IND-secure quantum symmetric encryption based on point obfuscation

Ranyiliu Chen, Tao Shang, and Jianwei Liu

School of Cyber Science and Technology, Beihang University, Beijing, CHINA,100191

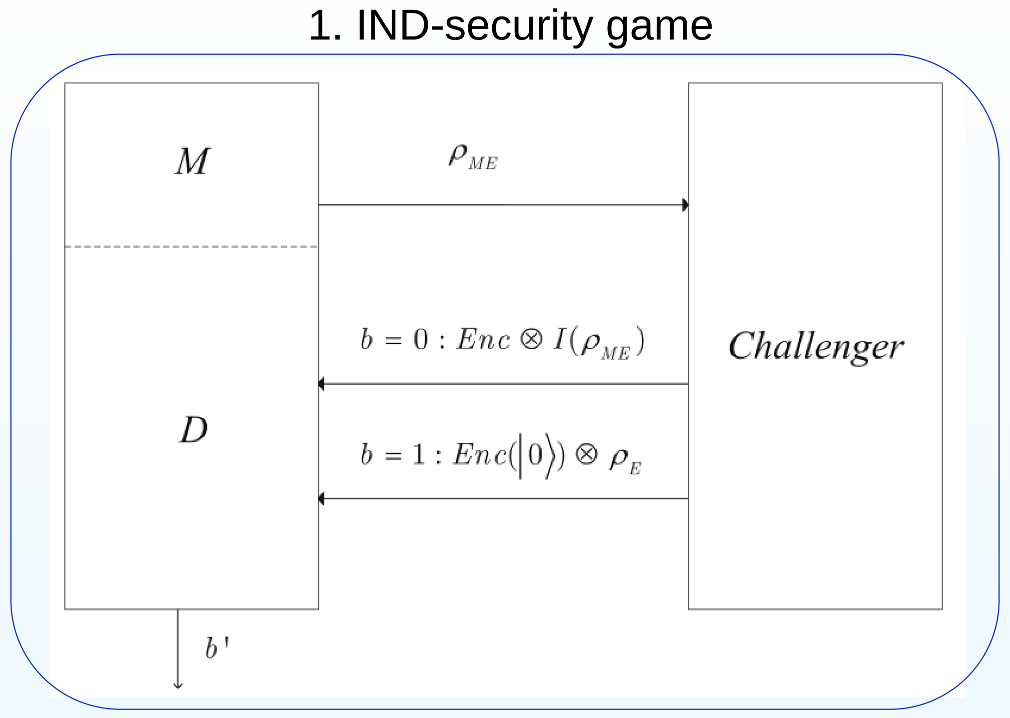
Email: shangtao@buaa.edu.cn

BACKGROUND

Quantum symmetric encryption

In the IND-security game, adversary *A* contrives the message ρ_{ME} and tries to distinguish if his message is encrypted. We denote the function of *A* by two separated quantum polynomial-time algorithm (QPT) *A = (M, D)*. *M* is the message generator, while *D* is the ciphertext distinguisher.

1. IND-security game



An IND-secure quantum symmetric encryption scheme is IND-CPA, if *A* has oracle access to Enc_k.

Quantum obfuscation

- (Polynomial expansion)

$$m = ploy(n)$$

- (Functional equivalence) for any possible ρ

$$\|\delta(O(C)\otimes\rho) - U_C\rho U_C^{\dagger}\|_{tr} \le negl(n)$$

- (Virtual black-box) for every QPT *A*, there exists a QPT S^{U_C} such that for any QPT distinguisher *D*

$$|pr\left[D\left(A(O(C))\right)=1\right] - \Pr[D(S^{U_C}(|0^n\rangle))=1] \le negl(n)$$

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

$$U_{\alpha,\beta}: |x,0^n\rangle \to |x,P_{\alpha,\beta}(x)\rangle$$

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

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

MOTIVATION

We rigorously construct an IND-secure quantum symmetric encryption scheme by means of quantum point obfuscation. Our work formally demonstrates the implementation and application of quantum obfuscation. We hope that such work will be constructive in the field of quantum obfuscation.

PROPOSED SCHEMES

1. Quantum point obfuscation with a general output

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

$$U_{\alpha,\beta}: |x,0^m\rangle \to |x,P_{\alpha,\beta}(x)\rangle$$

where $\alpha \in \{0,1\}^n$, $\beta \in \{0,1\}^m \backslash 0^m$, and $P_{\alpha,\beta}$ is a classical function working as:

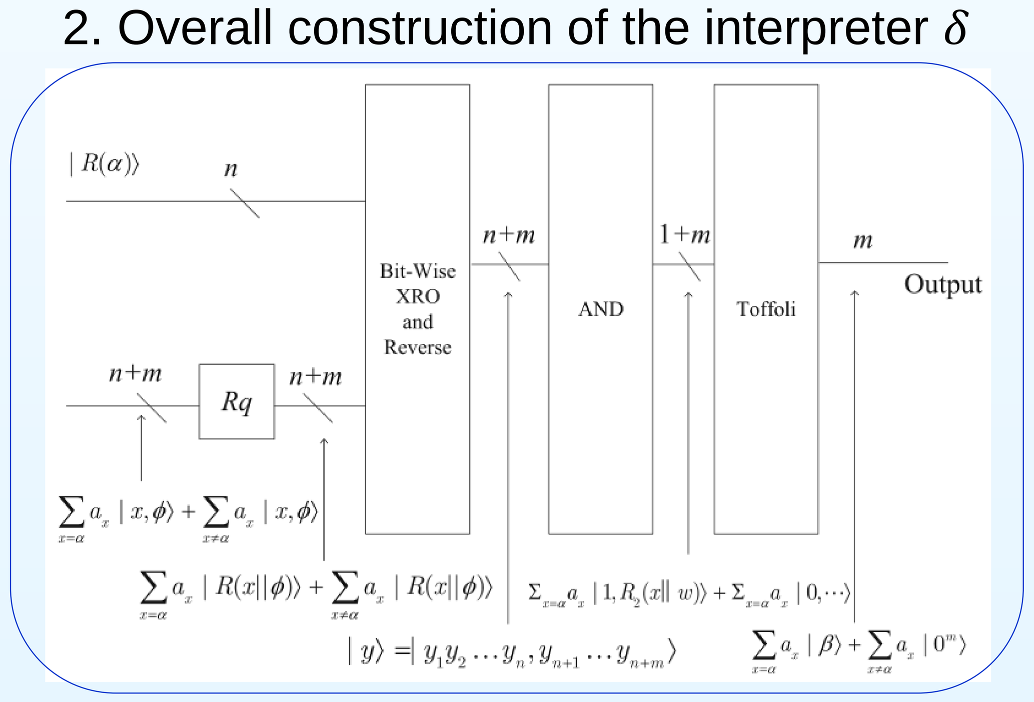
$$P_{\alpha,\beta}(x) = \begin{cases} \beta & if\ x=\alpha \\ 0^m & otherwise \end{cases}$$

We give the construction of the obfuscator *O* and the interpreter δ and then prove polynomial expansion, functional equivalence, and virtual black-box property of them. The obfuscator *O* works as follows. The obfuscator *O* randomly generates an *m*-bit classical string ω and then queries the quantum random oracle with $\alpha||\omega$. *O* computes $|R(\alpha||\omega)\otimes(0^n||\beta)\rangle$. The output of the obfuscation of $C_{\alpha,\beta}$, is

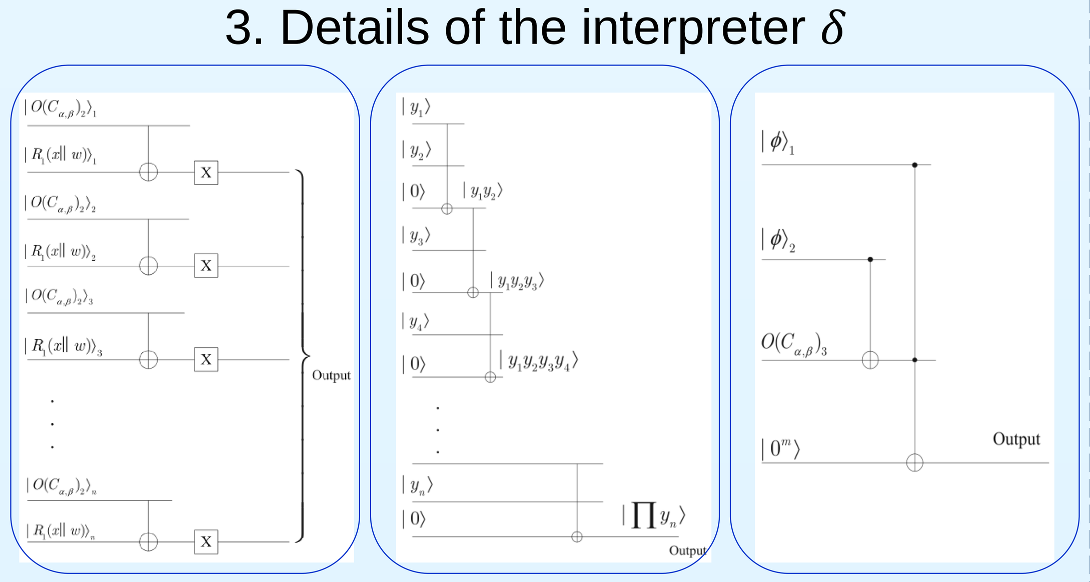
$$O(C_{\alpha,\beta}) = |\omega, |R(\alpha||\omega)\otimes(0^n||\beta)\rangle$$

$$= O(C_{\alpha,\beta})_1, O(C_{\alpha,\beta})_2, O(C_{\alpha,\beta})_3\rangle$$

2. Overall construction of the interpreter δ



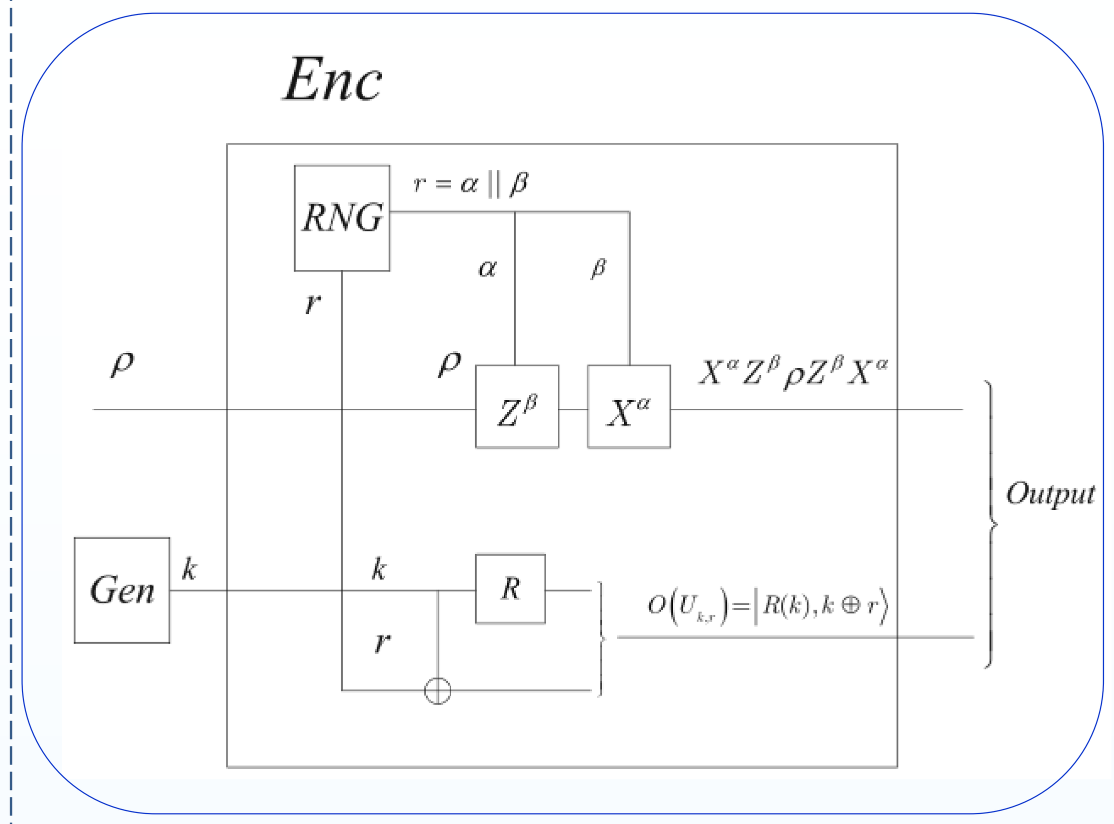
3. Details of the interpreter δ



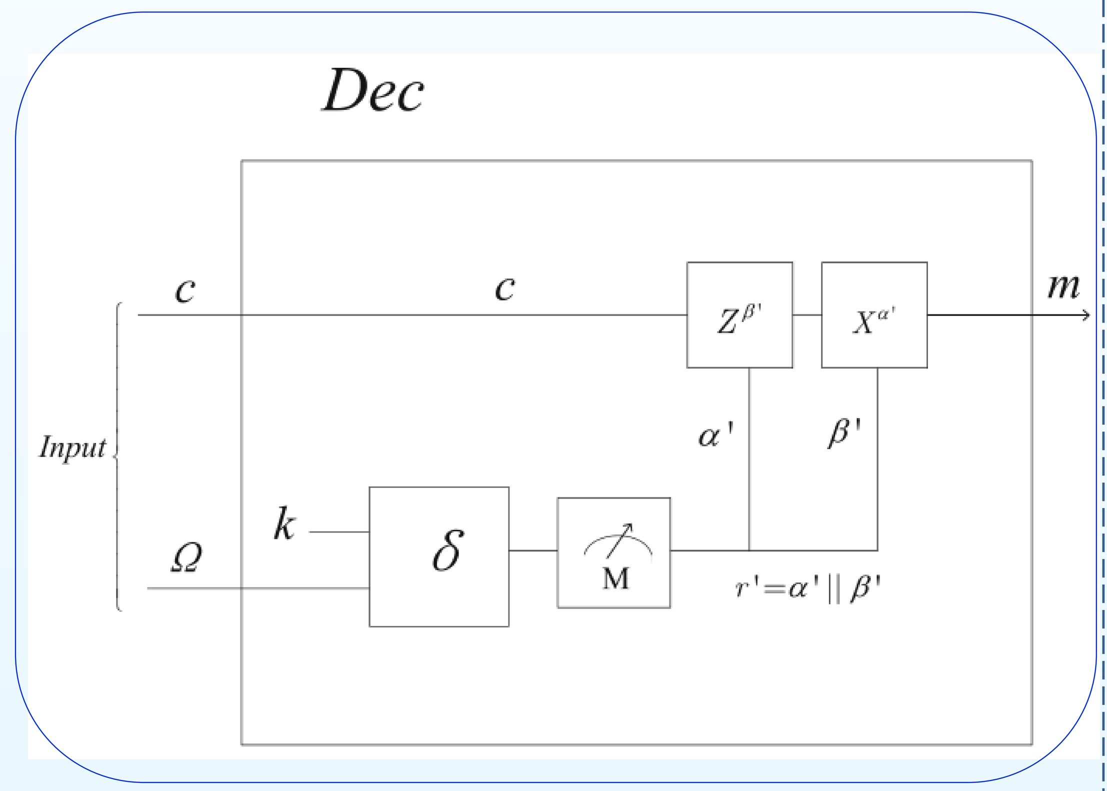
Bit-wise XOR and Reverse AND Toffoli

2. Quantum symmetric encryption scheme based on obfuscation

4. Quantum circuit of encryption



5. Quantum circuit of decryption



Scheme Let *O* be a quantum point obfuscator and $U_{k,r}$ be a quantum point function with a general output. A quantum symmetric encryption scheme based on point obfuscation is a triple QPT of following algorithms:

- (Key generation)$Gen(1^n) = k \in K_n$, where K_n is the uniform key space $\{0,1\}^n$, and Gen randomly chooses k from K_n,
- (Encryption) $Enc_k(\rho) = X^\alpha Z^\beta \rho Z^\beta X^\alpha \otimes O(U_{k,r})$, where r is randomly chosen from $\{0,1\}^{2n}$,α is the first *n* bits of r, and β is the last *n* bits of r,
- (Decryption) $Dec_k(c\otimes\Omega) = Z^{\beta'} X^{\alpha'} c X^{\alpha'} Z^{\beta'}$, wherer r' is the measurement result of $Tr_1[\delta(\Omega\otimes|k,0^{2n}\rangle\langle 0^{2n}|)]$, α' is the first *n* bits of r' , and β' is the last *n* bits of r' .

SCHEME ANALYSIS

1. IND-CPA-secure encryption from a self-combinable obfuscator

If a quantum point obfuscator *O* is self-combinable, then the quantum symmetric encryption scheme is IND-CPA-secure.

$$|\Pr\{D^{Enc}[(Enc_k\otimes I_E)\rho_{ME}]=1]\}$$
$$-\Pr\{D^{Enc}[(Enc_k\otimes I_E)(|0\rangle\langle 0|_M\otimes\rho_E)]$$
$$=1]\}|\le |\Pr\{A'[O(U_{k,r_1}),\dots,O(U_{k,r_t});\ Enc_k(\rho)]=1]|\}$$
$$-\Pr\{A'[O(U_{k,r_1}),\dots,O(U_{k,r_t});\ Enc_k(|0\rangle)]$$
$$=1]\Big|\le \Big|\Pr\left\{S^{O(U_{k,r_1}),\dots,O(U_{k,r_1})}[Enc_k(\rho)]=1]\Big]\right\}$$
$$-\Pr\left\{S^{O(U_{k,r_1}),\dots,O(U_{k,r_1})}[Enc_k(|0\rangle)]=1\Big]\right\}\Big| + negl(n)$$
$$\le negl(n)$$

2. Leakage-resilient encryption from an obfuscation with auxiliary input

If (O,δ) is an quantum point obfuscator with auxiliary input f , then the quantum symmetric encryption scheme is leakage-resilient against key information $f(k)$.

$$\Big|\Pr\{D[(Enc_k\otimes I_E)\rho_{ME}, f(k)]$$
$$=1\}-\Pr\{D\big[(Enc_k\otimes I_E)(|0\rangle\langle 0|_M\otimes\rho_E), f(k)\big]=1]\}$$
$$=|\Pr\left\{D\left[s, O(U_{k,r}), f(k)\right]\right.$$
$$=1\}-\Pr\{D[t, O(U_{k,r}), f(k)]=1\}|$$
$$\le \sum_{g(r)} |\Pr\{D[s,g(r)]=1\}-\Pr\{D[t,g(r)]$$
$$=1\Big|\Big\}.\Pr[D'[O(U_{k,r}), f(k)]=g(r)]$$

CONCLUSION

To develop the theory of quantum obfuscation, its application is crucial. In this paper, we demonstrated the usability of a quantum point obfuscator in quantum symmetric key encryption. We gave the construction of quantum point obfuscation and proposed an IND-secure quantum symmetric encryption scheme based on point obfuscation. Then we proved the corresponding relationship between IND-security and obfuscator for a quantum symmetric encryption. In particular, different encryption security can be implemented according to the properties of an obfuscator. While previous works on encrypting quantum data are either based on QOTP or lacking implementation, our work gives the first concrete construction of quantum data encryption with reusable private key. Further work lies in how to build a suitable obfuscator by means of quantum encryption schemes.