Provable security against Impossible Differential Cryptanalysis
Application to CS-Cipher

Thomas Roche[1 2 7], Roland Gillard[5 2 3], and Jean-Louis Roch[1 3 4 6]

[1] Laboratoire d'Informatique de Grenoble, 51 av. Jean Kuntzmann, 38330 Montbonnot-Saint-Martin, France, {Thomas.Roche, Jean-Louis.Roch}@imag.fr
[2] Université Joseph Fourier, Roland.Gillard@ujf-grenoble.fr
[3] Grenoble Université
[4] INRIA Rhône-Alpes
[5] Institut Fourier, 100 rue des Maths, BP74 38402 St Martin d'Hères, France
[6] Institut National Polytechnique de Grenoble (INPG)
[7] CS, Communication&Systems, 22 avenue Galilée, 92350 Le Plessis Robinson, France

Abstract. In this document we present a new way to bound the probability of occurrence of an n-round differential in the context of differential cryptanalysis. Hence this new model allows us to claim proof of resistance against impossible differential cryptanalysis, as defined by Biham and al. in 1999. This work will be described through the example of CS-Cipher, to which, assuming some non-trivial hypothesis, provable security against impossible differential cryptanalysis is obtained.

Key words: Impossible Differential cryptanalysis, Provable security, Symmetric ciphers

1 Introduction

The resistance against differential cryptanalysis has been studied since the attack invention by Biham and Shamir (1990 [2]). Formal proofs based on the Markov cipher approximation (Lai and Massey [3]) and related to the minimal number of active S-Boxes in a differential characteristic are now well known. On the other hand, it is hardly possible to evaluate a symmetric cipher w.r.t. impossible differential cryptanalysis. Inspired by the work of Sugita and al. in [7], we are going to introduce a new way to approach the probability of occurrence of an n-round differential. Although this approach does not give better upper bound than has already been done, it allows us to display a lower bound and then claim resistance against impossible differential for an example cipher. The study focuses on CS-Cipher (symmetric cipher introduced by Stern and Vaudenay in [6]); its resistance against differential and truncated differential cryptanalysis has been studied in [8]. As in [8] we will use the properties of CS-Cipher multipermutations in order to decrease the complexity of computing our bounds.

Let us note that our proof holds on the hypothesis that the symmetric cipher is a Markov cipher and a Support Markov cipher (notion about to be introduced in this document) with uniformly distributed round keys.

Notations and material

An iterated or block cipher performs a sequence of rounds to encrypt a plaintext of fixed size (block size). In all the sequel, the following notations and material are used with respect to an iterated or block cipher.

n, m : denotes respectively the block size in bits and in bytes (i.e. $n = 8 \times m$).

$\oplus$: denotes a group operation over the Galois field $GF(2)^8$ (in all the sequel this operation will be the bitwise addition modulo 2).

$\boldsymbol{\Delta_{\mathbf{x}}(\mathbf{x}')}$: denotes the *difference* between x and x' by the $\oplus$ operation. $x \oplus x' = \triangle_x(x')$. Noted $\triangle x$ when not ambiguous.

***i*-round Output ($\mathbf{O_i(x)}$)** : let x be a plaintext input of the cipher; $O_i(x)$ denotes the output after the i^{th} round.

***i*-round Differentials** : for an iterated cipher, a pair (α, β) is a possible i-round differential if and only if there is a pair of plaintext input (x, x') such that $x \oplus x' = \alpha$ and $O_i(x) \oplus O_i(x') = \beta$. Later on, a 1-round differential is simply called a *differential*.

***i*-round Characteristics** : for an iterated cipher, a set $\Omega = \{\omega_0, \omega_1, \ldots, \omega_i\}$ is a possible i-round characteristic if and only if there is a pair of plaintext input (x, x') such that $x \oplus x' = \omega_0$ and $\forall j \in \{1 \ldots i\}, O_j(x) \oplus O_j(x') = \omega_j$. Hence, an i-round characteristic is a sequence of i j-round differentials with $j \in \{1, \ldots, i\}$.

Probability of a differential ($\boldsymbol{DP^f}$) : given a boolean function $f : GF(2)^p \longrightarrow GF(2)^q$, for any $\alpha \in GF(2)^p$ and any $\beta \in GF(2)^q$ we note :

$$DP^f(\alpha, \beta) = \Pr_x\{x | f(x) \oplus f(x \oplus \alpha) = \beta\}$$

S-Boxes : substitution boxes are fairly common in block ciphers, they are functions that give the necessary non-linearity of encryption functions. The non-linearity with respect to differential cryptanalysis is evaluated by computing the DP^{S-Box}.

Active S-Boxes for a given characteristic (or differential) are the encryption function's S-Boxes that present a non null difference for input.

Multipermutations : the notion of multipermutation was introduced by Schnorr and Vaudenay in [5]. For our needs in this paper we will just define the general idea of a $(2, 2)$-multipermutation over $GF(2)^8$, of which complete description can be found in Vaudenay's PhD thesis ([4]). A $(2, 2)$-multipermutation over $GF(2)^8$ can be seen as a permutation over $GF(2)^{16}$ such that fixing the first half of the input (respectively the second part) makes both half of the output permutations of the second half of the input (respectively the first part).

Markov Chain : a sequence of discrete random variables $(X_r, \ldots, X_0)$ forms a Markov chain if and only if : $\forall i \in \{0 \ldots r-1\}$,

$$\Pr(X_{i+1} = x_{i+1} | X_i = x_i, \ldots, X_0 = x_0) = \Pr(X_{i+1} = x_{i+1} | X_i = x_i)$$

Markov Ciphers : denotes a subclass of iterated ciphers, first introduced by Lai, Massey and Murphy in [3] to give a formal environment to iterated ciphers and then lead to provable security against differential cryptanalysis. An r-round iterated cipher is a Markov cipher when the sequence $(\triangle x = \triangle y_0, \triangle y_1, \ldots, \triangle y_r)$ of round output *differences* forms a Markov chain. That is to say

$$\Pr(\triangle y_r = \omega_r | \triangle y_0 = \omega_0, \triangle y_1 = \omega_1, \ldots, \triangle y_{r-1} = \omega_{r-1}) = \Pr(\triangle y_r = \omega_r | \triangle y_{r-1} = \omega_{r-1})$$

CS-Cipher

CS-Cipher was introduced by Jacques Stern and Serge Vaudenay in [6]. In this section we will just introduce its main characteristics. For more information, the reader can refer to the original description.
CS-Cipher is an iterated block cipher of 64 bits block size, and 128 bits key size. It consists of 8 iterations of a round function E followed by a bit-width XOR operation ($\oplus$) with the last 64-bits round key.

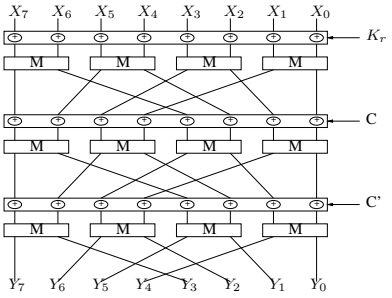

Fig. 1. CS-Cipher round Block diagram. Function E

Round description The Figure 1 presents one round of CS-Cipher. The XORed values K_r, C and C' are respectively the 64-bits round key, a first and a second constant.
By definition, $M(x, y) = (\mu(P(x), P(y))$ (see Figure 2) , the functions μ and P being respectively a $(2, 2)-$*multipermutation* over $GF(2)^8$ and a *non-linear* permutation over $GF(2)^8$. They are defined as follows:

- $\mu(a, b) = (\varphi(a) \oplus b, R_l(a) \oplus b)$. Where R_l is a $1-$bit shift circular rotation to the left and φ is defined by $\varphi(x) = (R_l(x) \wedge 0x55) \oplus x$ where $\wedge$ represents the bitwise AND. Hence the input/output pattern around a μ box will follow one out of those six patterns (Stars meaning any non-zero values):

$$\mu(0, 0) = (0, 0), \mu(*, 0) = (*, *), \mu(0, *) = (*, *)$$
$$\mu(*, *) = (*, *) \text{ or } (*, 0) \text{ or } (0, *)$$

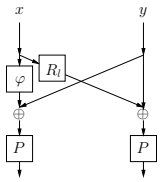

Fig. 2. CS-Cipher M box.

– P, defined by a 256-elements table, is CS-Cipher S-Box. Let us give upper and lower bounds of P's differential probability :

$$DP_{max} = \max_{a \neq 0, b} DP^P(a,b) \leq 2^{-4}$$
$$DP_{min} = \min_{a,b} DP^P(a,b) \geq 2^{-7}$$

These values are easy to compute, one has just to compute all the possible values of $DP^P(a,b)$ for any value (a,b) (there are 2^{16} pairs).

Differential and Linear Cryptanalysis In [8], Serge Vaudenay gives sufficient arguments to heuristically prove the security of CS-Cipher against differential and truncated differential (when considering characteristics and not simple differential). The formal treatment of differential cryptanalysis based on Markov cipher is not detailed in the present document, please refer to [3] for a more complete description.
Considering the probabilistic event :

$$E_{\omega_i,\omega_0} : \{O_i(x) \oplus O_i(x') = \omega_i \mid x \oplus x' = \omega_0\},$$

where (x, x') are two plaintexts.
Randomly chosen plaintexts pair of difference ω_0 will create an output difference ω_i after i rounds with probability $\Pr_{x,x'}(E_{\omega_i,\omega_0})$. Differential cryptanalysis works when one can find (ω_0, ω_i) for which the value $\Pr_{x,x'}(E_{\omega_i,\omega_0})$ is "high".
Vaudenay proves that CS-Cipher is immune against any cryptanalysis using statistics over differential characteristics which have more than 2 rounds. The author can then claim immunity against all kind of differential attacks when CS-Cipher has more than 4 rounds. Finally the study of resistance against truncated differential, which corresponds to group sets of characteristics in order to improve differential cryptanalysis, is evaluated to be strong enough after 5.33 rounds.

Impossible Differential Cryptanalysis This type of attack was introduced by Biham, Biryukov and Shamir in 1999 in [1]. From [1], in an Impossible differential attack, *"a differential predicts that particular differences should not occur (i.e., that their probability is exactly zero), and thus the correct key can never decrypt a pair of ciphertexts to that difference. Therefore, if a pair is decrypted*

to this difference under some trial key, then certainly this trial key is not the correct key. This is a sieving attack which finds the correct keys by eliminating all the other keys which lead to contradictions.“

CSC* For purpose of clarity, we are going to consider a slightly different cipher than CS-Cipher, CSC*. This variant was introduced by Vaudenay in [8] in order to simplify the proof of resistance. In CSC* the key schedule is replaced by a true random generator of 25 64-bits round keys. Hence the CS-Cipher round keys are replaced by 9 CSC* round keys and each XOR to constants C or C' is replaced by a XOR to one of the CSC* round keys. The new cipher CSC* can then be seen as a 24 rounds block cipher with a simple round function (see Figure 3). The results found in [8] for CSC* are believed to hold for CS-Cipher, and in this document we make the same assumption.

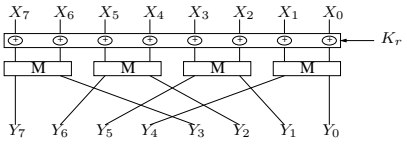

Fig. 3. CSC* round Block diagram.

Notations. In all the sequel, we will use [8]'s notations to describe CSC* components, thus the i^{th} round of CSC* can be written as follow :

$$\rho_i = L_\pi \circ P^8 \circ \mu^4 \circ s_{i-1}$$

where, for any 64-bits element $x = (x_7, x_6, x_5, x_4, x_3, x_2, x_1, x_0)$,

- $s_{i-1}(x) = x \oplus K_i$ (K_i is the i^{th} round key)
- $\mu^4(x) = (\mu(x_7, x_6), \mu(x_5, x_4), \mu(x_3, x_2), \mu(x_1, x_0))$
- $P^8(x) = (P(x_7), P(x_6), P(x_5), P(x_4), P(x_3), P(x_2), P(x_1), P(x_0))$
- $L_\pi(x) = (x_7, x_5, x_3, x_1, x_6, x_4, x_2, x_0)$

Hence, the block encryption CSC* can be written as :

$$Enc = s_{24} \circ \rho_{24} \circ \ldots \circ \rho_1$$

2 Output differential

In this section we are going to introduce the notion of *Support Markov Cipher* and show that under the hypothesis of Markov Cipher, Support Markov Cipher and uniformly distributed round keys it is possible to display a lower bound of r-round differential probability. Then, as an example we will apply this proof to CS-Cipher and show that it is indeed resistant against impossible differential.

2.1 Formal treatment for CSC*

Note: All probabilities are average probabilities over the key distribution (which is assumed to be uniform).

Definition 1. *The support function χ (referred as the characteristic function in [7])*

$$\chi : (GF(2)^k)^m \to (GF(2))^m, (x_0, \ldots, x_m) \longrightarrow (y_0, \ldots, y_m)$$

such that

$$y_i = \begin{cases} 0 \text{ if the k\_uplet } x_i = 0, \\ 1 \text{ otherwise.} \end{cases}$$

Remark : for CS-Cipher and CSC, $k = m = 8$.*

Lemma 1. *Let us consider a plaintext pair (x, x') such that $x \oplus x' = \triangle y_0$ and the output differences $(\triangle y_r, \ldots, \triangle y_0)$ generated by an encryption of x and x' by CSC*. We have for any i in $\{0, \ldots, r-1\}$:*

$$\chi(\triangle y_{i+1}) = \chi(L_\pi \circ \mu^4(\triangle y_i)).$$

Proof. The proof, easy to obtain, is provided in an online version of this paper.

Definition 2. *An r-round iterated cipher is a* Support Markov Cipher *when the sequence $(\chi(\triangle x = \triangle y_0), \chi(\triangle y_1), \ldots, \chi(\triangle y_r))$ of round output* differences *support forms a Markov chain.*

Hereafter, in order to simplify the formulas, the sequence round output *differences* as random variables will be referred as the sequence $(X_r, \ldots, X_0)$ instead of $(\triangle y_r, \ldots, \triangle y_0)$.

Lemma 2. *Let us consider a Markov cipher E and its associated Markov chain $(X_r, X_{r-1}, \ldots, X_1, X_0)$, we have trivially:*

$$Pr(X_1 = x_1 \mid X_0 = x_0) \leq DP_{max}^{h(x'_1)} Pr(\chi(X_1) = x'_1 \mid X_0 = x_0),$$

where $h : (GF(2))^m \to \{0, \ldots, m\}$ gives the Hamming weight.

Lemma 3. *Let us consider a Markov cipher E and its associated Markov chain $(X_r, X_{r-1}, \ldots, X_1, X_0)$, we have trivially:*
if $Pr(X_1 = x_1 \mid X_0 = x_0) \neq 0$ then

$$Pr(X_1 = x_1 \mid X_0 = x_0) \geq DP_{min}^{h(x'_1)} Pr(\chi(X_1) = x'_1 \mid X_0 = x_0),$$

where $h : (GF(2))^m \to \{0, \ldots, m\}$ gives the Hamming weight.

Theorem 1. *Let us consider CSC* as a Markov cipher and a Support Markov cipher E and its associated Markov chains $(X_r, X_{r-1}, \ldots, X_0)$.*

$$\begin{aligned} Pr(X_r = x_r \mid X_0 = x_0) \leq [DP_{max} \times (2^8 - 1)]^{h(x'_1)} \\ \times Pr(X_r = x_r \mid \chi(X_r) = x'_r, \chi(X_1) = x'_1) \\ \times Pr(\chi(X_r) = x'_r \mid \chi(X_1) = x'_1), \end{aligned}$$

where $h : (GF(2))^m \to \{0, \ldots, m\}$ gives the Hamming weight.

Proof. From the probability total formula

$$Pr(X_r = x_r \mid X_0 = x_0) = \sum_{x_1} Pr(X_r = x_r \mid X_1 = x_1, X_0 = x_0) \times Pr(X_1 = x_1 \mid X_0 = x_0)$$

From Lemma 2 and the fact that $(X_r, X_{r-1}, \ldots, X_0)$ is a Markov chain, we have

$$Pr(X_r = x_r \mid X_0 = x_0) \leq DP_{max}^{h(x'_1)} \times \sum_{x_1} [Pr(X_r = x_r \mid X_1 = x_1) \times Pr(\chi(X_1) = \chi(x_1) \mid X_0 = x_0)]$$

From Lemma 1 we have $\chi(X_1) = \chi(L_\pi \circ \mu^4(X_0))$ and then
$Pr(\chi(X_1) = \chi(x_1) \mid X_0 = x_0) = \begin{cases} 1 \text{ if } \chi(x_1) = \chi(L_\pi \circ \mu^4(x_0)) \\ 0 \text{ otherwise} \end{cases}$
Let us set $x'_1 = \chi(L_\pi \circ \mu^4(x_0))$, we have

$$Pr(X_r = x_r \mid X_0 = x_0) \leq DP_{max}^{h(x'_1)} \times \sum_{\substack{x_1 s.t. \\ \chi(x_1) = x'_1}} \frac{1}{Pr(X_1 = x_1)} \times Pr(X_r = x_r \ \& \ X_1 = x_1)$$

And since $Pr(X_1 = x_1)$ is a constant over all values of x_1, we have

$$Pr(X_r = x_r \mid X_0 = x_0) \leq DP_{max}^{h(x'_1)} \times \frac{Pr(\chi(X_1) = x'_1)}{Pr(X_1 = 0)} \times Pr(X_r = x_r \mid \chi(X_1) = x'_1)$$

Let us now introduce $\chi(X_r)$ in the equation

$$\begin{aligned} Pr(X_r = x_r \mid X_0 = x_0) \leq\ & [DP_{max} \times (2^8 - 1)]^{h(x'_1)} \\ & \times \sum_{x'_r} Pr(X_r = x_r \mid \chi(X_r) = x'_r, \chi(X_1) = x'_1) \\ & \times Pr(\chi(X_r) = x'_r \mid \chi(X_1) = x'_1) \end{aligned}$$

And since $Pr(X_r = x_r \mid \chi(X_r) = x'_r, \chi(X_1) = x'_1) = \begin{cases} 1 \text{ if } \chi(x_r) = x'_r \\ 0 \text{ otherwise} \end{cases}$
Let us set $x'_r = \chi(x_r)$

$$\begin{aligned} Pr(X_r = x_r \mid X_0 = x_0) \leq\ & [DP_{max} \times (2^8 - 1)]^{h(x'_1)} \\ & \times Pr(X_r = x_r \mid \chi(X_r) = x'_r, \chi(X_1) = x'_1) \\ & \times Pr(\chi(X_r) = x'_r \mid \chi(X_1) = x'_1) \end{aligned}$$

Theorem 2. *Let us consider CSC* as a Markov cipher and a Support Markov cipher E and its associated Markov chains $(X_r, X_{r-1}, \ldots, X_0)$.*

$$\begin{aligned} Pr(X_r = x_r \mid X_0 = x_0) \geq\ & [DP_{min} \times 2^{-4} \times (2^8 - 1)]^{h(x'_1)} \\ & \times Pr(X_r = x_r \mid \chi(X_r) = x'_r, \chi(X_1) = x'_1) \\ & \times Pr(\chi(X_r) = x'_r \mid \chi(X_1) = x'_1) \end{aligned}$$

where $h : (GF(2))^m \rightarrow \{0, \ldots, m\}$ gives the Hamming weight.

Proof. As in the proof of Theorem 1, let us first introduce X_1 in the equation

$$\begin{aligned} &Pr(X_r = x_r \mid X_0 = x_0) \\ &\quad = \sum_{x_1} Pr(X_r = x_r \mid X_1 = x_1, X_0 = x_0) \times Pr(X_1 = x_1 \mid X_0 = x_0) \end{aligned}$$

From Lemma 3 and the fact that $(X_r, X_{r-1}, \ldots, X_0)$ is a Markov chain, we have

$$\begin{aligned} &Pr(X_r = x_r \mid X_0 = x_0) \\ &\quad \geq DP_{min}^{h(x'_1)} \times \sum_{\substack{x_1,\ \text{s.t.} \\ DP(\mu^4(x_0), L_\pi^{-1}(x_1)) \neq 0}} Pr(X_r = x_r \mid X_1 = x_1) \end{aligned}$$

Let us set $\begin{cases} Poss_{x_0} = \{x,\ \text{s.t. } DP(\mu^4(x_0), L_\pi^{-1}(x)) \neq 0\} \\ Supp_{x_0} = \{x,\ \text{s.t. } \chi(x) = \chi(L_\pi \circ \mu^4(x_0))\} \end{cases}$

We are now going to estimate the value of

$$\sum_{x_1 \in Poss_{x_0}} Pr(X_r = x_r \mid X_1 = x_1) \text{ w.r.t. } \sum_{x_1 \in Supp_{x_0}} Pr(X_r = x_r \mid X_1 = x_1).$$

One can easily note that $Poss_{x_0} \subset Supp_{x_0}$ and from CSC* characteristics,

$$Card(\{Poss_{x_0}\}) \geq (2^{-4})^{h(\chi(\mu^4(x_0)))} Card(\{Supp_{x_0}\})$$

From the markovian property of the chain $(X_r, X_{r-1}, \ldots, X_0)$, the value of $Pr(X_r = x_r \mid X_1 = x_1)$ is independent to the fact that $x_1 \in Poss_{x_0}$ or $x_1 \in Supp_{x_0}$. Finally, we have

$$\begin{aligned} &Pr(X_r = x_r \mid X_0 = x_0) \\ &\quad \geq [DP_{min} \times (2^8 - 1)]^{h(x'_1)} \times (2^{-4})^{h(x'_1)} \times Pr(X_r = x_r \mid \chi(X_1) = x'_1) \end{aligned}$$

The proof ends exactly like in Theorem 1

2.2 Results for CSC*/CS-Cipher

Let us assume an uniform distribution of the round keys and that CSC* and CS-Cipher can be considered as Markov Ciphers and Support Markov Ciphers .

Theorem 1 and Theorem 2 give an upper and lower bound for the probability of occurrence of a r-round differential.
In order to evaluate these bounds, we have to approach the two values $Pr(\chi(X_r) = x'_r \mid \chi(X_1) = x'_1)$ and $Pr(X_r = x_r \mid \chi(X_r) = x'_r, \chi(X_1) = x'_1)$.

1. $Pr(\chi(X_r) = x'_r \mid \chi(X_1) = x'_1)$. By definition, the set $(\chi(X_r), \ldots, \chi(X_1))$ forms a Markov chain, hence the complexity of computing $P(\chi(X_r) = x'_r \mid \chi(X_1) = x'_1)$ for any value of x'_r and x'_1 is about $r \times 2^{3m}$ where m is the cipher's block size in byte (i.e. 2^{24} for CS-Cipher, 2^{48} for AES).
Let us detail the computation step :

Data: For a value x'_1 fixed
for $j = 1 \dots r$ **do**
  for $i = 0 \dots 2^m - 1$ **do**
    compute $Pr(\chi(X_j) = i | \chi(X_1) = x'_1)$:
    $\sum_{k=0}^{2^m-1} Pr(\chi(X_j) = i | \chi(X_{j-1}) = k) Pr(\chi(X_{j-1}) = k | \chi(X_1) = x'_1)$
  end
end

Note: From μ properties, we know there is at most $3^4 (< 2^8)$ values of k in the above sum where $Pr(\chi(X_j) = i \mid \chi(X_{j-1}) = k) \neq 0$. Hence the complexity of this computation is, for CSC*, slightly less than 2^{3m}.

2. $Pr(X_r = x_r \mid \chi(X_r) = x'_r, \chi(X_1) = x'_1)$. Evaluating such a probability is a hard problem in general, therefore we will discuss its approximation.
Due to the fact that the propagation of 0s bytes (i.e. non active S-Boxes) in a differential characteristic is much more predictable than propagations of non-0s bytes values (thanks to the non-linear permutations) we strongly believe that the influence of $\chi(X_1)$ on the value of non-0 bytes of X_r is substantially weaker than its influence on null bytes of X_r. That is to say, the influence of $\chi(X_1)$ on $\chi(X_r)$ is stronger than its influence on X_r given the value of $\chi(X_r)$. Thus, if we assume that
$Pr(\chi(X_r) = x'_r \mid \chi(X_1) = x'_1) = Pr(\chi(X_r) = x'_r) \pm \epsilon$
then
$Pr(X_r = x_r \mid \chi(X_r) = x'_r, \chi(X_1) = x'_1) = Pr(X_r = x_r \mid \chi(X_r) = x'_r) \pm \epsilon \pm O(\epsilon)$.

Results for CSC:*

- From computation we found that for $r \geq 11$

$$Pr(\chi(X_r) = x'_r) - 2^{-8*m} \leq Pr(\chi(X_r) = x'_r | \chi(X_1) = x'_1) \leq Pr(\chi(X_r) = x'_r) + 2^{-8*m}$$

- We deduce from the above bounds that for $r \geq 11$

$$Pr(X_r = x_r \mid \chi(X_r) = x'_r, \chi(X_1) = x'_1) \begin{cases} \geq Pr(X_r = x_r \mid \chi(X_r) = x'_r) - 2^{-8*m} \\ \leq Pr(X_r = x_r \mid \chi(X_r) = x'_r) + 2^{-8*m} \end{cases}$$

Finally, let us remark that

$$Pr(X_r = x_r \mid \chi(X_r) = x'_r) = (\tfrac{1}{2^8-1})^{h(x'_r)}$$
$$Pr(\chi(X_r) = x'_r) = (\tfrac{2^8-1}{2^8})^{h(x'_r)} \times (\tfrac{1}{2^8})^{m-h(x'_r)} = (2^8-1)^{h(x'_r)} \times 2^{-8*m}$$

And then after 11 rounds (i.e. 4 rounds of CS-Cipher) we have

$$Pr(X_r = x_r \mid X_0 = x_0)$$
$$\begin{cases} \geq ((\frac{1}{2^8-1})^{h(x'_r)} - 2^{-8*m})((2^8-1)^{h(x'_r)}2^{-8*m} - 2^{-8*m}) \times [DP_{min} \times (2^4 - 2^{-4})]^{h(x'_1)} \\ \leq ((\frac{1}{2^8-1})^{h(x'_r)} + 2^{-8*m})((2^8-1)^{h(x'_r)}2^{-8*m} + 2^{-8*m}) \times [DP_{max} \times (2^8 - 1)]^{h(x'_1)} \end{cases}$$

The final bounds of the probability of an r-round differential :

$$\boxed{Pr(X_r = x_r \mid X_0 = x_0) \begin{cases} \geq 2^{-8*m}[DP_{min} \times (2^4 - 2^{-4})]^{h(x'_1)} + O(2^{-8*2*m}) \\ \leq 2^{-8*m}[DP_{max} \times (2^8 - 1)]^{h(x'_1)} + O(2^{-8*m}) \end{cases}}$$

From the above lower bound, we claim that there is no impossible differential on CS-Cipher after 4 rounds and thus CS-Cipher is immune against impossible differential after 6 rounds.

3 Conclusion

Under the strong assumption that CS-Cipher acts very much like a Markov and a Support Markov cipher, we can prove its resistance against impossible differential. To our knowledge this is the first formal result on provable security against impossible differential, even though it remains to be proven that the model is a tight approximation of the cipher.
Future work should focus on this proof and expand the study to other ciphers (particularly AES that has common features with CS-Cipher).

References

1. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. In : LNCS, vol. 1592, pp. 12–23 (1999)
2. Biham, E., Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems. J. Cryptology 4, 1, 3–72 (1991)
3. Lai, X., Massey, J.L., Murphy, S.: Markov Ciphers and Differential Cryptanalysis. In : LNCS, vol. 547, pp. 17–38 (1991)
4. Schnorr, C.P., Vaudenay, S.: La Sécurité des Primitives Cryptographiques. Technical Report LIENS-95-10 of the Laboratoire d'informatique de L'Ecole Normale Supérieure (1995)
5. Schnorr, C.P., Vaudenay, S.: Black box cryptanalysis of hash networks based on multipermutations. In : LNCS, vol. 950, pp. 47–57 (1995)
6. Stern, J., Vaudenay, S.: CS-Cipher. In : FSE '98: Proceedings of the 5th International Workshop on Fast Software Encryption, vol. 1372, pp. 189–205, Springer-Verlag, Paris, France (1999)
7. Sugita, M., Kobara, K., Uehara, K., Kubota, S., Imai, H.: Relationships among Differential, Truncated Differential, Impossible Differential Cryptanalyses against Word-Oriented Block Ciphers like RIJNDAEL, E2. In : AES Candidate Conference, pp. 242–254 (2000)
8. Vaudenay, S.: On the Security of CS-Cipher. In : FSE '99: Proceedings of the 6th International Workshop on Fast Software Encryption, vol. 1636, pp. 260–274, Springer-Verlag, Rome, Italy (1999)