SCIENCE CHINA
Information Sciences

August 2023, Vol. 66 180510:1–180510:2
https://doi.org/10.1007/s11432-022-3680-9

• LETTER •
Special Topic: Quantum Information

Novel entanglement compression for QKD protocols using isometric tensors

Hong LAI[1*], Josef PIEPRZYK[2,3] & Lei PAN[4]

[1]*School of Computer and Information Science, Southwest University, Chongqing* 400715*, China;*
[2]*Commonwealth Scientific and Industrial Research Organisation, CSIRO, Sydney, NSW* 2122*, Australia;*
[3]*Institute of Computer Science, Polish Academy of Sciences, Warsaw* 01-248*, Poland;*
[4]*School of Information Technology, Deakin University, Geelong, VIC* 3220*, Australia*

Received 7 August 2022/Revised 16 October 2022/Accepted 10 January 2023/Published online 26 June 2023

Citation Lai H, Pieprzyk J, Pan L. Novel entanglement compression for QKD protocols using isometric tensors. Sci China Inf Sci, 2023, 66(8): 180510, https://doi.org/10.1007/s11432-022-3680-9

The problem of performing compression on a source of entangled states in quantum key distribution (QKD) protocols has become a hot research topic [1, 2]. Since quantum processors that are used to send quantum information between nodes are relatively primitive and low in power [3], and the preparation of many-photon entanglement is relatively difficult at present, finding suitable protocols for the compression of transmitted quantum data could bring important practical benefits. More generally, the quantum information theory investigates manipulating quantum data under locality constraints [4]. Although quantum data compression brings many advantages, it poses challenges. The most important one seems to how to construct local operators to realize locality constraints, i.e., entanglement compression.

In this study, by constructing isometric tensors, we address the challenging research problem aiming at achieving entanglement compression for QKD protocols. This compression significantly improves the QKD protocol's efficiency by saving quantum sources with better security against eavesdropping than the existing QKD protocols. First, we present three key definitions, and then design our novel entanglement compression for QKD protocol based on the first and second classes of generalized isometric tensors.

Definition 1 (Isometric matrix [5])**.** Given a $d_1 \times d_2$ matrix w such that $ww^\dagger = I$ (when $d_1 \leqslant d_2$) or $w^\dagger w = I$ (when $d_1 > d_2$), w is called an isometric matrix.

Definition 2 (The first class of generalized isometric tensors)**.** The first class of generalized isometric tensors w $(w_{n1}, w_{n2}, n \geqslant 2)$ is defined as follows:

$$w_{n1} = \begin{pmatrix} \frac{\sqrt{2}}{2} & 0 & \cdots & 0 & \frac{\sqrt{2}}{2} \\ 0 & \frac{\sqrt{2}}{2} & \cdots & \frac{\sqrt{2}}{2} & 0 \end{pmatrix}_{2\times 2^n} = \frac{\sqrt{2}}{2} \begin{pmatrix} 1 & 0 & \cdots & 0 & 1 \\ 0 & 1 & \cdots & 1 & 0 \end{pmatrix}_{2\times 2^n},$$

$$w_{n2} = \begin{pmatrix} 0 & \frac{\sqrt{2}}{2} & \cdots & \frac{\sqrt{2}}{2} & 0 \\ \frac{\sqrt{2}}{2} & 0 & \cdots & 0 & \frac{\sqrt{2}}{2} \end{pmatrix}_{2\times 2^n} = \frac{\sqrt{2}}{2} \begin{pmatrix} 0 & 1 & \cdots & 1 & 0 \\ 1 & 0 & \cdots & 0 & 1 \end{pmatrix}_{2\times 2^n},$$

where $w(w_{n1}, w_{n2})$ satisfies the following conditions:

$$w : \mathbb{V}_{\text{in}} \to \mathbb{V}_{\text{out}}, \quad |\varphi'\rangle = w|\varphi\rangle, \quad ww^\dagger = \mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

and

$$w^\dagger : \mathbb{V}_{\text{out}} \to \mathbb{V}_{\text{in}}, \quad |\varphi\rangle = w^\dagger|\varphi'\rangle.$$

The first class of generalized isometric tensors can be used to compress any N-photon GHZ entangled state $(N \geqslant 3)$ and Bell state into a single state.

Definition 3 (The second class of generalized isometric tensors)**.** The second class of generalized isometric tensors w' $(w_{N1}, w_{N2}, N \geqslant 3)$ is defined as follows:

$$w_{N1} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & \frac{1}{\sqrt{2^{N-1}-1}} & 0 & \frac{1}{\sqrt{2^{N-1}-1}} & 0 & \cdots & 0 \\ 0 & 0 & \frac{1}{\sqrt{2^{N-1}-1}} & 0 & \frac{1}{\sqrt{2^{N-1}-1}} & \cdots & 0 \\ 0 & 0 & 0 & 0 & 0 & \cdots & 1 \end{pmatrix}_{4\times 2^N},$$

where in the second and third rows of w_{N1}, the number of non-zero elements is $2^{N-1} - 1$;

$$w_{N2} = \begin{pmatrix} 0 & \frac{1}{\sqrt{2^{N-1}-1}} & 0 & \frac{1}{\sqrt{2^{N-1}-1}} & 0 & \cdots & 0 \\ 1 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & \frac{1}{\sqrt{2^{N-1}-1}} & 0 & \frac{1}{\sqrt{2^{N-1}-1}} & \cdots & 0 \end{pmatrix}_{4\times 2^N},$$

where in the first and fourth rows of w_{N2}, the number of non-zero elements is $2^{N-1} - 1$.

Note that $w'(w'_{N1}, w'_{N2})$ satisfies the following conditions:

$$w' : \mathbb{V}_{\text{in}} \to \mathbb{V}_{\text{out}}, \quad |\varphi'\rangle = w'|\varphi\rangle, \quad w'w'^\dagger = \mathbb{I} \otimes \mathbb{I} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$w'^\dagger : \mathbb{V}_{\text{out}} \to \mathbb{V}_{\text{in}}, \quad |\varphi\rangle = w'^\dagger|\varphi'\rangle.$$

The second class of generalized isometric tensors can be used to compress any N-photon GHZ entangled state $(N \geqslant 3)$ into a Bell state.

* Corresponding author (email: hlai@swu.edu.cn)

The protocol description. In this study, we describe a protocol of performing compression on a source of any Bell states or N-photon GHZ entangled states into a single state ($|0\rangle$ or $|1\rangle$) or a Bell state. Specifically, we demonstrate an optimal method to compress the states based on our proposed Definitions 2 and 3 for QKD that fully exploit the quantum entanglement correlations of the compressed state between Alice and Bob. Our QKD protocol follows five steps listed below.

Step 1. Preparation of compressed entangled states. The step is executed by Alice. Given the isometric matrices $w_{n1}, w_{n2}, n \geqslant 2$ and $w_{N1}, w_{N2}, N \geqslant 3$, the Bell states and any $N(N \geqslant 3)$-photon GHZ entangled states are compressed into the number states $|0\rangle$ or $|1\rangle$ or Bell state by Alice randomly. For the entangled state $\frac{\sqrt{2}}{2}(|00\rangle+|11\rangle)$, Alice uses w_{21} and w_{22} to compress it into the number states $|0\rangle$ and $|1\rangle$ by the following operations respectively:

$$w_{21}\left(\frac{\sqrt{2}}{2}(|00\rangle+|11\rangle)\right) = \frac{\sqrt{2}}{2}\begin{pmatrix}1&0&0&1\\0&1&1&0\end{pmatrix}\begin{pmatrix}\frac{\sqrt{2}}{2}\\0\\0\\\frac{\sqrt{2}}{2}\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} = |0\rangle,$$

$$w_{22}\left(\frac{\sqrt{2}}{2}(|00\rangle+|11\rangle)\right) = \frac{\sqrt{2}}{2}\begin{pmatrix}0&1&1&0\\1&0&0&1\end{pmatrix}\begin{pmatrix}\frac{\sqrt{2}}{2}\\0\\0\\\frac{\sqrt{2}}{2}\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} = |1\rangle.$$

Likewise, for the entangled state $\frac{\sqrt{2}}{2}(|01\rangle+|10\rangle)$, Alice uses w_{21} and w_{22} to compress it into $|0\rangle$ and $|1\rangle$, respectively. Moreover, $\frac{\sqrt{2}}{2}(|00\cdots0\rangle+|11\cdots1\rangle)$ can also be compressed into the number states $|0\rangle$ and $|1\rangle$ by using w_{n1}, w_{n2}, respectively. Similarly, $\frac{\sqrt{2}}{2}(|00\cdots0\rangle+|11\cdots1\rangle)$ can also be compressed into the Bell states $\frac{\sqrt{2}}{2}(|00\rangle+|11\rangle)$ and $\frac{\sqrt{2}}{2}(|01\rangle+|10\rangle)$ based on w_{N1}, w_{N2}, respectively.

Step 2. Transmission of compressed states. For compressed single states, Alice sends the compressed single states or one photon of every compressed Bell state (and she reserves the remaining one) to Bob via a quantum channel, which is protected by decoy particles. Details are given in Step 3 below. Note that at the initialization stage, Alice and Bob agree to encode the decompressed quantum states as follows:

• if the recovered entangled state is $\frac{\sqrt{2}}{2}(|00\cdots0\rangle+|11\cdots1\rangle)$, then the matching n-bit classical information is $00\cdots0$ and $11\cdots1$ for even and odd sites (here, site means the position in photon sequence), respectively, and if the recovered entangled state is $\frac{\sqrt{2}}{2}(|00\rangle+|11\rangle)/\frac{\sqrt{2}}{2}(|01\rangle+|10\rangle)$, then the matching two-bit classical information is 00/01 and 11/10 for even and odd sites, respectively; or odd sites, respectively; or

• if measured photon is $|0\rangle$ or $|1\rangle$ in odd sites, the corresponding Bell state is $\frac{\sqrt{2}}{2}(|00\rangle+|11\rangle)$, and if measured photon is $|0\rangle$ or $|1\rangle$ in even sites, the corresponding Bell state is $\frac{\sqrt{2}}{2}(|01\rangle+|10\rangle)$, and N-bit classical information $00\cdots0$ and $11\cdots1$ for decompressed Bell states $\frac{\sqrt{2}}{2}(|00\rangle+|11\rangle)$ and $\frac{\sqrt{2}}{2}(|01\rangle+|10\rangle)$ as $\frac{\sqrt{2}}{2}(|00\cdots0\rangle+|11\cdots1\rangle)$.

Step 3. Eavesdropping detection with decoy particles. Alice prepares some decoy particles/qubits at random. She uses two basis: rectilinear $B_z = \{|0\rangle, |1\rangle\}$ and diagonal $B_x = \{|+\rangle, |-\rangle\}$, where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. The decoy particles are then injected into a sequence of compressed states/qubits at random locations. The locations are recorded together with their qubit bases. Once a quantum communication session completes, Alice publishes the recorded locations and bases. Bob measures decoy qubits using appropriate bases and announces results via an authenticated broadcast channel. Alice compares Bob's results with her record of decoy bases to derive an error rate of decoy qubits. If the error rate is higher than an acceptable threshold, the protocol execution halts before it restarts from Step 1. Otherwise, the protocol execution continues.

Step 4. Measurement of compressed states. After receiving a compressed state, Bob randomly chooses a basis and measures the qubit. Next, he informs Alice about his basis choice using a classical authenticated broadcast channel. Finally, for the sifted and compressed entangled-state/qubit after the base alignment, Alice informs Bob which isometric tensor is used for the corresponding compressed state via the classical authenticated broadcast channel. Consequently, Alice and Bob can identify correct measurements and further obtain correct compressed number states. Finally, they decompress the identified compressed number-states using $w_{n1}^\dagger, w_{n2}^\dagger, w_{N1}^\dagger, w_{N2}^\dagger$.

For example,

$$w_{21}^\dagger|0\rangle = \frac{\sqrt{2}}{2}\begin{pmatrix}1&0\\0&1\\0&1\\1&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}\frac{\sqrt{2}}{2}\\0\\0\\\frac{\sqrt{2}}{2}\end{pmatrix} = \frac{\sqrt{2}}{2}(|0\rangle|0\rangle+|1\rangle|1\rangle), \quad (1)$$

$$w_{21}^\dagger|1\rangle = \frac{\sqrt{2}}{2}\begin{pmatrix}1&0\\0&1\\0&1\\1&0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\\frac{\sqrt{2}}{2}\\\frac{\sqrt{2}}{2}\\0\end{pmatrix} = \frac{\sqrt{2}}{2}(|0\rangle|1\rangle+|1\rangle|0\rangle). \quad (2)$$

Step 5. Key agreement. In this step, according to their prior agreements in Step 2, Alice and Bob can obtain the key based on their sifted and decompressed single states and Bell states. For example, when the final sifted state is $|0\rangle$ in even site. Alice first informs Bob that the corresponding isometric tensor is $w_{21}^\dagger$ through a classical authenticated broadcast channel. Then Bob decompresses it into $\frac{\sqrt{2}}{2}(|00\rangle+|11\rangle)$ with $w_{21}^\dagger$, according to (1). Next, according to their prior agreement in Step 2, Alice and Bob can agree with the classical information 00.

Conclusion. In this study, we have found that it is possible to exploit correlations in compression QKD protocols to improve encoding capacity and security. Meanwhile, we have shown how to obtain a similar isometric tensor for decompressing the compressed entangled states. Most importantly, our proposed protocols have also achieved the requirements of multi-mode storage and deterministic transmission simultaneously.

Acknowledgements Hong LAI has been supported by Natural Science Foundation of Chongqing, China (Grant No. CSTB2022NSCQ-MSX0749) and National Natural Science Foundation of China (Grant No. 61702427).

References

1 Zhang Q, Lai H, Pieprzyk J. Quantum-key-expansion protocol based on number-state-entanglement-preserving tensor network with compression. Phys Rev A, 2022, 105: 032439
2 Datta N, Renes J M, Renner R, et al. One-shot lossy quantum data compression. IEEE Trans Inform Theor, 2013, 59: 8057–8076
3 Cirac J I, Zoller P, Kimble H J, et al. Quantum state transfer and entanglement distribution among distant nodes in a quantum network. Phys Rev Lett, 1997, 78: 3221–3224
4 Bennett C H, DiVincenzo D P, Smolin J A, et al. Mixed-state entanglement and quantum error correction. Phys Rev A, 1996, 54: 3824–3851
5 Evenbly G. Number-state preserving tensor networks as classifiers for supervised learning. Front Phys, 2022, 10: 858388