Shannon-Limit Approached Information Reconciliation for Quantum Communication

arXiv:2003.03713

Bang-Ying Tang[1], Bo Liu[2], Wan-Rong Yu[1], Chun-Qing Wu[1]

[1] College of Computer Science and Technology, National University of Defense Technology, Changsha, 410073, China
[2] College of Advanced Interdisciplinary Studies, National University of Defense Technology, Changsha, 410073, China

ABSTRACT

To reduce the frame error rate of polar-based information reconciliation (IR) scheme with high reconciliation efficiency, we propose the **S**hannon-**l**imit **a**pproached (SLA) IR scheme, in which the block-checked decoder of polar code is proposed to determine the error sub-blocks in the forward reconciliation and the errors are corrected in the acknowledgment reconciliation. And the experimental results show that the SLA IR scheme reduces the ε-correctness to 10^{-8} and improves the efficiency to better than 1.091 with the IR block size of 128Mb. Otherwise, the SLA IR scheme reaches the efficiency of 1.055 with the quantum bit error rate (QBER) of 0.02, when the block length reaches to 1Gb, which is hundred times larger than the state-of-art implemented polar codes-based IR schemes and further reduce the finite length effect.

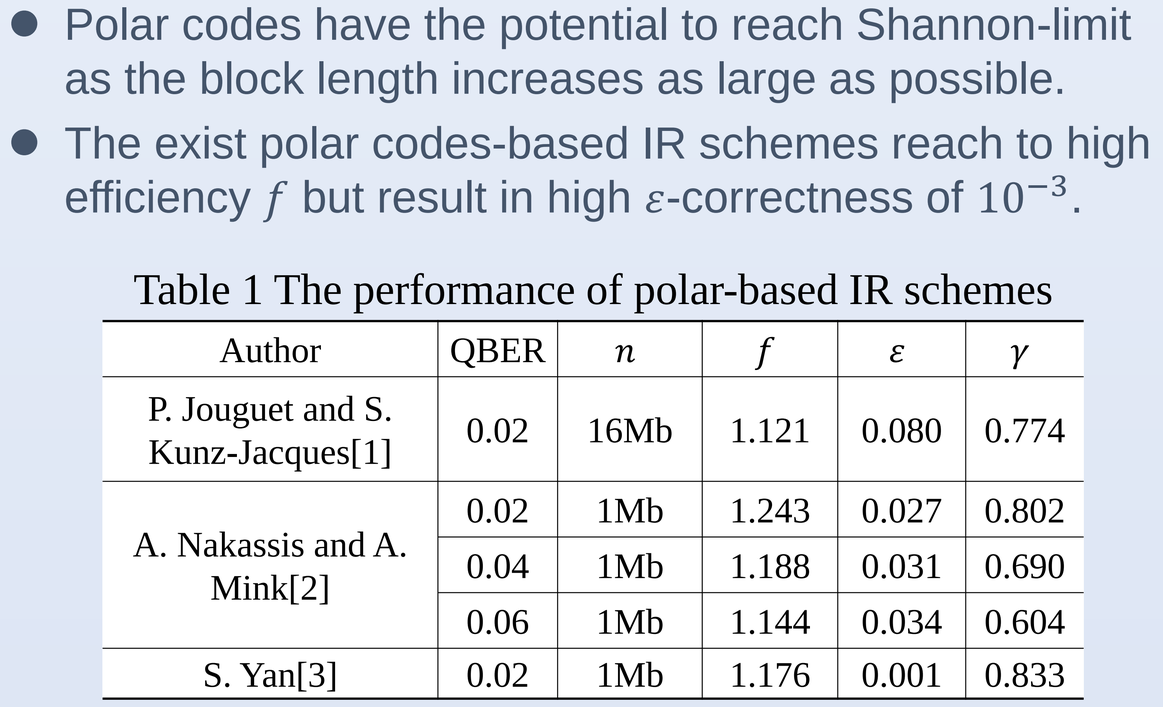
INTRODUCTION

- IR procedure corrects the error bits in sifted keys and ensures the correctness of quantum key distribution (QKD) systems.
- Polar codes have the potential to reach Shannon-limit as the block length increases as large as possible.
- The exist polar codes-based IR schemes reach to high efficiency f but result in high ε-correctness of 10^{-3}.

Table 1 The performance of polar-based IR schemes

Author	QBER	n	f	ε	γ
P. Jouguet and S. Kunz-Jacques[1]	0.02	16Mb	1.121	0.080	0.774
A. Nakassis and A. Mink[2]	0.02	1Mb	1.243	0.027	0.802
	0.04	1Mb	1.188	0.031	0.690
	0.06	1Mb	1.144	0.034	0.604
S. Yan[3]	0.02	1Mb	1.176	0.001	0.833

METHOD



- Block-checked SCL (BC-SCL) decoder
  - Check whether the sub-block is decoded successfully.
  - Reduce the ε-correctness.

RESULTS

- ε-correctness:
  - $\varepsilon < \varepsilon_{\mathrm{f}}[1-\left(1-\frac{l}{2^d}\right)^m + \varepsilon_{\mathrm{a}}]$
- Reconciliation efficiency f:
  - $f = f_{\mathrm{I}} + \frac{m(d+1)}{nH_2(E_\mu)} + \varepsilon_{\mathrm{f}} f_{\mathrm{II}} \frac{r}{m}$
- Entropy γ:
  - $\gamma = 1 - fH_2(E_\mu)$

Table 2 The performance of SLA IR scheme

E_μ	n = 1Mb			n = 16Mb			n = 128Mb		
	f	ε_f	γ	f	ε_f	γ	f	ε_f	γ
0.01	1.205	0.0164	0.903	1.114	0.0032	0.91	1.091	$\leq 10^{-4}$	0.912
0.02	1.146	0.005	0.838	1.085	0.0138	0.847	1.073	$\leq 10^{-4}$	0.848
0.03	1.124	0.0163	0.782	1.087	0.0005	0.789	1.062	0.0011	0.794
0.04	1.116	0.0072	0.73	1.072	0.0048	0.74	1.059	0.0033	0.743
0.05	1.107	0.0046	0.683	1.07	0.0022	0.694	1.055	$\leq 10^{-4}$	0.698
0.06	1.099	0.004	0.64	1.062	0.0050	0.652	1.049	0.0067	0.657
0.07	1.101	0.0012	0.597	1.066	0.0004	0.61	1.05	$\leq 10^{-4}$	0.616
0.08	1.104	0.0026	0.556	1.064	0.0001	0.572	1.048	$\leq 10^{-4}$	0.579
0.09	1.092	0.0037	0.523	1.056	0.0007	0.539	1.044	0.0015	0.544
0.1	1.083	0.0064	0.492	1.062	$\leq 10^{-4}$	0.502	1.042	$\leq 10^{-4}$	0.511
0.11	1.079	0.0024	0.461	1.057	$\leq 10^{-4}$	0.472	1.039	0.0050	0.481
0.12	1.072	0.0043	0.433	1.056	$\leq 10^{-4}$	0.441	1.037	0.0013	0.451

CONCLUSION

- The proposed SLA IR scheme mainly consists of two phase: the forward reconciliation phase and the acknowledgment reconciliation phase.
- The overall failure probability of SLA IR scheme is decreased to 10^{-8}.
- The reconciliation efficiency is improved to 1.205, 1.114 and 1.091 with the block length of 1Mb, 16Mb and 128Mb respectively.
- The SLA IR scheme reaches to the efficiency of 1.055 with QBER of 0.02, when the block length reaches to 1Gb.

ACKNOWLEDGEMENTS

- This work was supported in part by the National Natural Science Foundation of China under Grant No. 61972410 and the research plan of National University of Defense Technology under Grant No. ZK19-13.

REFERENCE

[1] P. Jouguet and S. Kunz-Jacques, "High Performance Error Correction For Quantum Key Distribution Using Polar Codes," *arxiv preprint arXiv:1204.5882,* 2012.

[2] A. Nakassis and A. Mink, "Polar Codes In A Qkd Environment," in *SPIE Sensing Technology + Applications*, 2014, vol. 9123: SPIE, p. 11.

[3] S. Yan, J. Wang, J. Fang, L. Jiang, and X. Wang, "An Improved Polar Codes-Based Key Reconciliation For Practical Quantum Key Distribution," *Chinese Journal of Electronics,* vol. 27, no. 2, pp. 250-255, 2018.