Fairness-Aware Quantum Anonymous Entanglement Distillation

Saw Nang Paing, Jinsung Cho, and Hyundong Shin
Department of Electronics and Information Convergence Engineering
Kyung Hee University, Yongin-si, 17104 Korea
Email: hshin@khu.ac.kr

***Abstract*—Quantum anonymous entanglement (QAE) is crucial for privacy-preserving information exchange in quantum anonymous communication. The effectiveness of this exchange depends on the fidelity of QAE, which varies in importance depending on the specific application. As a result, ensuring fairness in the distribution and quality of entanglement becomes essential. In this article, we introduce a fairness-aware QAE distillation approach, which balances throughput and equitable resource by adjusting a fairness parameter α within the utility function to accommodate different application needs.**

I. Introduction

Quantum anonymous entanglement (QAE) is crucial in privacy-preserving quantum communication tasks [1]. It involves the distribution of GHZ states among the network users. It necessitates local operations and classical communication (LOCC) to achieve QAE between anonymous sender and receiver [2]. However, if the channel is noisy during the distribution of GHZ states, it degrades the fidelity of QAE. As reliable communication require high-fidelity QAE pairs, these pairs must undergo the entanglement distillation process.

Entanglement distillation is a fundamental process in quantum communication, particularly in settings where high-fidelity entanglement is required for reliable information transmission. It enables the transformation of multiple low-fidelity or noisy entangled pairs into a smaller set of high-fidelity entangled states, suitable for use in advanced quantum protocols [3]. This procedure is probabilistic and resource-intensive, and it forms a critical component in the implementation of quantum repeaters, quantum key distribution (QKD), and distributed quantum computing.

In privacy-preserving quantum communication protocols, QAE is an essential ingredient to perform anonymous communication tasks. QAE involves the distribution of multipartite entangled states (e.g., GHZ states) among network participants, enabling generation of anonymous entanglement between anonymous sender and receiver via local operations and classical communication (LOCC). However, when GHZ states are distributed over noisy channels, the fidelity of the resulting shared entangled states degrades.

In practice, the amount of distillable entanglement depends strongly on the quality of the initial states, typically quantified by their fidelity. The minimum fidelity required by the distillation process is lower bounded by the hashing function [4]. Although the hashing bound offers a reliable lower limit on the distillable entanglement rate, it does not inform how resources should be used when fidelity varies or when distillation is constrained by time, hardware, or cost. This is where fairness becomes essential. By incorporating an α-fair utility model, we introduce a mechanism to prioritize distillation effort in a way that reflects operational goals: maximizing overall throughput ($\alpha = 0$) or favoring balanced resource use ($\alpha > 0$). In anonymous settings, where individual pairs cannot be selectively targeted, α-fairness offers to balance throughput and resource efficiency. Thus, fairness-aware design complements the physical bound, shaping not what is distillable, but how and where distillation is applied under anonymity. The remaining sections are arranged as follows. Section II details the QAE distillation and Section II-A introduces α-fairness in the utility function of QAE distillation. Finally, Section III provides the conclusion.

II. Quantum Anonymous Entanglement Distillation

The generation of QAE requires establishing an initial global multipartite entangled state among network users, typically a Greenberger–Horne–Zeilinger (GHZ) or W state, with the GHZ state being the standard choice in this work. The central server prepares the GHZ states and distributes individual qubits to each user. In practical settings, the transmitted state is degraded by various types of channel noise. In the worst-case scenario, it subjects to depolarizing noise which uniformly affects all qubits. For a network of N users, the density matrix of a noisy GHZ state is represented as [5]:

$$\rho_{\text{nghz}} = F_{\text{ghz}} \left|\mathsf{ghz}\right\rangle \left\langle\mathsf{ghz}\right| + (1 - F_{\text{ghz}}) \frac{\boldsymbol{I}_{2^N}}{2^N} \tag{1}$$

where $\left|\mathsf{ghz}\right\rangle = \frac{1}{2}(\left|0\right\rangle^{\otimes N} + \left|1\right\rangle^{\otimes N})$, F_{ghz} denotes the fidelity of GHZ state and $\boldsymbol{I}$ denotes the identity operator.

After receiving their qubits, all users except the anonymous sender and receiver measure in the Hadamard basis and announce their outcomes, while the anonymous parties announce random values. Based on these, they apply suitable $\boldsymbol{Z}$ corrections, yielding an ideal Bell state under noiseless conditions. Under depolarizing noise, this state becomes a Werner state, represented by

$$\rho_{\text{sr}} = F_{\text{ghz}} \left|\Psi^+\right\rangle_{\text{sr}} \left\langle\Psi^+\right| + (1 - F_{\text{ghz}}) \frac{\boldsymbol{I}_4}{4}, \tag{2}$$

where $|\Psi^+\rangle = \frac{1}{2}(|00\rangle + |11\rangle)$ represents a Bell state and s and r denotes anonymous sender and receiver respectively. The fidelity of the resulting state depends on the initial fidelity of shared GHZ state and its fidelity is [3]

$$F_{\text{sr}} = \frac{3F_{\text{ghz}} + 1}{4} \tag{3}$$

However, if the resulting fidelity is not strong enough to perform anonymous communication tasks, multiple ρ_{nghz} states need to be distilled to achieve high fidelity QAE. The basic entanglement distillation procedure applies local operations—specifically, bilateral controlled-NOT (CNOT) gates—on two noisy QAE pairs as follows:

$$\rho_{dsr} = \mathsf{CNOT}_{s_1 \to s_2} \mathsf{CNOT}_{r_1 \to r_2} (\rho_{\text{s}_1\text{r}_1} \otimes \rho_{\text{s}_2\text{r}_2}) \tag{4}$$

and classical communication of measurement results of qubits s_2 and r_2 anonymously. The QAE pair $\rho_{\text{s}_1\text{r}_1}$ is retained only if these outcomes match. The fidelity of distilled qubit pair is given by

$$F_{\text{dsr}} = \frac{F_{\text{sr}}^2}{F_{\text{sr}}^2 + (1 - F_{\text{sr}})^2}. \tag{5}$$

A. Quantum Utility of Distilled QAE

If the distillation process prioritizes high-fidelity QAE pairs, those with marginally lower fidelity become useless. However, these marginally lower-fidelity pairs can still be refined through successive rounds of distillation to achieve high-fidelity entanglement. To ensure equitable utilization of both strong and weak QAE pairs, a fairness parameter α can be introduced, enabling a controlled trade-off between optimal fidelity and resource fairness in the selection process.

To formalize the utility of a QAE pair, the hashing bound—a known lower bound on distillable entanglement—can serve as an effective utility function as follows [4]:

$$U(m, D_H(F_{\text{sr}})) = m \frac{D_H(F_{\text{sr}})^{1-\alpha}}{1 - \alpha} \tag{6}$$

where m is the number of total anonymous entangled pairs and the hashing bound is defined as

$$D_H(F_{\text{sr}}) = 1 + F_{\text{sr}} \log_2 F_{\text{sr}} + (1 - F_{\text{sr}}) \log_2 \frac{1 - F_{\text{sr}}}{3} \tag{7}$$

for $F_{\text{sr}} > 0.5$. This hashing bound estimates the number of high-fidelity QAE pairs that can be distilled from given noisy pairs. By integrating the hashing bound with a fairness parameter α, a fairness-aware QAE protocol can be achieved where resource utilization is both efficient and fair. In Fig. 1, the utility of QAE distillation of plotted over a range of QAE fidelities for $m = 1000$ and $\alpha = \{0, 0.5, 0.8\}$. Utility increases monotonically with F, with higher α values yielding greater utility due to more efficient distillation. For $\alpha = 0$, the growth is slow and near-linear, while for $\alpha = 0.8$, utility scales steeply with F, highlighting the significant impact of distillation efficiency on the number of high-fidelity pairs generated.

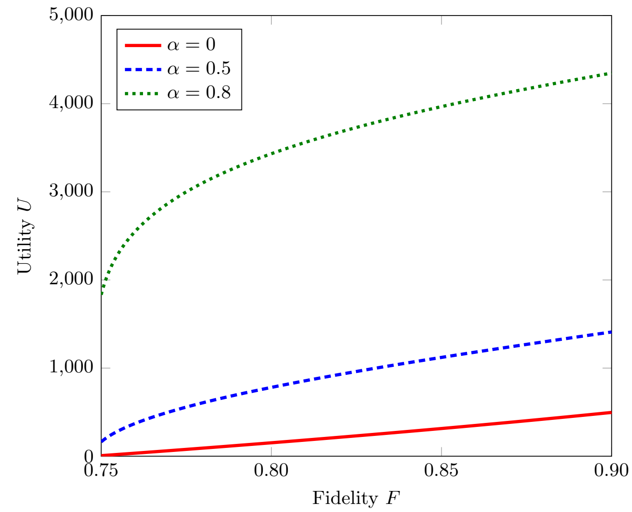

Fig. 1. Utility (U) of quantum anonymous entanglment distillation as a function of fidelity F for different fairness variable α.

III. Conclusions

We have presented a fairness-aware QAE distillation protocol that integrates the hashing bound with a tunable fairness parameter α. By adjusting α, the protocol can balance between throughput and fairness in resource utilization. Our results show that higher values of α prioritize throughput, significantly increasing utility at higher fidelities, while lower values maintain more equitable but less efficient resource usage. These findings highlight the trade-offs between fairness and performance, offering a flexible and application-adaptive approach to anonymous and resource-aware quantum communication.

Acknowledgment

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT) (NRF-2022R1A4A3033401), the MSIT (Ministry of Science and ICT), Korea, under the Convergence security core talent training business support program (IITP-2024-RS-2023-00266615) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation), and a grant from Kyung Hee University in 2023 (KHU-20233663).

References

[1] S. N. Paing, J. W. Setiawan, T. Q. Duong, D. Niyato, M. Z. Win, and H. Shin, "Quantum anonymous networking: A quantum leap in privacy," *IEEE Netw.*, vol. 38, no. 5, pp. 131–145, Sep. 2024.

[2] M. Christandl and S. Wehner, "Quantum anonymous transmissions," in *Proc. International Conference on the Theory and Application of Cryptology and Information Security*. Springer, Dec. 2005, pp. 217–235.

[3] E. M. Rains, "A semidefinite program for distillable entanglement," *IEEE Transactions on Information Theory*, vol. 47, no. 7, pp. 2921–2933, Nov. 2001.

[4] G. Vardoyan and S. Wehner, "Quantum network utility maximization," *arXiv:2210.08135*, 2022.

[5] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," *Phys. Rev. A*, vol. 54, no. 5, pp. 3824–3851, Nov. 1996.