Quantum Asymmetric Encryption Based on Quantum Point Obfuscation

Chuyue Pan[1], Tao Shang[2], and Jianwei Liu[3]

School of Cyber Science and Technology, Beihang University, Beijing, 100083 China
shangtao@buaa.edu.cn

Abstract. Quantum obfuscation means encrypting the functionality of circuits or functions by quantum mechanics. It works as a form of quantum computation to improve the security and confidentiality of quantum programs. Although some quantum encryption schemes have been discussed, any quantum asymmetric scheme based on quantum obfuscation is not still proposed. In this paper, we construct an asymmetric encryption scheme based on quantum point function, which applies the advantages of quantum obfuscation to quantum public-key encryption. As a start of the study on applications of quantum obfuscation to asymmetric encryption, our work will be helpful in the future quantum obfuscation theory and will therefore promote the development of quantum computation.

Keywords: Quantum computation · Quantum asymmetric encryption · Quantum obfuscation.

1 Introduction

Quantum computation combines ideas of classical information theory, computer science, and quantum physics [1]. It introduces some quantum concepts including quantum information, quantum algorithms and quantum error correction, etc. Among the existing quantum algorithms, quantum obfuscation, which means encrypting the functionality of circuits or functions by quantum mechanics, is an emergent branch to improve the security and confidentiality of quantum information. It is developed from the concept of classical obfuscation.

Classical obfuscation drives from code obfuscation in software engineering. It means reorganizing and processing the released program so that the processed code has the same function as previous one. In 2001, Barak et al. [2] first introduced the concept of obfuscation into cryptography and formally defined three properties of obfuscation. In 2004, Lynn et al. [3] put forward the first positive result of obfuscation and gave several provable schemes of point obfuscation based on complex access control under the random oracle model. In 2005, Goldwasser et al. [4] proved that obfuscation with auxiliary input cannot be realized no matter whether the auxiliary input is independent of obfuscation programs. In 2014, Alagic et al. [5] proposed a quantum obfuscator based on quantum topological computation. In 2016, Alagic et al. [6] formally put forward the definition of

ICCS Camera Ready Version 2021
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-77980-1_11

quantum obfuscation which is a form of quantum computation to protect quantum circuits. In 2019, Shang et al. [7,8] initiated the obfuscatibility of quantum point function and proposed the indistinguishability(IND)-secure quantum symmetric encryption scheme based on point obfuscation.

In this paper, we construct an asymmetric encryption scheme based on quantum point obfuscation. We combine the advantages of quantum obfuscation with asymmetric encryption to achieve indistinguishability security. Here, quantum point function is just an instantiation of quantum obfuscation. Asymmetric encryption schemes of other quantum functions still remain widely open.

2 Related Works

Definition 1 *If there exists (O, δ) in a QPT algorithm of indistinguishability obfuscation, then the following three conditions hold:*

1. Functional equivalence: *the obfuscation result $O(C)$ is interpreted as $\delta_{O(C)}$, which holds the same functionality as the input circuit C:*

$$\|\delta_{O(C)} - C\| \leq negl(n). \tag{1}$$

2. Polynomial slowdown: *the length of the obfuscator $O(C)$ must be limited to polynomial qubits, which refers to*

$$\|O(C)\| = poly(n). \tag{2}$$

3. Indistinguishability: *for any $\rho_n \in R_n$, $\sigma_n \in S_n$, there are three types of indistinguishability:*
   - *Perfect indistinguishability: $\rho_n = \sigma_n$.*
   - *Statistical indistinguishability: $\|\rho_n - \sigma_n\| \leq negl(n)$.*
   - *Computational indistinguishability: for any QPT interpreter δ, $\|\delta_{\rho_n} - \delta_{\sigma_n}\| \leq negl(n)$.*

Among the formula above, the interpreter $\delta(C)$ refers to a compiler interpreting the functionality of the circuit C from $O(C)$.

Definition 2 *A quantum point function $U_{\alpha,\beta}$ with a general output is*

$$U_{\alpha,\beta} : |x, 0^n\rangle \mapsto |x, P_{\alpha,\beta}(x)\rangle. \tag{3}$$

where $\alpha \in \{0,1\}^n$, $\beta \in \{0,1\}^n \backslash 0^n$, and $P_{\alpha,\beta}$ is a classical point function with a multi-bit output working as

$$P_{\alpha,\beta}(x) = \begin{cases} \beta & if\ x = \alpha \\ 0^n & otherwise \end{cases}. \tag{4}$$

By means of constructive proof, Shang et al. [7,8] demonstrated the obfuscatability of the quantum point function with a general output.

ICCS Camera Ready Version 2021
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-77980-1_11

3 Quantum Asymmetric Encryption Scheme

3.1 Basic Idea

Quantum asymmetric encryption scheme based on quantum obfuscation can be constructed as follows. Firstly, we implement operation of qubit rotation and measurement before we obtain a quantum state. Then we interact the quantum state with the obfuscated quantum point function to get the qubit $|0\rangle$ or $|1\rangle$. We consequently encrypt the coefficients of the quantum state of point obfuscation by the asymmetric encryption algorithm.

Definition 3 *Single-qubit rotation is a one-way function with a quantum trapdoor. The qubit is located in the x-z plane of three-dimensional Bloch sphere. The eigenstate* $|0\rangle$ *is located in the positive half axis of z-axis and the eigenstate* $|1\rangle$ *in the negative half. Single-qubit rotation is actually a rotation transformation around y-axis. That is*

$$\hat{\gamma} = i(|1\rangle\langle 0| - |0\rangle\langle 1|). \tag{5}$$

The eigenstates are transformed into quantum superposition states on x-z plane, and the sum probabilities of eigenstate $|0\rangle$ and $|1\rangle$ is 1 which can be written as trigonometric function:

$$|\varphi\rangle = \cos\frac{\alpha}{2}|0\rangle + \sin\frac{\alpha}{2}|1\rangle. \tag{6}$$

Supposing $\hat{\gamma} = i(|1\rangle\langle 0| - |0\rangle\langle 1|)$, we have

$$|\varphi_b(\alpha_k)\rangle = \cos\frac{b\alpha_k}{2}|0\rangle + \sin\frac{b\alpha_k}{2}|1\rangle = e^{\frac{ib\alpha_k\hat{\gamma}}{2}}|0\rangle = R(b\alpha_k)|0\rangle. \tag{7}$$

The first result $|\varphi_{b_i,m_i}(\alpha_k)\rangle_i$ is transformed by the second rotation on the basis of superposition state. When the output state $|m_i\rangle$ of quantum point obfuscation is $|0\rangle$, rotation about angle 0 is performed in Hilbert space. When the $|m_i\rangle$ is $|1\rangle$, rotation about angle π is performed. We can show the process with the formula

$$|\varphi_{b_i,m_i}(\alpha_k)\rangle_i = R(m_i\pi)|\varphi_{b_i}(\alpha_k)\rangle_i. \tag{8}$$

The previous result is inversely processed by qubit rotation shown in Fig. 1 and is subsequently measured after decryption. That is, if the information to be encrypted is $|0\rangle$, it will approach the positive half axis of z-axis with high probability after rotation. If it is $|1\rangle$, it will approach the negative half with high probability. After measurement, we can get specific plaintext m_i.

3.2 Scheme

Key generation Firstly, we randomly select an integer string $b = (b_1, b_2, \cdots, b_K)$ of length K, a rotation angle $\alpha_k = \frac{2\pi}{2^k} = \frac{\pi}{2^{k-1}}$ where k is a positive integer, and the eigenstate $|0\rangle^{\otimes d}$ of d qubits to generate the corresponding public and private keys. Here we introduce a randomly generated $2(d+1)$ bits string $s = \{0,1\}^{2d+2}$

ICCS Camera Ready Version 2021
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-77980-1_11

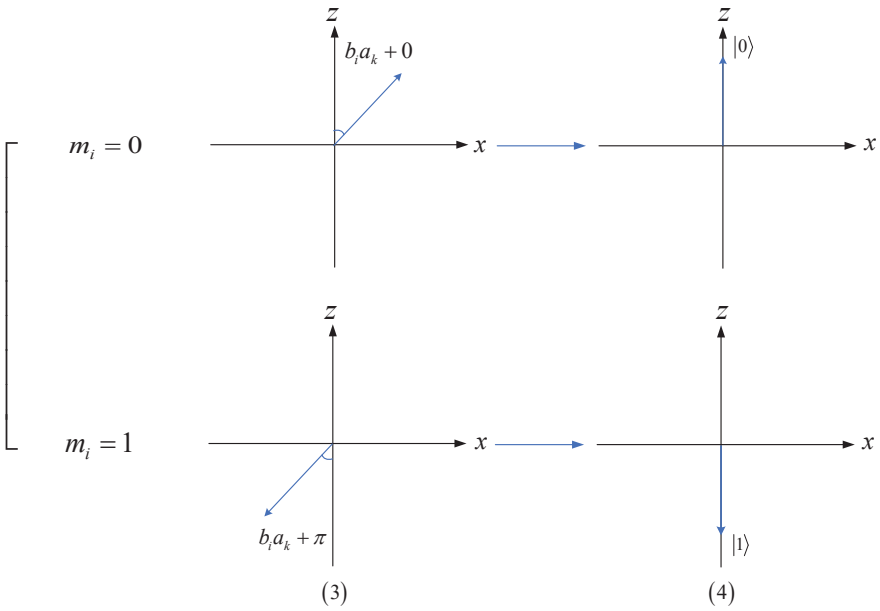

Fig. 1. Two dimensional planes of second qubit rotation.

and another random string $t = \{0,1\}^{2d+2}$ of the same length which is only known by sender (the public key holder). We define $C_{a,b}$ as a classical one-way trapdoor function and its trapdoor is $u = (C_{0,0}^{-1}, C_{0,1}^{-1}, \cdots, C_{K,0}^{-1}, C_{K,1}^{-1})$, where $C_{a,b}^{-1}$ represents the inverse function of $C_{a,b}$. The algorithm based on function $C_{a,b}$ is easy to generate but difficult to inverse unless trapdoor u is used. Supposing $a = 0, 1, \cdots, K$, the sender chooses $C_{a,0}$ or $C_{a,1}$ to encrypt the coefficients x or y of the superposition quantum state output from quantum obfuscation.

The private key of the encryption scheme is divided into two parts: $\{k, b\}$ and $u = (C_{0,0}^{-1}, C_{0,1}^{-1}, \cdots, C_{K,0}^{-1}, C_{K,1}^{-1})$. The former is used to decrypt the quantum obfuscated state so as to obtain the specific angle of the inverse rotation operation while the latter is used to decrypt the quantum state after the second rotation.

Encryption Alice wants to send Bob a multi-qubit string $|m\rangle = |(m_1, m_2, \cdots, m_d)\rangle$. Firstly, we need to compare d and K, if $d > K$, we need to extend the length of K in the public key. For the ith qubit $|m_i\rangle$, we interact it with quantum point function and obtain $|0\rangle$ or $|1\rangle$ after obfuscation. Then we implement qubit rotation operation to get $|\varphi_{b_i}(\alpha_k)\rangle_i = R(b_i\alpha_k)|0\rangle_i$ and consequently implement qubit rotation operation for the second time to get $q_i = |\varphi_{b_i,m_i}(\alpha_k)\rangle_i = R(m_i\pi)|\varphi_{b_i}(\alpha_k)\rangle_i$. Finally, we encrypt the quantum superposition state result $q_i = x|0\rangle + y|1\rangle$. The specific encryption steps are described as follows.

ICCS Camera Ready Version 2021
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-77980-1_11

The plaintext information to be encrypted is the coefficients of the superposition state $q = q_d q_{d-1} \cdots q_0$ of $(d+1)$ qubits. For example, the coefficients of the first qubit are encrypted by the sender as $C_{0,t_0}(x_0), C_{0,t_1}(y_0)$. In addition, Alice also sends a function of string $t = \{0,1\}^{2d+2}$. For any $a = 0, 1, \cdots, d$, the use of $C_{a,0}(t_a)$ or $C_{a,1}(t_a)$ depends on the fact that whether s_a is $|0\rangle$ or $|1\rangle$. Thus we have

$$En(q) = \left\{C_{0,t_0}(x_0), C_{0,t_1}(y_0), \cdots, C_{d,t_{2d}}(x_d), C_{d,t_{2d+1}}(y_d), F(t)\right\}, \quad (9)$$

$$F(t) = \{C_{0,s_0}(t_0), \cdots, C_{d,s_d}(t_d), C_{0,s_{d+1}}(t_{d+1}), \cdots, C_{d,s_{2d+1}}(t_{2d+1})\}. \quad (10)$$

In this way, Alice sends Bob the result $\left\{\left|\varphi_{b(PK)}(\alpha_k)\right\rangle, En(q)\right\}$.

Decryption Bob receives the ciphertext from Alice. Firstly, we get the quantum state $\left|\varphi_{b_i}(\alpha_k)\right\rangle_i$ corresponding to each qubit $|m_i\rangle$ with the private key $sk = \{k, b\}$. Thus we obtain the angle of the first qubit rotation operation. As we have defined above, the trapdoor of the abstract function is $u = (C_{0,0}^{-1}, C_{0,1}^{-1}, \cdots, C_{k,0}^{-1}, C_{k,0}^{-1})$. Next, we utilize the trapdoor in the public key to get the coefficients of $q = q_d q_{d-1} \cdots q_0$. We know $q_i = \left|\varphi_{b_i,m_i}(\alpha_k)\right\rangle_i = R(m_i\pi)\left|\varphi_{b_i}(\alpha_k)\right\rangle_i$, so we have

$$F^{-1}(t) = \{C_{0,s_0}^{-1}(t_0), \cdots, C_{d,s_d}^{-1}(t_d), C_{1,s+2}^{-1}(t_{d+2}), \cdots, C_{d,s_{2d+1}}^{-1}(t_{2d+1})\}, \quad (11)$$

$$Dn(q) = \{C_{0,t_0}^{-1}(x_0), C_{0,t_1}^{-1}(y_1), \cdots, C_{d,t_{2d}}^{-1}(x_d), C_{d,t_{2d+1}}^{-1}(y_d), F^{-1}(t)\}. \quad (12)$$

At this time, we measure $R(b_i\alpha_k)_i^{-1}\left|\varphi_{b_i,m_i}(\alpha_k)\right\rangle_i$ on the x-z plane of the Bloch sphere. If the qubit is on the positive half axis of the Z axis, the output of quantum point function is $|0\rangle$. If it is on the negative half, the output is $|1\rangle$. At this time, Alice replaces s with t and publishes the new private key sk.

4 Security Analysis

4.1 Key updating

This scheme updates s in the public key with the classical bit string $t = \{0,1\}^{2d+2}$ generated randomly each time. Alice generates t randomly, and Bob needs to use the private key $(C_{0,0}^{-1}, C_{0,1}^{-1}, \cdots, C_{K,0}^{-1}, C_{K,1}^{-1})$ to calculate t, and then obtain the coefficients of the quantum state $q_i = \left|\varphi_{b_i,m_i}(\alpha_k)\right\rangle_i = R(m_i\pi)\left|\varphi_{b_i}(\alpha_k)\right\rangle_i$.

Because t is not published to the public, Bob can verify the identity information of the encrypting party while using the private key. The encryption and decryption scheme can be carried out in two directions and circularly.

4.2 Indistinguishablility Security

Theorem 1 *If there exist quantum black-box obfuscation and secure quantum one-way trapdoor function, there also exists a quantum asymmetric encryption scheme which satisfies indistinguishability chosen-plaintext attack (IND-CPA) security.*

ICCS Camera Ready Version 2021
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-77980-1_11

Proof 1 *A quantum polynomial time interpreter δ with only black-box access to En_{sk} can be used to simulate the access of any QPT adversary. Because of the access to the quantum encryption circuit, the interpreter can select a random number to be used for encryption.*

For any QPT adversary, $A = \left(R, R^{-1}\right)$, $u = \left|\varphi_{b(PK)}\left(\alpha_k\right)\right\rangle \otimes R\left(m_j\right)$, $v = \left|\varphi_{b(PK)}\left(\alpha_k\right)\right\rangle \left(\left|0^d\right\rangle\left\langle 0^d\right| \otimes m_i\right)$, we have

$$\begin{aligned}
&\left|\Pr\left\{R^{-1}\left[PK \otimes R\left(m_i\right)\right]=1\right\}-\Pr\left\{R^{-1}\left[PK\left(\left|0^d\right\rangle\left\langle 0^d\right| \otimes m_i\right)\right]=1\right\}\right| \\
=&\left|\Pr\left\{R^{-1}\left[u, O\left(U_{b,k}\right)\right]=1\right\}-\Pr\left\{R^{-1}\left[v, O\left(U_{b,k}\right)\right]=1\right\}\right| \\
\leq&\sum_k\left|\Pr\left\{R^{-1}[u, \beta(b)]=1\right\}-\Pr\left\{R^{-1}[v, \beta(b)]=1\right\}\right| \cdot \Pr\left\{R_1^{-1}\left[u, O\left(U_{b,k}\right)=\beta(b)\right]\right\}.
\end{aligned} \tag{13}$$

Here R_1^{-1} is the subline of R^{-1}. Owing to the virtual black-box property, there is

$$\left|\Pr\left[R^{-1}\left(O\left(U_{b,k}\right)\right)=1\right]-\Pr\left[S^{U_{b,k}}\left(\left|0^d\right\rangle\right)=1\right]\right| \leq \operatorname{negl}(n) \tag{14}$$

And we have

$$\begin{aligned}
&\sum_k\left|\Pr\left\{R^{-1}[u, \beta(b)]=1\right\}-\Pr\left\{R^{-1}[v, \beta(b)]=1\right\}\right| \cdot \Pr\left\{R_1^{-1}\left[u, O\left(U_{b,k}\right)=\beta(b)\right]\right\} \\
\leq&\sum_k\left|\Pr\left\{R^{-1}[u, \beta(b)]=1\right\}-\Pr\left\{R^{-1}[v, \beta(b)]=1\right\}\right| \cdot\left|\Pr\left\{S^{U_{b,k}}\left(\left|0^d\right\rangle\right)=b\right\}+\operatorname{negl}(n)\right|
\end{aligned} \tag{15}$$

When S under the quantum-accessible random oracle accesses $U_{b,k}$ successfully, $\beta(b)=b_k$, otherwise $\beta(b)=0$. So

$$\begin{aligned}
&\sum_k\left|\Pr\left\{R^{-1}[u, \beta(b)]=1\right\}-\Pr\left\{R^{-1}[v, \beta(b)]=1\right\}\right| \cdot\left|\Pr\left\{S^{U_{b,k}}\left(\left|0^d\right\rangle\right)=b\right\}+\operatorname{negl}(n)\right| \\
=&\left|\Pr\left\{R^{-1}\left[u, b_k\right]=1\right\}-\Pr\left\{R^{-1}\left[v, b_k\right]=1\right\}\right| \cdot\left|\Pr\left\{S^{U_{b,k}}\left(\left|0^d\right\rangle\right)=b\right\}+\operatorname{negl}(n)\right| \\
&+\left|\Pr\left\{R^{-1}[u, 0]=1\right\}-\Pr\left\{R^{-1}[v, 0]=1\right\}\right| \cdot\left|\Pr\left\{S^{U_{b,k}}\left(\left|0^d\right\rangle\right)=0\right\}+\operatorname{negl}(n)\right|
\end{aligned} \tag{16}$$

Owing to $\Pr\left\{S^{U_{bk}}\left(\left|0^K\right\rangle\right)=b_k\right\}=\operatorname{poly}(n)/2^n \leq \operatorname{negl}(n)$ and IND-security of one-time pad, we have

$$\begin{aligned}
&\left|\Pr\left\{R^{-1}[u, 0]=1\right\}-\Pr\left\{R^{-1}[v, 0]=1\right\}\right| \\
=&\left|\Pr\left\{R^{-1}\left[\left|\varphi_{b(PK)}\left(\alpha_k\right)\right\rangle \otimes R\left(m_i\right)\right]=1\right\}\right. \\
&\left.-\Pr\left\{R^{-1}\left[\left|\varphi_{b(PK)}\left(\alpha_k\right)\right\rangle\left(\left|0^d\right\rangle\left\langle 0^d\right| \otimes m_i\right)\right]=1\right\}\right| \\
=&\operatorname{negl}(n)
\end{aligned} \tag{17}$$

Thus we have

$$\begin{aligned}
&\left|\Pr\left\{R^{-1}\left[PK \otimes R\left(m_i\right)\right]=1\right\}-\Pr\left\{R^{-1}\left[PK\left(\left|0^d\right\rangle\left\langle 0^d\right| \otimes m_i\right)\right]=1\right\}\right| \\
\leq&\left|\Pr\left\{R^{-1}\left[u, b_k\right]=1\right\}-\Pr\left\{R^{-1}\left[v, b_k\right]=1\right\}\right| \cdot|\operatorname{negl}(n)+\operatorname{negl}(n)| \\
&+\operatorname{negl}(n) \cdot\left|\Pr\left\{S^{U_{b,k}}\left(\left|0^d\right\rangle\right)=0\right\}+\operatorname{negl}(n)\right|=\operatorname{negl}(n)
\end{aligned} \tag{18}$$

In conclusion, the asymmetric encryption scheme of quantum obfuscation satisfies indistinguishability security.

ICCS Camera Ready Version 2021
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-77980-1_11

5 Conclusion

In this paper, we presented an asymmetric encryption scheme based on quantum point obfuscation. It not only achieves indistinguishability security without classical cryptography, but also solves the problem of key management in symmetric encryption. This work promotes the research on quantum computation and provides quantum obfuscation as a more secure method to achieve confidentiality of cryptography.

Acknowledgments

This project was supported by the National Natural Science Foundation of China (No. 61971021, 61571024) and the National Key Research and Development Program of China (No. 2016YFC1000307) for valuable helps.

References

1. A. Steane. Quantum Computing. Reports on Progress in Physics, 1997, 61(2):117.
2. B. Lynn, M. Prabhakaran, A. Sahai. Positive Results and Techniques for Obfuscation// Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings. DBLP, 2004:20-39.
3. B. Barak, O. Goldreich, R. Impagliazzo, et al. On the (Im)possibility of Obfuscating Programs// International Cryptology Conference on Advances in Cryptology. Springer-Verlag, 2001:1-18.
4. S. Goldwasser, Y. T. Kalai. On the impossibility of obfuscation with auxiliary input// Foundations of Computer Science, 2005. FOCS 2005. IEEE Symposium on. IEEE, 2005:553-562.
5. G. Alagic, S. Jefery, S. Jordan. Circuit obfuscation using braids. In: Proceedings of 9th Conference on Theory of Quantum Computation, Communication and Cryptography (TQC). May 21-23, 2014, Singapore. 2014:141-160. [DOI: 10.4230/LIPIcs.TQC.2014.141]
6. G. Alagic, B. Fefferman. On Quantum Obfuscation. *2016 ArXiv: Quantum Physics,* ArXiv Preprint ArXiv: 1602.01771.
7. T. Shang, R. Chen, J. Liu. On the obfuscatability of quantum point functions. Quantum Information Processing, 2019, 18:55. [DOI: 10.1007/s11128-019-2172-2].
8. R. Chen, T. Shang, J. Liu. IND-secure Quantum Symmetric Encryption Based on Point Obfuscation. *Quantum Inf. Process.,* vol. 18, no. 6, Jun. 2019, 161, DOI 10.1007/s11128-019-2280-z.

ICCS Camera Ready Version 2021
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-77980-1_11