A Multi-Valued Quantum Fully Homomorphic Encryption Scheme

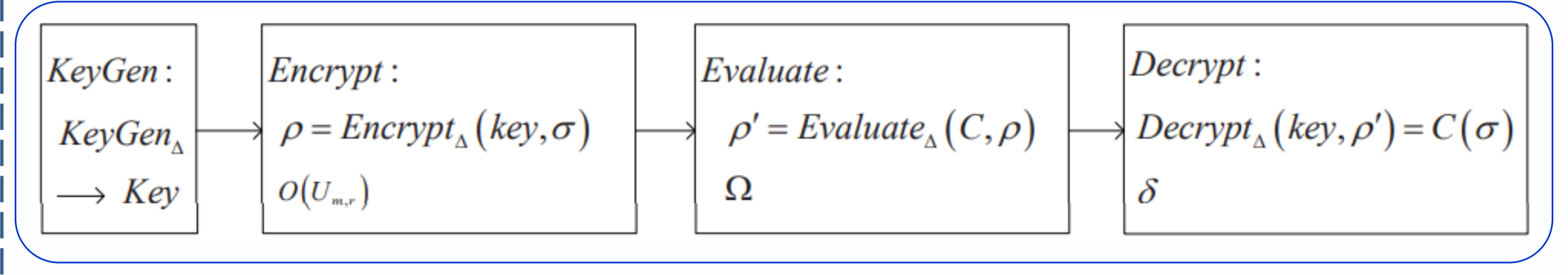
Yuanjing Zhang, Tao Shang, and Jianwei Liu
School of Cyber Science and Technology, Beihang University, Beijing, CHINA, 100083
Email: shangtao@buaa.edu.cn

BACKGROUND

1. Quantum homomorphic encryption（QHE）

We propose a QHE scheme based on point function obfuscation, including the following four algorithms.

1. QHE based on quantum obfuscation



$KeyGen$: $KeyGen_\Delta \longrightarrow Key$ → $Encrypt$: $\rho = Encrypt_\Delta(key,\sigma)$ $O(U_{m,r})$ → $Evaluate$: $\rho' = Evaluate_\Delta(C,\rho)$ Ω → $Decrypt$: $Decrypt_\Delta(key,\rho') = C(\sigma)$ δ

1) Key generation algorithm: In this algorithm, the encrypting party encodes the classical plaintext information into quantum state plaintext σ as required, and then uses the key generation algorithm $KeyGen_\Delta$ to randomly generate two keys $k, j \in \{0, 1, ..., d-1\}$ and save them.
2) Encryption algorithm: The encryption algorithm $Encrypt_\Delta$ performs encryption on the plaintext of quantum state according to the encryption key k, j to generate the quantum state ciphertext $\rho = Encrypt_\Delta(k,j,\sigma) = V_d^k W_d^j \sigma$. The encrypting party sends $\rho \otimes O(U_{m,r})$ to the evaluator, where k is the first bit of r and j is the last bit of r. The encrypting party must be fully quantum plaintext state and classical key information.
3) Evaluation algorithm: After the evaluator receives the quantum state ciphertext ρ from the encrypting party, it generates the evaluation parameters α, β according to its computing requirements. It performs the evaluation $\rho' = Evaluate\Delta(\alpha,\beta,\rho) = U_{\alpha,\beta} \cdot \rho$ on the received quantum state ciphertext, and sends the result $\rho' \otimes \Omega$ to the decrypting party via the quantum-secure channel.
4) Decryption algorithm: After the evaluator receives the calculation result of the evaluation, it uses interpreter δ to measure Ω to obtain k, j, and adopts the decryption algorithm $Decrypt_\Delta$ to perform the decryption $\sigma' = Decrypt_\Delta(k,j,\rho') = V_d^{-k} W_d^{-j} \rho' = U_{\alpha,\beta}\sigma$ based on the key k, j.

2. 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
$$|\Pr\left[D\left(A\big(O(C)\big)\right) = 1\right] - \Pr\left[D\big(S^{U_C}(|0^n\rangle)\big) = 1\right] \le negl(n)$$

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 a multi-valued quantum fully homomorphic encryption scheme by means of quantum point obfuscation. Our work formally demonstrates the scalability and application of quantum obfuscation. We hope that such work will be constructive in the field of quantum obfuscation.

PROPOSED SCHEMES

1. Multi-aluedv quantum random oracle model

The multi-valued quantum random oracle machine is a quantum polynomial time algorithm R_q that satisfies the following properties:

– When any party (adversary or challenger) accesses with the classical constant $k \in N$, the binary converter B will convert k into a classical bit string $\{0,1\}^m$.

– R_q randomly and uniformly generates the quantum state $|R_q(B(k))\rangle \in (H^2)^{\otimes s}$of s-qubits, where $s = ploy\ (m)$.

– The output of the different inputs of any pair of multi-valued quantum random oracles R_q is nearly orthogonal
$$|\langle R_q(B(k))|R_q(B(k'))\rangle|^2 < \varepsilon$$

Where $B(k) \neq B(k')$, ε is negligible for the parameter m.

– If R_q is accessed by the challenger as input k, the multi-valued quantum random oracle machine R_q produces c copies of the output to the adversary.

2. Multi-valued quantum point function

The multi-valued quantum single-point function is defined as follows:
$$U_{a,b}: |x, y, G_{l,j}\rangle \to |x, y, G_{l+P_a(x), j+P_b(y)}\rangle$$

Where $x, y \in G_{l,j}, j = 1, \dots, d, l = 0, \dots, d-1$, $P_a(x)$ and $P_b(y)$ are the following classical functions:
$$P_a(x) = \begin{cases} a & x = a \\ d - a & x \neq a \end{cases}$$
$$P_b(y) = \begin{cases} b & y = b \\ d - b & y \neq b \end{cases}$$

where $a, b \in \{1, \dots, d-1\}$.

We define $C_{a,b} = \{C_{a,b}: a, b \in \{0, \dots, d\}\}$, where $C_{a,b}$ is a quantum circuit that implements the corresponding function of the unitary matrix $U_{a,b}$. The structure of the multi-valued quantum single-point function obfuscator $O^{R_q}\ (U_{a,b})$ can be given as follows:

(Multi-valued quantum single-point obfuscation scheme) The obfuscator $O^{R_q}\ (U_{a,b})$ asks the multi-valued quantum random oracle machine R_q with a, b to obtain the quantum states$R_q(B(a)), R_q(B(b))$, and the obfuscator $O^{R_q}\ (U_{a,b})$ stores the obtained quantum state $r_a = R_q(B(a)), r_b = R_q(B(b))$, when inputting $x, y \in G_{l,j}$, will output $G_{l+a,j}$ if $R_q(B(x))$=r_a , $G_{l,j+b}$ if $R_q(B(y))$=r_b , $G_{l+a,j+b}$ if $R_q(B(x))$=r_a, $R_q(B(y))$=r_b , otherwise $G_{l+d-a,j+d-b}$.

The multi-valued quantum multi-point function is defined as follows:
$$U_{(a_1,b_1),\dots,(a_i,b_i)}: |x, y, G_{l,j}\rangle \to |x, y, G_{l+P_{a_1,\dots,a_i}(x), j+P_{b_1,\dots,b_i}(y)}\rangle$$

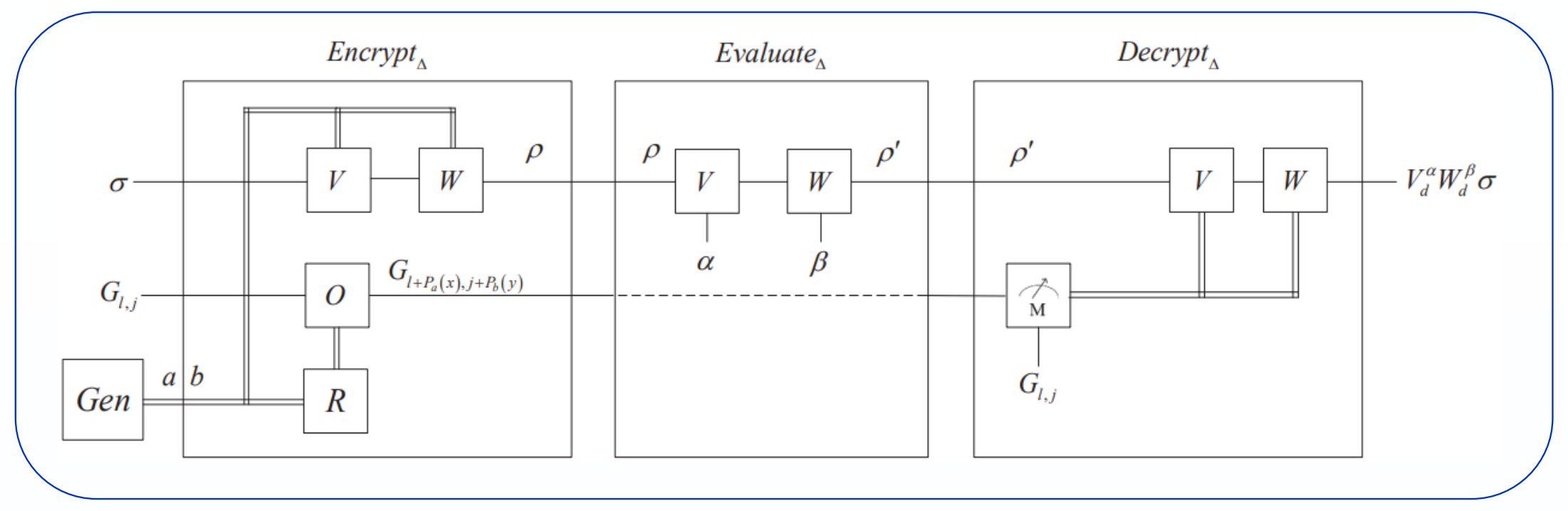
Where $x, y \in G_{l,j}, j = 1, \dots, d, l = 0, \dots, d-1$,$P_{a_1,\dots,a_i}(x)$and $P_{b_1,\dots,b_i}(y)$ are the following classical functions:
$$P_{a_1,\dots,a_i}(x) = \begin{cases} a_i & x = a_i \\ d - a_i x \neq a_i \end{cases}$$
$$P_{b_1,\dots,b_i}(y) = \begin{cases} b_i & y = b_i \\ d - b_i y \neq b_i \end{cases}$$

where $a_i, b_i \in \{1, \dots, d-1\}, i \in 1, \dots, n$.

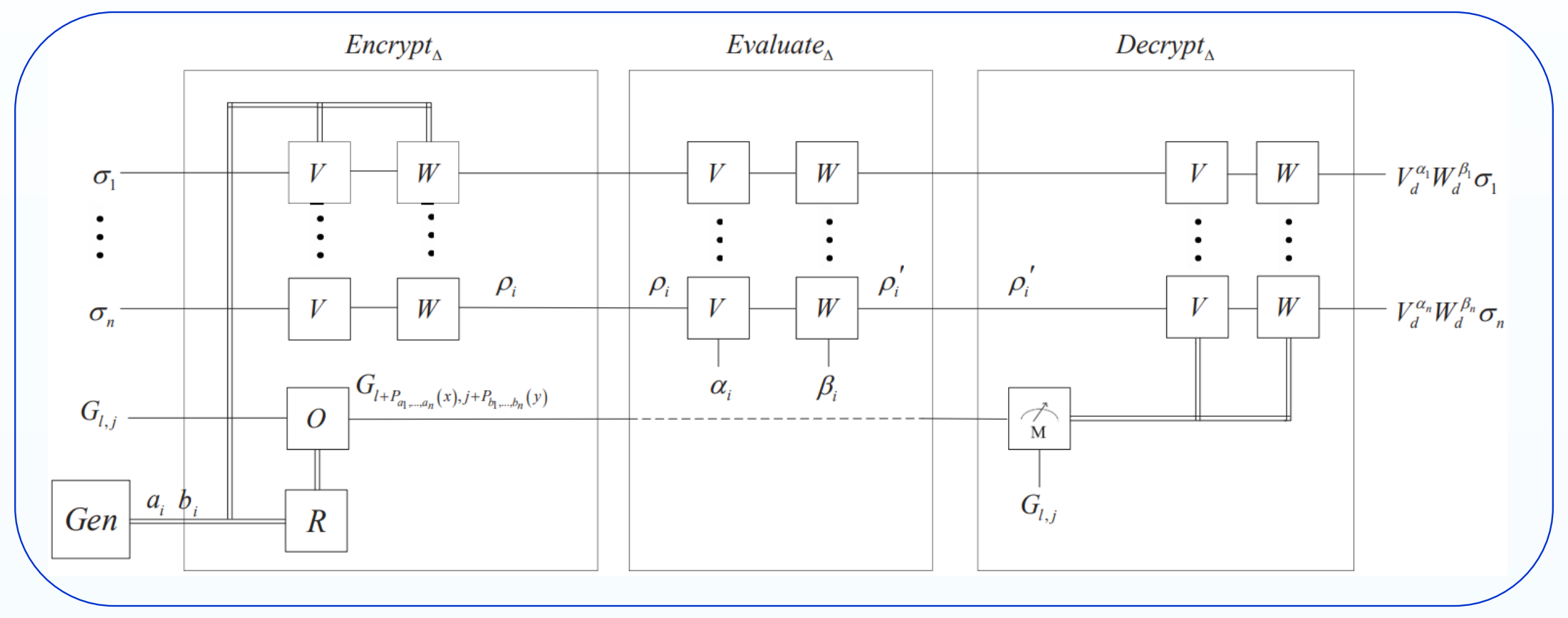
We define $C_{(a_1,b_1),\dots,(a_i,b_i)} = \{C_{(a_1,b_1),\dots,(a_i,b_i)}: a_i, b_i \in \{0, \dots, d\}\}$, where $C_{(a_1,b_1),\dots,(a_i,b_i)}$ is a quantum circuit that implements the corresponding function of the unitary matrix$U_{(a_1,b_1),\dots,(a_i,b_i)}$. The structure of the multi-valued quantum multi-point function obfuscator $O^{R_q}\ (U_{(a_1,b_1),\dots,(a_i,b_i)})$ is similar to $O^{R_q}\ (U_{a,b})$.

3. Quantum fully homomorphic encryption scheme

2. Quantum circuit diagram of the QFHE scheme with single qubit



3. Quantum circuit diagram of the QFHE scheme with multiple qubits



QFHE scheme with multi-valued quantum single-point obfuscation is a four-tuple of quantum algorithms：

(Key generation) $KeyGen_\Delta$: $(a, b, G_{l,j}) -> O$. The key generation algorithm $KeyGen_\Delta$ randomly generates two classical keys, $a, b \in \{1, \dots, d-1\}$. Then the obfuscator O asks the multi-valued quantum random oracle machine R_q with a, b to obtain the quantum state $R_q(B(a)), R_q(B(b))$, and the obfuscator O stores the obtained quantum state $r_a = R_q(B(a)), r_b = R_q(B(b))$, $G_{l,j}$ is the multi-valued quantum state randomly generated by the encrypting party and the decrypting party.

(Encryption) $Encrypt_\Delta: \sigma -> \rho$. The encryption algorithm $Encrypt_\Delta$ performs encryption on the plaintext σ of quantum state with the key a, b to generate the quantum state ciphertext $\rho = Encrypt_\Delta(a,b,\sigma))$. Then the encrypting party sends ρ to the evaluator via the quantum-secure channel and sends the result $G_{l+P_a(x),j+P_b(y)}$ of obfuscator O to the decrypting party.

(Homomorphic Evaluation) $Evaluate_\Delta$: $\rho -> \rho'$. After the evaluator receives the quantum state ciphertext ρ from the encrypting party, it generates the evaluation parameters α, β according to its computing requirements. It performs the evaluation $\rho' = Evaluate_\Delta(\alpha,\beta,\rho) = V_d^\alpha W_d^\beta \rho$ on the received quantum state ciphertext, and sends the result ρ' to the decrypting party via the quantum-secure channel.

(Decryption) $Decrypt_\Delta$: $\rho' -> \sigma'$. After the decrypting party receives the calculation result of the evaluator, it adopts the decryption algorithm $Decrypt_\Delta$ to perform the decryption $\sigma' = Decrypt_\Delta(a,b,\rho') = V_d^\alpha W_d^\beta \sigma$ based on the key a, b.

The structure of QFHE scheme with multi-valued quantum multi-point obfuscation is similar to the QFHE scheme with multi-valued quantum single-point obfuscation.

SCHEME ANALYSIS

QFHE scheme with multi-valued quantum single-point obfuscation is IND-CPA (indistinguishability under chosen plaintext attack)-secure.
$$\begin{aligned}
&|\Pr\{D^{Encrypt}[(Encrypt_\Delta \otimes I_E)\rho_{ME}] = 1]\} \\
&- \Pr\{D^{Encrypt}[(Encrypt_\Delta \otimes I_E)(|0\rangle\langle 0|_M \otimes \rho_E)] \\
&= 1]\}| \le |\Pr\{A'[O(U_{a_1,b_1}), \dots, O(U_{a_t,b_t});\ Encrypt_\Delta(\rho)] = 1]|\} \\
&- \Pr\{A'[O(U_{a_1,b_1}), \dots, O(U_{a_t,b_t}); Encrypt_\Delta(|0\rangle)] \\
&= 1]\,\Big| \le \Big|\Pr\left\{S^{O(U_{a_1,b_1}),\dots,O(U_{a_t,b_t})}[Encrypt_\Delta(\rho)] = 1]\right]\} \\
&- \Pr\left\{S^{O(U_{a_1,b_1}),\dots,O(U_{a_t,b_t})}[Encrypt_\Delta(|0\rangle)] = 1\right]\Big\}\Big| + negl(n) \\
&\le negl(n)
\end{aligned}$$

The outputs of the encryption algorithm and the evaluation algorithm of the QFHE scheme with single qubit are in completely mixed states, which means that an attacker cannot obtain any valuable information of the message sent by the encrypting party from the mixed state, so the scheme is information-theoretic security.
$$\begin{aligned}
&\frac{1}{d^2}\sum_{a,b\in\{0,\dots,d-1\}} V_d^a W_d^b \varphi (V_d^a W_d^b)^\dagger \\
&= \frac{1}{d^2}\sum_{a,b\in\{0,\dots,d-1\}} V_d^a W_d^b \varphi (W_d^b)^\dagger (V_d^a)^\dagger \\
&= \frac{1}{d^2}\sum_{a,b\in\{0,\dots,d-1\}} \left(\sum_{x=0}^{d-1} \omega^{x(a+bx)}|x\rangle \cdot \sum_{\mathrm{m}=0}^{d-1} p_m|m\rangle \cdot \sum_{x=0}^{d-1} \omega^{-x(a+bx)}|x\rangle\right) \\
&= \frac{1}{d^2}\sum_{a,b\in\{0,\dots,d-1\}} \left(\sum_{x=0}^{d-1} p_m \omega^{\mathrm{m}(a+bm)}|m\rangle\langle m| \cdot \sum_{x=0}^{d-1} \omega^{-x(a+bx)}|x\rangle\langle x|\right) \\
&= \frac{1}{d^2}\sum_{a,b\in\{0,\dots,d-1\}} \left(\sum_{x=0}^{d-1} p_m \omega^{\mathrm{m}(a+bm)} \omega^{-\mathrm{m}(a+bm)}|m\rangle\langle m|\right) \\
&= \frac{1}{d^2}\sum_{a,b\in\{0,\dots,d-1\}} p_m I_d
\end{aligned}$$

Similarly, QFHE scheme with multi-valued quantum multi-point obfuscation is also IND-CPA-secure and information-theoretic security.

CONCLUSION

To develop the theory of quantum obfuscation, its application is crucial. In this paper, from the perspective of quantum obfuscation, we proposed two QFHE schemes with multi-valued quantum point obfuscation, including single-qubit and multi-qubit QFHE schemes. The two schemes are completely independent of secret key. Since the mean value of the encryption output and the evaluation output are completely mixed, an attacker cannot obtain any information output without knowing the distribution of plaintext information of quantum state in advance, which further strengthens security.

With the development of quantum communication and quantum computation, the demand for entrusted computing in the quantum environment will greatly increase. Although the proposed schemes break through the limitation of low dimension, the demand for secure multi-party computation still needs to be considered in the future.