One-time Pad Cipher Based on Out-Key Distribution

Shengyuan Wu
Independent researcher, Ubit inventor, retired professor, Shandong University, Jinan, China

Abstract - *This paper presents a one-time pad cipher based on out-key distribution. Key is divided into in-key and out-key; in-key is used in cipher and decipher; out-key is used in key distribution and in-key generation based on in-out number relation. Only out-key is transferred, in-key is not transferred. The relation between in-keys and out-keys is truly randomly characterized; that is out-keys doesn't contain any information of in-keys. So, it's impossible for Eve to crack the ciphered data by intercepting out-keys. In-out key combined with in-out password, in-out nonce can further strengthen computer security; in-out password makes password unbreakable; and in-out nonce makes replay attacks useless.*

Key words: Cryptography; key; password; nonce; cipher; one-time pad

1. INTRODUCTION

Computer security mainly consists of three aspects: confidential, authentication and integrity. Key, password and nonce are three kernel elements in computer security.

In cryptography, the one-time pad is the only unbreakable cryptosystem that exhibits what is referred to as perfect secrecy, and can be proven to be perfectly secure. [1-6].

However, this cryptosystem has a drawback: Since for each message a new key is needed, a large amount of random secret numbers have to be distributed between all parties that wish to communicate [1-3].

As we know, there are two ways to realize one-time pad:

First: distribute secret key by diplomatic suitcase, a physical method;

Second: distribute secret key by quantum cryptography.

"Quantum cryptography" does not refer to quantum cryptosystems, but, somewhat misleadingly, to establishing a random secret key using quantum signals, i.e., implementing the one-time pad via quantum key distribution [1-3].

Theoretically, quantum key distribution is absolutely safe, one-time pad based on quantum key distribution is unbreakable and absolutely safe. However, the complexity and imperfectness of various parts in the quantum communication system makes it impossible to put broadly in use soon [2].

The difficulties stem from key, the key is used in cipher and decipher, the same key must be transferred; and the risk is just in key distribution.

Password is used in user authentication; password ideally should be easy to remember and hard to guess. Unfortunately these two goals are conflict with each other [6]; therefore, it isn't safe. The first line of security defense is password; however, weak and default passwords is a notable risk [7].

The difficulties of password is how to make password easy to remember and hard to guess.

Nonce is mainly used in against replay attacks, the most dangerous and the most difficult prevented attacks. The risk of nonce is the interception of nonce, because the same nonce must be transferred.

The weakness of key, password and nonce can be easily strengthened by in-out key, in-out password and in-out nonce based on in-out number relation.

This paper proposes to realize one-time pad cipher by three components: in-key is used in cipher and decipher; out-key is used for key distribution; only out-key needs to distribute, in-key is not transmitted.

The relation between in-keys and out-keys is truly randomly characterized, and in-out number relation is kept secret from Eve. Eve can intercept the ciphered data and the related out-key stream, but without the in-out number relation, she can't get the in-key stream by analyzing the out-key stream, so she can't crack the ciphered data.

This paper also proposes to realize user authentication by in-out password, out-password is easy to remember, and in-password is hard to guess.

This paper also proposes to against replay attacks by in-out nonce, challenge by out-nonce, and response by in-nonce.

The proposals can make key distribution and ciphered data absolutely safer, make password unbreakable; and make replay attacks useless.

2. ONE-TIME PAD CIPHER BASED ON OUT-KEY DISTRIBUTION

2.1 Review of one-time pad cipher

First, let us review one-time pad cipher, Vernam Cipher as showed in Fig. 1.

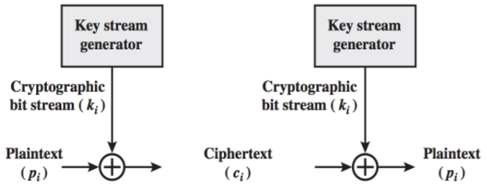


Figure 1. Vernam Cipher [5]

The system can be expressed as follows:

$c_i = p_i \oplus k_i$

$p_i = c_i \oplus k_i$

Where

p_i = ith binary digit of plaintext;

k_i = ith binary digit of key;

c_i = ith binary digit of ciphertext.

$\oplus$ = exclusive-or (XOR) operation

The essence of this technique is the means of construction of the key.

Vernam proposed the use of a running loop of tape that eventually repeated the key, so that in fact the system worked with a very long but repeating keyword [4].

Joseph Mauborgne proposed an improvement to the Vernam cipher that yields the ultimate in security. Mauborgne suggested using a random key that is as long as the message, so that the key need not be repeated. In addition, the key is to be used to encrypt and decrypt a single message, and then is discarded. The improved Vernam cipher is called as one-time pad, and is unbreakable [5-8].

However, Fig. 1 doesn't say how to generate cryptographic bit stream. Fig. 2 is a Vernam Cipher with key-controlled bit-stream generator, the two parties shares the key, and can generate the same cryptographic bit stream.

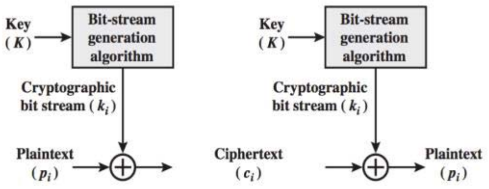

Key
(K)
Bit-stream generation algorithm
Cryptographic bit stream (k_i)
Plaintext (p_i)
Key
(K)
Bit-stream generation algorithm
Cryptographic bit stream (k_i)
Ciphertext (c_i)
Plaintext (p_i)

Figure 2. Vernam Cipher with key-controlled bit-stream generator [5]

However, the key stream must be provided to both users in advance via some independent and secure channel; this makes one-time pad cipher is hardly implemented [5]

Theoretically, one-time pad cipher based on quantum key distribution is absolutely safe; unfortunately, because the complexity and imperfectness of various parts in the quantum communication system makes it impossible to put broadly in use soon [2].

2.2 One-time pad cipher based on out-key distribution

Fig. 3 is a diagram of one-time pad cipher based on out-key distribution; here, key is divided into in-key and out-key.

The diagram relates to three kinds of ciphers.

The part below the short dash line relates to Vernam cipher as Fig. 1.

The part below the longer dash line relates to Vernam Cipher with key-controlled bit-stream generator as Fig. 2.

The whole diagram is one-time pad cipher based on out-key distribution. The extraordinary characteristic is that one-time pad cipher based on out-key distribution tells that two parties how to share keys, and how to generate the same cryptographic bit stream.

Here, only in-key is used to cipher and decipher; out-key is used in key distribution and controlling in-key generator.

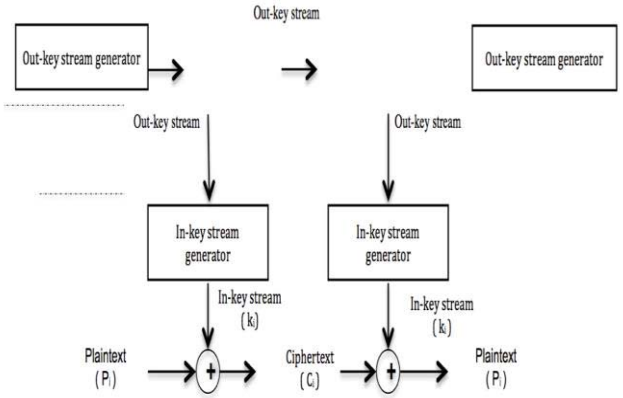


Figure 3. Diagram of one-time pad cipher based on out-key distribution.

Out-key stream generator is a random number generator; for Alice, it's used to control in-key stream generator to generate random in-key stream; out-key stream is also transferred to Bob, to control Bob's in-key stream generator to generate random in-key stream. Because Alice and Bob shares the same in-key stream generator, which is controlled by the same out-key stream; therefore, the in-key stream used in decipher is the same as in cipher.

The communication procedure is as following:

Alice generates out-key stream by out-key stream generator;

Alice generate in-key stream by in-key stream generator controlled by out-key stream;

Alice ciphers plaintext by in-key stream;

Alice sends ciphered text to Bob;

Alice also sends out-key stream to Bob;

Bob generates in-key stream by in-key stream generator controlled by Alice's out-key stream; Bob's in-key stream is the same as the Alice's in-key stream.

Bob deciphers the ciphered text by the in-key stream.

The difference between traditional one-time pad and one-time pad based on out-key distribution is as following:

In-key is used in cipher or decipher; but in-key is not transferred.

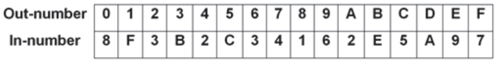
Only out-key is transferred.

Therefore, only out-key can be eavesdropped, but in-key is impossible to be eavesdropped, so in-key and ciphered text is absolutely safe.

However, if out-key stream contains any information about in-key stream; then Eve can know in-key stream by intercepting out-key stream, and crack the ciphered text.

2.3 In-key stream generator

In-out number relation is the core data structure in one-time pad cipher based on out-key distribution. Fig. 4 is a diagram of in-out number relation.



Out-number	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
In-number	8	F	3	B	2	C	3	4	1	6	2	E	5	A	9	7

Figure 4. Diagram of a simple in-out number relation

Out-number can be any length of binary digit, for example: 4 bit long, one byte long, two byte long, and so on. In Fig. 4, out-number is four bit long, represented in hex number; assume in-number is also hex number.

Usually out-number is arranged in order, ascending order as shown in Fig. 4; but in-number is set randomly

An in-key stream generated from an out-key stream is illustrated in the following simplified example.

Out-key stream generator generates an out-key stream,

Take each 4 bits from out-key stream, a hex number; assuming the out-key stream is 7846, 4 hex digits.

The first digit of out-key stream is “6”, search “6” in the out-number sequence in Fig. 4, find the related in-number is “3”;

The second digit of out-key stream is “4”, search “4” in Fig. 4, find the related in-number is “2”;

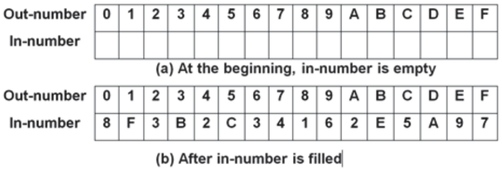
The third digit of out-key is “8”, search “8” in Fig. 4, find the related in-number is “1”;

The last digit of out-key is “7”, search “7” in Fig. 4, find the related in-number is “4”;

Then, in-key stream is 4123.

Similarly, for any random out-key stream, a random in-key stream can be generated based on in-out number relation.

Now, let’s discuss how to set up in-out number relation.



Out-number	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
In-number																

(a) At the beginning, in-number is empty

Out-number	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
In-number	8	F	3	B	2	C	3	4	1	6	2	E	5	A	9	7

(b) After in-number is filled

Figure 5. illustrating diagram of setting up in-out number relation

In Fig. 5 (a), out-number has been filled in ascending order; but in-number is empty, in-number can be filled randomly as the following:

Taking a16-sided die, labeled with the numbers 0 through F; each in-number is filled as the dice thrown or rolled, the die comes to rest showing on its upper surface a random integer from 0 to F, then the integer is filled in each column.

In-out number relation can be set by other method; but it must be kept to be random.

In-out number relation is random characterized, each out-number contains no information about related in-number, out-key stream consists of out-numbers, in-key stream consists of related in-numbers; therefore, the out-key stream contains no information about in-key stream.

Eve can intercept the ciphered data and the related out-key stream, but she can’t get the in-key stream by analyzing the out-key stream, so she can’t crack the ciphered data.

To keep ciphered message safe, in-out number relation must satisfy the three requirements:

1. For any random out-key stream, it can generate a related random in-key stream.

2. It can generate unlimited amount of in-key streams.

3. The relation between in-number and out-number is truly randomly characterized, so the relation of in-key stream and out-key stream is truly randomly characterized.

If out-key stream is generated by a true random number generator, then out-key stream is truly random, and the generated in-key stream is also truly random. A true random number generator can use a nondeterministic source to produce randomness, such as: by sound or video noise [5].

The relation between in-key stream and out-key stream is truly random, out-key stream bears no statistical relationship to in-key stream, and contains no information what so ever about the in-key stream.

Therefore, one-time pad based on out-key distribution is absolutely safe.

One-time pad based on out-key distribution can also be used in user authentication by sending an out-key to another party, and asking the party to send back the related in-key; the authentication fails if the party can’t send back the correct related in-key. This can efficiently against replay attack.

One-time pad based on out-key distribution can also be used to authenticate messages i.e. to identify their origin and integrity, and to identify user.

In practice, one-time pad based on out-key distribution integrates key, key distribution, encryption algorithm, data integrity, and user authentication as a whole.

2.4 The security of in-out number relation

In-out number relation is the core data structure in one-time pad cipher based on out-key distribution; its security depends on the security of in-out number relation.

First, like the master key distribution, an in-out number relation must be distributed in some noncryptographic way, such as physical delivery. However, the distribution of the in-out number relation is a bootstrap in-out number relation; because based on the in-out number relation, two parties can generates unlimited random keys; which can be used for one-time pad cipher; further, new in-out number relation can be safely transferred between the two parties by one-time pad cipher; therefore, the physically distribution of in-out number relation is similar to a bootstrap key in quantum key distribution for authentication. However, for mast key distribution, only a limited number of mast keys can be distributed one time; the limited master keys can't be used implementing one-time pad cipher; therefore, if new master keys needed, they still need to be distributed in some noncryptographic way, such as physical delivery.

Second, because in-out number relation is a bootstrap in-out number relation, the old in-out number relation can be replaced by a new one as needed; this strengthens the security of in-out number relation.

Third, in-out number relation is only kept by Bob and Alice, not transferred, it is impossible for Eve to intercept or to know it; this is different from master key, or session key; which must be transferred during key distribution although in encryption form.

Fourth, the in-number sequence and the out-number sequence of in-out number relation can be stored separately; for example in different media; this increases the difficulties if Eve tries physically or by malware to eavesdrop the in-out number relation.

2.5 A comparison between one-time pad based on out-key distribution and one-time pad based on quantum key distribution

1. For based on out-key distribution, in-key is not transmitted, and without the in-out number relation, Eve can't get the in-key stream by analyzing the out-key stream, absolutely safe; quantum encryption key must be distributed, theoretically, unbreakable and absolutely safe, but because of the complexity and imperfectness, vulnerabilities are inevitable;

2. Based on out-key distribution only uses classical channel; but quantum encryption uses both quantum and classical channels;

3. Based on out-key distribution integrates all five encryption elements, but quantum encryption doesn't;

4. Based on out-key distribution, the key management is simple and safe; however, quantum encryption key pool management is complicated;

5. Based on out-key distribution is implemented easily; however, quantum encryption theory and implementation is very complicated and difficult.

6. Based on quantum key distribution does not solve the key distribution problem without the need of a bootstrap key for authentication [1]. Neither based on out-key distribution, therefore, the first in-out number relation must be distributed physically.

In-out key can be combined with in-out password, in-out nonce in order to strengthen computer security.

3. IN-PASSWORD AND OUT-PASSWORD

Classical password, ideally should be easy to remember and hard to guess. Unfortunately these two goals are conflict with each other; therefore [6], it isn't safe.

The first line of security defense is password; however, weak and default passwords is a notable risk [7].

No one of the existed passwords can against all cracking methods today; for example, Finger print password is static, easily discovered, and easily attacked by replay; human body password, generated by password pill, is also breakable; therefore, personal, business's, and national confidential information eavesdropped and intercepted, huge money lost, moving vehicles in danger, even planted medical device in human's body can be cracked in danger.

However, based on in-out number relation, only owned by the user, password is divided into in-password and out-password, Out-password is short, simple and easily to remember, but in-password is long, extremely complex. Out-password is used to generate in-password; and in-password is used in authentication. For simplicity, assume out-password consists of digit 0-9 as shown in Table 1.

TABLE I. TABLE 1 IN-OUT NUMBER RELATION

Out-number	0	1	2	3	4	5	6	7	8	9
In-number	I_0	I_1	I_2	I_3	I_4	I_5	I_6	I_7	I_8	I_9

Assume the in-number is not simple as in Fig. 5; and the related in-number is: I_1=3er78⌘, I_2=90 , I_3=45uip♪, I_4=w ⌫

Assuming out-password is 1234.

As input out-password: 1234; then, the related in-password is: 3er78⌘90 45uip♪w ⌫.

Here, the out-password is short, simple, and easy to remember; however, the in-password is long and complicated; the in-password above also include invisible characters; all these make dictionary attack, brute force attack, offline cracking (rainbow attack) useless.

Suppose Eve viewed the whole procedure of your inputting password; because out-password is only used in transforming to in-password based on the in-out number relation. Therefore, even Eve knows the out-password, for example here: 1234; she has no way to input your in-password without the in-out number relation. Key logger, screen scrubbing and shoulder surfing are all useless.

Assume an attacker asks your password by telephone posing as an IT security guy; at most, he can get your out-password, because you really don't know or can't remember your in-password.

4. IN-NONCE AND OUT-NONCE

Nonce is often used to against replay attacks. The use of random numbers for the nonces frustrates an opponent's efforts to determine or guess the nonce [5].

However, a lot of difficulties exist in applying nonce in computer security, for examples: the timestamp approach should not be used for connection-oriented applications because of the inherent difficulties with this technique; the challenge-response approach is unsuitable for a connectionless type of application [5].

The most important problem of nonce is the weakness of nonce. A nonce must be transferred in communication channel at least twice; Alice sends a nonce to Bob, Bob sends back the nonce to Alice. Eve can intercept the nonce to fool Bob, because the nonce is same.

The difficulties and the weakness problem can be easily solved by out-nonce and in-nonce by sharing in-out number relation by Alice and Bob. Out-nonce is used in challenge stage; in-nonce is used in response stage. Eve can intercept out-nonce, but it is useless in response stage, because without in-out number relation, she has no way to know the in-nonce; therefore this makes reply attack useless.

For example, two parties share in-out number relation as shown in Fig. 4, which is used to transform an out-number to related in-number; If Alice sends out-nonce=7846 to Bob, then Bob responses the in-nonce=4123. Eve can intercept the out-nonce, but she can’t response the correct in-nonce without the in-out number relation.

In-nonce and out-nonce can be used in user authentication. If client and server share an in-out number relation; mutual authentication can be done. For example, an attacker intercepted your in-password; later try to enter your bank account; the bank sends her an out-nonce and asks to send back the related in-nonce; because in-out number relation is only shared by the client and server, attacker can’t send back the related in-nonce without the in-out number relation. The client can also check if a web site is a fishing site by sends it an out-nonce, and asks an answer.

As two parties share in-out number relation; then replay attack is also useless, for example, an attacker intercepted in-password sent by car’s remoter controller, later tries to open the car using the in-password; however, the car can sends her an out-nonce and asks her sends back the related in-nonce, however she can’t; because only the car and the car owner’s remote controller share the in-out number relation [8].

5. CONCLUSION

In-out key, in-out password, in-out nonce greatly strengthens computer security. The methods presented in this paper are easily implemented.

Computer security can be further strengthened by Ubit theory [9]. In-out key, in-out password and in-out nonce combined with Ubit theory can lay a solid foundation of computer security.

Acknowledgments Thank Bin Wu, my wife, for her great contributions and fully supporting.

References

[1] Gilles van Assche, Quantum Cryptography and Secret-Key Distillation, Cambridge University press. 2006

[2] Yin Hao, Han Yang, The principles and technology of quantum communication, Electronic Industry Press, 2013

[3] W. Beiglb?ck, J. Ehlers, K. Hepp, H. Weidenmüller, Quantum Information, Computation and Cryptography: An Introductory Survey of Theory, Technology and Experiments (Lecture Notes in Physics), Springer, Berlin Heidelberg 2010, P 279

[4] Shannon, Claude, "Communication Theory of Secrecy Systems". Bell System Technical Journal 28 (4): 656–715, 1949.

[5] William Stallings, Cryptography and Network Security principles and Practice, Fifth Edition, Pearson Education, Inc., 2011

[6] Michael T. Goodrich, Roberro Tamassia, Introduction to Computer Security, Pearson Education, 2012

[7] 2013 Trustwave Global Security Report

[8] Shengyuan Wu，Methods and apparatuses of digital data processing, PCTIB2013060369, 11, 2013

[9] Shengyuan Wu，Introduction to Ubit Semantic Computing, Proceedings of The 2014 International Conference on Semantic Web and Web Services of Computer Science (SWW’14), 07, 2014