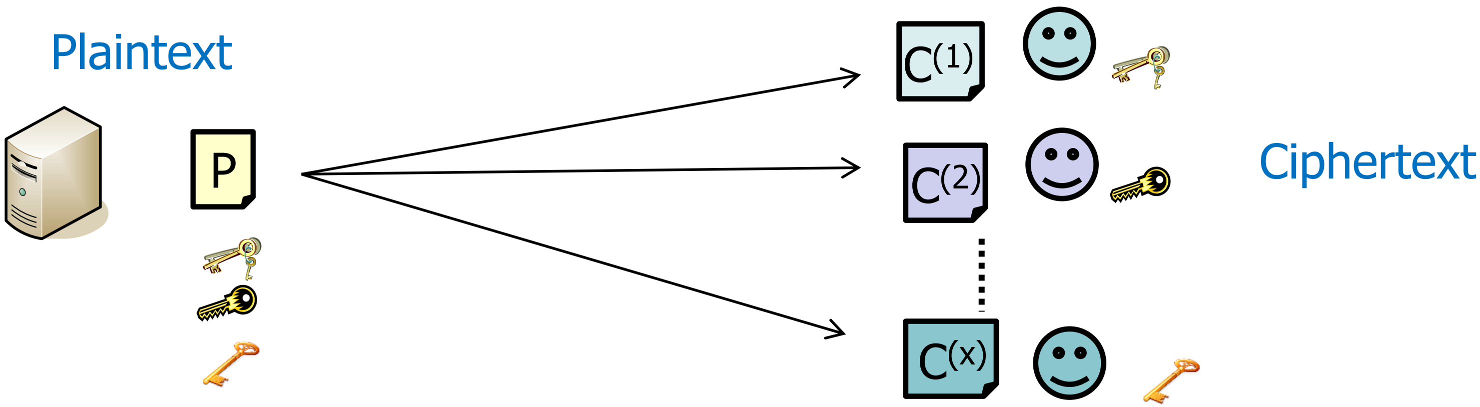
11 March, 2013
FSE 2013 @ Singapore

Full Plaintext Recovery Attack on Broadcast RC4

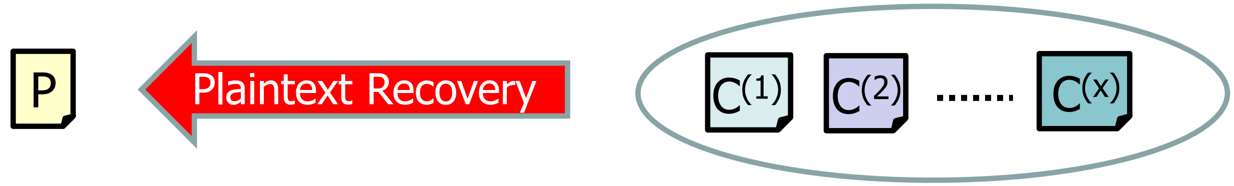
Takanori Isobe (Kobe University)
Toshihiro Ohigashi (Hiroshima University)
Yuhei Watanabe (Kobe University)
Masakatu Morii (Kobe University)

Target

- Broadcast setting
  - Same plaintext is encrypted with different (user) keys
    - Example : Group mail, multi session (SSL/TLS)



- Plaintext Recovery Attack in the broadcast setting
  - Recover the plaintext from ONLY ciphertexts encrypted by different keys
  - Passive attack
    - What attacker do is to collect ciphertexts.
    - NOT use additional information such as side channel information.



Summary of Our Results

Practical Security Evaluation of RC4 in the Broadcast Setting

Results

Efficient plaintext recovery attack in the first 257 bytes

- Based on strong biases set of the first 257 bytes including new biases
- Given 2^{32} ciphertexts with different keys, any byte of first 257 bytes of the plaintext are recovered with probability of more than 0.5.

2^{32} ciphertexts

Any byte of the first 257 bytes

Sequential plaintext recovery attack after 258 bytes

- Combine use of our bias set and Mantin's long term bias in EUROCRYPT 2005
- Given 2^{34} ciphertexts with different keys, contiguous 1000 T bytes of the plaintext are recovered with probability of 0.99

2^{34} ciphertexts

Contiguous First 1000 T bytes

Agenda

- RC4 Stream Cipher
- Known Plaintext Recovery Attacks
- Efficient Plaintext Recovery Attack of the first 257 bytes
- Sequential plaintext recovery attack after 258 bytes
- Conclusion

RC4

- Stream Cipher designed by Ron Rivest in 1987
  - One of most famous stream ciphers
    - Used in SSL/TLS, WEP/WPA and more.
- Parameter
  - 1-256 byte key (typically 16 byte (=128 bit) key)
  - State size N bytes (typically N = 256)

We focus on
- 16 byte (128 bit) key
- 256 byte state

Key → Key Scheduling Algorithm (KSA) → State → Pseudo Random Generator Algorithm (PRGA) → $Z_1, Z_2, \ldots$ Keystream

- Cryptanalysis
  - State Recovery attacks [KMPRV+98, MK08]
  - Distinguish attacks [FM00, M'05, SVV10, SMPS12]
  - Plaintext Recovery attacks [MS01, MPS11, SMPS12]
  - Other attacks
    - Key Collision [M'09, CM12]
    - Key Recovery from Internal State [SM07,BC08]

RC4

- Stream Cipher designed by Ron Rivest in 1987
  - One of most famous stream ciphers
    - Used in SSL/TLS, WEP/WPA and more.
- Parameter
  - 1-256 byte key (typically 16 byte (=128 bit) key)
  - State size N bytes (typically N = 256)

We focus on
- 16 byte (128 bit) key
- 256 byte state

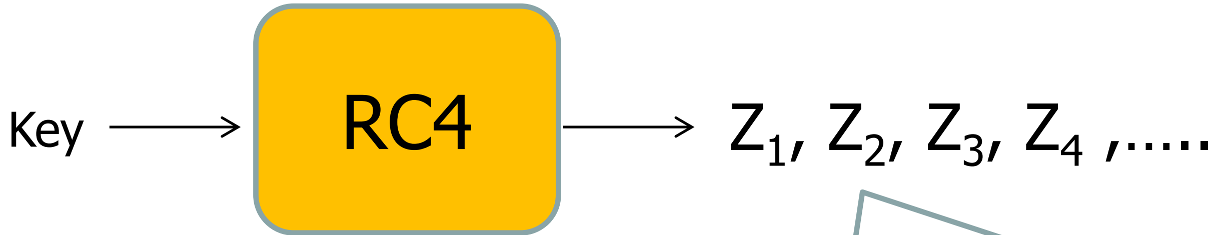
Key → Key Scheduling Algorithm (KSA) → State → Pseudo Random Generator Algorithm (PRGA) → $Z_1, Z_2, \ldots$ Keystream

- Cryptanalysis
  - State Recovery attacks [KMPRV+98, MK08]
  - Distinguish attacks [FM00, M'05, SVV10, SMPS12]
  - Plaintext Recovery attacks [MS01, MPS11, SMPS12]
  - Other attacks
    - Key Collision [M'09, CM12]
    - Key Recovery from Internal State [SM07,BC08]

Known Plaintext Recovery Attacks

Mantin-Shamir Attack [MS01]

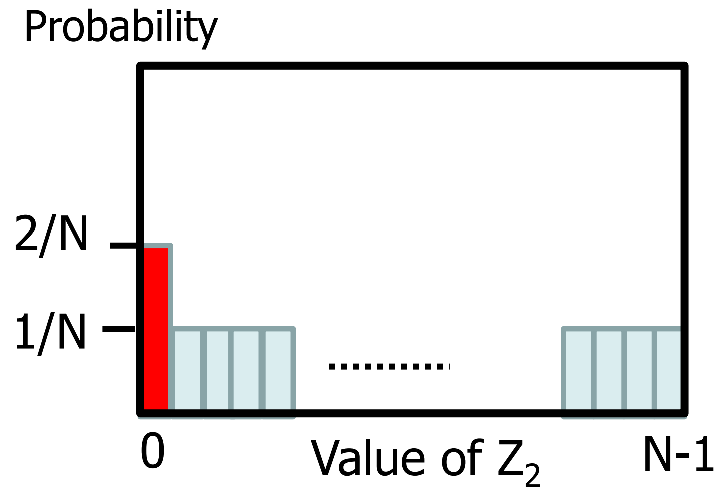
- Proposed in FSE 2001 [MS01]
- Second byte of the keystream is strongly biased to “0”



$Z_2 = 0$ occurs with twice the probability of a random one.

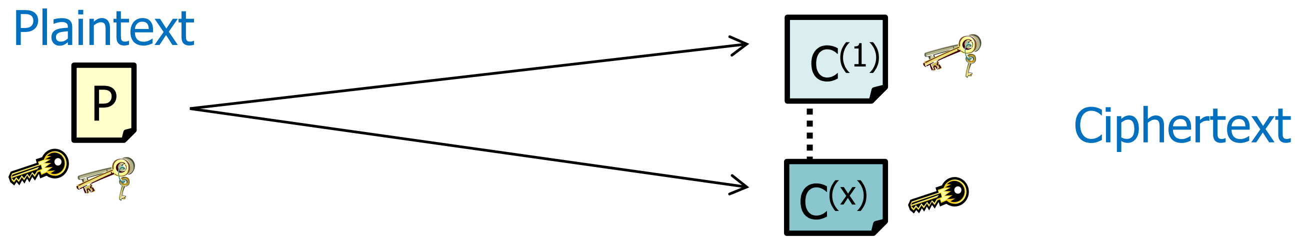
Ex.) $N = 256$,

$Pr(Z_2 = 0) = 2/256$



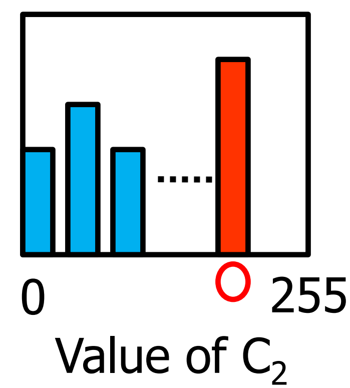
Plaintext Recovery Attack [MS01]

- **Broadcast setting** : same plaintext is encrypted with different keys



- **Relation** : "$C_2 = P_2$ XOR Z_2"
  - If $Z_2 = 0$ (strong bias), then $C_2 = P_2$
  - Most frequent value of C_2 can be regarded as P_2

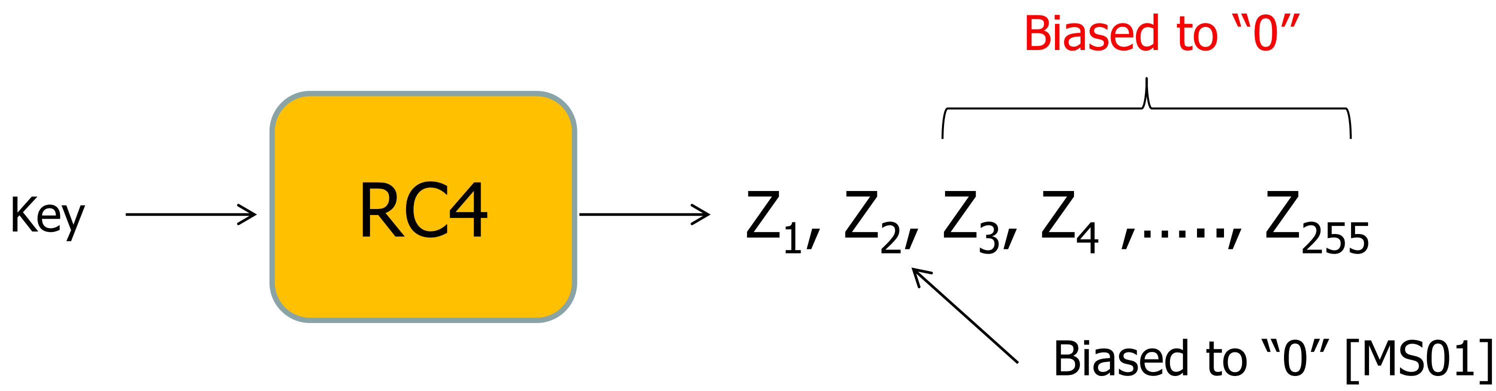
Frequency Table of C_2



- **Evaluation**
  - Given Ω (N) ciphertexts encrypted by different keys, P_2 can be extracted with high probability.

Maitra-Paul-Sen Gupta Attack [MPS11, SMPS12]

- Proposed in FSE 2011 (later improved in JoC [SMPS12])
- $Z_3 - Z_{255}$ are also biased to "0"
  - Exploit biases of the state after KSA



- Plaintext Recovery Attack in the Broadcast setting
  - $\Omega(N^3)$ ciphertexts encrypted by different keys allow us to extract $P_3, \ldots, P_{255}$ with high probability

Our Questions

- Biases of $Z_r = 0$ ($2<r<256$) are strongest biases for the initial bytes 1 to 255?
- While the previous results [MS01, MSP11] estimate only lower bounds (Ω), how many ciphertexts encrypted with different keys are actually required for a practical attack on broadcast RC4?
- Is it possible to efficiently recover the later bytes of the plaintext, after byte 256?

Our Questions

- Biases of $Z_r = 0$ ($2<r<256$) are strongest biases for the initial bytes 1 to 255?
- While the previous results [MS01, MSP11] estimate only lower bounds (Ω), how many ciphertexts encrypted with different keys are actually required for a practical attack on broadcast RC4?
- Is it possible to efficiently recover the later bytes of the plaintext, after byte 256?

We provide all answers to these questions

Our Questions

- Biases of $Z_r = 0$ ($2<r<256$) are strongest biases for the initial bytes 1 to 255?

- While the previous results [MS01, MSP11] estimate only lower bounds (Ω), how many ciphertexts encrypted with different keys are actually required for a practical attack on broadcast RC4?

- Is it possible to efficiently recover the later bytes of the plaintext, after byte 256?

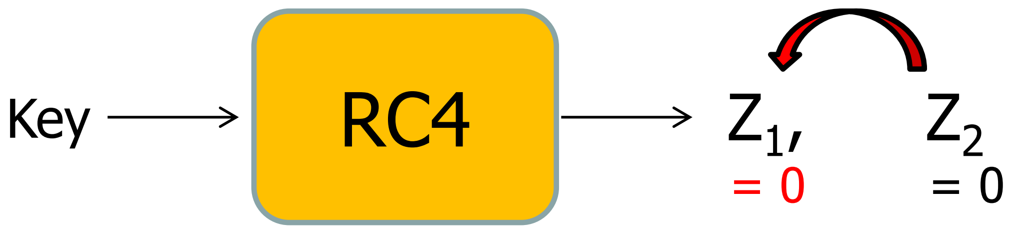
We provide all answers to these questions

New Strong Biases in the initial bytes

We show four new biases, which are stronger than $Z_r = 0$, with theoretical reasons.

New Strong Biases in the initial bytes

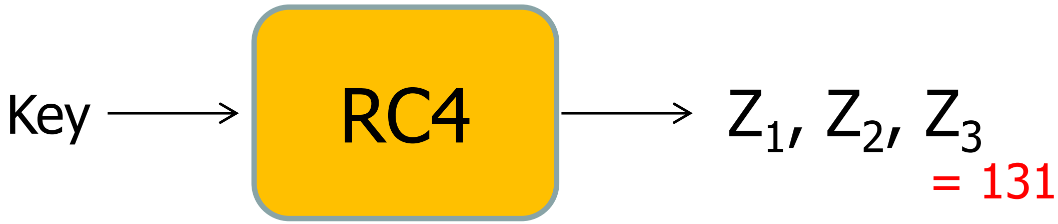
We show four new biases, which are stronger than $Z_r = 0$, with theoretical reasons.



- **Conditional bias regarding Z_1**
  - When $Z_2 = 0$, Z_1 is strongly biased to "0"
  - $\Pr(Z_1 = 0 \mid Z_2 = 0) = 2^{-8} (1 + 2^{-0.996})$
  - Similar biases was proposed by Fluhrer and McGrew as along term bias [FM00] but our bias is stronger than it.

New Strong Biases in the initial bytes

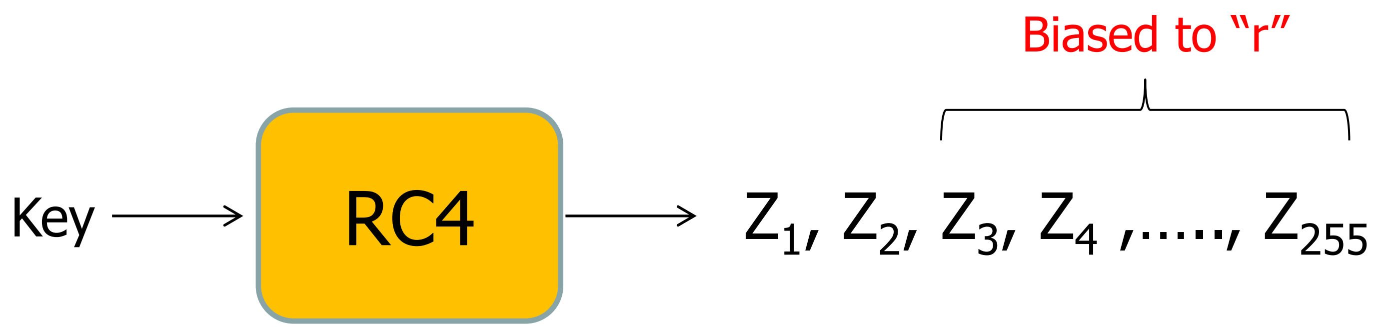
We show four new biases, which are stronger than $Z_r = 0$, with theoretical reasons.



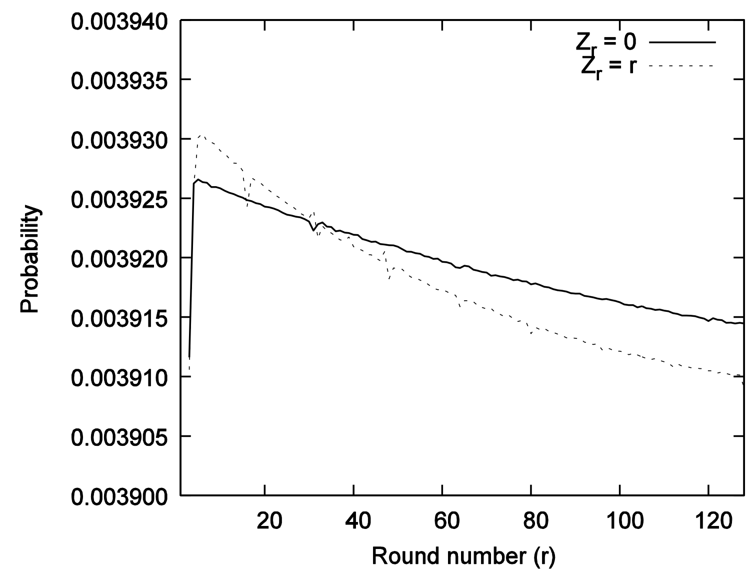
- **$Z_3 = 131$**
  - Strongest biases in Z_3
    - $\Pr(Z_3 = 0) = 2^{-8}(1 + 2^{-9.512})$ [MSP11]
    - $\Pr(Z_3 = 131) = 2^{-8}(1 + 2^{-8.089})$

New Strong Biases in the initial bytes

We show four new biases, which are stronger than $Z_r = 0$, with theoretical reasons.

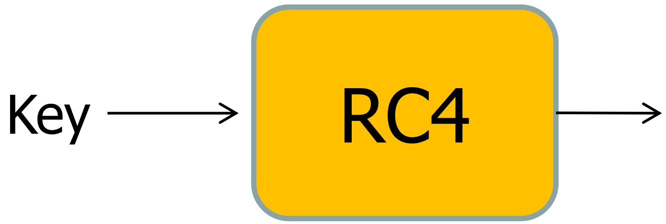


- **$Z_r = r$ $(3 \leqq r \leqq 255)$**
  - Occur in 3 to 255 bytes similar to $Z_r = 0$
    - Stronger than $Z_r = 0$ for $5 \leqq r \leqq 31$



New Strong Biases in the initial bytes

We show four new biases, which are stronger than $Z_r = 0$, with theoretical reasons.



$Z_1, .., Z_{16}, .., Z_{32}, .., Z_{48}, .., Z_{64}, .., Z_{80}, .., Z_{96}, .., Z_{112}$

=-16 [SVV10] =-32 =-48 =-64 =-80 =-96 =-112

- **Extended key length dependent bias**
  - A extension of key-length dependent biases s.t. $Z_l = -l$ (l : key length in byte) [SVV10, SMPS12]
  - $Z_{l \cdot x} = -l \cdot x$ for $x = 2, 3, 4, 5, 6, 7$ ($l = 16$)

Other new biases

We also experimentally found other two biases regarding "0" but there are no theoretical reasons.

Key → RC4 → $Z_1, Z_2, .., Z_{255}, Z_{256}, Z_{257}$

$=0$ $=0$

Negative

- **$Z_{256} = 0$**
  - Negative biases
  - $Pr(Z_{256} = 0) = 2^{-8}(1 - 2^{-9.407})$

- **$Z_{257} = 0$**
  - $Pr(Z_{256} = 0) = 2^{-8}(1 + 2^{-9.531})$

Six new biases, which is stronger than $Z_r = 0$, were found!

Cumulative list of strong biases

- Construct a set of known strongest biases in the first 257 bytes when a 128 bit key is used.
  - Consist of (non-conditional) strongest biases of each bytes except Z_1
    - We experimentally confirmed that these value are most/least frequency values of each bytes.

r	Strongest known bias of Z_r	Prob.(Theoretical)[4]	Prob.(Experimental)
1	$Z_1 = 0 \| Z_2 = 0$ (Our)	$2^{-8} \cdot (1+2^{-1.009})$	$2^{-8} \cdot (1+2^{-1.036})$
2	$Z_2 = 0$ [11]	$2^{-8} \cdot (1+2^{0})$	$2^{-8} \cdot (1+2^{0.002})$
3	$Z_3 = 131$ (Our)	$2^{-8} \cdot (1+2^{-8.089})$	$2^{-8} \cdot (1+2^{-8.109})$
4	$Z_4 = 0$ [8]	$2^{-8} \cdot (1+2^{-7.581})$	$2^{-8} \cdot (1+2^{-7.611})$
5–15	$Z_r = r$ (Our)	max: $2^{-8} \cdot (1+2^{-7.627})$ min: $2^{-8} \cdot (1+2^{-7.737})$	max: $2^{-8} \cdot (1+2^{-7.335})$ min: $2^{-8} \cdot (1+2^{-7.535})$
16	$Z_{16} = 240$ [5]	$2^{-8} \cdot (1+2^{-4.671})$	$2^{-8} \cdot (1+2^{-4.811})$
17–31	$Z_r = r$ (Our)	max: $2^{-8} \cdot (1+2^{-7.759})$ min: $2^{-8} \cdot (1+2^{-7.912})$	max: $2^{-8} \cdot (1+2^{-7.576})$ min: $2^{-8} \cdot (1+2^{-7.839})$
32	$Z_{32} = 224$ (Our)	$2^{-8} \cdot (1+2^{-5.176})$	$2^{-8} \cdot (1+2^{-5.383})$
33–47	$Z_r = 0$ [8]	max: $2^{-8} \cdot (1+2^{-7.897})$ min: $2^{-8} \cdot (1+2^{-8.050})$	max: $2^{-8} \cdot (1+2^{-7.868})$ min: $2^{-8} \cdot (1+2^{-8.039})$
48	$Z_{48} = 208$ (Our)	$2^{-8} \cdot (1+2^{-5.651})$	$2^{-8} \cdot (1+2^{-5.938})$
49–63	$Z_r = 0$ [8]	max: $2^{-8} \cdot (1+2^{-8.072})$ min: $2^{-8} \cdot (1+2^{-8.224})$	max: $2^{-8} \cdot (1+2^{-8.046})$ min: $2^{-8} \cdot (1+2^{-8.238})$
64	$Z_{64} = 192$ (Our)	$2^{-8} \cdot (1+2^{-6.085})$	$2^{-8} \cdot (1+2^{-6.496})$
65–79	$Z_r = 0$ [8]	max: $2^{-8} \cdot (1+2^{-8.246})$ min: $2^{-8} \cdot (1+2^{-8.398})$	max: $2^{-8} \cdot (1+2^{-8.223})$ min: $2^{-8} \cdot (1+2^{-8.376})$
80	$Z_{80} = 176$ (Our)	$2^{-8} \cdot (1+2^{-6.574})$	$2^{-8} \cdot (1+2^{-7.224})$
81–95	$Z_r = 0$ [8]	max: $2^{-8} \cdot (1+2^{-8.420})$ min: $2^{-8} \cdot (1+2^{-8.571})$	max: $2^{-8} \cdot (1+2^{-8.398})$ min: $2^{-8} \cdot (1+2^{-8.565})$
96	$Z_{96} = 160$ (Our)	$2^{-8} \cdot (1+2^{-6.970})$	$2^{-8} \cdot (1+2^{-7.911})$
97–111	$Z_r = 0$ [8]	max: $2^{-8} \cdot (1+2^{-8.592})$ min: $2^{-8} \cdot (1+2^{-8.741})$	max: $2^{-8} \cdot (1+2^{-8.570})$ min: $2^{-8} \cdot (1+2^{-8.722})$
112	$Z_{112} = 144$ (Our)	$2^{-8} \cdot (1+2^{-7.300})$	$2^{-8} \cdot (1+2^{-8.666})$
113–255	$Z_r = 0$ [8]	max: $2^{-8} \cdot (1+2^{-8.763})$ min: $2^{-8} \cdot (1+2^{-10.052})$	max: $2^{-8} \cdot (1+2^{-8.760})$ min: $2^{-8} \cdot (1+2^{-10.041})$
256	$Z_r = 0$(*negative bias*) (Our)	N/A	$2^{-8} \cdot (1-2^{-9.407})$
257	$Z_r = 0$ (Our)	N/A	$2^{-8} \cdot (1+2^{-9.531})$

Cumulative list of strong biases

- Construct a set of known strongest biases in the first 257 bytes when a 128 bit key is used.
  - Consist of (non-conditional) strongest biases of each bytes except Z_1
    - We experimentally confirmed that these value are most/least frequency values of each bytes.

r	Strongest known bias of Z_r	Prob.(Theoretical)[4]	Prob.(Experimental)
1	$Z_1 = 0 \| Z_2 = 0$ (Our)	$2^{-8} \cdot (1 + 2^{-1.009})$	$2^{-8} \cdot (1 + 2^{-1.036})$
2	$Z_2 = 0$ [11]	$2^{-8} \cdot (1 + 2^{0})$	$2^{-8} \cdot (1 + 2^{0.002})$
3	$Z_3 = 131$ (Our)	$2^{-8} \cdot (1 + 2^{-8.089})$	$2^{-8} \cdot (1 + 2^{-8.109})$
4	$Z_4 = 0$ [8]	$2^{-8} \cdot (1 + 2^{-7.581})$	$2^{-8} \cdot (1 + 2^{-7.611})$
5–15	$Z_r = r$ (Our)	max: $2^{-8} \cdot (1 + 2^{-7.627})$ min: $2^{-8} \cdot (1 + 2^{-7.737})$	max: $2^{-8} \cdot (1 + 2^{-7.335})$ min: $2^{-8} \cdot (1 + 2^{-7.535})$
16	$Z_{16} = 240$ [5]	$2^{-8} \cdot (1 + 2^{-4.671})$	$2^{-8} \cdot (1 + 2^{-4.811})$
		min: $2^{-8} \cdot (1 + 2^{-8.050})$	min: $2^{-8} \cdot (1 + 2^{-8.039})$
48	$Z_{48} = 208$ (Our)	$2^{-8} \cdot (1 + 2^{-5.651})$	$2^{-8} \cdot (1 + 2^{-5.938})$
49–63	$Z_r = 0$ [8]	max: $2^{-8} \cdot (1 + 2^{-8.072})$ min: $2^{-8} \cdot (1 + 2^{-8.224})$	max: $2^{-8} \cdot (1 + 2^{-8.046})$ min: $2^{-8} \cdot (1 + 2^{-8.238})$
64	$Z_{64} = 192$ (Our)	$2^{-8} \cdot (1 + 2^{-6.085})$	$2^{-8} \cdot (1 + 2^{-6.496})$
65–79	$Z_r = 0$ [8]	max: $2^{-8} \cdot (1 + 2^{-8.246})$ min: $2^{-8} \cdot (1 + 2^{-8.398})$	max: $2^{-8} \cdot (1 + 2^{-8.223})$ min: $2^{-8} \cdot (1 + 2^{-8.376})$
80	$Z_{80} = 176$ (Our)	$2^{-8} \cdot (1 + 2^{-6.574})$	$2^{-8} \cdot (1 + 2^{-7.224})$
81–95	$Z_r = 0$ [8]	max: $2^{-8} \cdot (1 + 2^{-8.420})$ min: $2^{-8} \cdot (1 + 2^{-8.571})$	max: $2^{-8} \cdot (1 + 2^{-8.398})$ min: $2^{-8} \cdot (1 + 2^{-8.565})$
96	$Z_{96} = 160$ (Our)	$2^{-8} \cdot (1 + 2^{-6.970})$	$2^{-8} \cdot (1 + 2^{-7.911})$
97–111	$Z_r = 0$ [8]	max: $2^{-8} \cdot (1 + 2^{-8.592})$ min: $2^{-8} \cdot (1 + 2^{-8.741})$	max: $2^{-8} \cdot (1 + 2^{-8.570})$ min: $2^{-8} \cdot (1 + 2^{-8.722})$
112	$Z_{112} = 144$ (Our)	$2^{-8} \cdot (1 + 2^{-7.300})$	$2^{-8} \cdot (1 + 2^{-8.666})$
113–255	$Z_r = 0$ [8]	max: $2^{-8} \cdot (1 + 2^{-8.763})$ min: $2^{-8} \cdot (1 + 2^{-10.052})$	max: $2^{-8} \cdot (1 + 2^{-8.760})$ min: $2^{-8} \cdot (1 + 2^{-10.041})$
256	$Z_r = 0$ (*negative bias*) (Our)	N/A	$2^{-8} \cdot (1 - 2^{-9.407})$
257	$Z_r = 0$ (Our)	N/A	$2^{-8} \cdot (1 + 2^{-9.531})$

We can obtain the stronger bias set in the first 257 byte

Our Questions

- Biases of $Z_r = 0$ $(2<r<256)$ are strongest biases for the initial bytes 1 to 255?

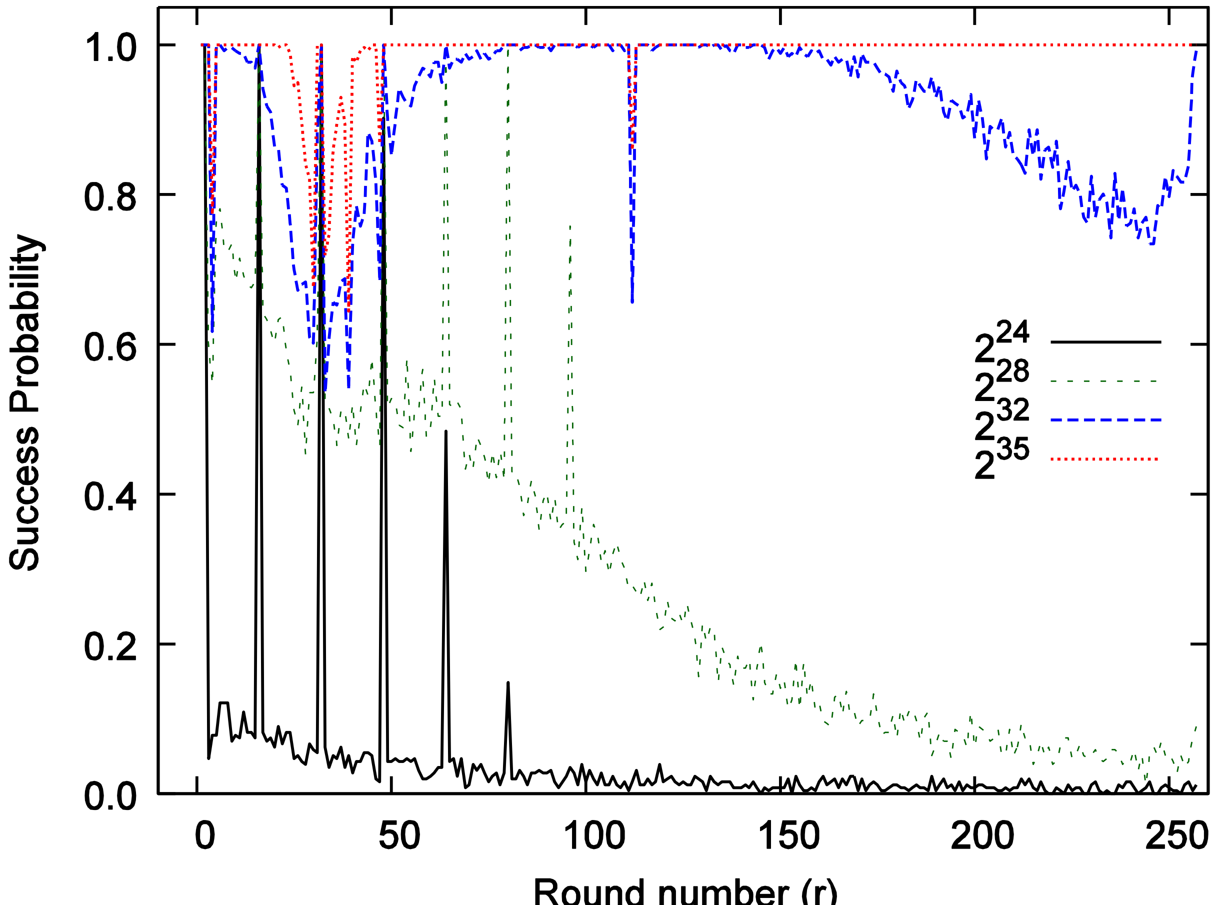
- While the previous results [MS01, MSP11] estimate only lower bounds (Ω), how many ciphertexts encrypted with different keys are actually required for a practical attack on broadcast RC4?

- Is it possible to efficiently recover the later bytes of the plaintext, after byte 256?

We provide all answers to these questions

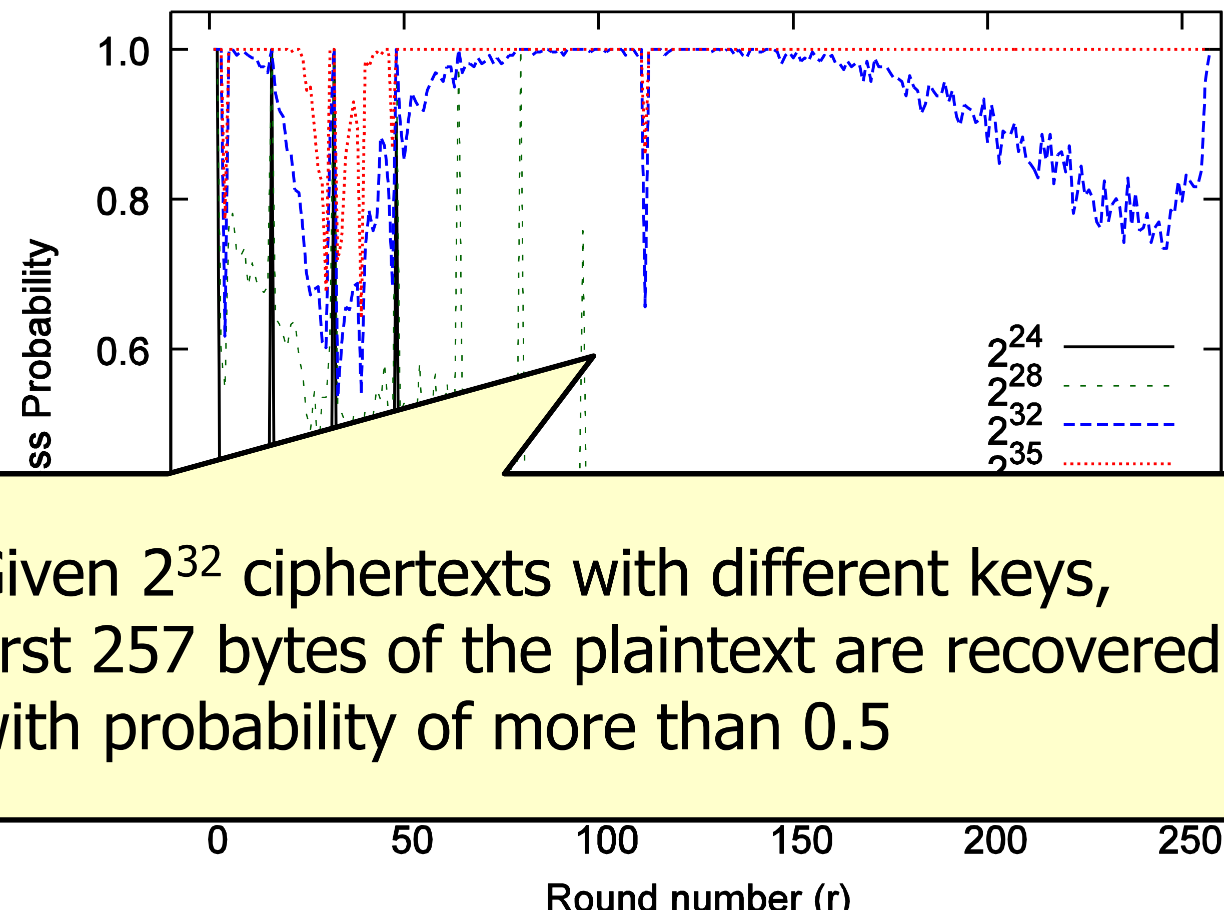
Experimental Results

- We have performed the experiment for in the cases where $2^6, 2^7, \ldots, 2^{35}$ ciphertexts with randomly-chosen keys are given.



Experimental Results

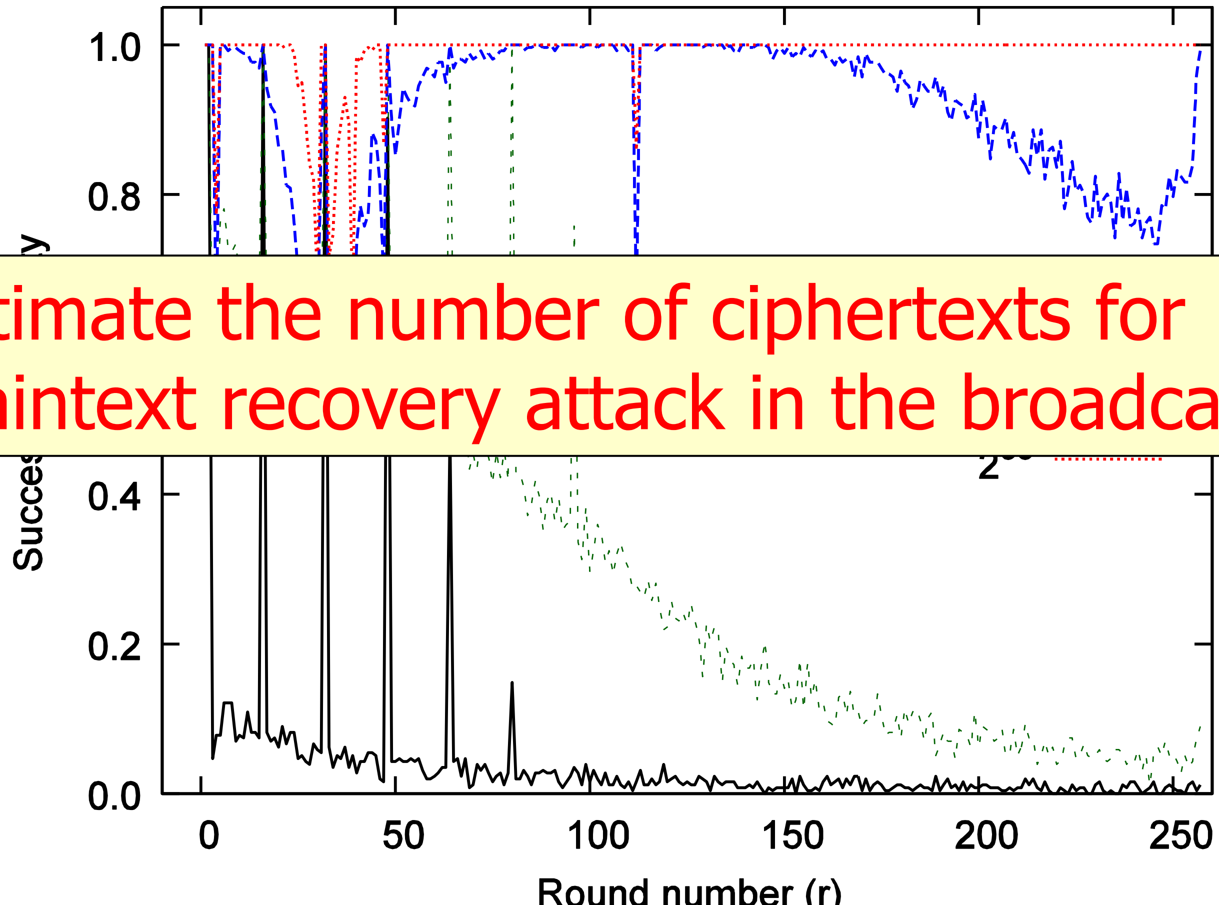
- We have performed the experiment for in the cases where $2^6, 2^7, \ldots, 2^{35}$ ciphertexts with randomly-chosen keys are given.



Given 2^{32} ciphertexts with different keys, first 257 bytes of the plaintext are recovered with probability of more than 0.5

Experimental Results

- We have performed the experiment for in the cases where $2^6, 2^7, . . . , 2^{35}$ ciphertexts with randomly-chosen keys are given.



We estimate the number of ciphertexts for the plaintext recovery attack in the broadcast setting

Our Questions

- Biases of $Z_r = 0$ $(2<r<256)$ are strongest biases for the initial bytes 1 to 255?

- While the previous results [MS01, MSP11] estimate only lower bounds (Ω), how many ciphertexts encrypted with different keys are actually required for a practical attack on broadcast RC4?

- Is it possible to efficiently recover the later bytes of the plaintext, after byte 256?

We provide all answers to these questions

How to Recover Later bytes

- Efficient method using the strong bias set are not directly applicable to later bytes, after Z_{258}.
  - We could not find such strong biases after Z_{258}
- Sequential method
  - Combination of our strong bias set and <u>long term biases</u>

=> occur any position of the keystream

-LSB bias by Golic in EUROCRYPT 1997
-Digraph biases by Fluhrer and McGrew in FSE 2000
-Digraph Repetition Bias by Mantin in EUROCYPT 2005

$$\overbrace{Z_1, Z_2, , \ldots, Z_{256}, Z_{257},}^{\text{Strong bias set}} \quad Z_{258}, \ Z_{259}$$

Long term bias

Digraph Repetition Bias

- Long term Bias
  - Proposed by I. Mantin in EUROCRYPT 2005
  - Known strongest long term bias
  - Same pattern appear after G bytes

Key Stream ....ABHLWECTSDGAB....

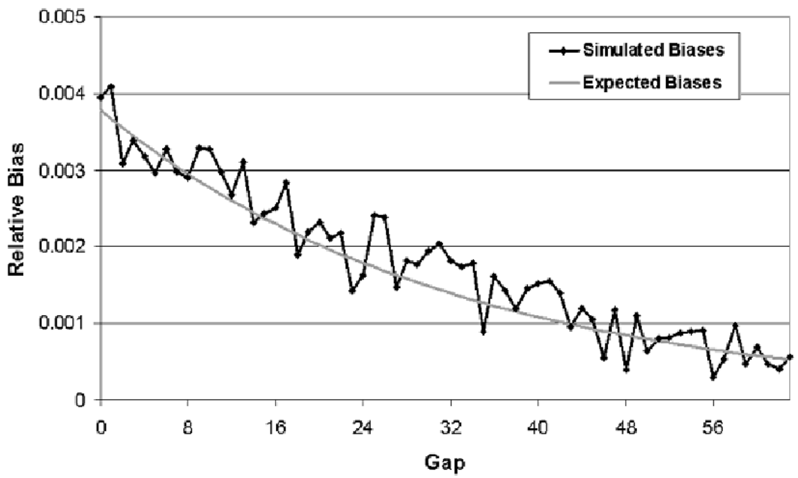
gap G

G=0
G=1
G=2
⋮
G=253

strong
bias
weak

$$Z_t \,||\, Z_{t+1} = Z_{t+2+G} \,||\, Z_{t+3+G}$$

Probability (ideal) : $1/N^2$
Probability (RC4) : $1/N^2 \cdot (1 + p)$



Our Sequential Method

- Algorithm
  - Step 1 : Collect X ciphertexts
  - Step 2 : Set i = 0
  - Step 3 : Obtain candidates of $P_1, \ldots, P_{257+i}$ by using our strong bias set
  - Step 4 : Guess P_{258+i} by using digraph biases for G = 1,…,63
  - Step 5 : Increment i and Repeat 3 and 4

$\boxed{P_1, P_2, , \ldots, P_{256}, P_{257},}$ $P_{258}, P_{259}, P_{260}, P_{261}$

Strong bias set
(step 3)

Our Sequential Method

- Algorithm
  - Step 1 : Collect X ciphertexts
  - Step 2 : Set i = 0
  - Step 3 : Obtain candidates of $P_1, \ldots, P_{257+i}$ by using our strong bias set
  - Step 4 : Guess P_{258+i} by using digraph biases for G = 1,…,63
  - Step 5 : Increment i and Repeat 3 and 4

$\boxed{P_1, P_2, , \ldots, P_{256}, P_{257},}\ P_{258},\ P_{259},\ P_{260},\ P_{261}$

Strong bias set
(step 3)

Long term bias (step 4)

$(C_r || C_{r+1}) \oplus (C_{r+2+G} || C_{r+3+G}) = (P_r || P_{r+2}) \oplus (P_{r+1} || P_{r+3+G})$

Obtained from Digraph Repetition Bias

Our Sequential Method

- Algorithm
  - Step 1 : Collect X ciphertexts
  - Step 2 : Set i = 0
  - Step 3 : Obtain candidates of $P_1, \ldots, P_{257+i}$ by using our strong bias set
  - Step 4 : Guess P_{258+i} by using digraph biases for G = 1,…,63
  - Step 5 : Increment i and Repeat 3 and 4

$\boxed{P_1, P_2, , \ldots, P_{256}, P_{257}, \quad P_{258},}\ P_{259}, \ P_{260}, \ P_{261}$

Strong bias set
(step 3)

Long term bias (step 4)

$$(C_r \| C_{r+1}) \oplus (C_{r+2+G} \| C_{r+3+G}) = (P_r \| P_{r+2}) \oplus (P_{r+1} \| P_{r+3+G})$$

Obtained from Digraph Repetition Bias

Our Sequential Method

- Algorithm
  - Step 1 : Collect X ciphertexts
  - Step 2 : Set i = 0
  - Step 3 : Obtain candidates of $P_1, \ldots, P_{257+i}$ by using our strong bias set
  - Step 4 : Guess P_{258+i} by using digraph biases for G = 1,…,63
  - Step 5 : Increment i and Repeat 3 and 4

$\boxed{P_1, P_2, , \ldots, P_{256}, P_{257}, \quad P_{258}, \quad P_{259},} \; P_{260}, \quad P_{261}$

Strong bias set (step 3)

Long term bias (step 4)

$$(C_r || C_{r+1}) \oplus (C_{r+2+G} || C_{r+3+G}) = (P_r || P_{r+2}) \oplus (P_{r+1} || P_{r+3+G})$$

Obtained from Digraph Repetition Bias

Our Sequential Method

- Algorithm
  - Step 1 : Collect X ciphertexts
  - Step 2 : Set i = 0
  - Step 3 : Obtain candidates of $P_1, \ldots, P_{257+i}$ by using our strong bias set
  - Step 4 : Guess P_{258+i} by using digraph biases for G = 1,…,63
  - Step 5 : Increment i and Repeat 3 and 4

$$\boxed{P_1, P_2, , \ldots, P_{256}, P_{257}, \quad P_{258}, \quad P_{259}, \quad P_{260},} \quad P_{261}$$

Strong bias set
(step 3)

Long term bias (step 4)

$$(C_r || C_{r+1}) \oplus (C_{r+2+G} || C_{r+3+G}) = (P_r || P_{r+2}) \oplus (P_{r+1} || P_{r+3+G})$$

Obtained from Digraph Repetition Bias

Experimental Results

- We have performed the experimentation.
  - P_{258}, …, P_{261} can be recovered from 2^{34} ciphertexts with probability of one

Table 1: Success Probability of our algorithm for recovering P_r ($r \geq 258$) on Broadcast RC4

	# of ciphertexts				
	2^{30}	2^{31}	2^{32}	2^{33}	2^{34}
P_{258}	0.0039	0.0391	0.3867	0.9648	1.0000
P_{259}	0.0039	0.0078	0.1523	0.9414	1.0000
P_{260}	0.0000	0.0039	0.0703	0.9219	1.0000
P_{261}	0.0000	0.0078	0.0273	0.9023	1.0000

- Theoretical estimation
  - Given 2^{34} ciphertexts with different keys, $2^{40} \fallingdotseq 1000$ T bytes of the plaintext are recovered with probability of 0.99

Conclusion

Evaluation of Practical Security of RC4 in Broadcast Setting

- Results
  - **Efficient plaintext recovery attack in first 257 bytes**

Any bytes of first 257 bytes

2^{32} ciphertexts

  - **Sequential plaintext recovery attack after 258 bytes**

Contiguous First 1000 T bytes

2^{34} ciphertexts

RC4 is not to be recommended for the broadcast encryption

Conclusion

- If the initial 256 bytes of the keystream are disregarded in the protocol, our attack does not work.
  - Same type of the attack seem to be applicable
- For SSL/TLS, the broadcast setting is converted into the multi-session setting where the target plaintext block are repeatedly sent in the same position in the plaintexts in multiple SSL/TLS sessions.

Thank you for your attention