<table>
<thead>
<tr>
<th>Title</th>
<th>New Analysis Based on Correlations of RC4 PRGA with Nonzero-Bit Differences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>MIYAJI, Atsuko; SUKEGAWA, Masahiro</td>
</tr>
<tr>
<td>Citation</td>
<td>IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, E93-A(6): 1066-1077</td>
</tr>
<tr>
<td>Issue Date</td>
<td>2010-06-01</td>
</tr>
<tr>
<td>Type</td>
<td>Journal Article</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/10119/9228">http://hdl.handle.net/10119/9228</a></td>
</tr>
</tbody>
</table>
New Analysis Based on Correlations of RC4 PRGA with Nonzero-Bit Differences**

Atsuko MIYAJI††, Member and Masahiro SUKEGAWA††, Nonmember

1. Introduction

RC4 is the stream cipher proposed by Rivest in 1987, which is widely used in a number of commercial products because of its simplicity and substantial security. RC4 exploits shuffle-exchange paradigm, which uses a permutation $S$. Many attacks have been reported so far. No study, however, has focused on correlations in the Pseudo-Random Generation Algorithm (PRGA) between two permutations $S$ and $S'$. Such differences occur with non negligible probability even after $i$ rounds. This reveals an inherent weakness of shuffle-exchange-type PRGA.

key words: RC4, correlation, shuffle-exchange structure, pseudo key collision

SUMMARY

RC4 is the stream cipher proposed by Rivest in 1987, which is widely used in a number of commercial products because of its simplicity and substantial security. Though many works have been reported so far [3]–[5], [7]–[9], [11], [12], [15]–[17], it has remained secure under proper use. As a result, RC4 is widely used in many applications such as Secure Sockets Layer (SSL), Wired Equivalent Privacy (WEP), etc.

RC4 is the stream cipher proposed by Rivest in 1987, which is widely used in a number of commercial products because of its simplicity and substantial security. Though many works have been reported so far [3]–[5], [7]–[9], [11], [12], [15]–[17], it has remained secure under proper use. As a result, RC4 is widely used in many applications such as Secure Sockets Layer (SSL), Wired Equivalent Privacy (WEP), etc.

RC4 exploits shuffle-exchange paradigm, which uses a permutation $S = (S[0], \cdots, S[N-1])$ given in the initial, and outputs 8-bit data in each round by updating the permutation $S$, where typically each $S[i]$ ($i \in [0, N-1]$) is 8 bits and $N = 256$. In more detail, RC4 consists of two algorithms, the Key Scheduling Algorithm (KSA) and the Pseudo Random Generation Algorithm (PRGA). KSA is given a secret key with $\ell$ bytes (typically, $5 \leq \ell \leq 16$) and generates the initial permutation $S_0$, which is an input of PRGA. PRGA is given the initial permutation $S_0$, uses two indices $i$ and $j$, (where $i$ is a public counter but $j$ is one element of secret state information), updates $S[i]$ and $S[j]$, and outputs $Z = S[i] + S[j]$ as a key stream at the end of each round.

There are mainly two approaches to the cryptanalysis of RC4. Analysis of the weaknesses of the KSA [1], [2], [13], and analysis of the weaknesses of the PRGA [5], [7], [11], [14]. In [5], the first state recovery attack was proposed, whose computational complexity is $2^{779}$. In [7], [11], [14], non-uniform distribution of the initial permutation $S_0$ was shown. Recently, the state key recovery attack is improved by [6], whose computational complexity is $2^{241}$.

Many works, however, focus on the bias between a secret key and the initial permutation, which is an input of PRGA. Some analysis of the weaknesses of the PRGA also focus on the correlation between the first keystream output of PRGA and the secret key. We have not seen any research on correlations in PRGA between two permutations with some differences. However, such correlations should be investigated, since it is reported that sets of two keys which output either the same initial permutations or initial permutations with differences of just a few bits can be intentionally induced [10]. Furthermore, correlations between outputs of two consecutive rounds is an inherent weakness of shuffle-exchange-type PRGA.

In this paper, we focus on a shuffle-exchange structure of PRGA, where 1 swap is executed in each round. We investigate how the structure mixes the permutation $S$, by observing correlations between two permutations, $S$ and $S'$, with some differences in the initial round. The set of indices where differences exist in the initial round is represented by $\text{Diff}_0$. The correlations are measured over (a) the difference of two permutations $\Delta S = S \oplus S'$, (b) the difference of two outputs of PRGA, $\Delta Z = Z \oplus Z'$, and (c) the difference between two indices $\Delta j = j \oplus j'$. We start with $\text{Diff}_0 = \{ \text{df}_0[1], \text{df}_0[2] \}$. Our results, however, are easily applicable to other cases where there exist differences $\text{Diff}_0$ with $\#\text{Diff}_0 > 2$ in the initial round.

We show theoretically that correlations between two permutations $S$ and $S'$, such as $\Delta Z = 0$, $\Delta j = 0$, and the hamming weight of $\Delta S$, remain when $i < \text{df}_0[1]$. Furthermore, we show that such correlations between two permutations $S$ and $S'$ remain with non negligible probability when $i \geq \text{df}_0[1]$, thus, the same correlations between permutations will be observed when $i < \text{df}_0[2]$. For example, the probability that such correlations remain when $i > \text{df}_0[1]$ is greater than 30% in the cases of $\text{df}_0[1] \geq 93$. We give the theoretical formulae of the probability of both outputs being equal when $i = \text{df}_0[1]$. All theoretical results have been
This paper is organized as follows. Section 2 summarizes the known facts on RC4 together with notation. Section 3 investigates correlations in each round between two permutations $S$ and $S'$ with some differences in the initial round. Section 4 investigates correlations in each round between outputs of two permutations $S$ and $S'$. Section 5 shows the experimental results which confirm all theories in Sects. 3 and 4. Section 6 investigates how to predict inner states.

2. Preliminary

This section presents the KSA and the PRGA of RC4, after explaining the notations used in this paper.

- $S, S'$: permutations
- $S_0, S_0'$: the initial permutations of PRGA
- $\text{Diff}_0$: the set of indices where differences between $S$ and $S'$ exist in the initial round
- $r$: number of rounds ($r = 0$ means the initial round)
- $d_{0}\{1\}, d_{0}\{2\}$: the positions where differences exist in the initial round
- $i, i'$: $j$ and $j'$ of $S$ ($S'$) after $r$ rounds
- $S_r (S_r')$: the permutation $S (S')$ after $r$ rounds
- $S_r[i](S_r'[i])$: the value of $S_r (S_r')$ in the position $i$ after $r$ rounds
- $\Delta S_r[i]: S_r \oplus S_r'$
- $\Delta S_r[i]$: the number of indices with $\Delta S_r[i] \neq 0$
- $Z_r (Z_r')$: the output under $S (S')$ at the $r$-th round
- $\Delta Z_r: Z_r \oplus Z_r'$
- $\Delta j$: $j \oplus j'$
- $\Delta \text{State}[0], \Delta \text{State}[1], \cdots$: the state differences between $S$ and $S'$ ($j$ and $j'$) in a round $r$. (The state differences of $i$ are omitted since the same $i$ is used each other.)

RC4 has a secret internal state which is a permutation of all the $N = 2^n$ possible $n$-bit words and index $j$. RC4 generates a pseudo-random stream of bits (a keystream) which, for encryption, is combined with the plaintext using XOR; decryption is performed in the same way. To generate the keystream, the cipher makes use of a secret internal state which consists of two parts (shown in Fig. 1): A key scheduling algorithm, KSA, which turns a random key (whose typical size is 40–256 bits) into an initial permutation $S_0$ of $\{0, \ldots, N - 1\}$, and an output generation algorithm, PRGA, which uses the initial permutation to generate a pseudo-random output sequence.

The algorithm KSA consists of $N$ loops. It initializes $S$ to be the identity permutation, and both $i$ and $j$ to 0, and then repeats three simple operations: increment $i$, which acts as a counter, set $j$ by using $S$ and a secret key $K$ with $\ell$ bytes where each word contains $n$ bits, and swap two values of $S$ in positions $i$ and $j$. Finally, it outputs a random permutation $S = S_0$.

The algorithm PRGA is similar to KSA. It repeats four simple operations: increment $i$, which act as a counter, set $j$ by using $S$ and the previous $j$, swap two values of $S$ in positions $i$ and $j$, and output the value of $S$ in position $S[i]+S[j]$. Each value of $S$ is swapped at least once (possibly with itself) within any $N$ consecutive rounds. All additions used in both KSA and PRGA are in general additions modulo $N$ unless specified otherwise.

3. State Analysis of Permutations with Some Differences

This section analyzes correlations between two permutations, $S$ and $S'$, with some differences in the initial round. The set of indices where differences exist in the initial round is represented by $\text{Diff}_0 = \{d_{0}\{1\}, d_{0}\{2\}, \cdots\}$. The indices with nonzero bit differences are arranged in order of positions that $i$ will reach after the next round. Therefore, if nonzero bit differences exist in positions 0 and $N - 1$ in the initial round, then $\text{Diff}_0 = \{d_{0}\{1\}, d_{0}\{2\}\} = \{N - 1, 0\}$ since $i$ will be incremented to 1 in the first round.

3.1 Overview of Analysis

Assume that two permutations $S$ and $S'$ with $\text{Diff}_0 = \{d_{0}\{1\}, d_{0}\{2\}\}$ in the initial round are given, where $(S_0[d_{0}\{1\}], S_0[d_{0}\{2\}]) = (a, b)$ and $(S_r'[d_{0}\{1\}], S_r'[d_{0}\{2\}]) = (b, a)$ (See Fig. 2). The initial state of differences between $S_0$ and $S_0'$ is:

$$\Delta \text{State}[0]: (\Delta S[x] \neq 0 \iff x \in \text{Diff}_0) \land (\Delta j = 0).$$

We analyze the conditions in each round in which the initial state changes from the current state to another, or remains the same.

The transitions of state are different according to the position of $i$, that is, $i < d_{0}\{1\}$; $i = d_{0}\{1\}$ and the nonzero bit difference still exists in the position $d_{0}\{1\}$; $i = d_{0}\{1\}$ but the nonzero bit difference does not exist in the position $d_{0}\{1\}$; $i = d_{0}\{1\}$ with $i = d_{0}\{1\}$. The transitions of state are different according to the position of $i$, that is, $i < d_{0}\{1\}$; $i = d_{0}\{1\}$ and the nonzero bit difference still exists in the position $d_{0}\{1\}$; $i = d_{0}\{1\}$ but the nonzero bit difference does not exist in the position...
sections. The following subsections describe each transition
3.2 Transitions of

This subsection shows the transitions from the initial state
in Event[1] and their associated probabilities. The state diagram is given in Fig. 6.

**Theorem 1:** Assume that two initial permutations \( S \) and \( S' \) are in the state of differences \( \Delta \text{State}[0] \) in the \(( r - 1)\)-th round, and that Event[1] occurs in the \( r \)-th round.

(1) The state changes to the state \( \Delta \text{State}[0] \) (resp. \( \Delta \text{State}[1] \), resp. \( \Delta \text{State}[2] \)) if \( j_r \not\in \text{Diff}_0 \) (resp. \( j_r = \text{df}_0[2] \), resp. \( j_r = \text{df}_0[1] \)), where

\[
\Delta \text{State}[0]: [\Delta S_r[x] \neq 0 \iff x \in \text{Diff}_0] \land [\Delta j_r = 0],
\]

\[
\Delta \text{State}[1]: [\Delta S'_r[x] \neq 0 \iff x \in \text{Diff}_1] \land [\Delta j_r = 0],
\]

\[
\Delta \text{State}[2]: [\Delta S'_r[x] \neq 0 \iff x \in \text{Diff}_2] \land [\Delta j_r = 0].
\]

and where \( \text{Diff}_1 = \{ \text{df}_1[1], \text{df}_1[2] \} = \{ \text{df}_0[1], i_r \} \) and \( \text{Diff}_2 = \{ \text{df}_2[1], \text{df}_2[2] \} = \{ \text{df}_0[2], i_r \} \).

(2) Each transition occurs with the following probabilities if \( j_r \) is distributed randomly:

\[
\text{Prob} [\Delta \text{State}[0]] = \frac{N - 2}{N},
\]

\[
\text{Prob} [\Delta \text{State}[1]] = \frac{1}{N}, \quad \text{and}
\]

\[
\text{Prob} [\Delta \text{State}[2]] = \frac{1}{N},
\]

where each probability is taken over choices of \( S \) and \( S' \) in state \( \Delta \text{State}[0] \) in the initial round.

**proof:** (1) It is clear that \( j_r = j'_r \) holds in any case, since \( j_r = j_{r-1} + S_{r-1}[i_r], \Delta j_{r-1} = 0, \) and \( i_r \not\in \text{Diff}_0 \). In the case of \( j_r \not\in \text{Diff}_0, \Delta S_{r-1}[i_r] = \Delta S_r[0] \) holds and, thus, positions of non-zero-bit differences remain the same as those in \(( r - 1)\)-round. Therefore, \( \Delta \text{State}[0] \) occurs. In the case of \( j_r = \text{df}_0[2] \),

\[
(S_r[i_r], S_r[j_r]) = (S_{r-1}[i_r], S_{r-1}[j_r]) = (b, S_{r-1}[i_r]),
\]

\[
(S'_r[i_r], S'_r[j'_r]) = (S'_{r-1}[j'_r], S'_{r-1}[i'_r]) = (a, S'_{r-1}[i'_r]);
\]

and, thus, the non-zero-bit difference in the position \( \text{df}_0[2] \) moves to the current \( i_r \). Therefore, \( \Delta \text{State}[1] \) occurs. In the case of \( j_r = \text{df}_0[1] \),

\[
(S_r[i_r], S_r[j_r]) = (S_{r-1}[j_r], S_{r-1}[i_r]) = (a, S_{r-1}[i_r]),
\]

\[
(S'_r[i_r], S'_r[j'_r]) = (S'_{r-1}[j'_r], S'_{r-1}[i'_r]) = (b, S'_{r-1}[i'_r]);
\]

and, thus, the non-zero-bit difference in the position \( \text{df}_0[1] \) moves to the current \( i_r \). Therefore, \( \Delta \text{State}[2] \) occurs.

(2) The probability that each state will occur follows from the above discussion.

Theorem 1 implies that
- \( [\Delta S_r] = 2 \) and \( \Delta j_r = 0 \) hold as long as \( i_r \) is not equal to the position that a nonzero bit difference exits in the initial round.
- If \( j_r = \text{df}_0[1] \) at least once in the \( r \)-th round during \( i_r < \text{df}_0[1] \), then the nonzero bit difference in the position \( \text{df}_0[1] \) moves to the current \( i_r \). As a result, the nonzero-bit difference that was originally in the position \( \text{df}_0[1] \) affects neither \( \Delta S_r \) nor \( \Delta j_r \) until the \(( r + N - 1)\)-th round.
This is the case in which Event[3] occurs.

The following corollary describes the detailed cases in which i is not equal to any position that a nonzero bit difference existed originally before the N-th round.

**Corollary 1**: Assume that two initial permutations S and S′ in the state of differences ΔState[0] are given. Then, if either of the following events occurs, then i is not equal to any position that a nonzero bit difference exits; and both |ΔS| = 2 and Δj = 0 hold until the N-th round.

- **Event[4]**: \[ j_r = d_{0[1]}[j] \land i < d_{0[1]}[j] \]
- **Event[5]**: \[ j_r = d_{0[2]}[j] \land i < d_{0[2]}[j] \]

Note that \( i_r < i_x \) and \( i_x < d_{0[1]} \).

**Proof**: Assume that Event[4] has occurred (\( j_r, j_r \)), that is, first \( j_r = d_{0[1]}[1] \) for \( i < i_r < d_{0[1]}[1] \) has occurred. This means that ΔState[2] has occurred in the index of \( i_r \) and, thus, \( \Delta S'[x] \neq 0 \iff x \in \text{Diff}_r \). Therefore, the nonzero bit difference in the position \( d_{0[1]}[1] \) moves to the position \( i_r \). Next, it is assumed that \( j_r = d_{0[2]}[1] \) for \( i_r < i_r < d_{0[2]}[1] \) has occurred. Then, \( \Delta S'[x] \neq 0 \iff x \in \text{Diff}_r \) by applying Theorem 1 to Diff_r. Thus, i is not equal to any position that a nonzero bit difference exits until the N-th round.

Assume that Event[5] has occurred (\( j_r, j_r \)), that is, first \( j_r = d_{0[2]}[1] \) for \( i < i_r < d_{0[2]}[1] \) has occurred. This means that ΔState[2] has occurred in the index of \( i_r \) and, thus, \( \Delta S'[x] \neq 0 \iff x \in \text{Diff}_r \). Then, the index \( d_{0[2]}[1] \) no longer indicates a nonzero bit difference. Next, it is assumed that \( j_r = d_{0[1]}[1] \) for \( i_r < i_r < d_{0[1]}[1] \) has occurred. Then, \( \Delta S'[x] \neq 0 \iff x \in \text{Diff}_r \) by applying Theorem 1 to Diff_r. Thus, i is not equal to any position that a nonzero bit difference exits until the N-th round.

**Event[3]** occurs if and only if \( j_r = d_{0[1]}[1] \) for \( i < i_r < d_{0[1]}[1] \). The probability that Event[3] occurs, \( \text{Prob}[\text{Event}[3]] \), is computed by the next theorems.

**Theorem 2**: Assume that two initial permutations S and S′ in the state of differences ΔState[0] with \( d_{0[1]}[1] \geq 5 \) are given. Then, the probability that Event[3] will occur in \( d_{0[1]}[1] \geq 5 \) is given as follows if each \( i \) is distributed randomly for any given S and S′:

\[
\text{Prob}[\text{Event}[3] \mid d_{0[1]}[1] \geq 5] = 1 - \left( \frac{N - 1}{N} \right)^{d_{0[1][1]}}
\]

where the probability is taken over choices of S and S′ with differences in Diff_r in the initial round.

**Proof**: Event[2], the complement of Event[3], occurs if and only if \( j \neq d_{0[1]}[1] \) during \( i < d_{0[1]}[1] \). Therefore, \( \text{Prob}[\text{Event}[3] \mid d_{0[1]}[1] \geq 5] = 1 - \left( \frac{N - 1}{N} \right)^{d_{0[1][1]}} \) if \( j \) is distributed randomly.

In the case of \( d_{0[1]}[1] < 5 \), we can describe \( \text{Prob}[\text{Event}[3]] \) by the conditions of \( S_0 \) as follows:

**Theorem 3**: Assume that two initial permutations S and S′ in the state of differences ΔState[0] with \( d_{0[1]}[1] < 5 \) are given. Then, Event[3] will occur in the following probability if \( S_0[1], S_0[2], \) and \( S_0[3] \) are distributed randomly:

1. In the case of \( d_{0[1]}[1] = 2 \), \( \text{Prob}[\text{Event}[3] \mid d_{0[1]}[1] = 2] = \frac{1}{N} \).
2. In the case of \( d_{0[1]}[1] = 3 \), \( \text{Prob}[\text{Event}[3] \mid d_{0[1]}[1] = 3] = \frac{2N - 3}{N(N - 1)} \).
3. In the case of \( d_{0[1]}[1] = 4 \), \( \text{Prob}[\text{Event}[3] \mid d_{0[1]}[1] = 4] = \frac{2(2N - 3)}{N(N - 1)} \).

where the probability is taken over choices of S and S′ with differences in Diff_r in the initial round.

**Proof**: (1) Let \( d_{0[1]}[1] = 2 \). Then, Event[3] occurs if and only if \( j_1 = d_{0[1]}[1] = 2 \), where \( j_1 = j_0 + S_0[1] = S_0[1] \). Therefore, \( \text{Prob}[\text{Event}[3] \mid d_{0[1]}[1] = 2] = \frac{1}{N} \).

(2) Let \( d_{0[1]}[1] = 3 \). Then, Event[3] occurs if and only if either \( j_1 = d_{0[1]}[1] = 3 \) or \( j_2 = d_{0[1]}[1] = 3 \). If \( S_0[1] = 3 \), then we get \( j_1 = j_0 + S_0[1] = S_0[1] = 3 \). If \( S_0[1] \neq 2 \), then \( S_0[1] = j_1 \neq 2 \), which means that \( S_0[1] \) is not swapped with \( S_0[2] \) in the first round. This implies that \( S_0[2] = S_0[1] \) and, if \( S_0[2] \neq 2, 3 \) and \( S_0[0] + S_0[2] = 3 \), we get \( j_2 = j_1 + S_0[2] = j_1 + S_0[2] = S_0[1] = 3 \). Therefore, \( \text{Prob}[\text{Event}[3] \mid d_{0[1]}[1] = 3] = \frac{1}{N} \).

(3) Let \( d_{0[1]}[1] = 4 \). Then, Event[3] occurs if and only if either \( j_1 = d_{0[1]}[1] = 4 \), \( j_2 = d_{0[1]}[1] = 4 \), or \( j_3 = d_{0[1]}[1] = 4 \). In \( S_0[1] = 4 \), then we get \( j_1 = j_0 + S_0[1] = S_0[1] = 4 \). If \( S_0[1] = 2 \), then \( j_1 = j_0 + S_0[1] = 2 \); and, \( S_0[1] \) is swapped with \( S_0[2] \). And, we get \( j_2 = j_1 + S_0[2] = j_1 + S_0[2] = 4 = d_{0[1]}[1] \). Note that \( S_0[1] \) is swapped with \( S_0[2] \) if and only if \( S_0[1] \) is swapped with \( S_0[2] \), which implies that \( S_0[3] = S_0[1] \). Then, in the 2nd round, \( j_2 = j_1 + S_0[2] = j_1 + S_0[2] = 4 = d_{0[1]}[1] \). If \( S_0[1] = 3 \) and \( S_0[2] = N - 2 \), then \( j_1 = S_0[1] = 3 \) and \( S_0[3] = S_0[1] \). Thus, in the 3rd round, we get \( j_3 = j_2 + S_0[3] = 4 \). Note that \( S_0[1] \) is swapped with \( S_0[2] \) if and only if \( S_0[1] \) is swapped with \( S_0[2] \). If \( S_0[1] \neq 2, 3, 4; \) and \( S_0[1] + S_0[2] + S_0[3] = 4 \), then we get \( j_3 = j_2 + S_0[3] = 4 \). To sum up all conditions, which are independent of each other, \( \text{Prob}[\text{Event}[3]] = \frac{N}{N} + \frac{N}{N} + \frac{N}{N} = \frac{N}{N} \).
### 3.3 Transitions of ΔState[0] on the Nonzero Bit Difference

This subsection shows each transition of the initial state ΔState[0] and the probability of its occurrence when Event[2] occurs. The state diagram is given in Fig. 7.

**Theorem 4:** Assume that two permutations S and S' are in the state of differences ΔState[0] in the \((r - 1)\)-th round. 

1. The state changes to ΔState[3] (resp. ΔState[3']), ΔState[4] (resp. ΔState[5]), ΔState[6]), if \(j_r = df_0[2] \land \lnot [j_r' \neq df_0] \land \lnot \exists t \in \text{Diff}_0 \) where

\[
\begin{align*}
\text{Diff}_3 &= \{df_6[1], df_2[2]\} \\
\text{Diff}_y &= \{df_6[1], df_y[2]\} \\
\text{Diff}_4 &= \{df_6[1], df_2[2], df_3[3]\} \\
\text{Diff}_5 &= \{df_6[1], df_2[2], df_3[3]\} \\
\text{Diff}_5 &= \{df_6[1], df_2[2], df_3[3]\}
\end{align*}
\]

(2) Each transition occurs with the following probability, if \(j\) is distributed randomly:

\[
\begin{align*}
\text{Prob}[\text{ΔState}[3] \lor \text{ΔState}[3']] &= \text{Prob}[\text{Event}[2]] \cdot \frac{2(N-2)}{N(N-1)} \\
\text{Prob}[\text{ΔState}[4] \lor \text{ΔState}[4']] &= \text{Prob}[\text{Event}[2]] \cdot \frac{2(N-2)}{N(N-1)} \\
\text{Prob}[\text{ΔState}[5]] &= \text{Prob}[\text{Event}[2]] \cdot \frac{(N-2)(N-3)}{N(N-1)} \\
\text{Prob}[\text{ΔState}[6]] &= \text{Prob}[\text{Event}[2]] \cdot \frac{2}{(N-1)}
\end{align*}
\]

**Proof:** (1) It is clear that \(j \neq j'\) in each case, since \(\Delta j_r = \Delta j_{r-1} + \Delta S_{r-1}[i_r] \neq 0\). In the case of \(j_r = df_0[2]\) and \(j_r' \neq df_0\), \(S_{r-1}[i_r] = S_{r-1}[df_0[1]] = a\) is swapped with \(S_{r-1}[j_r] = b\); \(S_{r-1}[j_r] = S_{r-1}[df_0[1]] = b\) is swapped with \(S_{r-1}[j_r] = a\), which implies that \(S_{r-1}[df_0[2]] = a\) remains the same. Thus, we get \(\Delta S_r[x] \neq 0 \iff x \in \text{Diff}_3\) after the \(r\)-th round. In the case of \(j_r' = df_0[2]\) and \(j_r \neq df_0\), the same also holds.

In the case of \(j_r = df_0[1]\) and \(j_r' \neq df_0\), \(S_{r-1}[i_r] = a\) (resp. \(S_{r-1}[i_r] = b\)) is swapped with \(S_{r-1}[j_r]\) (resp. \(S_{r-1}[j_r]\)), where nonzero-bit difference did not exist; and both \(S_{r-1}[df_0[2]] = b\) and \(S_{r-1}[df_0[2]] = a\) still remain the same. Thus, we get \(\Delta S_r[x] \neq 0 \iff x \in \text{Diff}_4\) after the \(r\)-th round.

In the case of \(j_r, j_r' \neq df_0\), \(S_{r-1}[i_r] = a\) (resp. \(S_{r-1}[i_r] = b\)) is swapped with \(S_{r-1}[j_r]\) (resp. \(S_{r-1}[j_r]\)), where all nonzero-bit differences disappear after swapping in the \(r\)-th round. The same also holds in the case of \(j_r', j_r = df_0[2]\).

(2) The probability that each state will occur follows from the above discussion.

### 4. Correlation between Outputs and State Transitions

This section analyzes the differences between outputs of two permutations \(S\) and \(S'\) in each transition described in Sect. 3, where two initial permutations \(S\) and \(S'\) are in the state of differences ΔState[0].

#### 4.1 Outputs before the Nonzero-Bit Difference

This subsection investigates the correlation between outputs of two permutations in each transition before the first nonzero-bit difference (i.e. \(i < df_0[1]\)). The states of differences of two permutations in any round \(r < df_0[1]\) are ΔState[0], ΔState[1], or ΔState[2] from Theorem 1.
Proposition 1: Assume that two initial permutations $S$ and $S'$ are in the state of differences $\Delta S[0]$ in the $(r-1)$-th round, and that Event[1] occurs in the $r$-th round. Then, $\Pr[\Delta Z = 0]$ in each state is as follows:

$$\Pr[\Delta Z = 0] = \frac{N-2}{N} \cdot \frac{2}{N(N-1)}, \quad \text{or} \quad \frac{2}{N(N-1)}$$

if $\Delta S[0]$, $\Delta S[1]$, or $\Delta S[2]$ occurs, respectively.

Proof: Theorem 1 has shown that

- $\Delta j_r = 0$ and $j_r, i \notin \Diff_0$ if $\Delta S[0]$,
- $\Delta j_r = 0$, $i \in \Diff_1$ and $j_r \notin \Diff_1$ if $\Delta S[1]$,
- $\Delta j_r = 0$, $i \in \Diff_1$ and $j_r \notin \Diff_2$ if $\Delta S[2]$.

Then, the necessary and sufficient conditions for $\Delta Z = 0$ in each state are as follows.

In $\Delta S[0]$: $\Delta Z = 0$

$$\iff [\Delta (S, [i_r] + S, [j_r]) = 0] \land [S, [i_r] + S, [j_r] \notin \Diff_0]$$

Thus, $\Pr[\Delta Z = 0] = \frac{N-2}{N}$. 

In $\Delta S[1]$: $\Delta Z = 0$

$$\iff [\Delta (S, [i_r] + S, [j_r]) = 0] \land [S, [i_r] + S, [j_r] \notin \Diff_1]$$

Thus, $\Pr[\Delta Z = 0] = \frac{2}{N(N-1)}$ since $\#\Diff = 2$ and $S, [i_r] + S, [j_r] \notin S', [i_r] + S', [j_r]$.

In $\Delta S[2]$: $\Delta Z = 0$

$$\iff [\Delta (S, [i_r] + S, [j_r]) = 0] \land [S, [i_r] + S, [j_r] \notin \Diff_2]$$

Thus, $\Pr[\Delta Z = 0] = \frac{2}{N(N-1)}$ since $\#\Diff = 2$ and $S, [i_r] + S, [j_r] \notin S', [i_r] + S', [j_r]$.

From the above, Proposition 1 follows.

From Theorem 1 and Proposition 1, the probability of $\Pr[\Delta Z = 0]$ if $r < \Diff_0[1]$ (i.e., $i < \Diff_0[1]$) can be computed as follows.

Corollary 2: Assume that two initial permutations $S$ and $S'$ with $\Diff_0 = \{\Diff_0[1], \Diff_0[2]\}$ are given. Then, $\Pr[\Delta Z = 0] = \left(\frac{N-2}{N}\right)^2 + \frac{2}{N(N-1)}$, if $r < \Diff_0[1]$.

4.2 Outputs on the Nonzero-Bit Difference

This subsection investigates the correlation between outputs of two permutations in each transition when $r = \Diff_0[1]$ (i.e., $i = \Diff_0[1]$). The probability that both outputs are equal, $\Pr[\Delta Z = 0]$, is given in the next theorem.

Proposition 2: Assume that two initial permutations $S$ and $S'$ are in the state of differences $\Delta S[0]$ in the $(r-1)$-th round, and that Event[2] occurs in the $r$-th round. Then, $\Pr[\Delta Z = 0]$ in each state is as follows:

$$\Pr[\Delta Z = 0] = \begin{cases} \frac{2}{N(N-1)} & \text{if}\ \Delta S[3] \lor \Delta S[3'] \\ \frac{N-3}{N(N-2)} + \frac{3}{N(N-1)} & \text{if}\ \Delta S[4] \lor \Delta S[4'] \\ \frac{N-4}{N(N-3)} + \frac{4}{N(N-1)} & \text{if}\ \Delta S[5] \\ 0 & \text{if}\ \Delta S[6] \end{cases}$$

Proof: Let $c$ and $c' \in [0, N-1]$ be values in positions of $j_r$ and $j_r'$, before swapping in the $r$-th round, that is, $(c, c') = (S, [i_r] + S, [j_r])$. On the other hand, $(a, b) = (S, [i_r] + \Diff_0[1], S, [j_r] + \Diff_0[2]) = (S, [i_r] + \Diff_0[1], S, [j_r] + \Diff_0[1])$. (See Fig. 2). Theorem 4 has shown that

$$\Delta S[3] = \{S, [i_r] + S, [j_r] = (b, a) \land (S', [i_r] + S', [j_r]) = (c', b) \quad \text{(i.e.} \ c = b \neq a, b)\}$$

$$\Delta S[4] = \{S, [i_r] + S, [j_r] = (a, a) \land (S', [i_r] + S', [j_r]) = (c', b) \quad \text{(i.e.} \ c = c' \neq a, b)\}$$

$$\Delta S[5] = \{S, [i_r] + S, [j_r] = (c, a) \land (S', [i_r] + S', [j_r]) = (b', a) \quad \text{(i.e.} \ c \neq c', c \neq a, b)\}$$

$$\Delta S[6] = \{\Delta S = 0, S, [i_r] + S, [j_r] = (a, a) \land (S', [i_r] + S', [j_r]) = (b, b) \quad \text{(i.e.} \ i = j_r)\}$$

Therefore, the necessary and sufficient conditions of $\Delta Z = 0$ in each state are as follows.

In $\Delta S[3]$: $\Delta Z = 0$

$$\iff [S, [i_r] + S, [j_r] = (b, a) \land (S', [i_r] + S', [j_r]) = (c', b) \land \Delta S(\Diff_0[1] + \Diff_0[2]) = 0]$$

Thus, $\Pr[\Delta Z = 0] = \frac{N-2}{N}$. Since $a + b \neq c' + b$.

The same reasoning holds in the case of $\Delta S[3']$.

In $\Delta S[4]$: $\Delta Z = 0$

$$\iff [S, [i_r] + S, [j_r] = (a, a) \land (S', [i_r] + S', [j_r]) = (c', b) \land \Delta S(\Diff_0[1] + \Diff_0[2]) = 0]$$

Thus, $\Pr[\Delta Z = 0] = \frac{N-2}{N}$. Since $a + b \neq c' + b$.

The same reasoning holds in the case of $\Delta S[4']$. Therefore,
In ΔState(6) : Prob [ΔZ = 0] = 0.
Because Δ(S_r[i] + S_r[j]) ≠ 0 and ΔS_r = 0.
From the above, the proposition follows.

The probability Prob [ΔZ = 0] when i = df_o[1] follows immediately from Theorem 4 and Proposition 2.

Corollary 3: Assume that two permutations S and S′ in the (r − 1)-th round are in ΔState(0) and Event[2] occurs in the r-th round. Then, the probability that both outputs are equal in the r-th round, Prob [ΔZ = 0], is given as follows:

\[
\text{Prob}[\Delta Z = 0] = \text{Prob}[\text{Event}[2]] \times \left( \frac{N^2 - 4N + 2}{N^2(N-1)} + \frac{2(2N-1)(N-2)}{N^2(N-1)^2} \right)
\]

From the above, the proposition follows.

Theorem 5 follows from this fact.

The probability Prob [ΔZ = 0] when i = df_o[1] follows immediately from Theorem 4 and Proposition 2.

Corollary 3: Assume that two permutations S and S′ in the (r − 1)-th round are in ΔState(0) and Event[2] occurs in the r-th round. Then, the probability that both outputs are equal in the r-th round, Prob [ΔZ = 0], is given as follows:

\[
\text{Prob}[\Delta Z = 0] = \text{Prob}[\text{Event}[2]] \times \left( \frac{N^2 - 4N + 2}{N^2(N-1)} + \frac{2(2N-1)(N-2)}{N^2(N-1)^2} \right)
\]

From the above, the proposition follows.

Theorem 5 follows from this fact.

Remarks 1: 1. The second term of

\[
\left( \frac{N^2 - 4N + 2}{N^2(N-1)} + \frac{2(2N-1)(N-2)}{N^2(N-1)^2} \right)
\]

can be dealt with as an error term if df_o[1] is large, which will be discussed in Sect. 5.

2. \(P_2 = \text{Prob}[\text{Event}[3]]\) can be computed explicitly by Theorems 2 and 3. Thus, \(P_1 = \text{Prob}[\Delta Z = 0]\) in the round \(r = df_o[1]\) can be explicitly estimated for each \(df_o[1]\).

5. Experimental Results and New Bias

This section shows experimental results of Theorems 2, 3, and 5, and Corollary 2 in Sects. 3 and 4. All experiments were conducted under the following conditions: execute KSA of RC4 with \(N = 256\) for \(10^9\) randomly chosen keys of 16 bytes, generate the initial permutation \(S_0\), and set another initial permutation \(S'_0\) with \(\text{Diff}_0\). Experiments are executed over the following sets of \(\text{Diff}_0\): \(df_o[1] = 2, 3, 4, 5\) for Theorems 2 and 3; and \(df_o = \{df_o[1], df_o[2]\} = \{2 - 254, 255\}, \{2, 3 - 255\}, \{3, 4 - 255\}\) for Theorem 5 and Corollary 2. The percentage absolute error \(\epsilon\) of experimental results compared with theoretical results is computed by

\[
\epsilon = \frac{|\text{experimental value} - \text{theoretical value}|}{\text{experimental value}} \times 100(\%),
\]

which is also used in [14].

5.1 Experimental Results of Event[3]

Figure 8 shows experimental results of \(\text{Prob}[\text{Event}[3]]\) and its associated percentage absolute error, where the theoretical value is computed by Theorems 2 and 3. The horizontal axis represents \(df_o[1] = 2, 3, 4, 5\). The left side of vertical axis represents \(\text{Prob}[\text{Event}[3]]\), and the right side represents the percentage absolute error. Table 1 shows the cases of \(df_o[1] \leq 6\) in detail.

Only the cases of \(2 \leq df_o[1] \leq 6\) give the percentage absolute error \(\epsilon \geq 5\), and, thus, our theoretical formulæ closely match the experimental results if \(df_o[1] > 6\). The

\(\text{Event}[3]\) does not depend on \(df_o[2]\). See Theorems 2 and 3.
initial permutation $S_0$, that is the output of KSA, has a great influence on Event[3] when $df_0[1]$ is small. Our results indicate that the bias in $S_0$ is propagated to $\text{Prob}[\text{Event}[3]]$ as the bias in $S_0$ has been reported in [7], [11], [14].

Figure 8 also indicates that the nonzero bit difference in the position $df_0[1]$ moves to another position until $i = df_0[1]$ with $\text{Prob}[\text{Event}[3]] > 30\%$ when $df_0[1] \geq 93$. In this case, the correlations between $S$ and $S'$ such as $\Delta j = 0$ and $|\Delta S| = 2$ remain the same until $i = df_0[2]$.

5.2 Experimental Results of Outputs

Figure 9 shows experimental results of $\text{Prob}[\Delta Z = 0]$ in $r = df_0[1] - 1$, $df_0[1]$, and $df_0[1] + 1$, and percentage absolute error in $r = df_0[1]$ (i.e. $i = df_0[1]$), where the theoretical value is computed by Theorem 5. The horizontal axis represents $df_0[1] = 2, \cdots , 253$. The left side of vertical axis represents $\text{Prob}[\Delta Z = 0]$, and the right side represents the percentage absolute error. By using the experimental results, we investigate each case of outputs before or on the nonzero-bit difference.

Outputs before the nonzero-bit difference:

Let us discuss $\text{Prob}[\Delta Z = 0]$ in $r = df_0[1] - 1$ (i.e. $i = df_0[1] - 1$) for $df_0[1] = 2, \cdots , 254$. The probability is theoretically estimated in Corollary 2. Our theoretical and experimental results indicate that both outputs of two permutations are coincident with a high probability $\text{Prob}[\Delta Z = 0] > 0.98$ during $i < df_0[1]^1$.

Our experimental results show that $\text{Prob}[\Delta Z = 0]$ in the round $df_0[1] + 1$ is almost the same as in the round $df_0[1]$, which reflects the results in Theorem 1. To sum up, we see that it is highly probable that both outputs of permutations are coincident as long as $i$ does not indicate the index of nonzero bit difference in the current round.

Table 1 Experimental results with $\epsilon \geq 5$ of Event[3].

<table>
<thead>
<tr>
<th>$df_0[1]$</th>
<th>Theoretical value</th>
<th>Experimental value</th>
<th>$\epsilon(%)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0.003906</td>
<td>0.003530</td>
<td>26.991</td>
</tr>
<tr>
<td>3</td>
<td>0.007797</td>
<td>0.009069</td>
<td>14.027</td>
</tr>
<tr>
<td>4</td>
<td>0.015548</td>
<td>0.018221</td>
<td>14.667</td>
</tr>
<tr>
<td>5</td>
<td>0.015534</td>
<td>0.016751</td>
<td>7.265</td>
</tr>
<tr>
<td>6</td>
<td>0.019379</td>
<td>0.020501</td>
<td>5.472</td>
</tr>
</tbody>
</table>

1 Similar experimental results to $i = df_0[1] - 1$ hold during $i < df_0[1] - 1$.

11 The case of $df_0[1] = 254$ is omitted since $i$ indicates the second nonzero bit difference $df_0[2] = 255$.

11 If Event[3] has occurred in the round $r < df_0[1]$, then $df_0[1]$ is not an index of nonzero bit difference.

Fig. 9 $\text{Prob}[\Delta Z = 0](df_0[2] = 255)$.
the right side represents the percentage absolute error. Experimental results show that $\epsilon_1 < 5$ (resp. 10) if $df_0[1] > 15$ (resp. $df_0[1] > 9$). From these theoretical and experimental results, we see that the observable event $AZ = 0$ can indicate that the internal event Event[3] occurs with extremely high probability.

Figure 11 shows experimental results of $\text{Prob} [ AZ = 0 ]$ in the round $df_0[1] = 3$ in each case of $4 \leq df_0[2] \leq 255$ ($df_0[1] = 3$), and percentage absolute error. The horizontal axis represents $df_0[2]$. The left side of vertical axis represents $\text{Prob} [ AZ = 0 ]$, and the right side represents the percentage absolute error. The percentage absolute error $\epsilon < 0.8$ holds in $4 \leq V df_0[2] \leq 255$. We see that our theoretical formulae closely match the experimental results independent of another nonzero-bit difference $df_0[2]$.

5.3 Experimental Results of Biases in $S_0[1]$ and $S_0[2]$

Let us discuss Event[3] when $df_0[1] = 3$ in detail, where the error $\epsilon > 10$ (Table 1). Theorem 3 says that both $S_0[1]$ and $S_0[2]$ determine Event[3], that is, $\text{Event}[3] \iff S_0[1] = 3 \lor (S_0[1] \neq 2,3) \land S_0[1] + S_0[2] = 3$. Here we investigate the bias in $S_0[1]$ and $S_0[2]$ from the point of view of Event[3].

Figure 12 shows experimental results concerning the occurrence of $S_0[1]$ with $0 \leq S_0[1] \leq 255$, and the percentage absolute error, where the theoretical value (a random association) of occurrence of each $S_0[1]$ is $\frac{1}{N} = 3.906 \times 10^{-3}$. Figure 13 shows experimental results concerning the occurrence of $S_0[2]$ when $S_0[1] = 3$, and the percentage absolute error, where the theoretical value (a random association) of occurrence of each $(S_0[1] = 3, S_0[2])$ is $\frac{1}{N(N-1)} = 1.532 \times 10^{-5}$. The horizontal axis represents $S_0[1]$ or $S_0[2]$. The left side of vertical axis represents each probability, and the right side represents each percentage absolute error.

These experimental results indicate a non-uniform distribution of $S_0[1]$ and $S_0[2]$ when $S_0[1] = 3$. Tables 2 and 3 show some cases that indicate a non-uniform distribution as follows:

\[
\begin{align*}
\text{Prob} [ S_0[1] = 3 ] &= 5.303 \times 10^{-3} > 3.906 \times 10^{-3}, \\
\text{Prob} [ S_0[1] = 3 \land S_0[2] = x ] &= 2.0 \times 10^{-5} > 1.532 \times 10^{-5} \text{ for } x \leq 135, \\
\text{Prob} [ S_0[1] = 3 \land 0 \leq S_0[2] \leq 128 ] &= 3.05299 \times 10^{-3}
\end{align*}
\]
Here we investigate how to analyze the internal state of $S$ or $j$. Assume that two permutations $S$ and $S'$ with $\text{Diff}_0 = \{d_{0[1]}, d_{0[2]}\}$ in the initial round are given, and that both $d_{0[1]}$ and $d_{0[2]}$ are nonzero.

These non-uniform distribution will be used for a new cryptanalytic analysis in Sect. 6.

### Table 2 Probability of occurrence $S_{0[1]}$.

<table>
<thead>
<tr>
<th>$S_{0[1]}$</th>
<th>Probability of occurrence $S_{0[1]}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0–9</td>
<td>0.0039 0.0039 0.0054 0.0053 0.0053 0.0054 0.0054 0.0054 0.0054</td>
</tr>
<tr>
<td>10–19</td>
<td>0.0052 0.0052 0.0052 0.0052 0.0052 0.0051 0.0051 0.0051 0.0051</td>
</tr>
<tr>
<td>20–29</td>
<td>0.0051 0.0050 0.0050 0.0050 0.0050 0.0050 0.0050 0.0050 0.0050</td>
</tr>
<tr>
<td>30–39</td>
<td>0.0049 0.0049 0.0049 0.0049 0.0049 0.0048 0.0048 0.0048 0.0048</td>
</tr>
</tbody>
</table>

### Table 3 Probability of occurrence $S_{0[2]}$ in $S_{0[1]} = 3$.

<table>
<thead>
<tr>
<th>$S_{0[2]}$</th>
<th>Probability of occurrence $S_{0[2]}$ in $S_{0[1]} = 3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0–3</td>
<td>0.0000211 0.0000227 0.0000207 0.0000211 0.0000280 0.0000281</td>
</tr>
<tr>
<td>7–13</td>
<td>0.0000280 0.0000278 0.0000278 0.0000277 0.0000278 0.0000273 0.0000274</td>
</tr>
<tr>
<td>14–20</td>
<td>0.0000273 0.0000270 0.0000270 0.0000270 0.0000270 0.0000269 0.0000269</td>
</tr>
<tr>
<td>108–114</td>
<td>0.0000216 0.0000213 0.0000213 0.0000206 0.0000206 0.0000207 0.0000207 0.0000207 0.0000207</td>
</tr>
<tr>
<td>115–121</td>
<td>0.0000212 0.0000216 0.0000204 0.0000207 0.0000210 0.0000202 0.0000218</td>
</tr>
<tr>
<td>122–128</td>
<td>0.0000210 0.0000211 0.0000206 0.0000206 0.0000205 0.0000208 0.0000206</td>
</tr>
</tbody>
</table>

$> 1.9531 \times 10^{-3}$.

### Fig. 12 Occurrence of $S_{0[1]}$. | Occurrence of $S_{0[1]}$ when $S_{0[1]} = 3$. | Occurrence of $S_{0[2]}$ in $S_{0[1]} = 3$.
outputs of PRGA are observable.

Then, by observing both outputs Z and Z' of PRGA, we can recognize the index of the first nonzero-bit difference from the first round in which both outputs are not equal. This is investigated in Sect. 5.2. Therefore, if neither $d_0[1]$ nor $d_0[2]$ are known, the first nonzero-bit difference is probabilistically predictable.

Consider the case of $d_0[1] = 2$. By checking whether $\Delta Z = 0$ in the 2nd round, we can recognize whether $\text{Event}[3]$ has occurred. If $\text{Event}[3]$ has occurred, then $S_0[1] = 2$ holds from Theorem 3. The experimental result shows $\text{Prob} \{ \text{Event}[3] \mid d_0[1] = 2 \} = 0.005350$ (see Table 1). However, if we try to predict $S_0[1]$ from a random association, then the probability is $1/256 = 0.003906$. Therefore, one can guess $S_0[1]$ with an additional advantage of $0.005350 - 0.003906 = 36.9\%$.

Consider the case of $d_0[1] = 3$. By checking whether $\Delta Z = 0$ in the 3rd round, we can recognize whether $\text{Event}[3]$ has occurred. Let us discuss how to predict both $S_0[1]$ and $S_0[2]$. If $\text{Event}[3]$ has occurred, then $\{ S_0[1] = 3 \} \lor \{ S_0[1] \neq 2, 3 \land S_0[1] + S_0[2] = 3 \}$ holds, from Theorem 3. The case of $S_0[1] = 3$, the experimental results show that $\text{Prob} \{ \text{Event}[3] \mid d_0[1] = 3 \} = 0.009069$ (see Table 1) and $\text{Prob} \{ S_0[1] = 3 \} = 0.0053$ (see Table 2). On the other hand, we predict $S_0[2]$ with the probability $1/255$. Therefore, we can predict $(S_0[1], S_0[2])$ with the probability $0.0053 \times 1/255 = 2.078431 \times 10^{-5}$. (2) If $S_0[1] \neq 2, 3 \land S_0[1] + S_0[2] = 3$, if $S_0[1]$ is predicted, then $S_0[2]$ can be predicted promptly. We find that $\text{Prob} \{ \text{Event}[3] \mid S_0[1] \neq 2, 3 \land S_0[1] + S_0[2] = 3 \} = (0.009069 - 0.0053) \times 1/254 = 1.483858 \times 10^{-5}$. Therefore, we can predict $(S_0[1], S_0[2])$ with the probability $1.483858 \times 10^{-5}$. Taking both together, the probability to predict $(S_0[1], S_0[2])$ is $2.078431 \times 10^{-5} + 1.483858 \times 10^{-5} = 3.562289 \times 10^{-5}$. On the other hand, if we try to predict $(S_0[1], S_0[2])$ from a random association, then the probability is $1/256 \times 1/255 = 1.531863 \times 10^{-5}$. Therefore, one can guess $(S_0[1], S_0[2])$ with an additional advantage of $3.562289 - 1.531863 \times 100 = 132.54\%$.

Further Discussion

Here we discuss how we generalize our analysis to RC4. In this paper, we start with $\text{Diff} = \{ d_0[1], d_0[2] \}$. However, our results can be generalized to cases where there exist differences $\text{Diff}$ with $\#\text{Diff} > 2$ in the initial round. Then, we could apply our analysis to any given two $S$ and $S'$ as follow. Set the first index, whose values of both $S$ and $S'$ differ each other, to $d_0[1]$. That is, the following holds: $S_0[i] = S_0'[i]$ for $(0 \leq i < d_0[1])$ and $S_0[d_0[1]] \neq S_0'[d_0[1]]$. Then, by applying our discussion to the above case, we could compute the probability that both outputs are equal to each other in $r < d_0[1]$ theoretically. Furthermore, by observing two outputs, we could predict inner states whether $\text{Event}[3]$ has occurred or not. Then, in the special case of a small $d_0[1]$, we could guess inner states such as $S$ and $j$.

7. Conclusion

In this paper, we have investigated, for the first time, correlations between two permutations, $S$ and $S'$, with some differences in the initial round. We have shown that correlations between two permutations $S$ and $S'$ remain before "3" is in the position where the nonzero-bit difference exists in the initial round, and that the correlations remain with non negligible probability even after "4" passed by the position. All theoretical results have been confirmed experimentally.

Our results imply that the same correlations between two permutations will be observed with non negligible probability after the 255-th round. This reveals a new inherent weakness of shuffle-exchange-type PRGA. We have also investigated how to predict inner states such as $S$ and $j$ by using observable two outputs $Z$ and shown its additional advantage compared with prediction from a random association.

Acknowledgments

The authors express our gratitude to anonymous referees for invaluable comments.

References


Atsuko Miyaji received the B.Sc., the M.Sc., and the Dr.Sci. degrees in mathematics from Osaka University, Osaka, Japan in 1988, 1990, and 1997 respectively. She joined Panasonic Co., LTD from 1990 to 1998 and engaged in research and development for secure communication. She was an associate professor at the Japan Advanced Institute of Science and Technology (JAIST) in 1998. She has joined the computer science department of the University of California, Davis since 2002. She has been a professor at the Japan Advanced Institute of Science and Technology (JAIST) since 2007 and the director of Library of JAIST since 2008. Her research interests include the application of number theory into cryptography and information security. She received the IPSJ Sakai Special Researcher Award in 2002, the Standardization Contribution Award in 2003, Engineering Sciences Society: Certificate of Appreciation in 2005, the AWARD for the contribution to CULTURE of SECURITY in 2007, IPSJ/ITSCI Project Editor Award in 2007, 2008, and 2009, the Director-General of Industrial Science and Technology Policy and Environment Bureau Award in 2007, Editorial Committee of Engineering Sciences Society: Certificate of Appreciation in 2007, and DoCoMo Mobile Science Awards in 2008. She is a member of the International Association for Cryptologic Research, the Institute of Electronics, Information and Communication Engineers, the Information Processing Society of Japan, and the Mathematical Society of Japan.

Masahiro Sukegawa received the B.Eng. degree from the Tokyo University of Science in 2006 and the M. Info. Sci. degree from the Japan Advanced Institute of Science and Technology in 2009.