Cryptanalysis of RC4-like Stream Ciphers

Goutam Paul

Jadavpur University*, *Kolkata*, *India

Joint work with

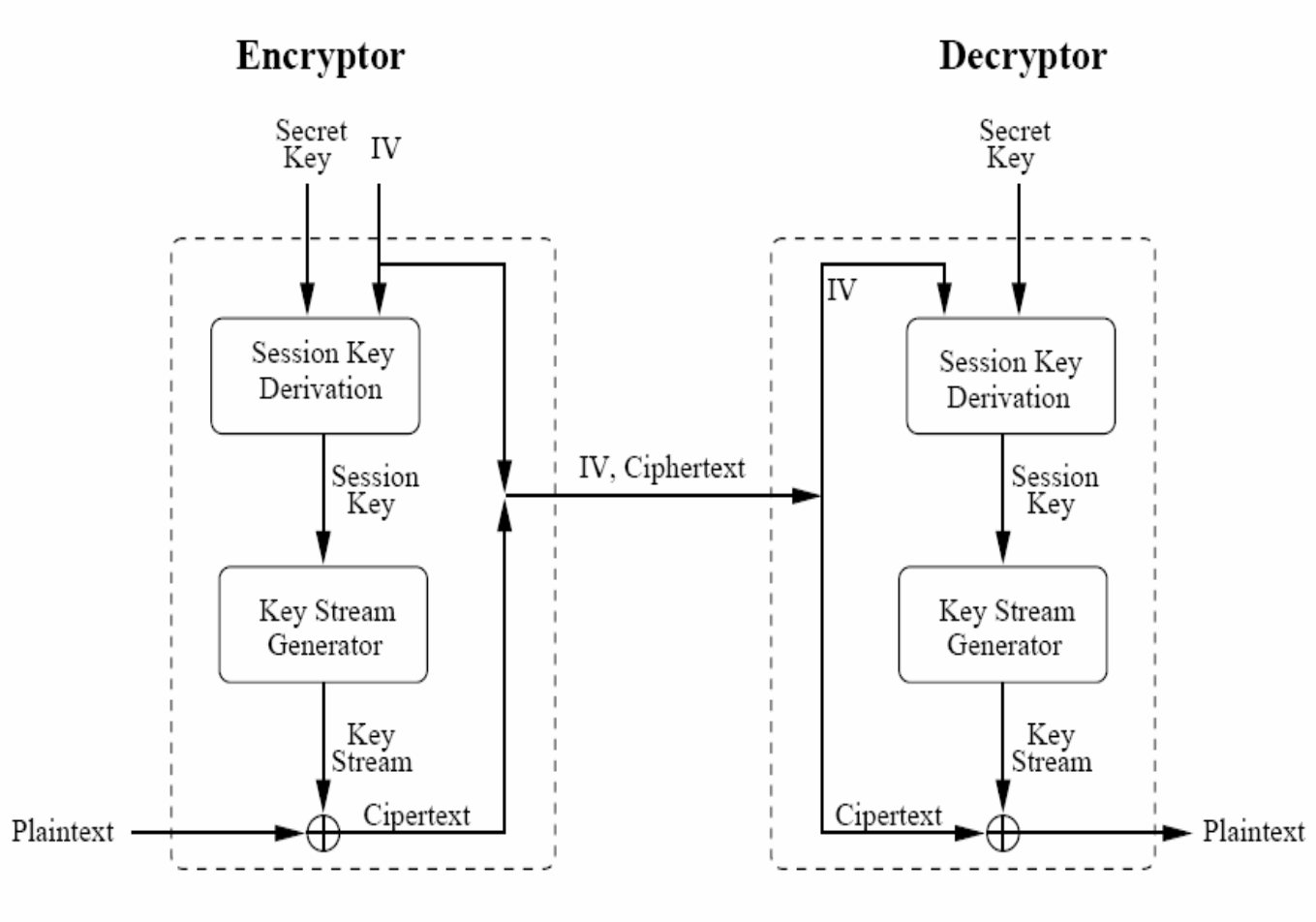
Subhamoy Maitra

Indian Statistical Institute*, *Kolkata*, *India

Prior Works

- Finney (1994), Roos (1995), Jenkins (1996),
- Knudsen, Rijmen et. al. (1998),
- Mantin (2001-05), Shamir (2001-04),
- Paul & Preneel (2003-04), Biham (2005-08),
- Klein (2006), Tews (2007), Vaudenay (2007),
- Maximov (2005-08),
- Akgun et. al. and Khazaei & Meier (2008).

General Model of Stream Cipher



RC4

- One of the most popular stream ciphers.
- Designed by Ron Rivest in 1987.
- Generally used with 5 to 16 bytes key.
- Applications
  - Protecting Internet Traffic
    - SSL, TLS, WEP, WPA, AOCE
  - Others
    - Microsoft Windows, Lotus Notes, Oracle Secure SQL etc.

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 :

For $i = 0, \ldots, N-1$

$S[i] = i;$

$j = 0;$

Scrambling :

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 :

$$i = i + 1;$$

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

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

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

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

RC4 Security Issues

- Design extremely simple, analysis is not.
- More than 20 years of cryptanalysis.
- RC4 is quite secure to be used as an 128-bit stream cipher, if
  - IV's are incorporated with proper care and
  - some amount of initial keystream bytes are thrown away.

Key-Output Correlations

- Proved new bias of the first keystream byte towards the first three bytes of the secret key (WCC 2007 / DCC 2008).
- Proved Roos' Empirical Observation (1995) of a conditional bias in the first keystream byte towards the third key byte (WCC 2007 / DCC 2008).
- Proved New Biases in initial as well as in the 256-th and 257-th keystream bytes (FSE 2008).

Key-Permutation Correlations

- Proved Roos' Empirical Observation (1995) regarding bias of initial permutation bytes towards linear combinations of secret key bytes (SAC 2007).
  - Proved that such biases are intrinsic to shuffle exchange type KSA

- Generalized the biases to nested indices, i.e., $S[y]$, $S[S[y]]$, $S[S[S[y]]]$ etc. (FSE 2008).

Key Recovery from Permutation

- Proposed the first algorithm for complete key recovery from the final permutation after the KSA, without any assumption on the key or IV (SAC 2007).
- Subsequent extension by others for better success probability (Biham & Carmeli, FSE 2008 and Akgun et. al., Indocrypt 2008).
- Recently, we have discovered a bidirectional key search that gives the best performance for 16 bytes key.

State Recovery with *j* stuck (ACISP 2008)

Case	Data Complexity (#Keystream Bytes)	Time Complexity
j stuck at unknown value, *i* at stuck-point unknown	2^{11}	2^{25}
j stuck at known value, *i* at stuck-point known	2^{11}	2^{14}
if we have 2^{16} keystream bytes after *j* is stuck (*i,j* known / unknown)	2^{16}	2^{8}

Complete Characterization of PRGA Evolution (JMC 2008)

- Non-uniform distribution of z given i, j.
- The index j is not produced uniformly at random given the value of j two steps ago.
- Information on j is leaked from z.
- A new (weak) distinguisher (for equality of any two consecutive bytes).
- All the results hold, even if any amount of initial keystream bytes are thrown away.

RC4+: A Stronger Variant of RC4 (Indocrypt 2008)

- Goal is to keep the simple structure of RC4 and add a few steps to the existing algorithm so as to remove the weaknesses of RC4.
- Three-Layer KSA: Basic Scrambling, Scrambling with IV and Zigzag scrambling.
- Does not reveal a permutation byte in the output, which is now sum of two permutation bytes, XOR-ed with a third one.

Summary

- Cryptanalysis of RC4 is an active research area.
- Every now and then newer and newer weaknesses are being discovered.
- The cipher is not yet completely broken and is subject to further analysis.
- Recently, we have found 30 new distinguishers for HC-128, extending the LSB-based distinguisher of Wu to the other bits.

Thank You !

Questions / Comments ?