New Form of Permutation Bias and Secret Key Leakage in Keystream Bytes of RC4

Subhamoy Maitra, *ISI*, *Kolkata*

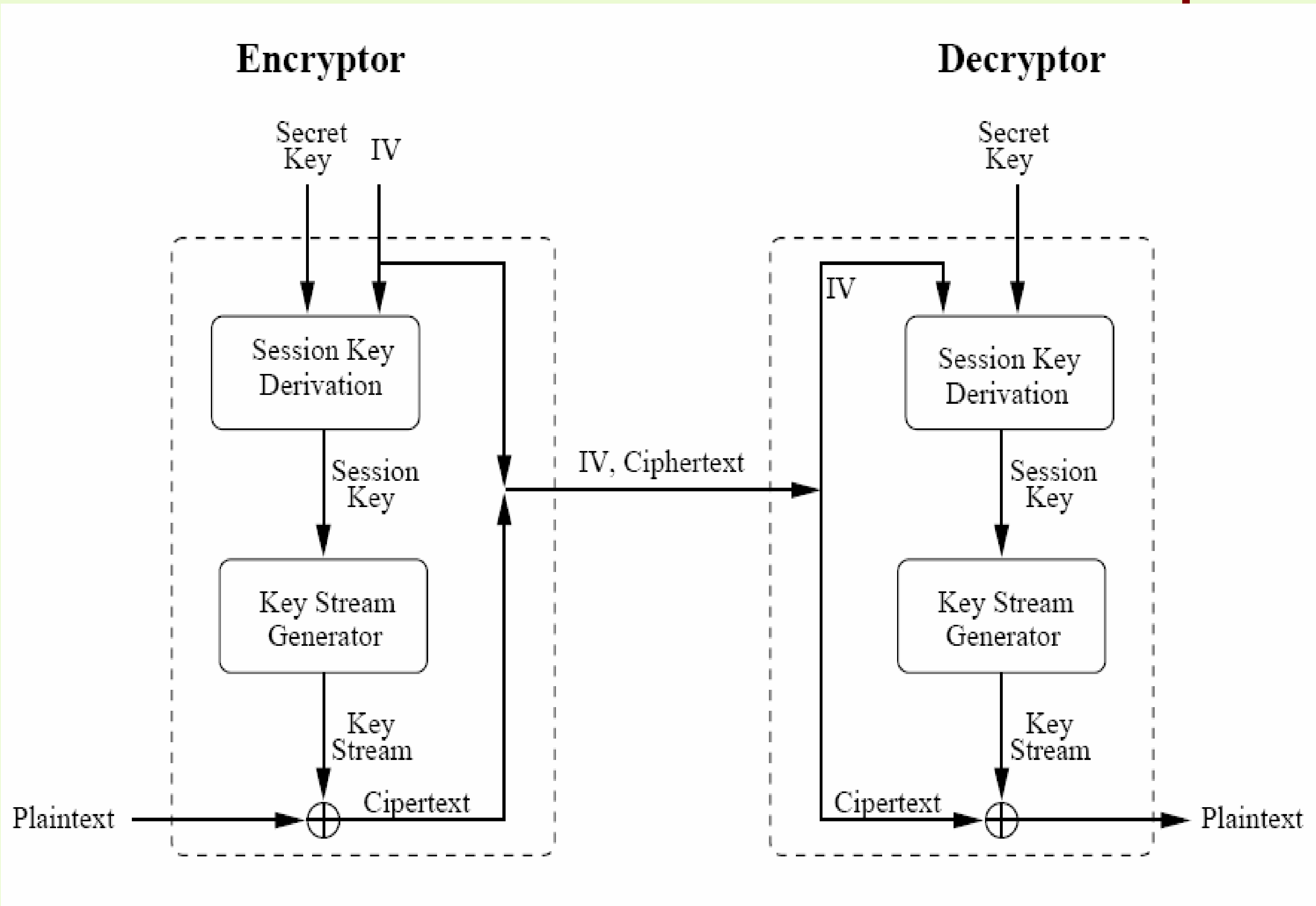
Goutam Paul, *Jadavpur University*, *Kolkata*

Roadmap

- Introduction
- Related Work and Contribution
- Bias in the Permutation
- Key Leakage in the Keystream
- Conclusion

Introduction

General Structure of Stream Cipher



RC4

- One of the most popular stream ciphers
- Designed by Ron Rivest in 1987
- Used in SSL, TLS, WEP, WPA, AOCE, Oracle Secure SQL etc.
- Not completely cracked yet, even after two decades of its discovery

Data Structure of RC4

$S[0,\ldots,N-1]$: A permutation of $\{0,1,\ldots,N\text{-}1\}$.

$key[0,\ldots,l-1]$: The secret key of l bytes.

$K[0,\ldots,N-1]$: $K[i] = key[i \bmod l]$.

i : Deterministic index.

j : Pseudorandom index.

All additions are additions modulo N.

Key Scheduling Algorithm (KSA)

Initialization:

$$\text{For } i = 0, \ldots, N-1$$
$$S[i] = i;$$
$$j = 0;$$

Scrambling:

$$\text{For } i = 0, \ldots, N-1$$
$$j = j + S[i] + K[i];$$
$$\text{Swap}(S[i], S[j]);$$

Pseudo-Random Generation Algorithm (PRGA)

$Initialization:$

$$i = j = 0;$$

$Output\ Keystream\ Generation\ Loop:$

$$i = i + 1$$

$$j = j + S[i];$$

$$\mathrm{Swap}(S[i], S[j]);$$

$$t = S[i] + S[j];$$

$$\mathrm{Output}\ z = S[t];$$

Related Work
and Contribution

Important Existing Results

- Roos (sci.crypt 1995) observed some correlation between
  - the permutation bytes $S[y]$ and some functions $f[y]$ of the secret key bytes
  - the first keystream byte z_1 and the initial key bytes subject to some conditions

- G. Paul and S. Maitra (SAC 2007) proved
  - the above empirical observations of Roos
  - that such weakness is *intrinsic* to the KSA

- G. Paul, S. Rathi and S. Maitra (WCC 2007) showed
  - a new bias of the first output byte z_1 towards the first three secret key bytes

Important Existing Results …*contd*

- Fluhrer, Mantin and Shamir (SAC 2001)
  - the invariance weakness, known-IV attack and related key attack
- Mantin (Asiacrypt 2005)
  - using above, showed secret key leakage at the 257-th keystream output byte
- Mantin and Shamir (FSE 2001)
  - a bias in the second output byte, namely, bias of $z_2 = 0$
- S. Paul and Preneel (FSE 2004)
  - a bias in the equality of the first two output bytes, i.e., bias of $z_1 = z_2$
- Klein (Draft 2006) and Tews *et. al.* (Eprint 2007/120)
  - bias in the initial keystream bytes z_r towards the functions $f[r]$ of the secret key bytes

Our Contributions

1. A new form of bias:

   $S[S[y]]$ with functions $f[y]$ of the secret key bytes

2. A general framework for identifying biases in the keystream bytes and use it to find

   (a) Biases at the 256th and 257th keystream output bytes
   (difference with *Mantin,2005*: no conditions on the secret key and IV)

   (b) New biases in the initial keystream output bytes, namely, biases of z_r towards the functions $f[r-1]$
   (a new type, completely different from *Klein, 2006* and *Tews, 2007*)

3. Propagation of biases beyond 257th rounds of PRGA:

   Chain-like propagation, if j is known

Bias in the Permutation

Our Notations

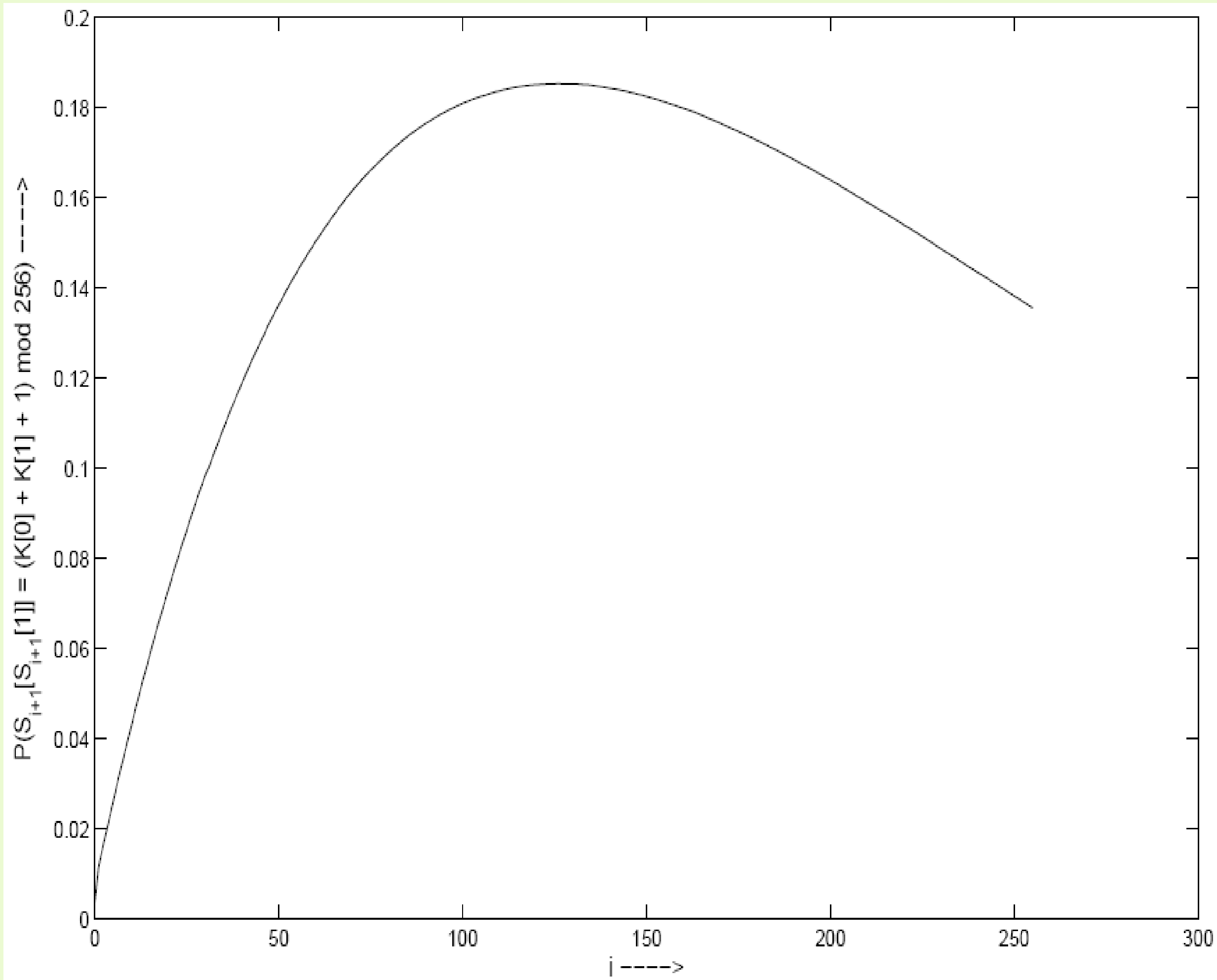
S_r : Permutation after the r-th round of the KSA, $1 \le r \le N$.

Note that $r = i + 1,\ 0 \le i \le N - 1$.

S_0 : The initial (typically, identity) permutation.

$$f_y = \frac{y(y+1)}{2} + \sum_{x=0}^{y} K[x],\ 0 \le y \le N - 1.$$

How $P(S_r[S_r[1]] = f_1)$ Changes with KSA Rounds r, $1 \leq r \leq N$



After the 2nd Round of KSA

Lemma 1:

(a) $P\left(S_2\left[S_2[1]\right] = f_1\right) = \frac{3}{N} - \frac{4}{N^2} + \frac{2}{N^3}.$

(b) $P\left(\left(S_2\left[S_2[1]\right] = f_1\right) \wedge \left(S_2[1] \leq 1\right)\right) \approx \frac{2}{N}.$

Note that $f_1 = K[0] + K[1] + 1.$

Recursion

Lemma 2:

Let $p_r = P\left(\left(S_r[S_r[1]] = f_1\right) \wedge \left(S_r[1] \le r-1\right)\right)$, for $r \ge 2$.

Then for $r \ge 3$,

$$p_r = \left(\frac{N-2}{N}\right) p_{r-1} + \frac{1}{N}\left(\frac{N-2}{N}\right)\left(\frac{N-1}{N}\right)^{2(r-2)}.$$

After the Complete Key Scheduling

Theorem 1:

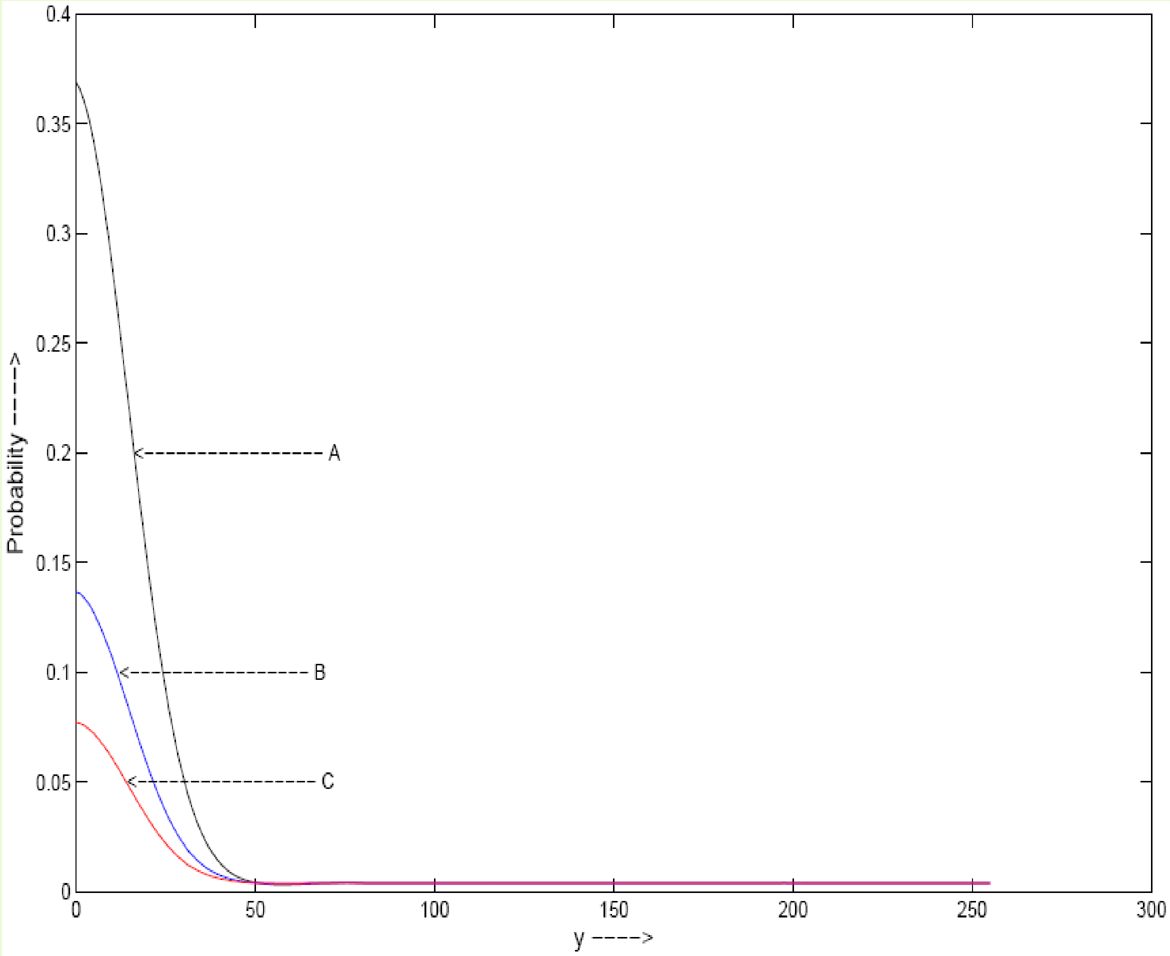
$$P\left(S_N\left[S_N[1]\right] = K[0] + K[1] + 1\right)$$

$$= \frac{2}{N}\left(\frac{N-1}{N}\right)^{2(N-2)} + \left(\frac{N-2}{N}\right)\left(\frac{N-1}{N}\right)^{2(N-1)}$$

$$\approx \left(\frac{N-1}{N}\right)^{2(N-1)}.$$

For $N = 256$, this value ≈ 0.136

Generalizations: $P(S_N[y] = f_y)$, $P(S_N[S_N[y]] = f_y)$, $P(S_N[S_N[S_N[y]]] = f_y)$ vs. y



Result for Two Levels of Nesting

Theorem 2:

For $0 \le y \le 31$, $P\left(S_N\left[S_N[y]\right] = f_y\right)$

$$\approx \frac{y}{N}\left(\frac{N-1}{N}\right)^{\frac{y(y+1)}{2}+2(N-2)} + \frac{1}{N}\left(\frac{N-1}{N}\right)^{\frac{y(y+1)}{2}-y+2(N-1)}$$

$$+\left(\frac{N-y-1}{N}\right)\left(\frac{N-y}{N}\right)\left(\frac{N-1}{N}\right)^{\frac{y(y+1)}{2}+2N-3}.$$

Where Does It Lead to

- In a similar manner, the association of $S_N[S_{N...}[S_N[y]]...]$ and f_y can be studied
- These results are combinatorially interesting
- Cryptanalytic implications are not immediate, but possible
- We use the nonrandom association of $S_N[S_N[1]]$ with $f[1]$ to find a new bias at the 257^{th} keystream byte z_{257}

Key Leakage in the Keystream

Some More Notations

S_r^G : Permutation after the r-th round of the PRGA, $r \geq 1$.

i_r^G and j_r^G : The indices after the r-th round of the PRGA, $r \geq 1$.

S_0^G : Permutation before the PRGA

(i.e., the permutation S_N after the KSA).

z_r : Keystream output byte after the r-th round of the PRGA, $r \geq 1$.

Recall: $f_y = \frac{y(y+1)}{2} + \sum_{x=0}^{y} K[x], 0 \leq y \leq N-1.$

Existing Results Needed

Proposition 1 (Paul and Maitra, SAC 2007):

$$P\left(S_N[y] = f_y\right) \approx \left(\frac{N-y}{N}\right)\left(\frac{N-1}{N}\right)^{\frac{y(y+1)}{2}+N} + \frac{1}{N}, 0 \le y \le N-1.$$

Proposition 2 (Jenkins, 1996):

$$P\left(z_r = r - S_{r-1}^G\left[i_r^G\right]\right) = \frac{2}{N}, r \ge 1.$$

Framework for New Biases

Lemma 3:

Let $P\left(S_t^G\left[i_r^G\right]=X\right)=q_{t,r}$ for some X. Then for $t+2\le r\le t+N$,

$$P\left(S_{r-1}^G\left[i_r^G\right]=X\right)=q_{t,r}\left[\left(\frac{N-1}{N}\right)^{r-t-1}-\frac{1}{N}\right]+\frac{1}{N}.$$

Corollary 2:

For $2\le r\le N-1$,

$$P\left(S_{r-1}^G[r]=f_r\right)=\left[\left(\frac{N-r}{N}\right)\left(\frac{N-1}{N}\right)^{\frac{r(r+1)}{2}+N}+\frac{1}{N}\right]\left[\left(\frac{N-1}{N}\right)^{r-1}-\frac{1}{N}\right]+\frac{1}{N}.$$

Framework for New Biases …*contd*

Lemma 4:

$$\text{Let } P\left(S_{r-1}^{G}\left[i_r^G\right] = f_{i_r^G}\right) = w_r,\ r \geq 1. \text{ Then}$$

$$P\left(z_r = r - f_{i_r^G}\right) = \frac{1}{N}\left(1 + w_r\right),\ r \geq 1.$$

Bias in the Initial Keystream Bytes

Theorem 3:

(1) $$P\left(z_1 = 1 - f_1\right) = \frac{1}{N}\left(1 + \left(\frac{N-1}{N}\right)^{N+2} + \frac{1}{N}\right).$$

(2) For $2 \le r \le N-1$,

$$P\left(z_r = r - f_r\right) = \frac{1}{N}\left(1 + \left[\left(\frac{N-r}{N}\right)\left(\frac{N-1}{N}\right)^{\frac{r(r+1)}{2}+N} + \frac{1}{N}\right]\left[\left(\frac{N-1}{N}\right)^{r-1} - \frac{1}{N}\right] + \frac{1}{N}\right).$$

Probability Values Given by Theorem 3

r	$P(z_r = r - f_r)$							
1-8	0.0053	0.0053	0.0053	0.0053	0.0052	0.0052	0.0052	0.0051
9-16	0.0051	0.0050	0.0050	0.0049	0.0048	0.0048	0.0047	0.0047
17-24	0.0046	0.0046	0.0045	0.0045	0.0044	0.0044	0.0043	0.0043
25-32	0.0043	0.0042	0.0042	0.0042	0.0041	0.0041	0.0041	0.0041
33-40	0.0041	0.0040	0.0040	0.0040	0.0040	0.0040	0.0040	0.0040
41-48	0.0040	0.0040	0.0040	0.0040	0.0040	0.0039	0.0039	0.0039

Bias in the 256th Keystream Byte

Theorem 4:

$$P(z_N = N - f_0) = \frac{1}{N}\left(1 + \left(\frac{N-1}{N}\right)^{2N-1} + \frac{1}{N^2}\left(\frac{N-1}{N}\right)^{N-1} - \frac{1}{N^2} + \frac{1}{N}\right).$$

For $N = 256$, this value ≈ 0.0045.

Bias in the 257th Keystream Byte

Theorem 5:

$$P\left(z_{N+1} = N+1- f_1\right) = \frac{1}{N}\left(1+\left(\frac{N-1}{N}\right)^{3(N-1)} - \frac{1}{N}\left(\frac{N-1}{N}\right)^{2(N-1)} + \frac{1}{N}\right).$$

For $N = 256$, this value ≈ 0.0041.

More New Types of Biases in the Initial Keystream Bytes

Theorem 6:

For $3 \le r \le N$, $P(z_r = f_{r-1})$

$$= \left(\frac{N-1}{N}\right)\left(\frac{N-r}{N}\right)\left(\left(\frac{N-r+1}{N}\right)\left(\frac{N-1}{N}\right)^{\frac{r(r-1)}{2}+r} + \frac{1}{N}\right).$$

$$\left(\frac{N-2}{N}\right)^{N-r+1}\left(\frac{N-3}{N}\right)^{r-2}\eta_r + \frac{1}{N},$$

where $\eta_r = \frac{1}{N}\left(\frac{N-1}{N}\right)^{N-r-1} + \frac{1}{N}\left(\frac{N-1}{N}\right) - \frac{1}{N}\left(\frac{N-1}{N}\right)^{N-r}.$

Probability Values Given by Theorem 6

r	$P(z_r = f_{r-1})$							
1-8	0.0043	0.0039	0.0044	0.0044	0.0044	0.0044	0.0043	0.0043
9-16	0.0043	0.0043	0.0043	0.0042	0.0042	0.0042	0.0042	0.0042
17-24	0.0041	0.0041	0.0041	0.0041	0.0041	0.0040	0.0040	0.0040
25-32	0.0040	0.0040	0.0040	0.0040	0.0040	0.0040	0.0040	0.0040
33-40	0.0039	0.0039	0.0039	0.0039	0.0039	0.0039	0.0039	0.0039
41-48	0.0039	0.0039	0.0039	0.0039	0.0039	0.0039	0.0039	0.0039

Further Biases if *j* is known

- Assume that j_t^G is known after round t
- The value V at index j_t^G remains there with high probability until j_t^G is touched by i for the first time after a few more rounds
- This immediately leaks V in the keystream output byte
- Key leaked, if V is biased to the secret key

Example of Such Biases

- Suppose, we know that $j_5^G=18$
- With probability β_5 (given by Corollary 2), $S_4^G[5]$ would have remained f_5 which would move to index 18 due to the swap in round 5, i.e., $S_5^G[18]= f_5$
- With approx. $\beta_5\,[((N\text{-}1)/N)^{18\text{-}5\text{-}1} - 1/N] + 1/N$ probability (by Lemma 3), f_5 would remain in index 18 till the end of round 18-1=17
- So (by Lemma 4) we get a bias at z_{18} with $18\text{-}f_5$

Example …*contd*

- Moreover, in round 18, f_5 would move from index 18 to j_{18}^G
- If (in addition to j_5^G) the value of j_{18}^G is also known, say $j_{18}^G = 3$, then we would have $S_{18}^G[3]= f_5$
- Applying the same line of arguments for round 256+3 = 259, we get a bias of z_{259} with 259-f_5
- Experiments with 1 billion random keys demonstrate that in this scenario, the bias of z_{18} towards 18-f_5 is 0.0052 and the bias of z_{259} towards 259-f_5 is 0.0044 (which conform to theoretical values)

CONCLUSION

- We present several new observations on the weaknesses of RC4
- This is the first attempt to formally analyze biases of $S[S[y]]$ towards the secret key
- We use the above bias (at $y = 1$) to obtain a new bias in the keystream towards the secret key beyond the first 256 rounds of the PRGA
- We also discover another new set of biases in the first 32 keystream bytes towards the secret key
- We analyze how these biases propagate further down the keystream, if j is known at some stage of the PRGA