Improvement of One Quantum Encryption Scheme

Zhengjun Cao
Departement D'informatique, University Libre de Bruxelles. Belgium.
zhencao@ulb.ac.be

Abstract Zhou et al proposed a quantum encryption scheme based on quantum computation in 2006. Each qubit of the ciphertext is constrained to two pairs of conjugate states. So its implementation is feasible with the existing technology. But it is inefficient since it entails six key bits to encrypt one message bit, and the resulting ciphertext for one message bit consists of three qubits. In addition, its security can not be directly reduced to the well-known BB84 protocol. In this paper, we revisit it using the technique developed in BB84 protocol. The new scheme entails only two key bits to encrypt one message bit. The resulting ciphertext is just composed of two qubits. It saves about a half cost without the loss of security. Moreover, the encryption scheme is probabilistic rather than deterministic.

1 Introduction

Quantum cryptography uses quantum mechanics to guarantee secure communication. The security of quantum cryptography relies on the foundations of quantum mechanics, in contrast to traditional public key cryptography which relies on the computational difficulty of certain mathematical functions. Quantum communication involves encoding information in quantum states, or qubits. Usually, photons are used for these quantum states.

The first quantum cryptographic protocol aims to establish a fresh key between two users, which is invented by Charles H. Bennett and Gilles Brassard [1] and referred to as BB84. In practice, any two pairs of conjugate states can be used for the protocol. The security of the protocol comes from encoding the information in non-orthogonal states. Quantum indeterminacy means that these states cannot generally be measured without disturbing the original state. With the development of quantum cryptography (it is only used to produce and distribute a key in the early days), quantum encryption becomes attractive.

Probabilistic encryption is the use of randomness in an encryption algorithm, so that when encrypting the same message several times it will, in general, yield different ciphertexts. The term "probabilistic encryption" is typically used in reference to public key encryption algorithms, however various symmetric key encryption algorithms achieve a similar property. To be semantically secure, that is, to hide even partial information about the plaintext, an encryption algorithm must be probabilistic. An intuitive approach to converting a deterministic

encryption scheme into a probabilistic one is to simply pad the plaintext with a random string before encrypting with the deterministic algorithm. Conversely, decryption involves applying a deterministic algorithm and ignoring the random padding. The first provably-secure probabilistic public-key encryption scheme was proposed by Goldwasser and Micali [4], based on the hardness of the quadratic residuosity problem and had a message expansion factor equal to the public key size. There are many efficient probabilistic encryption algorithms, including Optimal Asymmetric Encryption Padding (OAEP) [2] and [7].

In 2006, Zhou et al proposed a quantum block encryption algorithm [10] (ZZNXZ for short), which can be used to encrypt classical messages as well as quantum messages. The algorithm does not require any quantum state pre-shared or stored, which makes it encrypt classical messages possible in real applications. With the existing technology, its implementation becomes feasible. But it has two limitations. One is that six classical key bits should be used to encrypt one message bit. The other is that the resulting ciphertext for one message bit is composed of three qubits. Thus, the original algorithm is a little inefficient. In addition, its security can not be directly reduced to the well-known BB84 protocol. In this paper, we revisit it using the technique developed in BB84 protocol. The new scheme entails only two key bits to encrypt one message bit. The resulting quantum state for one message bit is just composed of two qubits other than three qubits. It saves about a half cost without the loss of security. Moreover, the encryption scheme is probabilistic other than deterministic.

2 Related work

In 2000, Horace P. Yuen [8] proposed a new approach to quantum cryptography, which is called KCQ (keyed communication in quantum noise). It is developed on the basis of quantum detection and communication theory for classical information transmission. By the use of a shared secret key that determines the quantum states generated for different data bit sequences, the users may employ the corresponding optimum quantum measurement to decode the data. In Yuen's protocol, let ρ_x^k be the quantum state corresponding to the data x (single bit or a bit sequence) and running key sequence k that is used to determine the basis and/or polarity of the qk scheme for that length of x. For $M/2$ possible bases and a single bit x, there is $1 + \log_2(M/2)$ bits in k for both basis and polarity determination. Each ρ_x^k can be represented as a real vector $|r_x^k\rangle$ of norm 1 on the great circle, the angle between any two nearest neighbor vectors is $2\pi/M$ radian. Notice that in the Yuen's protocol, the quantum state ρ_x^k is no longer constrained to two pairs of conjugate states. Therefore, the difficulty of modulating related quantum states arises imperceptibly. This may be the reason that the Yuen's protocol is rarely implemented than BB84. As for the security proof of Yuen's protocol, we refer to [5].

In Eurocrypt'04, I. Damgård et al [3] considered the scenario where Alice wants to send a secret classical n-bit message to Bob using a classical key, and where only one-way quantum transmission from Alice to Bob is possible. They suggest an application of their results in the case where only a short secret key is available and the message is much longer. Concretely, one can use a pseudorandom generator to produce from the short key a stream of keys for a quantum

cipher, using each of them to encrypt an n-bit block of the message. Their results suggest that an adversary with bounded resources in a known plaintext attack may potentially be in a much harder situation against quantum stream-ciphers than against any classical stream-cipher with the same parameters. For illustration, they presented a method for designing quantum ciphers which can be described as follows. Given message $b_1, b_2, \cdots, b_n$ and key $c, k_1, \cdots, k_n$, it outputs the following n q-bit state as ciphertext: $(H^{\otimes n})^c(X^{k_1} \otimes X^{k_2} \otimes \cdots \otimes X^{k_n}|b_1 b_2 \cdots b_n\rangle)$, where X is the bit-flip operator and H is the Hadamard transform. Namely, it uses the last n bits of key as a one-time pad, and the first key bit determines whether or not we do a Hadamard transform on all n resulting q-bits. Decryption uses the operator $(X^{k_1} \otimes X^{k_2} \otimes \cdots \otimes X^{k_n})(H^{\otimes n})^c$, which is the inverse of the encryption operator. In this scheme, the resulting ciphertext states are also constrained to the four states $|1\rangle, |0\rangle, |+\rangle, |-\rangle$. That means it can be realistically implemented with the current technology. But there is one point that is noteworthy, i.e., its encryption algorithm is deterministic.

In 2007, Zhou et al proposed another quantum block encryption algorithm with hybrid keys. In the encryption algorithm, two kinds of keys are involved. One is the quantum key as follows $|K_1\rangle = |k_{11}\rangle \oplus |k_{12}\rangle \cdots \oplus |k_{1m}\rangle,\ |k_{1i}\rangle = a_i|0\rangle + b_i|1\rangle$, where $|a_i|^2 + |b_i|^2 = 1$. The other is the classical binary key $K_2 = k_{21}k_{22}\cdots k_{2l},\ k_{2j} \in \{0, 1\}$. Since each qubit of the resulting ciphertext is not constrained to two pairs of conjugate quantum states, the difficulty of modulating related quantum states occurs. We refer to [9] for details.

3 Review of ZZNXZ scheme

The scheme requires communicators to pre-share four groups of classical keys: one for the choice of quantum ancilla bits, one for the choice of the Controlled-NOT operation, one for the bits permutation, and another one for the choice of the quantum logic operation making the ciphertext non-orthogonal. The resulting quantum ciphertext for one classical bit is composed of three qubits. Each qubit is constrained to two pairs of conjugate states.

3.1 Encryption process

Consider the encryption of the ith classical plaintext bit using the corresponding ith key element of each group of keys. If the keys are used up, reuse the remaining secure keys.

Step 1: Preparation. Given a classical message bit to be encrypted is $m \in \{0, 1\}$, Alice prepares the quantum state $|k_1^1 k_1^2 m\rangle$ according to the first group key k_1, where k_1^1 and k_1^2 are two key elements of k_1. The result C_1 of this step may be one of the possible states $|000\rangle, |010\rangle, |100\rangle, |110\rangle, |001\rangle, |011\rangle, |101\rangle$ and $|111\rangle$.

Step 2: Controlled-NOT operation. Alice performs a Controlled-NOT operation on the third qubit (message qubit), according to the second group key k_2. The whole possible ciphertext states are listed in Table 1. The third qubit in each state of C_1 is the original information qubit, but in resulting state of C_2 it is the result of the Controlled-NOT transformation and is no longer the original information qubit itself, where the subscript m denotes the bit related to the

original message bit.

Step 3: Permutation. Alice permutes two qubits in the state C_2 by the following table 2, according to the third group key k_3. The resulting states C_3 in the step are different in form from those in C_1, the second and the third qubits of each state of C_3 may involve information about the message (plaintext), unlike those of C_1 where the information about the plaintext is just confined to the third qubit. Thus the ciphertext space is doubled.

Step 4: Non-orthogonality. Alice carries out quantum computation on the ciphertext states in C_3 under the control of the fourth group key k_4, according to the following table 3. Some quantum computations such as Controlled-NOT gate, bit swapping, Hadamard gate and Z gate are involved during the process. For the circuits of Controlled-NOT gate, bit swap gate, H gate and Z gate, we refer to [6]. The resulting quantum ciphertext C_4 is composed of three qubits. Each qubit is constrained to two pairs conjugate states. The definition of the Controlled-NOT gate is $C_{A,B}|A\rangle|B\rangle \rightarrow |A\rangle|A \oplus B\rangle$, where $A, B \in \{0, 1\}$,

$$C_{A,B} = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix}, \text{ where } X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

The matrix forms of H and Z are

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}}(X + Z), \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Clearly, $H|0\rangle = |+\rangle, H|1\rangle = |-\rangle$, where $|0\rangle = \binom{1}{0}, |1\rangle = \binom{0}{1}, |\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$.

Table 1: The first encryption transformation

C_1	$k_2 = 0$	C_2	$k_2 = 1$	C_2
$\|000_m\rangle$		$\|000_m\rangle$		$\|000_m\rangle$
$\|010_m\rangle$		$\|010_m\rangle$		$\|011_m\rangle$
$\|100_m\rangle$		$\|101_m\rangle$		$\|100_m\rangle$
$\|110_m\rangle$		$\|111_m\rangle$		$\|111_m\rangle$
$\|001_m\rangle$		$\|001_m\rangle$		$\|001_m\rangle$
$\|011_m\rangle$		$\|011_m\rangle$		$\|010_m\rangle$
$\|101_m\rangle$		$\|100_m\rangle$		$\|101_m\rangle$
$\|111_m\rangle$		$\|110_m\rangle$		$\|110_m\rangle$

3.2 Decryption process

Step 1: Decrypting C_4 with k_4. If the key element is 01, i.e. the H gate is applied while encrypting, one applies the same H gate to the ciphertext while decrypting. If the key element is 10, i.e. the ZH gate is applied while encrypting, one applies the HZ gate to the ciphertext while decrypting. If the key element is 00 or 11, let the ciphertext stay put.

Step 2: Decrypting C_3 with k_3. If the key element is 0, leave it alone. If the key element is 1, permute the second and the third qubits with the bit swap circuit.

Table 2: The second encryption transformation

C_2	$k_3 = 0$	C_3	$k_3 = 1$	C_3
$\|000_m\rangle$		$\|000_m\rangle$		$\|00_m0\rangle$
$\|001_m\rangle$		$\|001_m\rangle$		$\|01_m0\rangle$
$\|010_m\rangle$		$\|010_m\rangle$		$\|00_m1\rangle$
$\|011_m\rangle$		$\|011_m\rangle$		$\|01_m1\rangle$
$\|100_m\rangle$		$\|100_m\rangle$		$\|10_m0\rangle$
$\|101_m\rangle$		$\|101_m\rangle$		$\|11_m0\rangle$
$\|110_m\rangle$		$\|110_m\rangle$		$\|10_m1\rangle$
$\|111_m\rangle$		$\|111_m\rangle$		$\|11_m1\rangle$

Table 3: The third encryption transformation

C_3	$k_4 = 00$ or 11	$k_4 = 01$	$k_4 = 10$	C_3	$k_4 = 00$ or 11	$k_4 = 01$	$k_4 = 10$
$\|000_m\rangle$	$\|000_m\rangle$	$\|00+_m\rangle$	$\|00-_m\rangle$	$\|00_m0\rangle$	$\|00_m0\rangle$	$\|00_m+\rangle$	$\|00_m-\rangle$
$\|001_m\rangle$	$\|001_m\rangle$	$\|00-_m\rangle$	$\|00+_m\rangle$	$\|00_m1\rangle$	$\|00_m1\rangle$	$\|00_m-\rangle$	$\|00_m+\rangle$
$\|010_m\rangle$	$\|010_m\rangle$	$\|01+_m\rangle$	$\|01-_m\rangle$	$\|01_m0\rangle$	$\|01_m0\rangle$	$\|01_m+\rangle$	$\|01_m-\rangle$
$\|011_m\rangle$	$\|011_m\rangle$	$\|01-_m\rangle$	$\|01+_m\rangle$	$\|01_m1\rangle$	$\|01_m1\rangle$	$\|01_m-\rangle$	$\|01_m+\rangle$
$\|100_m\rangle$	$\|100_m\rangle$	$\|10+_m\rangle$	$\|10-_m\rangle$	$\|10_m0\rangle$	$\|10_m0\rangle$	$\|10_m+\rangle$	$\|10_m-\rangle$
$\|101_m\rangle$	$\|101_m\rangle$	$\|10-_m\rangle$	$\|10+_m\rangle$	$\|10_m1\rangle$	$\|10_m1\rangle$	$\|10_m-\rangle$	$\|10_m+\rangle$
$\|110_m\rangle$	$\|110_m\rangle$	$\|11+_m\rangle$	$\|11-_m\rangle$	$\|11_m0\rangle$	$\|11_m0\rangle$	$\|11_m+\rangle$	$\|11_m-\rangle$
$\|111_m\rangle$	$\|111_m\rangle$	$\|11-_m\rangle$	$\|11+_m\rangle$	$\|11_m1\rangle$	$\|11_m1\rangle$	$\|11_m-\rangle$	$\|11_m+\rangle$

Step 3: Decrypting C_2 with k_2. The decryption is described as

$$|A\rangle|A \oplus B\rangle \rightarrow |A\rangle|A \oplus (A \oplus B)\rangle = |A\rangle|B\rangle$$

where $A, B \in \{0, 1\}$, and this transformation is still a Controlled-NOT transformation.

Step 4: Transforming C_1. The third bit of each 3-bit quantum state in the result derived in Step 3 corresponds to initial classical message bit. Cascading all the initial classical message bits, Bob gets the bit string of plaintext.

3.3 Two limitations of the ZZNXZ scheme

As mentioned before, the ZZNXZ quantum encryption scheme is feasibly implemented with the existing technology since only tow pairs of conjugate states are involved. But we observe that there are two limitations. One is that six classical key bits should be used to encrypt one classical message bit. The requirement for a long key is a bit impressive. The other is that the resulting ciphertext for one message bit should be composed of three qubits. Apparently, it is applicable if a cipher entails less qubits and less key bits. In addition, its security can not be directly reduced to the well-known BB84 protocol.

By the way, we also observe that the description of the ZZNXZ scheme is not clearly specified

(see Table 2 and Table 3). Actually, there is no any difference between $|000_m\rangle$ and $|00_m0\rangle$. Both of them are composed of three qubits $|0\rangle$. It is not necessary to list them respectively.

In what follows, we shall present an improvement of the ZZNXZ scheme without the loss of security, which entails less qubits and less key bits. Moreover, the new scheme is no longer deterministic, instead probabilistic.

4 ZZNXZ scheme revisited

4.1 Description

Either the encryption algorithm or the decryption algorithm in the revisited scheme is implemented by quantum computation, which can be realized by current technology. We now describe it as follows.

Encryption algorithm: Input a message bit m and a secret key $K = k_1k_2$. Output the quantum ciphertext $c = |\alpha\beta\rangle$, where $|\alpha\rangle, |\beta\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$.

E1 Padding. Pick a random bit $b \in \{0, 1\}$, concatenate b with m and modulate the quantum state $|bm\rangle$.

E2 Transformation. Compute the ciphertext c by the following table 4. The encryption transformation is defined by

$$c = |\alpha\beta\rangle = \begin{cases} |bm\rangle, & k_1k_2 = 00 \\ |bm_1\rangle, & k_1k_2 = 11 \\ |bm_2\rangle, & k_1k_2 = 01 \\ |bm_3\rangle, & k_1k_2 = 10 \end{cases}$$

where $|m_1\rangle = X|m\rangle, |m_2\rangle = H|m\rangle, |m_3\rangle = ZH|m\rangle$,
$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

Table 4: Encryption transformation

$\|bm\rangle$	$k_1k_2 = 00$	$k_1k_2 = 11$	$k_1k_2 = 01$	$k_1k_2 = 10$
$\|00\rangle$	$\|00\rangle$	$\|01\rangle$	$\|0+\rangle$	$\|0-\rangle$
$\|10\rangle$	$\|10\rangle$	$\|11\rangle$	$\|1+\rangle$	$\|1-\rangle$
$\|01\rangle$	$\|01\rangle$	$\|00\rangle$	$\|0-\rangle$	$\|0+\rangle$
$\|11\rangle$	$\|11\rangle$	$\|10\rangle$	$\|1-\rangle$	$\|1+\rangle$

Decryption algorithm: Input a quantum ciphertext $c = |\alpha\beta\rangle$ and a secret key $K = k_1k_2$. Output a classical message bit m.

The decryption transformation is defined by

$$|m\rangle = \begin{cases} |\beta\rangle, & k_1k_2 = 00 \\ X|\beta\rangle, & k_1k_2 = 11 \\ H|\beta\rangle, & k_1k_2 = 01 \\ HZ|\beta\rangle, & k_1k_2 = 10 \end{cases}$$

Remark 1 The padding bit b has no relation to the decryption transformation. That is to say, the encryption scheme is probabilistic other than deterministic.

4.2 Security analysis

The security of the scheme is directly based on BB84 protocol. In some sense, it is just the generalization of BB84 protocol in the scenario of two users communicating with the help of a shared key. We now give a brief argument for the security of the improved scheme.

Given a ciphertext $|\alpha\beta\rangle$, an adversary cannot derive $|m\rangle$ without the information of k_1k_2, because the qubit $|\beta\rangle$ is constrained to the two pairs of conjugate states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$. By the encryption transformation, the adversary cannot determine which operator of the possible operators I, X, H, ZH has been used. For each bit, the probability is bounded by $\frac{1}{4}$. Suppose the length of the encrypted message block is n, the probability is bounded by $\frac{1}{4^n}$, which is negligible.

Furthermore, if the adversary can obtain the multiple duplications of the second qubit and measure them, he also cannot determine the bit m because the four states are uniformly distributed in the second position. For example, if the adversary obtains $|1+\rangle$ and knows each qubit, he can still not determine m because there are two preimages, $|10\rangle$ and $|11\rangle$. In that case, its security reduced to the following transformation (Table-5):

Table 5: The reduced transformation

$\|bm\rangle$	$k_1k_2 = 00$	$k_1k_2 = 11$
$\|00\rangle$	$\|00\rangle$	$\|01\rangle$
$\|10\rangle$	$\|10\rangle$	$\|11\rangle$
$\|01\rangle$	$\|01\rangle$	$\|00\rangle$
$\|11\rangle$	$\|11\rangle$	$\|10\rangle$

The reduced transformation is equal to the following conventional transformation (Table-6): So far, the conventional transformation remains secure even through quantum computers become true.

Finally, the adversary cannot derive $|m\rangle$ from the qubit $|\alpha\rangle$ since the padding bit b has no relation to m. This comes from the fact that all quantum operators are performed on the second qubit.

Table 6: A conventional transformation

bm	$k=0$	$k=1$
00	00	01
10	10	11
01	01	00
11	11	10

4.3 Comparison

We now make a comparison between the new scheme and the ZZNXZ scheme. The results are listed in the following Table-7.

Table 7: Comparison for generating a ciphertext for one message bit

Scheme	key-bit	qubit	conjugate states	probabilistic
Improvement	2	2	$\|0\rangle, \|1\rangle, \|+\rangle, \|-\rangle$	Yes
ZZNXZ	6	3	$\|0\rangle, \|1\rangle, \|+\rangle, \|-\rangle$	No

Roughly speaking, the revisited scheme saves about a half cost, if we think of that the cost of permuting two qubits in the original step 3 is equal to that of modulating a quantum ancilla state. The improved scheme is of a peculiar characteristic, probabilistic property, which is practically appreciated. Besides, the security of the new scheme can be directly reduced to that of BB84 protocol.

5 Conclusion

In this paper, we present an improvement of the ZZNXZ quantum encryption scheme and show its security. Interestingly, our scheme can be viewed as the generalization of BB84 protocol in the scenario of two users communicating with the help of a shared key.

Acknowledgement Cryptasc Project (Institute for the Encouragement of Scientific Research and Innovation of Brussels).

References

[1] C.H. Bennett, G. Brassard, Quantum cryptography:Public key distribution and coin tossing, Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing, Bangalore, India (IEEE, Los Alamitos, CA), pp. 175-179 (1984)

[2] M. Bellare, P. Rogaway. Optimal Asymmetric Encryption - How to encrypt with RSA. Extended abstract in Advances in Cryptology - Eurocrypt'94, Lecture Notes in Computer Science Vol. 950, Springer-Verlag (1995)

[3] I. Damgård, T. Pedersen, L. Salvail, On the Key-Uncertainty of Quantum Ciphers and the Computational Security of One-Way Quantum Transmission, Proceedings of Eurocrypt'04, LNCS 3027, Springer-Verlag, pp. 91-108 (2004)

[4] S. Goldwasser, S. Micali. Probabilistic Encryption, Special issue of Journal of Computer and Systems Sciences, Vol. 28, No. 2, pp. 270-299 (1984)

[5] O. Hirota, Practical security analysis of a quantum stream cipher by the Yuen 2000 protocol, PHYSICAL REVIEW A 76, 032307 (2007)

[6] M.A. Nielsen, I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University press, 2000.

[7] T. Okamoto, S. Uchiyama. A New Public-key Cryptosystem as Secure as Factoring, Advances in Cryptology - EUROCRYPT'98, Lecture Notes in Computer Science Vol. 1403, pp. 308-318 (1998)

[8] H. P. Yuen, KCQ: A New Approach to Quantum Cryptography I. General Principles and Key Generation, arXiv:quant-ph/0311061v6

[9] N. Zhou, Ye Liu, G. Zeng, J. Xiong, F. Zhu, Novel qubit block encryption algorithm with hybrid keys, Physica A 375, pp. 693-698 (2007)

[10] N. Zhou, G. Zeng, Y. Nie, J. Xiong, F. Zhu, A novel quantum block encryption algorithm based on quantum computation, Physica A 362, pp. 305-313 (2006)