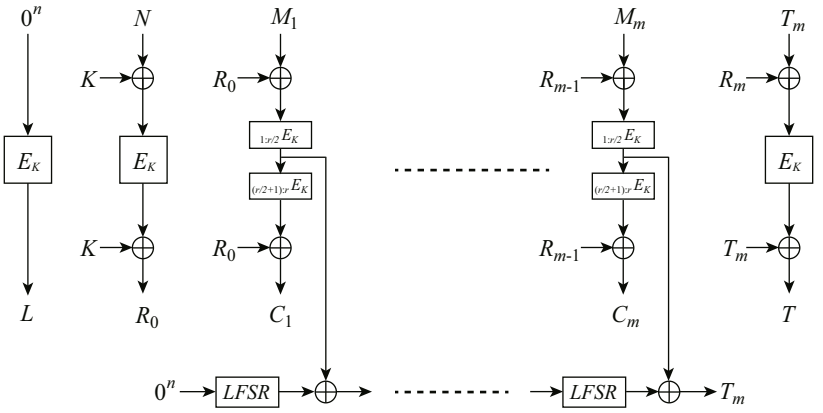

Fig. 1. Cipher-State Mode

2.3 Security Definitions

Adversaries. An *adversary* is a program with access to an oracle. Oracle queries are tuples of strings. An adversary is *nonce-respecting* if it never repeats the first component, N, to its oracle, regardless of oracle responses. In this paper, adversaries are always assumed to be nonce-respecting. We write an oracle as superscript to the adversary that uses it.

AE-schemes. We use the syntax of a nonce-using authenticated-encryption schemes and their security given by Bellare et al. [6] and extended by Rogaway et al. [15] [14]. An *authenticated-encryption scheme* (an AE-scheme) is a triple $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ and an associated number n (the blockcipher length). Here $\mathcal{K}$ is a finite set and $\mathcal{E}$ and $\mathcal{D}$ are deterministic algorithms. Encryption algorithm $\mathcal{E}$ takes $K \in \mathcal{K}$, $N \in \{0,1\}^n$, and $M \in \{0,1\}^*$, and returns a string $C \leftarrow \mathcal{E}_K(N, M)$. Decryption algorithm $\mathcal{D}$ takes $K \in \mathcal{K}$, $N \in \{0,1\}^n$, and $C \in \{0,1\}^*$, and returns $\mathcal{D}_K(N, M)$, which is either a string $M \in \{0,1\}^*$ or a distinguished symbol INVALID. If $C \leftarrow \mathcal{E}_K(N, M)$ then $\mathcal{D}_K(N, C) = M$.

Privacy. Consider an adversary $\mathcal{A}$ that has one of two types of oracles: a "real" encryption oracle or a "fake" encryption oracle. A real encryption oracle, $\mathcal{E}_K(\cdot,\cdot)$, takes as input N, M and returns $C \leftarrow \mathcal{E}_K(N, M)$. Assume that $|C| = l(|M|)$ depends only on $|M|$. A fake encryption oracle, $\$(\cdot,\cdot)$ takes as input N, M and returns a random string $C \xleftarrow{\$} \{0,1\}^{l(|M|)}$. Given adversary $\mathcal{A}$ and encryption scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, define

$$\mathbf{Adv}^{\mathrm{priv}}_{\Pi} = |\Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{\mathcal{E}_K(\cdot,\cdot)} \Rightarrow 1] - \Pr[\$(\cdot,\cdot) \xleftarrow{\$} \mathrm{Rand}(*,*) : \mathcal{A}^{\$(\cdot,\cdot)} \Rightarrow 1]|.$$

Authenticity. Fix an encryption scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ and run an adversary $\mathcal{A}$ with an oracle $\mathcal{E}_K(\cdot,\cdot)$ for some key K. Adversary $\mathcal{A}$ *forges* (in this run) if $\mathcal{A}$ is nonce respecting, $\mathcal{A}$ outputs (N, C), where $\mathcal{D}_K(N, C) \neq$ INVALID, and $\mathcal{A}$ made no earlier query (N, M) that resulted in a response C. Let $\mathbf{Adv}^{\mathrm{auth}}_{\Pi} = \Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{\mathcal{E}_K(\cdot,\cdot)}$ forges]. We stress that the nonce used in the forgery attempt may coincide with a nonce used in one of the adversary's queries.

Pseudorandom Functions. A *function family* from n-bit to n-bit is a map $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$, where $\mathcal{K}$ is a finite set of strings. It is a *blockcipher* if each $E_K(\cdot) = E(K,\cdot)$ is a permutation. Let $\mathrm{Rand}(n)$ denote the set of all functions from $\{0,1\}^n$ to $\{0,1\}^n$. These sets can be regarded as function families by imagining that each member is specified by a string. For $\pi \in \mathrm{Perm}(n)$, let $\pi^{-1}(Y)$ be the unique string X such that $\pi(X) = Y$. Let

$$\mathbf{Adv}^{\mathrm{prf}}_{E}(\mathcal{A}) = |\Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{E_K(\cdot)} \Rightarrow 1] - \Pr[\rho \xleftarrow{\$} \mathrm{Rand}(n) : \mathcal{A}^{\rho(\cdot)} \Rightarrow 1]|$$
$$\mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{A}) = |\Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{E_K(\cdot)} \Rightarrow 1] - \Pr[\pi \xleftarrow{\$} \mathrm{Perm}(n) : \mathcal{A}^{\pi(\cdot)} \Rightarrow 1]|$$
$$\mathbf{Adv}^{\mathrm{sprp}}_{E}(\mathcal{A}) = |\Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{E_K(\cdot),E_K^{-1}(\cdot)} \Rightarrow 1] - \Pr[\pi \xleftarrow{\$} \mathrm{Perm}(n) : \mathcal{A}^{\pi(\cdot),\pi^{-1}(\cdot)} \Rightarrow 1]|$$

be defined for the advantages of adversary $\mathcal{A}$ attacking blockcipher E. The security of E is defined as the maximum over all advantages of the adversaries with time complexity t, making at most q queries with at most σ blocks. If the advantage $\mathbf{Adv}^{\mathrm{prf}}_{E}(t, q, \sigma)$ is negligible, then E is said to be a *pseudorandom function* (PRF). The notions of *pseudorandom permutation* (PRP) and *strong pseudorandom permutation* (SPRP) are defined similarly.

Unpredictability. The notion of "*unpredictablilty*" is first proposed by Goldreich et al. in 1986 [11]. Let E be a blockcipher and $\mathcal{A}$ be an adversary with access to E for some key K. Consider this experiment.

Experiment $\mathbf{Exp}^{\mathrm{up}}_{E}(\mathcal{A})$
  $K \xleftarrow{\$} \mathcal{K}$
  when $\mathcal{A}$ makes a query M to $E_K(\cdot)$, do
    $C \leftarrow E_K(M)$
    return C to $\mathcal{A}$
  until $\mathcal{A}$ stops and outputs (M', C') such that
    – $E_K(M') = C'$, and
    – M' was never queried to $E_K(\cdot)$
  then return 1 else return 0

Let

$$\mathbf{Adv}^{\mathrm{up}}_{E}(\mathcal{A}) = \Pr[\mathbf{Exp}^{\mathrm{up}}_{E}(\mathcal{A}) = 1]$$
$$\mathbf{Adv}^{\mathrm{up}}_{E}(t, q, \sigma) = \max_{\mathcal{A}}\{\mathbf{Adv}^{\mathrm{up}}_{E}(\mathcal{A})\}$$

where t, q, σ stand for the total time, number of queries, and the total length of queries respectively. If $\mathbf{Adv}^{\mathrm{up}}_{E}(t, q, \sigma)$ is sufficiently small, we say E is unpredictable. Unpredictable is a wekaer notion than pseudorandomness, examples can be found in [2].

3 Attacks against CS

In this section, we will show CS mode could not be secure with some special SPRPs $F : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$. By constructing three different SPRPs, we give a distinguishing attack, a forgery attack and a key-recovery attack against CS$[F]$ respectively, with only one query of length no more than two blocks.

3.1 Distinguishing Attack against CS

Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a randomly chosen SPRP, and $A \in \{0,1\}^n$ be a randomly chosen constant. The special permutation $F : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ is built with E with a special property: $F_K(K \oplus A) = K$ for any key $K \in \{0,1\}^n$. This will help us building the distinguishing attack against CS mode.

$$F_K(M) = \begin{cases} K & \text{if } M = K \oplus A, \\ E_K(K \oplus A) & \text{if } M = E_K^{-1}(K), \\ E_K(M) & \text{else.} \end{cases}$$

A similar PRP (PRP-RK) has been constructed with $A = 0^{n-1}1$ by Peng Wang et al. to show that 2-Key XCBC using this PRP (PRP-RK) is totally insecure[17]. They proved that the special permutation F is a PRP as long as E is a PRP. And more specifically, F and E are indistinguishable. We can show that F is an SPRP as long as E is an SPRP.

Theorem 1. *If E is an SPRP, then F is an SPRP. More spexifically, for any adversary $\mathcal{A}$ with q queries trying to distinguish F and E, there exists an adversary $\mathcal{B}$ with no more than $(q+1)$ queries such that*

$$|\Pr[\mathcal{A}^{F,F^{-1}} \Rightarrow 1] - \Pr[\mathcal{A}^{E,E^{-1}} \Rightarrow 1]| \leq 2q\mathbf{Adv}_E^{\mathrm{sprp}}(\mathcal{B}) + \frac{2q}{2^n - q}.$$

Furthermore, $\mathcal{B}$ runs in approximately the same time as $\mathcal{A}$.

If CS takes F as its underlying blockcipher, it is distinguishable from CS with a random permutation. Let $\mathcal{O}$ be an oracle, with equal probability to be CS[F] or CS[π], where π is a random permutation. One query with nonce $N = A$ will lead to $R_0 = E_K(N \oplus K) \oplus K = 0^n$. Notice that if $R_0 = 0^n$, the algorithm will set $R_0 = K$. A distinguishing algorithm is built using this information:

Algorithm $\mathcal{A}^{\mathcal{O}(\cdot,\cdot)}$:
query (A, A) to $\mathcal{O}(\cdot,\cdot)$ and get (C, T)
if $C = 0^n$ return 1
else return 0

We can see that $\Pr[\mathcal{A}^{\mathrm{CS}[F_K]} \Rightarrow 1] = 1$ and $\Pr[\mathcal{A}^{\mathrm{CS}[\pi]} \Rightarrow 1] = 1/2^n$, so the advantage is $1 - 1/2^n$.

3.2 Forgery Attack against CS

Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a randomly chosen SPRP and $I : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be an identity function. The special permutation F is built by combining E and I: ${}_{1:r/2}F_K(\cdot) = E_K(\cdot)$, ${}_{(r/2+1):r}F_K(\cdot) = I(\cdot)$. Obviously, F is an SPRP as long as E is an SPRP. Taking F as the underlying blockcipher, there will be $C_j \oplus R_{j-1} = Z_{j-1} (j = 1, \ldots, c)$ in CS.

Noticing that the tag T is generated by underlying blockcipher $E_K(\cdot)$ with R_m and $T_m = \sum_{i=1}^{m} Z_i \cdot x^{m-i}$, and verified with R_c and $T_c = \sum_{j=1}^{c} Z_j \cdot x^{m-j}$, where $Z_i (i = 1, \ldots, m)$ in former situation is the internal state of $E_K(M_i \oplus R_{j-1})$ and $Z_j (j = 1, \ldots, c)$ in latter situation is the internal state of $E_K^{-1}(C_j \oplus R_{j-1})$. Suppose (N, C, T) is valid, if we can find $C_1^*, \ldots, C_c^*$ satisfying

$$\sum_{j=1}^{c} {}_{1:r/2}E^{-1}(C_j^* \oplus R_{j-1}) \cdot x^{m-j} = \sum_{j=1}^{c} {}_{1:r/2}E^{-1}(C_j \oplus R_{j-1}) \cdot x^{m-j},$$

then (N, C^*, T) will be valid. A forgery attack using only one query of two blocks to CS.Enc can be built as following.

Algorithm $\mathcal{A}^{\mathrm{CS}[F](\cdot,\cdot)}$:
randomly choose $N, M_1, M_2 \in \{0,1\}^n$
query $(N, M_1||M_2)$ to $\mathcal{O}(\cdot,\cdot)$ and get $(C_1||C_2, T)$
randomly choose $C_1^* \in \{0,1\}^n$ satisfying $C_1^* \neq C_1$
let $C_2^* = C_2 \oplus (C_1 \oplus C_1^*) \cdot x$
forgery$(N, C_1^*||C_2^*, T)$

We can see that

$$\begin{aligned} T_2^* &= Z_1^* \cdot x \oplus Z_2^* \\ &= (C_1^* \oplus R_0) \cdot x \oplus (C_2^* \oplus R_1) \\ &= (C_1 \oplus R_0) \cdot x \oplus (C_2 \oplus R_1) \\ &= Z_1 \cdot x \oplus Z_2 \\ &= T_2 \end{aligned}$$

Therefore, $T^* = F_K(T_2^* \oplus R_2) \oplus T_2^* = F_K(T_2 \oplus R_2) \oplus T_2 = T$. The probability of the forgery success is 1.

This attack shows the CS security requires some randomness on the blockcipher internal states. We will show unpredictability is a proper choice in Section 4.

3.3 Key-Recovery Attack against CS

Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a randomly chosen SPRP. Similar to the permutation we used in distinguishing attack, by modifying several ordered pairs in $E_K(\cdot)$ we can get:

$$F_K(M) = \begin{cases} E_K(A_1) & \text{if } M = A_2 \oplus K, \\ A_3 \oplus E_K(A_1) & \text{if } M = A_3 \oplus K \oplus E_K(A_1), \\ E_K(A_2 \oplus K) & \text{if } M = A_1, \\ E_K(A_3 \oplus K \oplus E_K(A_1)) & \text{if } M = E_K^{-1}(A_3 \oplus E_K(A_1)), \\ E_K(M) & \text{else.} \end{cases}$$

where A_1, A_2, A_3 are randomly chosen from $\{0,1\}^n$. What we do is exchanging the values of $E_K(A_1)$ and $E_K(A_2 \oplus K)$, and the values of $E_K(A_3 \oplus K \oplus E_K(A_1))$ and $E_K(E_K^{-1}(A_3 \oplus E_K(A_1)))$. Noting that, some chooses of (A_1, A_2, A_3) may lead to collisions happen in $\mathcal{X} = \{A_2 \oplus K, A_3 \oplus K \oplus E_K(A_1), A_1, E_K^{-1}(A_3 \oplus E_K(A_1))\}$, which may make this construction fail. The probability of no collision happens in $\mathcal{X}$ is more than at least $1 - 6/2^n$. We can proof that F is an SPRP as long as E is an SPRP.

If CS takes this permutation F as underlying blockcipher, then we can build a key-recovery attack as following.

Algorithm $\mathcal{A}^{\mathrm{CS}[F](\cdot,\cdot)}$:
query (A_2, A_3) to $\mathrm{CS}[F](\cdot,\cdot)$ and get (C, T)
$K \leftarrow C \oplus A_3$
return K

Noting that $R_0 = K \oplus E_K(A_1)$, and

$$\begin{aligned} C \oplus A_3 &= (F_K(M \oplus R_0) \oplus R_0) \oplus A_3 \\ &= (F_K(A_3 \oplus (K \oplus E_K(A_1))) \oplus (K \oplus E_K(A_1))) \oplus A_3 \\ &= ((A_3 \oplus E_K(A_1)) \oplus (K \oplus E_K(A_1))) \oplus A_3 \\ &= (A_3 \oplus K) \oplus A_3 \\ &= K \end{aligned}$$

Noting that, some choices of (A_1, A_2, A_3) may lead this attack to fail. For example, if $E_K(A_1) = 0^n$ and R_0 will be set to K not $E_K(A_1)$. The probability of choosing such (A_1, A_2, A_3) is less than $1/2^{n-1}$. Therefore, the success probability of this attack is at least $(1 - 6/2^n)(1 - 1/2^{n-1})$.

4 Fixing CS and Its Security Proof

The main problem of CS comes from the method for generating the initial whitening value R_0 with nonce and key. We naturally consider modifying only the generation method of R_0 and analyze the fixing mode CS*.

4.1 CS* Mode

CS* mode retains the updating way of R_i unchanged, but changes the method for generating the initial whitening value R_0.

$$R_0 = E_K(N \oplus L) \oplus L \quad \text{with } L = E_K(0^n).$$

To make the mode simpler, the LFSR in T_i's updating and the unnecessary pre-whiten and post-whiten process in generating a tag from T_m are taken away.

The algorithm given below illustrates the CS* construction for a m-block message, $M = M_1, \ldots, M_m$, initialization vector, IV, and encryption key, K. Let E_K be a r-round blockcipher.

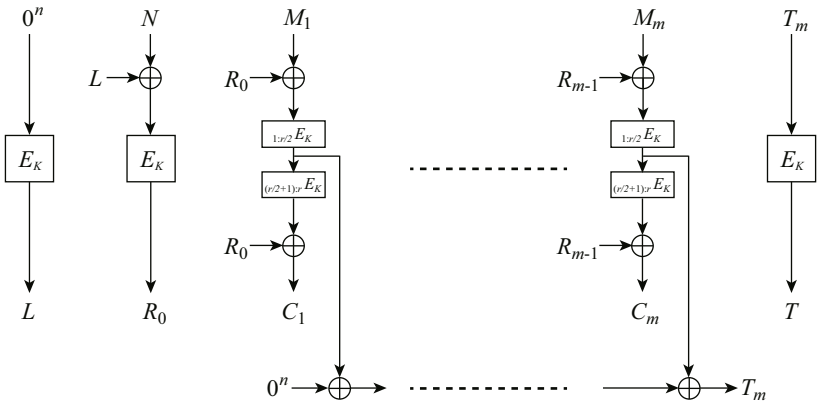

Fig. 2. CS* Mode

Algorithm $\mathrm{CS.Enc}_K(N, M)$	**Algorithm** $\mathrm{CS.Dec}_K(N, C, T)$
Partition M **into** $M_1 \cdots M_m$	**Partition** C **into** $C_1 \cdots C_c$
$L \leftarrow E_K(0^n)$	$L \leftarrow E_K(0^n)$
$T_0 = 0^n$	$T_0 = 0^n$
$R_0 \leftarrow E_K(N \oplus L)$	$R_0 \leftarrow E_K(N \oplus L)$
for $i \leftarrow 1$ **to** m **do** $R_i \leftarrow R_{i-1} \cdot x$	**for** $i \leftarrow 1$ **to** c **do** $R_i \leftarrow R_{i-1} \cdot x$
for $i \leftarrow 1$ **to** m **do**	**for** $i \leftarrow 1$ **to** c **do**
$Z_i \leftarrow_{1:r/2} E_K(M_i \oplus R_{i-1})$	$Z_i \leftarrow_{1:r/2} E_K^{-1} E_K(C_i \oplus R_i)$
$C_i \leftarrow_{(r/2+1):r} E_K(Z_i) \oplus R_{i-1}$	$M_i \leftarrow_{(r/2+1):r} E_K^{-1}(Z_i) \oplus R_{i-1}$
$T_i \leftarrow T_{i-1} \oplus Z_i$	$T_i \leftarrow T_{i-1} \oplus Z_i$
$T \leftarrow E_K(T_m)$	$T' \leftarrow E_K(T_m)$
return (C, T)	**if** $T = T'$ **then return** M
	else return $\perp$

Fig. 3. The specification of CS*

4.2 The Security of CS* Mode

We now proceed to show the security of CS*. For this we assume the underlying blockcipher of CS*, P, is an SPRP and it can be split into two unpredictable permutations P_1 and P_2 satisfying $P = P_2^{-1} \circ P_1$. Theorems as following show the information-theoretic bounds and the computational bounds on the privacy and authenticity of CS*.

Theorem 2. *Let $\mathcal{A}$ be a nonce-respecting adversary that asks q queries and then makes its forgery attempt. Suppose the q queries have aggregate length of σ blocks, and the adversary's forgery attempt has at most c blocks. Then*

$$\mathbf{Adv}^{\mathrm{priv}}_{\mathrm{CS}^*[\mathrm{Perm}(n)]}(\mathcal{A}) \leq \frac{(\sigma + 2q + 1)^2}{2^n} + 1.5(\sigma + q + 1)^2 \mathbf{Adv}^{\mathrm{up}}_{P_1}(t, q, \sigma),$$
$$\mathbf{Adv}^{\mathrm{auth}}_{\mathrm{CS}^*[\mathrm{Perm}(n)]}(\mathcal{A}) \leq \frac{(\sigma + 2q + c + 3)^2}{2^n} + 1.5(\sigma + 2q + c + 2)^2 \mathbf{Adv}^{\mathrm{up}}_{P_1, P_2}(t, q, \sigma).$$

This theorem can be easily translated to the computational complexity setting by adding a advantage of distinguishing blockcipher E and its inverse E^{-1} with a random permutation π and π^{-1}, where E can be split into two unpredictable permutation E_1 and E_2^{-1}.

Theorem 3. *Suppose $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ is an SPRP-secure blockcipher. Let $E_1 =_{1:r/2} E$ and $E_2 =_{1:r/2} E^{-1}$. Let $\mathcal{A}$ be an nonce-respecting adversary that asks q queries and then makes its forgery attempt. Suppose the q queries have aggregate length of σ blocks, and the adversary's forgery attempt has at most c blocks. Then*

$$\mathbf{Adv}^{\mathrm{priv}}_{\mathrm{CS}^*[E]}(\mathcal{A}) \leq \frac{(\sigma+2q+1)^2}{2^n} + 1.5(\sigma+q+1)^2\mathbf{Adv}^{\mathrm{up}}_{E_1}(t,q,\sigma) + \mathbf{Adv}^{\mathrm{sprp}}_{E}(t',q',\sigma'),$$

$$\mathbf{Adv}^{\mathrm{auth}}_{\mathrm{CS}^*[E]}(\mathcal{A}) \leq \frac{(\sigma+2q+c+3)^2}{2^n} + 1.5(\sigma+2q+c+2)^2\mathbf{Adv}^{\mathrm{up}}_{E_1,E_2}(t,q,\sigma) + \mathbf{Adv}^{\mathrm{sprp}}_{E,E^{-1}}(t',q',\sigma'),$$

where $t' = t$, $q' = q+1$, *and* $\sigma' = \sigma + c + 2q + 3$.

For privacy, the initial whitening value R_0 is generated by $E_K(\cdot)$ with a new nonce N in each query and is kept secret from $\mathcal{A}$. Pre-whiten values are then generated from R_0 and they make the inputs to blockciphers pair-wise distinct, resulting in random ciphertexts because E is an SPRP. Furthermore, noticing E_1 is unpredictable, it is easy to find T_m is collision-resistant, and the final tag T is random after the final encryption. Therefore, both the ciphertexts and the tag are random bits. For authenticity, if the forgery is composed with a new nonce N, then it has a close-to-1 probability that the inputs to E_2 are pairwise distinct and also distinct from former blockcipher outputs. By the unpredictability of E_2, T_m would be new and the final tag is random. On the other side, if the forgery is composed with a used nonce N, then there still exists large probability that at least one of the inputs to E_2 is new, resulting in a new T_m by the unpredictability of E_2 and a random tag by the SPRP of E. In either case, the probability to make a valid forgery is negligible.

In CS* mode, the internal states of the underlying blockcipher are hidden from adversaries and their sum is again encrypted before being output, these features result in no information leakage, except the collision before the last blockcipher encryptions for authentication.

Noting that, in our proofs, we assume that the underlying blockcipher E is an SPRP and constructed by $E = E_2^{-1} \circ E_1$, where E_1, E_2 are two independently unpredictable permutations. However, this doesn't mean in theory that the concatenation of two unpredictable permutations can make up an SPRP.

Despite the above, our assumption on blockciphers for the security of CS* is no stronger than the usual and solo SPRP assumption. This can also be reflected by the security of practical blockciphers. That is, a full-round blockcipher behaves like an SPRP and its internal states are unpredictable for adversaries.

5 Conclusion

The CS mode was submitted to NIST in 2004, and is still in NIST's modes development list. However, only a few of papers involve this mode in and no formal proof has been proposed before. In this paper, we pointed out that there exist some security problems in its method for generating initial whiten values. By constructing a special SPRP F, a key-recovery attack against CS[F] with a single block query can be made.

A slight modification for generating initial whiten values leads to a new authenticated encryption mode, CS*, which uses the same way of generating initial whiten values as the OCB mode and retains most parts of CS. Assuming internal states of the underlying blockcipher behave as "unpredictable" while the blockcipher is super pseudorandom, it can be proved that CS* is a secure AE scheme.

Acknowledgments. The authors would like to thank the anonymous referees for their valuable comments. This work was supported by the National Grand Fundamental Research 973 Program of China (Grant No. 2013CB338002), and the National Natural Science Foundation of China (Grant No. 61272476,61232009,61272477 and 61202422).

References

1. CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness (2013), http://competitions.cr.yp.to/index.html
2. An, J.H., Bellare, M.: Constructing VIL-MACs from FIL-MACs: message authentication under weakened assumptions. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 252–269. Springer, Heidelberg (1999)
3. Anderson, E., Beaver, C., Draelos, T., Schroeppel, R., Torgerson, M.: ManTiCore: encryption with joint Cipher-State authentication. In: Wang, H., Pieprzyk, J., Varadharajan, V. (eds.) ACISP 2004. LNCS, vol. 3108, pp. 440–453. Springer, Heidelberg (2004)
4. Anderson, E., Beaver, C., Draelos, T., Schroeppel, R., Torgerson, M.: Submission to NIST: Cipher-State (CS) mode of operation for AES (2004), http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/cs/cs-spec.pdf
5. Anderson, E., Beaver, C., Draelos, T., Schroeppel, R., Torgerson, M.: Manticore and CS mode: parallelizable encryption with joint Cipher-State authentication (2004), http://dx.doi.org/10.2172/919631
6. Bellare, M., Desai, A., Jokipii, E., Rogaway, P.: A concrete security treatment of symmetric encryption: analysis of the DES modes of operation. In: Goldberg, A.V., Rao, S. (eds.) FOCS 1997, pp. 394–403. ACM Press, IEEE (1997)
7. Bellare, M., Namprempre, C.: Authenticated encryption: relations among notions and analysis of the generic composition paradigm. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 531–545. Springer, Heidelberg (2000)
8. Bellare, M., Rogaway, P.: Encode-then-encipher encryption: How to exploit nonces or redundancy in plaintexts for efficient cryptography. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 317–330. Springer, Heidelberg (2000)
9. Furuya, S., Sakurai, K.: Risks with raw-key maksing - the security evaluations of 2-key XCBC. In: Deng, R.H., Qing, S., Bao, F., Zhou, J. (eds.) ICICS 2002. LNCS, vol. 2513, pp. 327–341. Springer, Heidelberg (2002)
10. Gligor, V., Donescu, P.: Fast encryption and authentication: XCBC encryption and XECB authentication modes. In: Matsui, M. (ed.) FSE 2001. LNCS, vol. 2355, pp. 92–108. Springer, Heidelberg (2002)
11. Goldreich, O., Goldwasser, S., Micali, S.: How to construct random function. Journal of the ACM 33(4), 792–807 (1986)

12. Jutla, C.: Encryption modes with almost free message integrity. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 529–544. Springer, Heidelberg (2001)
13. Katz, J., Yung, M.: Unforgeable encryption and chosen ciphertext secure modes of operation. In: Schneier, B. (ed.) FSE 2000. LNCS, vol. 1978, pp. 284–299. Springer, Heidelberg (2001)
14. Rogaway, P.: Authenticated-encryption with associated-data. In: Atluri, V. (ed.) CCS 2002, pp. 98–107. ACM, ACM press (2002)
15. Rogaway, P., Bellare, M., Black, J.: OCB: A block-cipher mode of operation for efficient authenticated encryption. ACM Trans. on Information and System Security 6(3), 365–403 (2003); Earlier version, with Krovetz, T. in CCS 2001
16. Švenda, P.: Basic comparison of modes for authenticated-encryption (IAPM, XCBC, OCB, CCM, EAX, CWC, GCM, PCFB, CS) (2004), `http://www.fi.muni.cz/~xsvenda/docs/AE_comparison_ipics04.pdf`
17. Wang, P., Feng, D., Wu, W., Zhang, L.: On the unprovable security of 2-key XCBC. In: Mu, Y., Susilo, W., Seberry, J. (eds.) ACISP 2008. LNCS, vol. 5107, pp. 230–238. Springer, Heidelberg (2008)