Technology to limit the available number of chosen-plaintext

Ichiroh Kazawa

Corresponding author:
Ichiroh Kazawa[1]

Email address: contact@XORveR.com

ABSTRACT

This technology sets an upper limit on the number of available pairs for chosen-plaintext and ciphertext in any chosen-plaintext-attack (CPA).
By applying the typical implementation of 128-bit encryption, all CPAs cannot use more than 16 chosen-plaintexts.

It does not encrypt the plaintext directly with this technique.
256 kinds of variations are created from the plaintext.
It then chooses one variation at random to encrypt.

Unless the secret key is used in decryption, it is impossible to find out which of the 256 kinds of variations was used for the ciphertext.
A CPA when used for multiple chosen-plaintexts would need to repeat the comparison for the total amount of combinations of the chosen-plaintext.

If the CPA increases the total amount of chosen-plaintexts by one, the number of generated encryption keys increased by 256 times.
$256^{16}(== 2^{128})$ encryption keys will be generated from the 16 chosen-plaintexts.

Since the the total key possibilities generated exceed the total number of encryption keys, it is not possible for CPA to win with a brute force attack.

$$\frac{Secret\ Key\ Size_{(bit\ length)}}{Variations\ Count_{(bit\ length)}} > Chosen\ Plaintexts\ Count_{(useable\ count)}$$

** Industrial significance **

RC4 is no longer recommended.
However, the compactness of RC4 in embedded devices (e.g. RF-ID) has a big advantage in regards to block ciphers such as AES.

RC4 can regain its security with this technology.
Compacting embedded devices will lead mainly to the reduction of costs.

It is believed that this technology will contribute greatly to the IoT.

”XORveR”, is this technologies codename.

1 INTRODUCTION

This technology, set an upper limit on the available number of pairs of chosen-plaintext and ciphertext in any chosen-plaintext attack(CPA).

By applying the typical implementation of 128-bit encryption and this technology, all CPAs can't use more than 16 chosen-plaintexts.

Then, the technology we call currently "XORveR".

2 IMPLEMENTATION

2.1 Random Number Sequence Matrix (RNSM)

An array of random number sequences (RNS) are defined in advance.

This matrix will be provided based on the encryption and or decryption.
Since, its intended use is for public communications, the RNSM is published as a specification.

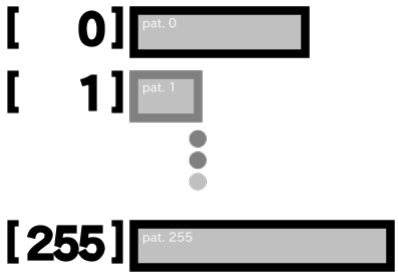

Figure 1. An RNSM image.

Number of elements in the array is recommended 256 from convenience.
It is recommended that the length of each random number sequence is a coprime.

2.2 Random Number Sequence Index (RNSI)

The index of a RNSM.

It is selected each time the encryption process is performed.

Number of bits is recommend 8-bit from convenience.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.2534v1 | CC BY 4.0 Open Access | rec: 17 Oct 2016, publ: 17 Oct 2016

2.3 CaMouflaged-PlainText (CMPT)

The next step is to camouflage the plaintext.

1. Using a random number generator (RNG) will get the RNSI.

Figure 2. An RNSI create.

2. Get the RNSM index of the RNS.

Figure 3. Select one of RNSM.

3. With the XOR operation of plaintext and RNS, generate a camouflage plaintext.

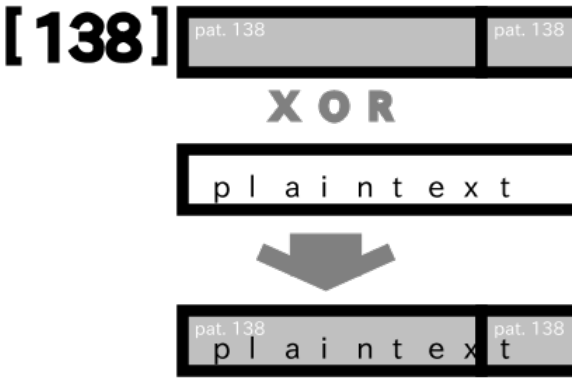

Figure 4. The camouflage plaintext create.

4. Create a CMPT by combining camouflage plaintext with RNSI.

Figure 5. The CMPT create.

CMPT will return to plaintext by reversing the procedure.

2.4 XORveR ciphertext

It describes the XORveR ciphertext.

Encrypts the CMPT in any encryption scheme.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.2534v1 | CC BY 4.0 Open Access | rec: 17 Oct 2016, publ: 17 Oct 2016

3 VERIFICATION

3.1 The premise of the verification

It describes the premise of the Verification.

Weak ciphers to the ciphertext-only attack (COA) will never use.
In order to know that the encryption key is correct, CPA will need to decrypt the ciphertext.

If the CPA can know that the encryption key is correct without decryption, it will be COA problem exists.

The encryption scheme that can be decoded without using the secret key should not be used.

3.2 Successful attack conditions

It describes the successful attack conditions.

How do we determine whether the attack was successful?

Execution time is essential for a CPA to decrypt.
The common operation for a CPA is the decryption process.

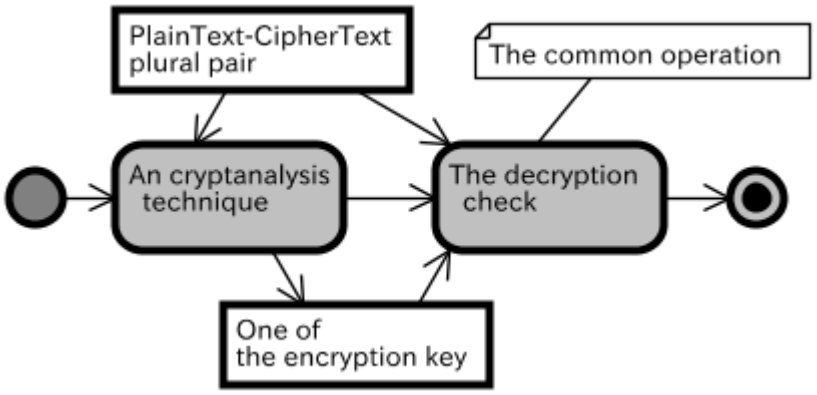

Figure 6. a CPA activity.

In order to make verification simple, only the processing time of decryption is assumed.
And, the CPA will find the complete encryption key of the candidate.
In the brute-force-attack, there is no extra processing performed other than decoding.
Therefore, these conditions are favorable for a CPA.
As a result, these conditions argue that they are not favorable for XORveR technology.

In XORveR technology, we assume that the number of decryption processes represents the execution time.

A brute-force-attack against the L-bit encryption performs the decryption 2^L times. If the CPA can find the correct encryption key after less decryptions than 2^L times, CPA is considered superior to the brute-force-attack.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.2534v1 | CC BY 4.0 Open Access | rec: 17 Oct 2016, publ: 17 Oct 2016

3.3 Verification

It describes the Verification.

The validation assumes that the attack is on a 128-bit encryption.

One of the chosen-plaintext will be one of the 2^8 *kinds of CMPT. In addition, the RNSI is independent for each ciphertext.*

Therefore, CPA will need to generate a encryption key combination for 256 types of different CMPT for each ciphertext.

If a CPA requires the M chosen-plaintext, the number of encryption keys will reach 256^M.

All CPAs will need to check whether the decryptions generated with the encryption keys are correct.

If a CPA requires 16 chosen-plaintexts, the number of encryption keys will reach 256^{16} ($==2^{128}$).

Since the number of decryptions required for CPA is the total number of encryption keys, the attack failed.

Therefore, by applying the typical implementation of 128-bit encryption, all CPAs can't use more than 16 chosen-plaintexts.

And, by applying the typical implementation of 256-bit encryption, all CPAs can't use more than 32 chosen-plaintexts.

And, by applying the typical implementation of 2048-bit encryption (full size RC4), all CPAs can't use more than 256 chosen-plaintexts.

4 DISCUSSION

1. Q. Is it weak against initial vector fixing attacks?
   A. Yes. Care must be taken so that the initial vector is not fixated by the attack.

2. Q. In a stream cipher, can a bias attack be stopped?
   A. Yes. If half of the RNSM elements are made with the reverse of the other half, Each bit of CMPT will be generated as completely uniform random numbers.

3. Q. In a stream cipher, can a correlation attack be stopped?
   A. It is unknown. However, generating a CMPT from diving plaintext into non-predefined lengths is thought of as one way to stop it.

Figure 7. CMPT for each part.

4. Q. Whether the patent has been acquired?
   A. Yes. In Japan, patent has acquired (JP5992651). It is pending in such as the United States.

5 CONCLUSION

If the bit length of the secret key was KEY_{bits}, the bit length of the RNSI $RNSI_{bits}$, the value of the number $SAMPLE_{count}$ of chosen-plaintext is represented by the following inequality.

$$\frac{KEY_{bits}}{RNSI_{bits}} > SAMPLE_{count}$$

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.2534v1 | CC BY 4.0 Open Access | rec: 17 Oct 2016, publ: 17 Oct 2016