Generalized one-way function and its application

Hua-Lei Yin[1, *]

[1] *Department of Physics and Beijing Key Laboratory of Opto-electronic Functional Materials and Micro-nano Devices, Key Laboratory of Quantum State Construction and Manipulation (Ministry of Education), Renmin University of China, Beijing 100872, China*

(Dated: August 27, 2024)

One-way functions are fundamental to classical cryptography and their existence remains a long-standing problem in computational complexity theory [1, 2]. Recently, a provable quantum one-way function has been identified, which maintains its one-wayness even with unlimited computational resources [3]. Here, we extend the mathematical definition of functions to construct a generalized one-way function by virtually measuring the qubit of provable quantum one-way function and randomly assigning the corresponding measurement outcomes with identical probability. Remarkably, using this generalized one-way function, we have developed an unconditionally secure key distribution protocol based solely on classical data processing, which can then utilized for secure encryption and signature. Our work highlights the importance of information in characterizing quantum systems and the physical significance of the density matrix. We demonstrate that probability theory and randomness are effective tools for countering adversaries with unlimited computational capabilities.

Cryptography plays a crucial role in protecting personal privacy, safeguarding national security, and advancing the digital economy. Modern cryptography originated from Shannon's introduction of information theory into cryptanalysis, where the one-time pad was demonstrated to offer unconditional security through probability theory [4]. Specifically, the posterior probability of the plaintext, given the ciphertext in the one-time pad, remains equal to the prior probability of the plaintext, even when adversaries have unlimited computational resources [4, 5]. To address key length and key reuse issues, Shannon introduced the concepts of diffusion and confusion [4], which facilitated the development of symmetric encryption algorithms such as the Advanced Encryption Standard [6]. To tackle key distribution challenges in large user networks, public-key cryptography was developed [7]. Central to this is the concept of the one-way function, which provides asymmetry [1] and is a critical resource for designing digital signatures [2], zero-knowledge proof [8], and secure multiparty computation [9].

One-way function is a particular type of function f that is computationally easy to evaluate in the forward direction but difficult to invert. Specifically, for each input x, $f(x)$ can be computed in polynomial time. However, given a random output $f(x)$, it is infeasible to determine the input x using a deterministic Turing machine in polynomial time [1]. Although the existence of one-way functions remains unproven, Numerous public-key cryptographic systems [7, 10–16] have been proposed based on the assumption of specific one-way functions, with some of these systems evolving into widely adopted standards on the Internet. Indeed, proving the existence of one-way functions would also substantiate the conjecture that $\mathcal{P} \neq \mathcal{NP}$, one of the seven Millennium Prize Problems. However, the truth of $\mathcal{P} \neq \mathcal{NP}$ does not necessarily imply the existence of one-way functions.

Unfortunately, certain problems traditionally considered as one-way functions have been compromised by known quantum algorithms [17]. For instance, the quantum Fourier transform can efficiently solve period-finding problems, encompassing prime factorization and discrete logarithm among others. Additionally, the hidden subgroup problem in finite abelian groups is vulnerable to exponential speedup attacks by quantum computations [18]. Consequently, the latest development in public-key cryptography, post-quantum cryptography [19], is regarded as resistant to quantum computing attacks [20]. For instance, lattice-based cryptography [21, 22], which relies on non-commutative hidden subgroup problems, is a prominent example. Table I summarizes various public-key cryptographic systems and the one-way functions upon which they are based. Actually, even if one-way functions exist, public-key cryptography cannot be secure against adversaries with unlimited computational resources, as such adversaries could potentially exhaustively explore all possible results to find the correct solution. Here, we develop a generalized one-way function with rigorous one-wayness and applied it to the design of unconditionally secure key distribution.

Generalized one-way function

To introduce our generalized one-way function, let us first retrospect a quantum system fundamentally distinct from its classical counterpart (Fig. 1A). A two-dimensional quantum system can be represented on the Bloch sphere, where a pure state is described by $|\phi(\theta,\varphi)\rangle = \cos\frac{\theta}{2}|+z\rangle + e^{\mathbf{i}\varphi}\sin\frac{\theta}{2}|-z\rangle$, lying on the sphere's surface. Here, $|\phi(\theta,\varphi)\rangle$ represents a superposition of $|+z\rangle$ and $|-z\rangle$ with a fixed phase φ. Measuring in the $\mathcal{X}$ ba-

TABLE I. Summary of notable public-key cryptographic systems, outlining the task, one-way function and the level of security.

Scheme	Cryptographic task	One-way function	Computational security (Quantum)	Unconditional security
Diffie-Hellman [7]	Key distribution	Discrete logarithm	No	No
Rivest-Shamir-Adleman [10]	Encryption and signature	Prime factorization	No	No
ElGamal [11]	Encryption and signature	Discrete logarithm	No	No
Elliptic-curve [12, 13]	Key distribution Encryption and signature	Discrete logarithm	No	No
CRYSTALS-Kyber [14]	Encryption	Learning with errors	Maybe	No
CRYSTALS-Dilithium [15]	Signature	Learning with errors Short integer solution	Maybe	No
SPHINCS$^+$ [16]	Signature	Stateless hash function	Maybe	No

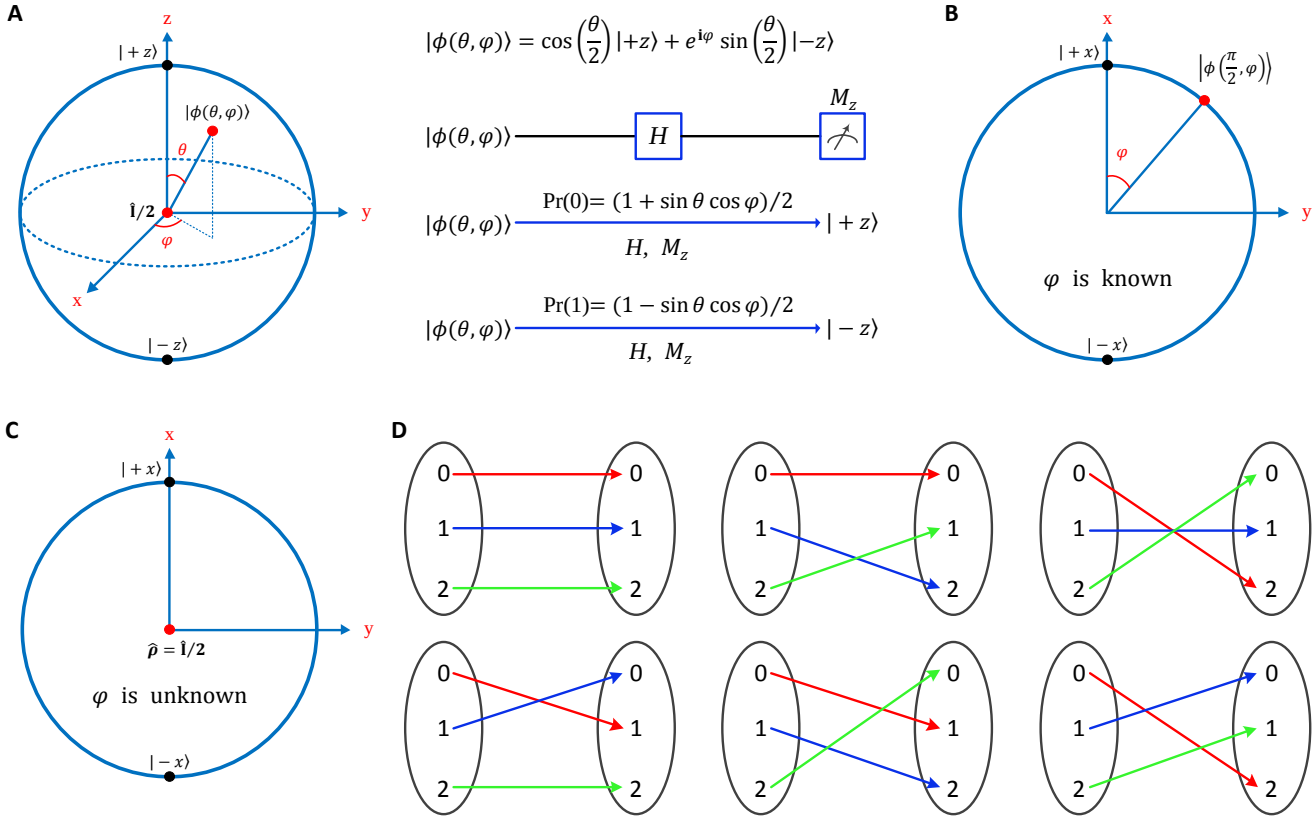

FIG. 1. **Pure state and mixed state of a two-dimensional quantum system.** (**A**) Bloch sphere representation of a density matirx. A superposition state, when measured in the $\mathcal{X}$ basis–which is realized by a Hadamard gate H followed by a $\mathcal{Z}$ basis measurement M_z–will collapse randomly into one of the eigenstates of the measurement operator with a certain probability. (**B**) A quantum system can be represented as a pure state $|\phi(\frac{\pi}{2},\varphi)\rangle$ on the periphery of the x − y circle if one has the phase information φ and $\theta = \frac{\pi}{2}$. (**C**) A quantum system can only be represented as the maximally mixed state $\hat{\mathbf{I}}/2$ if $\theta = \frac{\theta}{2}$ and no phase information φ is available. (**D**) The random mapping rule $f_k : j \to j'$. There are $m!$ (with $m = 3$ as an example) possible random mappings from a finite domain of size m to a finite codomain of size m.

sis yields $|+z\rangle$ with probability $(1 + \sin\theta\cos\varphi)/2$ and $|-z\rangle$ with probability $(1 - \sin\theta\cos\varphi)/2$. The maximally mixed state $\hat{\mathbf{I}}/2$ is located at the center of the Bloch sphere. A quantum system is considered a pure state only if the parameters θ and φ are known. Specifically, $|\phi(\theta = \frac{\pi}{2},\varphi)\rangle = \left(|+z\rangle + e^{i\varphi}|-z\rangle\right)/\sqrt{2}$ lies on the edge of the x − y circle (Fig. 1B). Conversely, if the phase is unknown and random, the system is in a maximally mixed

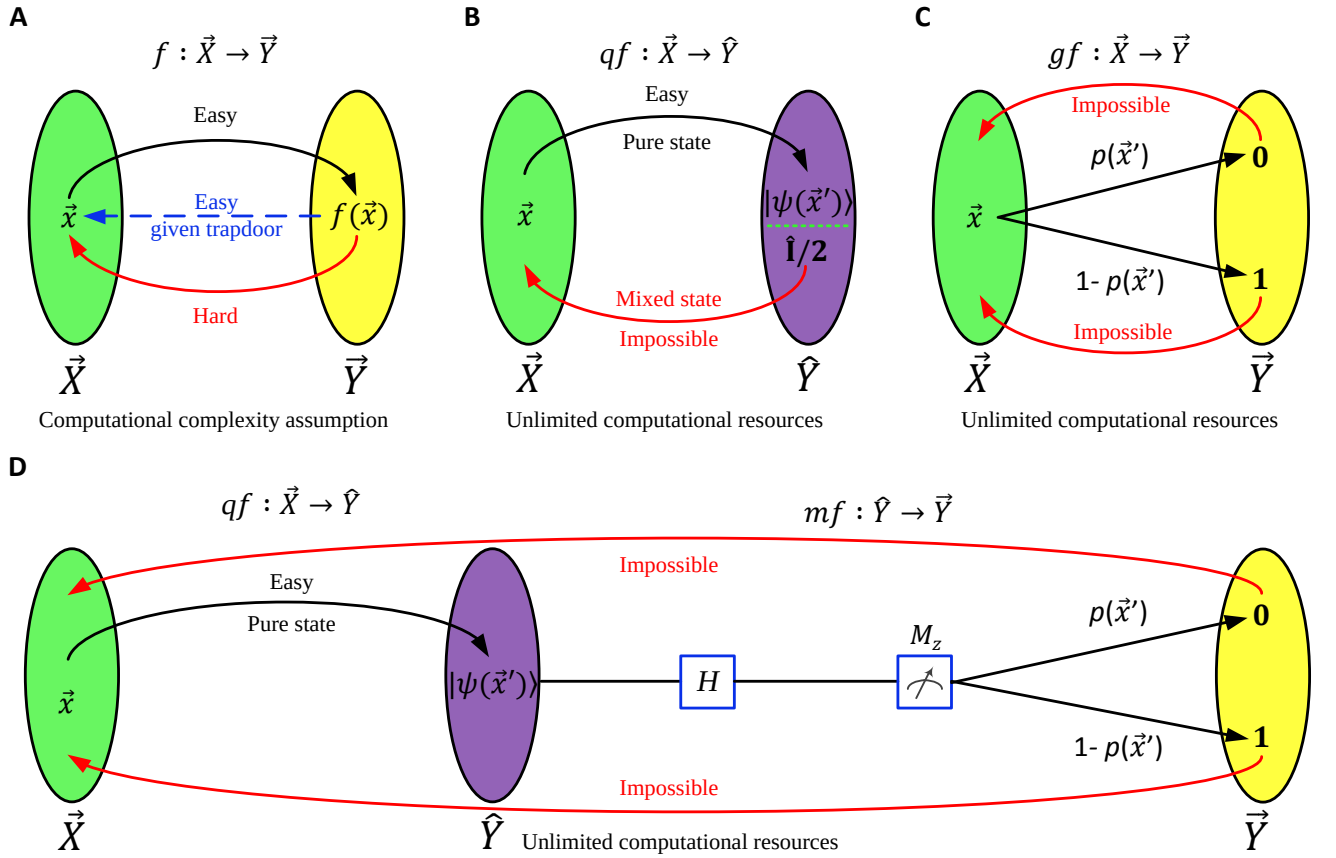

FIG. 2. **Comparison of several one-way functions.** (**A**) Traditional one-way function based on the computational complexity assumptions. The forward computation is straightforward, while the reverse problem is very difficult. Once the trapdoor information is acquired, the solution becomes easily accessible. (**B**) Provable quantum one-way function. The one-wayness is rigorously maintained even with unlimited computational resources. The forward and backward quantum states are entirely distinct, as the quantum state of a system evolves with the information acquired. (**C**) Generalized one-way function. (**D**) Provable quantum one-way function combined with the $\mathcal{X}$ basis measurement. For each input $\vec{x}$ (where the random mapping rule transforms $\vec{x}$ to $\vec{x}'$), there is a probability $p(\vec{x}')$ of obtaining output 0 and $1-p(\vec{x}')$ of obtaining output 1.

state $\hat{\mathbf{I}}/2$ (Fig. 1C). Thus, the quantum state of the same system can vary depending on the observer's information.

In a game between a sender and a receiver, the sender randomly selects one of m symmetric qubits, $|\psi(j)\rangle = \left(|+z\rangle + e^{\mathbf{i}\frac{2\pi}{m}j}|-z\rangle\right)/\sqrt{2}$, with equal probability based on a random index $j \in \{0,1,\ldots,m-1\}$, and sends it to the receiver. The receiver's task is to identify which of the m states was chosen (i.e., determine j). From the receiver's perspective, since the phase $\varphi = \frac{2\pi}{m}j$ is completely unknown, the received qubit can only be perceived as a maximally mixed state,

$$\hat{\rho} = \frac{1}{m}\sum_{j=0}^{m-1}|\psi(j)\rangle\langle\psi(j)| = \frac{\hat{\mathbf{I}}}{2}. \tag{1}$$

The minimum probability of an incorrect answer by the receiver is $1-2/m$ when the process is repeated independently a sufficient number of times (see supplementary materials). It is close to the error rate of $1-1/m$ that would be achieved by guessing one of the m states completely at random when m is large. To prevent the adversary from inferring fixed bit values based on the phase interval, the concept of a random mapping rule is introduced [3]. *Random Mapping* [2]: Let $\mathcal{K}_m$ denote the collection of all one-to-one mappings from the domain $\{0,1,\ldots,m-1\}$ to the codomain $\{0,1,\ldots,m-1\}$. The k-th element of $\mathcal{K}_m$ is referred to as a k-th random mapping rule $f_k : j \to j'$. Clearly, there are $|\mathcal{K}_m| = m!$ possible mapping rules (see Fig. 1D). Assuming that every mapping in $\mathcal{K}_m$ is equally likely, it can be determined by random numbers consisting of $m\log_2 m$ bits [3]. Under the random mapping rule $f_k : j \to j'$, even if the phases of two qubits are nearly identical, their corresponding indices are entirely unrelated.

In public-key cryptography utilizing traditional one-way functions $f:\vec{X}\to\vec{Y}$ (see Fig. 2A), the output $f(\vec{x})$

derived from the input $\vec{x}$ is classical data. This output is deterministic and accessible to all parties, including potential adversaries. Consequently, the adversary can employ the output $f(\vec{x})$, leveraging unlimited computational resources, to successfully decipher the original input $\vec{x}$. In contrast, with our provable quantum one-way function $qf : \vec{X} \to \hat{Y}$ (see Fig. 2B), the output is a quantum system. Due to the application of the random mapping rule $f_k : \vec{x} \to \vec{x}'$ and random input x, the adversary lacks any knowledge of the original input $\vec{x}$, even when provided with unlimited computational resources. From the adversary's perspective, the quantum system cannot be described as a pure state $|\psi(\vec{x}')\rangle$ but must instead be represented by a maximally mixed state $\hat{\mathbf{I}}/2$. This directly provides an asymmetry between the adversary and the legitimate user. This implies that, regardless of the classical or quantum operations performed by the adversary on the quantum system within the framework of the provable quantum one-way function, the one-wayness remains rigorously maintained. If we focus solely on the input $\vec{X}$ and output $\vec{Y}$, it becomes evident that the generalized one-way function $gf : \vec{X} \to \vec{Y}$ (see Fig.2C) is equivalent to the provable quantum one-way function $qf : \vec{X} \to \hat{Y}$ combined with the $\mathcal{X}$ basis measurement $mf : \hat{Y} \to \vec{Y}$ (see Fig.2D). The rigorous one-wayness of the generalized one-way function is preserved because the $\mathcal{X}$ basis measurement can be conceptually regarded as a special quantum operation performed by the adversary in the context of the provable quantum one-way function.

Generalized One-Way Function: Consider a set of independent and randomly generated binary bit substrings $\vec{x}_i \in \{0,1\}^{\log_2 m}$, where $i \in \{1,2,\ldots,n\}$, which together constitute the input data string $\vec{X} = \vec{x}_1||\vec{x}_2||\ldots||\vec{x}_n$. The k-th ($k \in \{1,2,\ldots,m!\}$) random mapping rule transforms $\vec{x}_i$ into $\vec{x}'_i$, such that $f_k(\vec{x}_i) = \vec{x}'_i$. The binary bit value $\vec{y}_i \in 0,1$ will form the output data string $\vec{Y} = \vec{y}_1||\vec{y}_2||\ldots||\vec{y}_n$. The generalized one-way function $gf : \vec{X} \to \vec{Y}$ is defined as a multivalued function that maps the input data string $\vec{X} \in \{0,1\}^{n\log_2 m}$ to the output data string $\vec{Y} \in \{0,1\}^n$. The mapping is given by:

$$\vec{y}_i = gf(\vec{x}_i) = \begin{cases} 0, & \text{probability } \frac{1+\cos\left[\frac{2\pi}{m} f_k(\vec{x}_i)\right]}{2}, \\ 1, & \text{probability } \frac{1-\cos\left[\frac{2\pi}{m} f_k(\vec{x}_i)\right]}{2}, \end{cases} \tag{2}$$

where m is a sufficiently large integer. Note that the binary bit string is automatically converted to a decimal value as needed during calculations. When preparing n qubit states $\bigotimes_{i=1}^{n} |\psi(\vec{x}'_i)\rangle$, the output data string $\vec{Y}$ can be directly obtained using the $\mathcal{X}$ basis measurement acting on each qubit state. To introduce an equivalent *virtual measurement* employed in our generalized one-way function, consider the following steps: First, nb-bit quantum random numbers are used to form bit string $\vec{A} = \vec{a}_1||\vec{a}_2||\cdots||\vec{a}_n$ with $\vec{a}_i \in \{0,1\}^b$. Second, if $0 \le \vec{a}_i < 2^{b-1}\left[1+\cos\left(\frac{2\pi}{m}\vec{x}'_i\right)\right]$, then $\vec{y}_i = 0$; otherwise, $\vec{y}_i = 1$.

In fact, the rigorous one-wayness of the generalized one-way function can be proven not only using provable quantum one-way function based on density matrix theory, but also through probability theory method. By calculation (see supplementary materials), we find that

$$\Pr[\vec{x}_i|\vec{y}_i] = \frac{\Pr[\vec{y}_i|\vec{x}_i]\Pr[\vec{x}_i]}{\Pr[\vec{y}_i]} = \Pr[\vec{x}_i], \tag{3}$$

and if m is sufficiently large, the following holds:

$$\Pr[\vec{X}|\vec{Y}] \sim \Pr[\vec{X}]. \tag{4}$$

Thus, the a posteriori probability that the input data is $\vec{X}$, given that the output $\vec{Y}$ is observed, is nearly identical to the prior probability that the input is $\vec{X}$. In other words, after applying the generalized one-way function to a completely random input data string $\vec{X}$, we cannot exclude any possible values of $\vec{X}$; all values of $\vec{X}$ are almost equally probable if we only know the output data string $\vec{Y}$.

Probability key distribution

A direct application of the generalized one-way function is the construction of an unconditionally secure key distribution protocol, referred to as Probability Key Distribution (PKD). As illustrated in Fig. 3, our PKD protocol employs full classical data processing, allowing it to be readily implemented in any network environment. A notable feature of PKD is that Alice and Bob are required to share random bit strings $\vec{K} \in \{0,1\}^s$, $\vec{K}_{\text{fix}} \in \{0,1\}^{s+t-1}$, and $K_0 \in \{0,1\}^{m\log_2^m}$. Specifically, the random bit strings $\vec{K}$ and K_0 are used only once per session and are updated in subsequent sessions, whereas the random bit string $\vec{K}_{\text{fix}}$ is reused across thousands of sessions before being updated.

For each session, Alice employs quantum random numbers to decide the k-th random mapping rule f_k [3]. She uses the random bit string $\vec{K}_0$ as a key and transmits the mapping rule f_k to Bob using the one-time pad. Alice utilizes quantum random numbers to construct the input data string $\vec{X} = \vec{x}_1||\vec{x}_2||\cdots||\vec{x}_n \in \{0,1\}^{n\log_2^m}$, which is then mapped to $\vec{X}' = \vec{x}'_1||\vec{x}'_2||\cdots||\vec{x}'_n$ using the random mapping rule $f_k : \vec{x}_i \to \vec{x}'_i$. Alice then applies the virtual measurement operation to obtain the output data string $\vec{Y}$. To meet the criteria of a generalized one-way function $\vec{X} \to \vec{Y}$, the generated data string $\vec{D} \in \{0,1\}^{n\log_2^m}$ must cover all possible values in each session, given that Eve has access to $\vec{X} \oplus \vec{D}$. Thus, let $\vec{D} = \vec{K}\mathbf{H}$, where $\mathbf{H}$ is a Toeplitz matrix with s rows and t columns ($t = n\log_2 m$), generated from the random bit string $\vec{K}_{\text{fix}}$. Due to the rigorous one-wayness of the generalized one-way function, the bit strings $\vec{K}$ and $\vec{K}_{\text{fix}}$ remain unknown and random

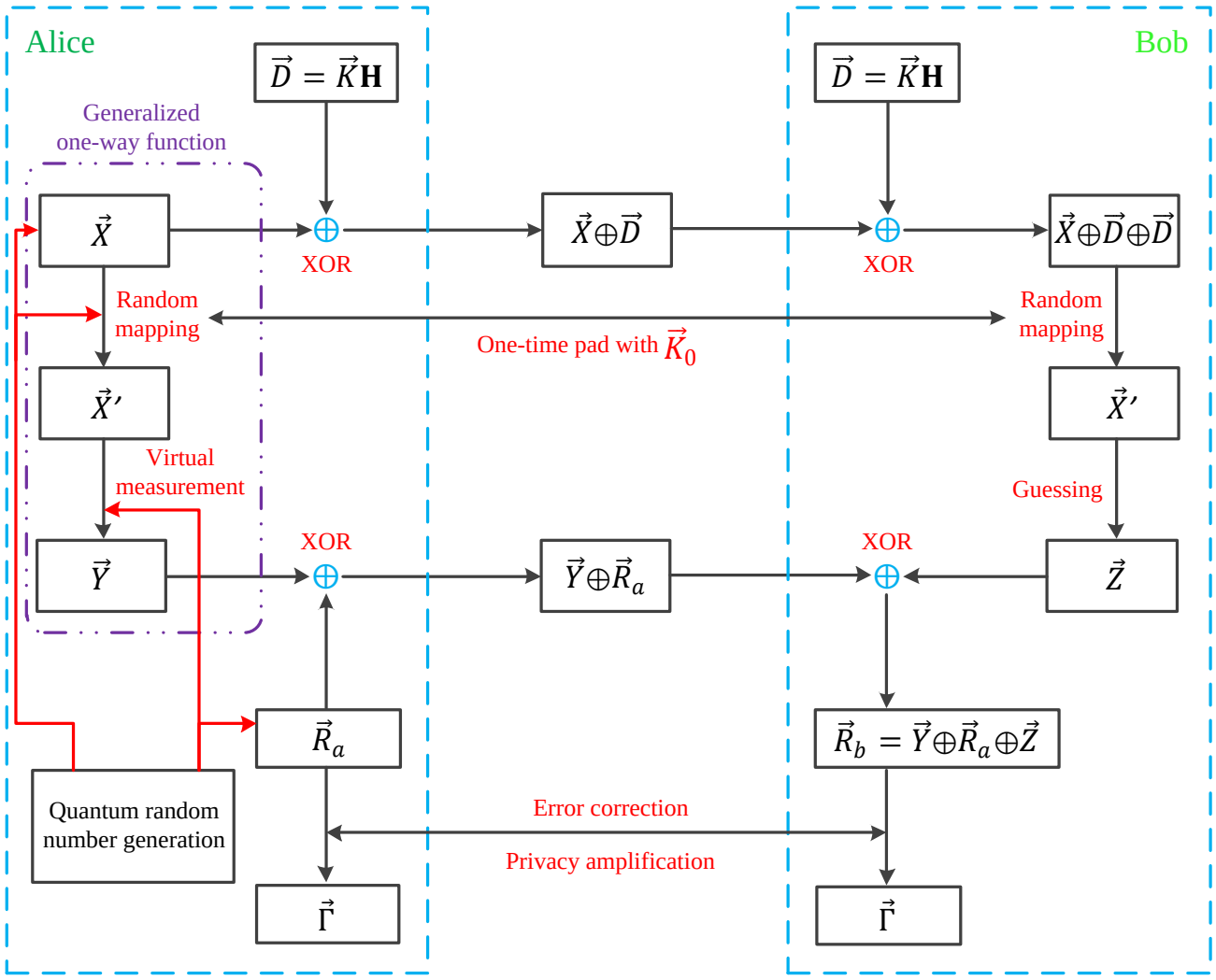

FIG. 3. **Schematic diagram of PKD protocol.** In each session, Alice uses the generalized one-way function to generate a bit string $\vec{Y}$ based on the input random bit string $\vec{X}$. Alice and Bob exchange the random bit string $\vec{X}$ using a data string $\vec{D}$, which is produced from the pre-shared bit string $\vec{K}$ and a Toeplitz matrix $\mathbf{H}$. Alice then announces the XOR results $\vec{Y}\oplus\vec{R}_a$, where $\vec{R}_a$ is her raw key. Bob guesses the bit string $\vec{Y}$ to obtain $\vec{Z}$ based on the received $\vec{X}$. To deduce Alice's raw key $\vec{R}_a$, Bob computes his own raw key $\vec{R}_b$ by performing an XOR operation between $\vec{Y}\oplus\vec{R}_a$ and $\vec{Z}$. Finally, Alice and Bob apply error correction and privacy amplification to derive an identical and secret key bit string $\vec{\Gamma}$.

from Eve's perspective, even if Eve knows $\vec{Y}$. Consequently, only Alice and Bob can access the bit string $\vec{X}$. To correctly deduce Alice's raw key $\vec{R}_a$, Bob uses the same mapping rule f_k to derive $\vec{X}'$ and attempts to estimate $\vec{Y}$ as accurately as possible, resulting in bit string $\vec{Z} = \vec{z}_1||\vec{z}_2\cdots||\vec{z}_n$. One possible approach is to set $\vec{z}_i = 0$ if $0 \le \vec{x}'_i < m/4$ or $3m/4 \le \vec{x}'_i < m$, and $\vec{z}_i = 1$ if $m/4 \le \vec{x}'_i < 3m/4$.

The value of $\vec{z}_i$ is deterministically associated with the interval of $\vec{x}'_i$, so Bob cannot disclose any information about his own raw key $\vec{R}_a = \vec{R}_a \oplus \vec{Y} \oplus \vec{Z}$ throughout the error correction process. Using Alice's raw key $\vec{R}_a$ as a reference, Bob corrects his raw key $\vec{R}_b$ to align with Alice's through an error correction algorithm, such as a low-density parity check code. The amount of information required for the error correction step is $\lambda = nfh(E)$. The Shannon entropy function is $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$. $E = \frac{1}{2} - \frac{1}{\pi} \simeq 18.2\%$ ($f \ge 1$) is the bit error rate (the error correction efficiency) between $\vec{R}_a$ and $\vec{R}_b$. After error correction, error verification and privacy amplification, if the secret key length ℓ of one session satisfies [3]

$$\ell \le n - \lambda - \log_2 \frac{2}{\varepsilon_{\rm cor}} - 2\log_2 \frac{3}{2\varepsilon_{\rm sec}}, \tag{5}$$

our PKD protocol is $\varepsilon_{\rm cor}$-correct and $\varepsilon_{\rm sec}$-secret. The

net remaining secret key length for each session is $\ell - s - m\log_2 m$, as $\vec{K}_{\text{fix}}$ is updated only after thousands of sessions, making its cost negligible. The secret key rate of our OKD primarily depends on the data processing rate of system and the quantum random number generation rate. For optional parameters, we set $m = 2^{10}$, $n = 10^{10}$, $s = 10^4$, $b = 12$, $\varepsilon_{\text{cor}} = 10^{-15}$ and $\varepsilon_{\text{sec}} = 10^{-10}$. Actually, if both error correction and error verification communications utilize one-time pad encrypted transmission, one can obtain a nearly perfectly secret key without employing complex privacy amplification post-processing.

On one hand, combining PKD with a one-time pad achieves unconditionally secure encryption, ensuring the confidentiality of information processing [4]. On the other hand, integrating PKD with one-time universal hashing and secret sharing enables unconditionally secure signatures, providing authenticity, integrity, and non-repudiation in information processing [23].

Outlook

In summary, we have developed a generalized one-way function with rigorous one-wayness, addressing a long-standing open problem in computational complexity and cryptography. We have also proposed an unconditionally secure key distribution protocol based on this function, relying entirely on classical data processing. The core of our unconditional security is founded on the randomness of quantum physics, the density matrix theory of quantum mechanics, and probability theory of mathematics. Compared to our recent result [3], this work employs phase-randomized qubit superposition states rather than phase-randomized weak coherent states, which directly translates the quantum state preparation and measurement into a fully classical process. Additionally, the bit error rate of raw keys has improved from 25% to 18.2%. These advancements make our PKD protocol suitable for widespread and cost-effective deployment in the emerging digital economy, with high efficiency and unconditional security. We also anticipate that the generalized one-way function will find broad applications in other unconditionally secure cryptographic primitives.

Acknowledgements

We gratefully acknowledge the support from the National Natural Science Foundation of China (No. 12274223).

* hlyin@ruc.edu.cn

[1] Goldreich, O. *Foundations of Cryptography: Basic Techniques* (Cambridge University Press, 2001).
[2] Menezes, A. J., van Oorschot, P. C. & Vanstone, S. A. *Handbook of applied cryptography* (CRC press, 1996).
[3] Yin, H.-L. Unconditionally secure key distribution without quantum channel (2024).
[4] Shannon, C. E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **28**, 656–715 (1949).
[5] Stinson, D. R. *Cryptography: theory and practice* (CRC Press, 1995).
[6] Daemen, J. & Rijmen, V. *The design of Rijndael*, vol. 2 (Springer, 2002).
[7] Diffie, W. & Hellman, M. E. New directions in cryptography. *IEEE Transactions on Information Theory* **22**, 644–654 (1976).
[8] Goldwasser, S., Micali, S. & Rackoff, C. The knowledge complexity of interactive proof-systems. In *Proceedings of the 17th Annual ACM Symposium on Theory of Computing*, 291–304 (1985).
[9] Yao, A. C. Protocols for secure computations. In *23rd annual symposium on foundations of computer science (sfcs 1982)*, 160–164 (IEEE, 1982).
[10] Rivest, R. L., Shamir, A. & Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM* **21**, 120–126 (1978).
[11] ElGamal, T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory* **31**, 469–472 (1985).
[12] Koblitz, N. Elliptic curve cryptosystems. *Mathematics of computation* **48**, 203–209 (1987).
[13] Miller, V. S. Use of elliptic curves in cryptography. In *Advances in Cryptology—CRYPTO'85 Proceedings. Lecture Notes in Computer Science.*, vol. 85, 417–426 (Springer, 1985).
[14] Bos, J. *et al.* Crystals-kyber: a cca-secure module-lattice-based kem. In *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, 353–367 (IEEE, 2018).
[15] Ducas, L. *et al.* Crystals-dilithium: A lattice-based digital signature scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems* **2018**, 238–268 (2018).
[16] Bernstein, D. J. *et al.* The sphincs$^+$ signature framework. In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, 2129–2146 (2019).
[17] Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review* **41**, 303–332 (1999).
[18] Mosca, M. & Ekert, A. The hidden subgroup problem and eigenvalue estimation on a quantum computer. In *NASA International Conference on Quantum Computing and Quantum Communications*, 174–188 (Springer, 1998).
[19] Bernstein, D. J. & Lange, T. Post-quantum cryptography. *Nature* **549**, 188–194 (2017).
[20] Alagic, G. *et al.* Status report on the third round of the nist post-quantum cryptography standardization process (2022).
[21] Ajtai, M. Generating hard instances of lattice problems. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 99–108 (1996).
[22] Micciancio, D. & Regev, O. Lattice-based cryptography. In *Post-quantum cryptography*, 147–191 (Springer, 2009).
[23] Yin, H.-L. *et al.* Experimental quantum secure network with digital signatures and encryption. *Natl. Sci. Rev.* **10**, nwac228 (2023).

Supplementary Information for "Generalized one-way function and its application"

Hua-Lei Yin[1,*]

[1]*Department of Physics and Beijing Key Laboratory of Opto-electronic Functional Materials and Micro-nano Devices, Key Laboratory of Quantum State Construction and Manipulation (Ministry of Education), Renmin University of China, Beijing 100872, China*

(Dated: August 27, 2024)

I. MINIMUM ERROR DISCRIMINATION

For m possible states $\{\hat{\rho}_j\}_{j=0}^{m-1}$ with associated a priori probabilities $\{p_j\}_{j=0}^{m-1}$, there is a POVM $\{E_j\}_{j=0}^{m-1}$ with m elements that can achieve minimum error discrimination. For many cases, the minimum error discrimination measurement is the square-root measurement. In addition, there is an important conclusion for square-root measurements; i.e., for any set of pure states, there is at least one set of prior probabilities such that the minimum error discrimination measurement for this set of states is the square root measurement. The POVM elements of the square-root measurement can be given by [1]

$$\hat{E}_j = p_j \hat{\rho}^{-1/2} \hat{\rho}_j \hat{\rho}^{-1/2}, \tag{S1}$$

where $\hat{\rho} = \sum_{j=0}^{m-1} p_j \hat{\rho}_j$. Obviously, the above operator E_j is positive, and $\sum_{j=0}^{m-1} \hat{E}_j = \hat{\mathbf{I}}$.

The square-root measurement is the minimum error discrimination measurement for symmetric pure states. Considering m symmetric pure states $\left\{|\psi(j)\rangle = \frac{1}{\sqrt{2}}(|+z\rangle + e^{\mathbf{i}2\pi j/m}|-z\rangle)\right\}_{j=0}^{m-1}$ with a uniform priori probability of $p_j = 1/m$. The Gram matrix of the states we are trying to distinguish between is an $m \times m$ matrix, where the matrix element $G_{i,j}$ of the i-th row and j-th column can be defined as

$$\begin{aligned} G_{i,j} = \langle\psi(i)|\psi(j)\rangle &= \frac{1}{\sqrt{2}}\left(\langle+z| + e^{-\mathbf{i}2\pi i/m}\langle-z|\right)\frac{1}{\sqrt{2}}\left(|+z\rangle + e^{\mathbf{i}2\pi j/m}|-z\rangle\right) \\ &= \frac{1}{2}\left[1 + e^{\mathbf{i}2\pi(j-i)/m}\right], \end{aligned} \tag{S2}$$

where $i, j = 0, 1, \ldots, m-1$. Note that we let the matrix start with zero rows and zero columns instead of one row and one column for consistency. Obviously, the Gram matrix G is a circulant matrix since it relies only on the difference $j - i$. It can be diagonalized with the unitary discrete Fourier transform. The eigenvalue λ_r of Gram matrix G can be given by

$$\lambda_r = \sum_{k=0}^{m-1} c_k \omega^{kr} \tag{S3}$$

where we have $r = 0, 1, \ldots, m-1$, $\omega = e^{\mathbf{i}2\pi/m}$ and $c_k = \frac{1}{2}\left(1 + e^{\mathbf{i}2\pi k/m}\right)$. The optimal minimum error discrimination probability $P_{\min}$ can be written as [2]

$$\begin{aligned} P_{\min} &= 1 - \frac{1}{m^2}\left|\sum_{r=0}^{m-1}\sqrt{\lambda_r}\right|^2 \\ &= 1 - \frac{1}{m^2}\left|\sum_{r=0}^{m-1}\sqrt{\sum_{k=0}^{m-1}\frac{e^{\mathbf{i}2\pi kr/m}}{2}(1 + e^{\mathbf{i}2\pi k/m})}\right|^2, \\ &= 1 - \frac{2}{m}. \end{aligned} \tag{S4}$$

*Electronic address: hlyin@ruc.edu.cn

We also have an intuitive explanation of the above minimum error discrimination results $P_{\min} = 1 - 2/m$ if m is even. Let two qubit states $\{|\psi(k)\rangle, |\psi(k+m/2)\rangle\}$ be the k-th set ($0 \le k \le m/2-1$), there are $m/2$ different sets. The density matrix of each set is identical to the maximally mixed state, i.e.,

$$\begin{aligned}\hat{\rho}_k &= \frac{1}{2}\left[|\psi(k)\rangle\langle\psi(k)| + |\psi(k+m/2)\rangle\langle\psi(k+m/2)|\right] \\ &= \frac{1}{2}(|+z\rangle\langle+z| + |-z\rangle\langle-z|) = \frac{\hat{\mathbf{I}}}{2}.\end{aligned} \tag{S5}$$

Obviously, no one can distinguish the $m/2$ different sets with the same density matrix. The adversary can only randomly guess one set from $m/2$ sets, and the probability of guessing error is $1 - 2/m$. Besides, in each set, the two qubit states are orthogonal and thus can be distinguished with 100% probability. Therefore, the minimum error discrimination probability is $P_{\min} = 1 - \frac{2}{m}$ for m symmetric qubit states.

We remark that m symmetric pure qubit states $\{|\psi(j)\rangle\}_{j=0}^{m-1}$ are linearly dependent quantum states

$$\begin{aligned}\hat{\rho} &= \frac{1}{m}\sum_{j=0}^{m-1}|\psi(j)\rangle\langle\psi(j)| \\ &= \frac{1}{2}(|+z\rangle\langle+z| + |-z\rangle\langle-z|) = \frac{\hat{\mathbf{I}}}{2},\end{aligned} \tag{S6}$$

where unambiguous quantum state discrimination cannot be successfully performed. An unambiguous state discrimination measurement among m linearly dependent qubit states is only possible when at least $m-1$ copies of the states are available [3].

If the adversary does not have the quantum state, who can only randomly guess and has an error probability of $1 - \frac{1}{m}$. For sufficiently large m, the minimum error discrimination is almost the same as a random guess. If we go from guessing the quantum state to guessing the encoded bit substring corresponding to the quantum state, the random mapping rule $f_k : j \to j'$ further removes the difference between the minimum error discrimination measurement and random guessing since each qubit state corresponds to all possible bit substrings.

Consider a quantum system consisting of n subsystems, where each subsystem is one of m symmetric qubits with equal probability. Clearly, the quantum-state sender perceives the entire system as a pure state comprising n qubits. In contrast, from the recipient's perspective, the system appears as a mixed state, represented by $\hat{\rho}^{\otimes n}$, which is the tensor product of n copies of the state $\hat{\rho}$. The mixed state representation $\hat{\rho}^{\otimes n}$ of quantum system can be written as

$$\begin{aligned}\hat{\rho}^{\otimes n} = \frac{\hat{\mathbf{I}}^{\otimes n}}{2^n} &= \left(\frac{1}{m}\sum_{j=0}^{m-1}|\psi(j)\rangle\langle\psi(j)|\right)^{\otimes n} \\ &= \frac{1}{m^n}\left\{\sum_{\substack{r_0+r_1+\cdots+r_{m-1}=n \\ r_j\ge 0,\ 0\le j\le m-1}}\left[\binom{n}{r_1, r_2, \cdots, r_{m-1}}\bigotimes_{0\le j\le m-1}\left(|\psi(j)\rangle\langle\psi(j)|\right)^{\otimes r_j}\right]\right\},\end{aligned} \tag{S7}$$

where $r_j \ge 0$ is integer and multinomial coefficient is given by

$$\binom{n}{r_1, r_2, \cdots, r_{m-1}} = \frac{n!}{\prod_{j=0}^{m-1} r_j!}. \tag{S8}$$

Each subsystem is measured independently in the $\mathcal{X}$ basis for the virtual generalized one-way function.

II. CONDITIONAL PROBABILITY DISTRIBUTION OF RANDOM VARIABLE

In this section, we first review the generalized one-way function in the main text. *Generalized one-way function*: Let independent and random binary bit substrings $\vec{x}_i \in \{0,1\}^{\log_2 m}$ with $i = \{1, 2, \ldots, n\}$ constitute the input data string $\vec{X} = \vec{x}_1||\vec{x}_2|\ldots||\vec{x}_n$. The k-th ($k \in \{1, 2, \ldots, m!\}$) random mapping rule makes the $\vec{x}_i$ map to $\vec{x}'_i$, i.e., $f_k(\vec{x}_i) = \vec{x}'_i$. The binary bit value $\vec{y}_i \in \{0, 1\}$ will consist the output data string $\vec{Y} = \vec{y}_1||\vec{y}_2||\ldots||\vec{y}_n$. Thus, a multivalue function

maps the input data string $\vec{X} \in \{0,1\}^{n\log_2 m}$ to the output data string $\vec{Y} \in \{0,1\}^n$ is the generalized one-way function $gf : \vec{X} \to \vec{Y}$ if we have

$$\vec{y}_i = gf(\vec{x}_i) = \begin{cases} 0, & \text{probability} \frac{1+\cos\left[\frac{2\pi}{m} f_k(\vec{x}_i)\right]}{2}, \\ 1, & \text{probability} \frac{1-\cos\left[\frac{2\pi}{m} f_k(\vec{x}_i)\right]}{2}, \end{cases} \tag{S9}$$

where m is large enough.

A. Independent attack

Let us introduce three random variables $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{K}$. Let $\vec{x}_i \in \{0,1\}^{\log_2 m}$, $\vec{y}_i \in \{0,1\}$ and $k \in \{1,2,\ldots,m!\}$ be the values of random variables $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{K}$, respectively. According to the definition of the generalized one-way function above, the conditional probability distribution of the random variable $\mathcal{Y}$ can be given by

$$\Pr[\mathcal{Y} = \vec{y}_i | (\mathcal{K} = k, \mathcal{X} = \vec{x}_i)] = \frac{\Pr(\mathcal{Y} = \vec{y}_i, \mathcal{K} = k, \mathcal{X} = \vec{x}_i)}{\Pr(\mathcal{K} = k, \mathcal{X} = \vec{x}_i)} = \frac{1 + (-1)^{\vec{y}_i} \cos\left[\frac{2\pi}{m} f_k(\vec{x}_i)\right]}{2}, \tag{S10}$$

where we have probability

$$\Pr(\mathcal{K} = k, \mathcal{X} = \vec{x}_i) = \frac{1}{m!}\frac{1}{m}. \tag{S11}$$

Therefore, the joint probability distribution of three random variables $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{K}$ can be written as

$$\Pr(\mathcal{Y} = \vec{y}_i, \mathcal{K} = k, \mathcal{X} = \vec{x}_i) = \frac{1 + (-1)^{\vec{y}_i} \cos\left[\frac{2\pi}{m} f_k(\vec{x}_i)\right]}{2m(m!)}. \tag{S12}$$

Obviously, for any integer $m \geq 2$, one can obtain the following conclusions:

$$\frac{1}{m}\sum_{j=0}^{m-1} \frac{1 \pm \cos[2\pi j/m]}{2} = \frac{1}{2}, \tag{S13}$$

and

$$\begin{aligned} \Pr[\mathcal{Y} = \vec{y}_i] &= \sum_{k,\vec{x}_i} \Pr[\mathcal{Y} = \vec{y}_i, \mathcal{K} = k, \mathcal{X} = \vec{x}_i] = \frac{1}{2}, \\ \Pr[\mathcal{Y} = \vec{y}_i | \mathcal{X} = \vec{x}_i] &= \frac{\Pr(\mathcal{Y} = \vec{y}_i, \mathcal{X} = \vec{x}_i)}{\Pr(\mathcal{X} = \vec{x}_i)} = \frac{\sum_k \Pr(\mathcal{Y} = \vec{y}_i, \mathcal{K} = k, \mathcal{X} = \vec{x}_i)}{\Pr(\mathcal{X} = \vec{x}_i)} = \frac{1}{2}. \end{aligned} \tag{S14}$$

Using Bayes' theorem, we have

$$\begin{aligned} \Pr[\mathcal{X} = \vec{x}_i | \mathcal{Y} = \vec{y}_i] &= \frac{\Pr[\mathcal{Y} = \vec{y}_i | \mathcal{X} = \vec{x}_i] \times \Pr[\mathcal{X} = \vec{x}_i]}{\Pr[\mathcal{Y} = \vec{y}_i]} \\ &= \Pr[\mathcal{X} = \vec{x}_i] = \frac{1}{m}. \end{aligned} \tag{S15}$$

One can obtain the simplified form $\Pr[\vec{x}_i|\vec{y}_i] = \Pr[\vec{x}_i]$. That is, the a posteriori probability $\vec{x}_i$, given that the result $\vec{y}_i$ is observed, is identical to the a priori probability $\vec{x}_i$. Therefore, if the adversary considers the individual output bits of the generalized one-way function, then all the inputs are equally likely. The adversary cannot obtain any information of the input data $\vec{X}$ from the output data $\vec{Y}$ according to the generalized one-way function.

B. Joint attack

However, the adversary can also perform a joint analysis of multiple output bits or even entire output bit strings. Here, we provide a direct analysis showing that multi-bit joint analysis approximates single-bit independent analysis in terms of conditional probability and Shannon entropy. For the input data string $\vec{X} = \vec{x}_1||\vec{x}_2|\ldots||\vec{x}_n$ and random bit substrings $\vec{x}_i \in \{0,1\}^{\log_2 m}$ with $i = \{1,2,\ldots,n\}$, consider a string $\vec{Y}_d$ of output bits at any d positions and the corresponding input string $\vec{X}_d$, given the independence of random bit substrings $\vec{x}_i$. Although the random mapping rule is unknown, it is fixed, meaning that identical input bit strings $\vec{x}_i$ will produce identical states.

1. Arbitrary two-bit

Considering that $d = 2$ and $i = j, s$, the conditional probability of output $\vec{y}_j||\vec{y}_s$ given input $\vec{x}_j||\vec{x}_s$ can be given by

$$\Pr[(\vec{y}_j||\vec{y}_s)|(\vec{x}_j||\vec{x}_s)] = \frac{1}{m!}\sum_k \frac{1+(-1)^{\vec{y}_j}\cos\left[\frac{2\pi}{m}f_k(\vec{x}_j)\right]}{2}\frac{1+(-1)^{\vec{y}_s}\cos\left[\frac{2\pi}{m}f_k(\vec{x}_s)\right]}{2}. \tag{S16}$$

If bit substrings $\vec{x}_j \neq \vec{x}_s$, we have conditional probabilities

$$\begin{aligned}\Pr[(11)|(\vec{x}_j||\vec{x}_s)] = \Pr[(00)|(\vec{x}_j||\vec{x}_s)] &= \frac{1}{m!}\sum_k \frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_j)\right]}{2}\frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_s)\right]}{2} \\ &= \frac{1}{m(m-1)}\sum_{i=0}^{m-1}\sum_{u=0,u\neq i}^{m-1}\frac{1+\cos\frac{2\pi i}{m}}{2}\frac{1+\cos\frac{2\pi u}{m}}{2} \\ &= \frac{2m-3}{8(m-1)},\end{aligned} \tag{S17}$$

and

$$\begin{aligned}\Pr[(10)|(\vec{x}_j||\vec{x}_s)] = \Pr[(01)|(\vec{x}_j||\vec{x}_s)] &= \frac{1}{m!}\sum_k \frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_j)\right]}{2}\frac{1-\cos\left[\frac{2\pi}{m}f_k(\vec{x}_s)\right]}{2} \\ &= \frac{1}{m(m-1)}\sum_{i=0}^{m-1}\sum_{u=0,u\neq i}^{m-1}\frac{1+\cos\frac{2\pi i}{m}}{2}\frac{1-\cos\frac{2\pi u}{m}}{2} \\ &= \frac{2m-1}{8(m-1)}.\end{aligned} \tag{S18}$$

If bit substrings $\vec{x}_j = \vec{x}_s$, we have conditional probabilities

$$\begin{aligned}\Pr[(11)|(\vec{x}_j||\vec{x}_s)] = \Pr[(00)|(\vec{x}_j||\vec{x}_s)] &= \frac{1}{m!}\sum_k \frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_j)\right]}{2}\frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_s)\right]}{2} \\ &= \frac{1}{m}\sum_{i=0}^{m-1}\frac{1+\cos\frac{2\pi i}{m}}{2}\frac{1+\cos\frac{2\pi i}{m}}{2} \\ &= \frac{3}{8},\end{aligned} \tag{S19}$$

and

$$\begin{aligned}\Pr[(10)|(\vec{x}_j||\vec{x}_s)] = \Pr[(01)|(\vec{x}_j||\vec{x}_s)] &= \frac{1}{m!}\sum_k \frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_j)\right]}{2}\frac{1-\cos\left[\frac{2\pi}{m}f_k(\vec{x}_s)\right]}{2} \\ &= \frac{1}{m}\sum_{i=0}^{m-1}\frac{1+\cos\frac{2\pi i}{m}}{2}\frac{1-\cos\frac{2\pi i}{m}}{2} \\ &= \frac{1}{8}.\end{aligned} \tag{S20}$$

Obviously, $\Pr[00] = \Pr[01] = \Pr[10] = \Pr[11] = \frac{1}{4}$. Therefore, the posterior probabilities can be written as

$$\Pr[(\vec{x}_j||\vec{x}_s)|(11)] = \Pr[(\vec{x}_j||\vec{x}_s)|(00)] = \begin{cases}\frac{2m-3}{2(m-1)m^2}, & \vec{x}_j \neq \vec{x}_s, \\ \frac{3}{2m^2}, & \vec{x}_j = \vec{x}_s,\end{cases} \tag{S21}$$

and

$$\Pr[(\vec{x}_j||\vec{x}_s)|(10)] = \Pr[(\vec{x}_j||\vec{x}_s)|(01)] = \begin{cases}\frac{2m-1}{2(m-1)m^2}, & \vec{x}_j \neq \vec{x}_s, \\ \frac{1}{2m^2}, & \vec{x}_j = \vec{x}_s.\end{cases} \tag{S22}$$

Actually, we have the prior probabilities $\Pr[\vec{x}_j \neq \vec{x}_s] = 1 - \frac{1}{m}$ and $\Pr[\vec{x}_j = \vec{x}_s] = \frac{1}{m}$. For a sufficiently large m, according to Eqs. (S21) and (S22), we have the conclusion that

$$\Pr[(\vec{x}_j||\vec{x}_s)|(\vec{y}_j||\vec{y}_s)] \simeq \frac{1}{m^2} = \Pr[\vec{x}_j||\vec{x}_s]. \tag{S23}$$

This implies that the posterior probability of the input data being $\vec{x}_j||\vec{x}_s$, given the observed output $\vec{y}_j||\vec{y}_s$, is nearly identical to the prior probability of the input being $\vec{x}_j||\vec{x}_s$.

Given the output data $\vec{y}_j||\vec{y}_s$, the Shannon entropy of the input data $\vec{x}_j||\vec{x}_s$ can be given by

$$\begin{aligned}
H[(\vec{x}_j||\vec{x}_s)|(00)] = H[(\vec{x}_j||\vec{x}_s)|(11)] &= -\frac{2m-3}{2m}\log_2\frac{2m-3}{2(m-1)m^2} - \frac{3}{2m}\log_2\frac{3}{2m^2} \\
&= 2\log_2 m - \left(1-\frac{3}{2m}\right)\log_2\frac{2m-3}{2(m-1)} - \frac{3}{2m}\log_2\frac{3}{2} \\
&\simeq 2\log_2 m = H[\vec{x}_j||\vec{x}_s], \\
H[(\vec{x}_j||\vec{x}_s)|(01)] = H[(\vec{x}_j||\vec{x}_s)|(10)] &= -\frac{2m-1}{2m}\log_2\frac{2m-1}{2(m-1)m^2} - \frac{1}{2m}\log_2\frac{1}{2m^2} \\
&= 2\log_2 m - \left(1-\frac{1}{2m}\right)\log_2\frac{2m-1}{2(m-1)} + \frac{1}{2m} \\
&\simeq 2\log_2 m = H[\vec{x}_j||\vec{x}_s],
\end{aligned} \tag{S24}$$

where we assume that m is big enough.

2. *Arbitrary three-bit*

Considering $d = 3$ and $i = j, s, t$, the probability of output $\vec{y}_j||\vec{y}_s||\vec{y}_t$ given input $\vec{x}_j||\vec{x}_s||\vec{x}_t$ can be given by

$$\Pr[(\vec{y}_j||\vec{y}_s||\vec{y}_t)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \frac{1}{m!}\sum_k \frac{1+(-1)^{\vec{y}_j}\cos\left[\frac{2\pi}{m}f_k(\vec{x}_j)\right]}{2}\frac{1+(-1)^{\vec{y}_s}\cos\left[\frac{2\pi}{m}f_k(\vec{x}_s)\right]}{2}\frac{1+(-1)^{\vec{y}_t}\cos\left[\frac{2\pi}{m}f_k(\vec{x}_t)\right]}{2}. \tag{S25}$$

If $\vec{x}_j \neq \vec{x}_s \neq \vec{x}_t$, we have conditional probabilities $\Pr[(111)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \Pr[(000)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)]$,

$$\begin{aligned}
\Pr[(000)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] &= \frac{1}{m!}\sum_k \frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_j)\right]}{2}\frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_s)\right]}{2}\frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_t)\right]}{2} \\
&= \frac{1}{m(m-1)(m-2)}\sum_{i=0}^{m-1}\sum_{u=0,u\neq i}^{m-1}\sum_{v=0,v\neq i,v\neq u}^{m-1}\frac{1+\cos\frac{2\pi i}{m}}{2}\frac{1+\cos\frac{2\pi u}{m}}{2}\frac{1+\cos\frac{2\pi v}{m}}{2} \\
&= \frac{2m^2-9m+10}{16(m-1)(m-2)},
\end{aligned} \tag{S26}$$

and $\Pr[(001)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \Pr[(010)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \Pr[(011)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \Pr[(100)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \Pr[(101)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \Pr[(110)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)]$,

$$\begin{aligned}
\Pr[(001)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] &= \frac{1}{m!}\sum_k \frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_j)\right]}{2}\frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_s)\right]}{2}\frac{1-\cos\left[\frac{2\pi}{m}f_k(\vec{x}_t)\right]}{2} \\
&= \frac{1}{m(m-1)(m-2)}\sum_{i=0}^{m-1}\sum_{u=0,u\neq i}^{m-1}\sum_{v=0,v\neq i,v\neq u}^{m-1}\frac{1+\cos\frac{2\pi i}{m}}{2}\frac{1+\cos\frac{2\pi u}{m}}{2}\frac{1-\cos\frac{2\pi v}{m}}{2} \\
&= \frac{2m^2-5m+2}{16(m-1)(m-2)},
\end{aligned} \tag{S27}$$

If $\vec{x}_j = \vec{x}_s \neq \vec{x}_t$, we have conditional probabilities $\Pr[(111)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \Pr[(000)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)]$,

$$\begin{aligned}\Pr[(000)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] &= \frac{1}{m!}\sum_k \frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_j)\right]}{2}\frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_s)\right]}{2}\frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_t)\right]}{2} \\ &= \frac{1}{m(m-1)}\sum_{i=0}^{m-1}\sum_{u=0,u\neq i}^{m-1}\frac{1+\cos\frac{2\pi i}{m}}{2}\frac{1+\cos\frac{2\pi i}{m}}{2}\frac{1+\cos\frac{2\pi u}{m}}{2} \\ &= \frac{3m-5}{16(m-1)},\end{aligned} \tag{S28}$$

and $\Pr[(110)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \Pr[(001)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)]$,

$$\begin{aligned}\Pr[(001)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] &= \frac{1}{m!}\sum_k \frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_j)\right]}{2}\frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_s)\right]}{2}\frac{1-\cos\left[\frac{2\pi}{m}f_k(\vec{x}_t)\right]}{2} \\ &= \frac{1}{m(m-1)}\sum_{i=0}^{m-1}\sum_{u=0,u\neq i}^{m-1}\frac{1+\cos\frac{2\pi i}{m}}{2}\frac{1+\cos\frac{2\pi i}{m}}{2}\frac{1-\cos\frac{2\pi u}{m}}{2} \\ &= \frac{3m-1}{16(m-1)},\end{aligned} \tag{S29}$$

and $\Pr[(010)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \Pr[(011)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \Pr[(100)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \Pr[(101)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)]$,

$$\begin{aligned}\Pr[(010)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] &= \frac{1}{m!}\sum_k \frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_j)\right]}{2}\frac{1-\cos\left[\frac{2\pi}{m}f_k(\vec{x}_s)\right]}{2}\frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_t)\right]}{2} \\ &= \frac{1}{m(m-1)}\sum_{i=0}^{m-1}\sum_{u=0,u\neq i}^{m-1}\frac{1+\cos\frac{2\pi i}{m}}{2}\frac{1-\cos\frac{2\pi i}{m}}{2}\frac{1+\cos\frac{2\pi u}{m}}{2} \\ &= \frac{1}{16}.\end{aligned} \tag{S30}$$

If $\vec{x}_j = \vec{x}_t \neq \vec{x}_s$, we have conditional probabilities $\Pr[(111)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \Pr[(000)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)]$,

$$\begin{aligned}\Pr[(000)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] &= \frac{1}{m!}\sum_k \frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_j)\right]}{2}\frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_s)\right]}{2}\frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_t)\right]}{2} \\ &= \frac{1}{m(m-1)}\sum_{i=0}^{m-1}\sum_{u=0,u\neq i}^{m-1}\frac{1+\cos\frac{2\pi i}{m}}{2}\frac{1+\cos\frac{2\pi u}{m}}{2}\frac{1+\cos\frac{2\pi i}{m}}{2} \\ &= \frac{3m-5}{16(m-1)},\end{aligned} \tag{S31}$$

and $\Pr[(101)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \Pr[(010)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)]$,

$$\begin{aligned}\Pr[(010)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] &= \frac{1}{m!}\sum_k \frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_j)\right]}{2}\frac{1-\cos\left[\frac{2\pi}{m}f_k(\vec{x}_s)\right]}{2}\frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_t)\right]}{2} \\ &= \frac{1}{m(m-1)}\sum_{i=0}^{m-1}\sum_{u=0,u\neq i}^{m-1}\frac{1+\cos\frac{2\pi i}{m}}{2}\frac{1-\cos\frac{2\pi u}{m}}{2}\frac{1+\cos\frac{2\pi i}{m}}{2} \\ &= \frac{3m-1}{16(m-1)},\end{aligned} \tag{S32}$$

and $\Pr[(001)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \Pr[(011)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \Pr[(100)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \Pr[(110)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)]$,

$$\begin{aligned}\Pr[(001)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] &= \frac{1}{m!}\sum_k \frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_j)\right]}{2}\frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_s)\right]}{2}\frac{1-\cos\left[\frac{2\pi}{m}f_k(\vec{x}_t)\right]}{2}\\ &= \frac{1}{m(m-1)}\sum_{i=0}^{m-1}\sum_{u=0,u\neq i}^{m-1}\frac{1+\cos\frac{2\pi i}{m}}{2}\frac{1+\cos\frac{2\pi u}{m}}{2}\frac{1-\cos\frac{2\pi i}{m}}{2}\\ &= \frac{1}{16}.\end{aligned} \tag{S33}$$

If $\vec{x}_j \neq \vec{x}_s = \vec{x}_t$, we have conditional probabilities $\Pr[(111)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \Pr[(000)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)]$,

$$\begin{aligned}\Pr[(000)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] &= \frac{1}{m!}\sum_k \frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_j)\right]}{2}\frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_s)\right]}{2}\frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_t)\right]}{2}\\ &= \frac{1}{m(m-1)}\sum_{i=0}^{m-1}\sum_{u=0,u\neq i}^{m-1}\frac{1+\cos\frac{2\pi u}{m}}{2}\frac{1+\cos\frac{2\pi i}{m}}{2}\frac{1+\cos\frac{2\pi i}{m}}{2}\\ &= \frac{3m-5}{16(m-1)},\end{aligned} \tag{S34}$$

and $\Pr[(011)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \Pr[(100)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)]$,

$$\begin{aligned}\Pr[(100)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] &= \frac{1}{m!}\sum_k \frac{1-\cos\left[\frac{2\pi}{m}f_k(\vec{x}_j)\right]}{2}\frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_s)\right]}{2}\frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_t)\right]}{2}\\ &= \frac{1}{m(m-1)}\sum_{i=0}^{m-1}\sum_{u=0,u\neq i}^{m-1}\frac{1-\cos\frac{2\pi u}{m}}{2}\frac{1+\cos\frac{2\pi i}{m}}{2}\frac{1+\cos\frac{2\pi i}{m}}{2}\\ &= \frac{3m-1}{16(m-1)},\end{aligned} \tag{S35}$$

and $\Pr[(001)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \Pr[(011)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \Pr[(100)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \Pr[(110)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)]$,

$$\begin{aligned}\Pr[(001)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] &= \frac{1}{m!}\sum_k \frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_j)\right]}{2}\frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_s)\right]}{2}\frac{1-\cos\left[\frac{2\pi}{m}f_k(\vec{x}_t)\right]}{2}\\ &= \frac{1}{m(m-1)}\sum_{i=0}^{m-1}\sum_{u=0,u\neq i}^{m-1}\frac{1+\cos\frac{2\pi u}{m}}{2}\frac{1+\cos\frac{2\pi i}{m}}{2}\frac{1-\cos\frac{2\pi i}{m}}{2}\\ &= \frac{1}{16}.\end{aligned} \tag{S36}$$

If $\vec{x}_j = \vec{x}_s = \vec{x}_t$, we have conditional probabilities $\Pr[(111)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \Pr[(000)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)]$,

$$\begin{aligned}\Pr[(000)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] &= \frac{1}{m!}\sum_k \frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_j)\right]}{2}\frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_s)\right]}{2}\frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_t)\right]}{2}\\ &= \frac{1}{m}\sum_{i=0}^{m-1}\frac{1+\cos\frac{2\pi i}{m}}{2}\frac{1+\cos\frac{2\pi i}{m}}{2}\frac{1+\cos\frac{2\pi i}{m}}{2}\\ &= \frac{5}{16},\end{aligned} \tag{S37}$$

and $\Pr[(001)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \Pr[(010)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \Pr[(011)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \Pr[(100)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \Pr[(101)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] = \Pr[(110)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)]$,

$$\begin{aligned}\Pr[(001)|(\vec{x}_j||\vec{x}_s||\vec{x}_t)] &= \frac{1}{m!}\sum_{k}\frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_j)\right]}{2}\frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x}_s)\right]}{2}\frac{1-\cos\left[\frac{2\pi}{m}f_k(\vec{x}_t)\right]}{2}\\ &= \frac{1}{m}\sum_{i=0}^{m-1}\frac{1+\cos\frac{2\pi i}{m}}{2}\frac{1+\cos\frac{2\pi i}{m}}{2}\frac{1-\cos\frac{2\pi i}{m}}{2}\\ &= \frac{1}{16}.\end{aligned} \tag{S38}$$

Obviously, $\Pr[000] = \Pr[001] = \Pr[010] = \Pr[011] = \Pr[100] = \Pr[101] = \Pr[110] = \Pr[111] = \frac{1}{8}$. Therefore, the conditional probabilities can be written as $\Pr[(\vec{x}_j||\vec{x}_s||\vec{x}_t)|(111)] = \Pr[(\vec{x}_j||\vec{x}_s||\vec{x}_t)|(000)]$,

$$\Pr[(\vec{x}_j||\vec{x}_s||\vec{x}_t)|(000)] = \begin{cases}\frac{2m^2-9m+10}{2(m-1)(m-2)m^3}, & \vec{x}_j \neq \vec{x}_s \neq \vec{x}_t,\\ \frac{3m-5}{2(m-1)m^3}, & \vec{x}_j = \vec{x}_s \neq \vec{x}_t,\\ \frac{3m-5}{2(m-1)m^3}, & \vec{x}_j = \vec{x}_t \neq \vec{x}_s,\\ \frac{3m-5}{2(m-1)m^3}, & \vec{x}_j \neq \vec{x}_s = \vec{x}_t,\\ \frac{5}{2m^3}, & \vec{x}_j = \vec{x}_s = \vec{x}_t,\end{cases} \tag{S39}$$

and $\Pr[(\vec{x}_j||\vec{x}_s||\vec{x}_t)|(001)] = \Pr[(\vec{x}_j||\vec{x}_s||\vec{x}_t)|(110)]$,

$$\Pr[(\vec{x}_j||\vec{x}_s||\vec{x}_t)|(001)] = \begin{cases}\frac{2m^2-5m+2}{2(m-1)(m-2)m^3}, & \vec{x}_j \neq \vec{x}_s \neq \vec{x}_t,\\ \frac{3m-1}{2(m-1)m^3}, & \vec{x}_j = \vec{x}_s \neq \vec{x}_t,\\ \frac{1}{2m^3}, & \vec{x}_j = \vec{x}_t \neq \vec{x}_s,\\ \frac{1}{2m^3}, & \vec{x}_j \neq \vec{x}_s = \vec{x}_t,\\ \frac{1}{2m^3}, & \vec{x}_j = \vec{x}_s = \vec{x}_t,\end{cases} \tag{S40}$$

and $\Pr[(\vec{x}_j||\vec{x}_s||\vec{x}_t)|(010)] = \Pr[(\vec{x}_j||\vec{x}_s||\vec{x}_t)|(101)]$,

$$\Pr[(\vec{x}_j||\vec{x}_s||\vec{x}_t)|(010)] = \begin{cases}\frac{2m^2-5m+2}{2(m-1)(m-2)m^3}, & \vec{x}_j \neq \vec{x}_s \neq \vec{x}_t,\\ \frac{1}{2m^3}, & \vec{x}_j = \vec{x}_s \neq \vec{x}_t,\\ \frac{3m-1}{2(m-1)m^3}, & \vec{x}_j = \vec{x}_t \neq \vec{x}_s,\\ \frac{1}{2m^3}, & \vec{x}_j \neq \vec{x}_s = \vec{x}_t,\\ \frac{1}{2m^3}, & \vec{x}_j = \vec{x}_s = \vec{x}_t,\end{cases} \tag{S41}$$

and $\Pr[(\vec{x}_j||\vec{x}_s||\vec{x}_t)|(011)] = \Pr[(\vec{x}_j||\vec{x}_s||\vec{x}_t)|(100)]$,

$$\Pr[(\vec{x}_j||\vec{x}_s||\vec{x}_t)|(100)] = \begin{cases} \frac{2m^2-5m+2}{2(m-1)(m-2)m^3}, & \vec{x}_j \neq \vec{x}_s \neq \vec{x}_t, \\ \frac{1}{2m^3}, & \vec{x}_j = \vec{x}_s \neq \vec{x}_t, \\ \frac{1}{2m^3}, & \vec{x}_j = \vec{x}_t \neq \vec{x}_s, \\ \frac{3m-1}{2(m-1)m^3}, & \vec{x}_j \neq \vec{x}_s = \vec{x}_t, \\ \frac{1}{2m^3}, & \vec{x}_j = \vec{x}_s = \vec{x}_t. \end{cases} \tag{S42}$$

Actually, we have the prior probabilities $\Pr[\vec{x}_j \neq \vec{x}_s \neq \vec{x}_t] = \frac{(m-1)(m-2)}{m^2}$ and $\Pr[\vec{x}_j = \vec{x}_s \neq \vec{x}_t] = \Pr[\vec{x}_j = \vec{x}_t \neq \vec{x}_s] = \Pr[\vec{x}_j \neq \vec{x}_s = \vec{x}_t] = \frac{m-1}{m^2}$ and $\Pr[\vec{x}_j = \vec{x}_s = \vec{x}_t] = \frac{1}{m^2}$. For a sufficiently large m, we have the conclusion that

$$\Pr[(\vec{x}_j||\vec{x}_s||\vec{x}_t)|(y_j||y_s||y_t)] \simeq \frac{1}{m^3} = \Pr[\vec{x}_j||\vec{x}_s||\vec{x}_t]. \tag{S43}$$

Given the output data $y_j||y_s||y_t$, the Shannon entropy of the input data can be given by $H[(\vec{x}_j||\vec{x}_s||\vec{x}_t)|(000)] = H[(\vec{x}_j||\vec{x}_s||\vec{x}_t)|(111)]$,

$$\begin{aligned} H[(\vec{x}_j||\vec{x}_s||\vec{x}_t)|(000)] &= -\frac{2m^2-9m+10}{2m^2}\log_2\frac{2m^2-9m+10}{2(m-1)(m-2)m^3} - \frac{3(3m-5)}{2m^2}\log_2\frac{3m-5}{2(m-1)m^3} - \frac{5}{2m^2}\log_2\frac{5}{2m^3} \\ &\simeq 3\log_2 m = H[\vec{x}_j||\vec{x}_s||\vec{x}_t], \end{aligned} \tag{S44}$$

and $H[(\vec{x}_j||\vec{x}_s||\vec{x}_t)|(001)] = H[(\vec{x}_j||\vec{x}_s||\vec{x}_t)|(010)] = H[(\vec{x}_j||\vec{x}_s||\vec{x}_t)|(011)] = H[(\vec{x}_j||\vec{x}_s||\vec{x}_t)|(100)] = H[(\vec{x}_j||\vec{x}_s||\vec{x}_t)|(101)] = H[(\vec{x}_j||\vec{x}_s||\vec{x}_t)|(110)]$,

$$\begin{aligned} H[(\vec{x}_j||\vec{x}_s||\vec{x}_t)|(001)] &= -\frac{2m^2-5m+2}{2m^2}\log_2\frac{2m^2-5m+2}{2(m-1)(m-2)m^3} - \frac{(3m-1)}{2m^2}\log_2\frac{3m-1}{2(m-1)m^3} - \frac{2m-1}{2m^2}\log_2\frac{1}{2m^3} \\ &\simeq 3\log_2 m = H[\vec{x}_j||\vec{x}_s||\vec{x}_t]. \end{aligned} \tag{S45}$$

3. Arbitrary d-bit

From the above calculation, several characteristics can be discerned. First, if the input bit substrings $\vec{x}_i$ are not identical, the conditional (posterior) probability suggests that the output string is close to a random guess outcome. Second, if the input bit substrings $\vec{x}_i$ are all identical, the conditional (posterior) probability is maximized when the output data string is either all zeros $\vec{y}_i = 0$ or all ones $\vec{y}_i = 1$. Third, if the input bit substrings $\vec{x}_i$ are identical, the conditional (posterior) probability is minimized when the output data string contains an equal number of zeros and ones.

For d identical input bit substrings $\vec{x}_i = \vec{x}$, the maximum conditional probability $\Pr[(11\cdots1)|(\vec{x}||\vec{x}||\cdots||\vec{x})] = \Pr[(00\cdots0)|(\vec{x}||\vec{x}||\cdots||\vec{x})]$ can written as

$$\begin{aligned} \Pr[(00\cdots0)|(\vec{x}||\vec{x}||\cdots||\vec{x})] &= \frac{1}{m!}\sum_k \left\{\frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x})\right]}{2}\right\}^d \\ &= \frac{1}{m}\sum_{i=0}^{m-1}\left(\frac{1+\cos\frac{2\pi i}{m}}{2}\right)^d \\ &= \frac{1}{2\pi}\int_0^{2\pi}\left(\frac{1+\cos t}{2}\right)^d dt \\ &= {}_2F_1\left(\frac{1}{2}, -2d; 1; 2\right) \leq \frac{1}{2}, \end{aligned} \tag{S46}$$

where ${}_2F_1\left(a,b;c;z\right)$ is the Gaussian hypergeometric function and we utilized the conversion between integration and summation.

For d identical input bit substrings $\vec{x}_i=\vec{x}$, the minimum conditional probability is that the number of bits of 0 in the output string is the closest to the number of bits of 1. If d is even, the minimum conditional probability can be given by

$$\begin{aligned}\Pr[(00\cdots0||11\cdots1)|(\vec{x}||\vec{x}||\cdots||\vec{x})] &= \frac{1}{m!}\sum_k\left\{\frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x})\right]}{2}\right\}^{d/2}\left\{\frac{1-\cos\left[\frac{2\pi}{m}f_k(\vec{x})\right]}{2}\right\}^{d/2}\\ &= \frac{1}{m}\sum_{i=0}^{m-1}\left(\frac{1+\cos\frac{2\pi i}{m}}{2}\right)^{d/2}\left(\frac{1-\cos\frac{2\pi i}{m}}{2}\right)^{d/2}\\ &= \frac{1}{2\pi}\int_0^{2\pi}\left(\frac{1+\cos t}{2}\right)^{d/2}\left(\frac{1-\cos t}{2}\right)^{d/2}dt\\ &= \frac{d!}{2^{2d}\left(\frac{d}{2}!\right)^2}\leq\frac{1}{2^{2d-1}}.\end{aligned}\tag{S47}$$

If d is odd, the minimum conditional probability can be given by

$$\begin{aligned}\Pr[(00\cdots0||11\cdots1)|(\vec{x}||\vec{x}||\cdots||\vec{x})] &= \frac{1}{m!}\sum_k\left\{\frac{1+\cos\left[\frac{2\pi}{m}f_k(\vec{x})\right]}{2}\right\}^{(d+1)/2}\left\{\frac{1-\cos\left[\frac{2\pi}{m}f_k(\vec{x})\right]}{2}\right\}^{(d-1)/2}\\ &= \frac{1}{m}\sum_{i=0}^{m-1}\left(\frac{1+\cos\frac{2\pi i}{m}}{2}\right)^{(d+1)/2}\left(\frac{1-\cos\frac{2\pi i}{m}}{2}\right)^{(d-1)/2}\\ &= \frac{1}{2\pi}\int_0^{2\pi}\left(\frac{1+\cos t}{2}\right)^{(d+1)/2}\left(\frac{1-\cos t}{2}\right)^{(d-1)/2}dt\\ &= \frac{(d-1)!}{2^{2d-1}\left(\frac{d-1}{2}!\right)^2}\leq\frac{1}{2^{2d-1}}.\end{aligned}\tag{S48}$$

Through straightforward analysis, we find that the conditional probability of the output bit string corresponding to the other input bit string cases must be between the maximum and minimum values of the above identical input bit substrings case. Therefore, we obtain the following inequality:

$$\frac{1}{2^{2d-1}}\leq\Pr[\vec{Y}_d|\vec{X}_d]\leq\frac{1}{2}.\tag{S49}$$

Note that, the prior probability that all d input bit substrings $\vec{x}_i$ are identical is m^{-d}, which is very small when both m and d are large. In many instances, the conditional probability closely approximates the probability of a random guess, that is, $\Pr[\vec{Y}_d|\vec{X}_d]\approx 2^{-d}$.

According to Bayes' theorem, we have

$$\begin{cases}\Pr[\vec{X}_d|\vec{Y}_d] &= \frac{\Pr[\vec{Y}_d|\vec{X}_d]\Pr[\vec{X}_d]}{\Pr[\vec{Y}_d]}\leq\frac{\frac{1}{2}m^{-d}}{2^{-d}}=\frac{2^{d-1}}{m^d}\simeq\frac{1}{m^d}=\Pr[\vec{X}_d],\\ \Pr[\vec{X}_d|\vec{Y}_d] &= \frac{\Pr[\vec{Y}_d|\vec{X}_d]\Pr[\vec{X}_d]}{\Pr[\vec{Y}_d]}\geq\frac{2^{-2d+1}m^{-d}}{2^{-d}}=\frac{2^{-d+1}}{m^d}\simeq\frac{1}{m^d}=\Pr[\vec{X}_d],\end{cases}\tag{S50}$$

where we assume that m is sufficiently large, for example, $m=2^{10}$. Therefore, we conclude that $\Pr[\vec{X}|\vec{Y}]\sim\Pr[\vec{X}]$.

[1] Barnett, S. M. & Croke, S. Quantum state discrimination. *Adv. Opt. Photonics* **1**, 238–278 (2009).

[2] Wallden, P., Dunjko, V. & Andersson, E. Minimum-cost quantum measurements for quantum information. *J. Phys. A: Math. and Theor.* **47**, 125303 (2014).

[3] Chefles, A. Unambiguous discrimination between linearly dependent states with multiple copies. *Phy. Rev. A* **64**, 062305 (2001).