# Short Codes and Entanglement-based Quantum Key Distribution via Satellite

Xiaoyu Ai,[1] Robert Malaney,[1] Soon Xin Ng,[2] Lajos Hanzo[2]

[1]School of Electrical Engineering and Telecommunications at the University of New South Wales, Sydney, NSW 2052, Australia.

[2] School of Electronics and Computer Science, University of Southampton, U.K.

Correspondence: r.malaney@unsw.edu.au.

## Background

Very recently, ubiquitous deployment of such entanglement-based QKD over large distances has moved closer to reality, as verified by quantum entanglement distribution from a low Earth orbit satellite. We will demonstrate that this robust form of QKD via space will require a renewed focus on short-block length error-correcting codes in order to facilitate the reconciliation phase of the key distribution. Our results highlight the trade-off between the attainable key throughput vs the communication latency encountered in space-based implementations of this ultra-secure technology.

## System Model

The two legitimate users, Alice and Bob, are two ground stations, at a distance of about 1000km from each other. A satellite, used to generate and distribute entangled pairs of photons, is considered to be approximately overhead the two geographically distant ground stations.

The version of the DI-QKD protocol we adopt in this work follows the one studied in [2]. We introduce all the phases of this protocol as follows:

- **Distribution and measurement of the entangled states:** Alice and Bob share $N_{ent}$ pairs of entangled photons. These states are represented by

$$|s\rangle = \frac{(m\,|01\rangle - |10\rangle)}{\sqrt{m^2+1}}.$$

  where $m \in \mathbb{R}$. We will also assume that the only source of error is due to imperfect entanglement (non-maximal, $m \neq 1$). For the $i^{th}$ photon pair ($i = [1, 2, ...N_{ent}]$) Alice and Bob perform a quantum measurement in a basis randomly chosen from $C = \{|m_\alpha^{(0)}\rangle, |m_\alpha^{(1)}\rangle\}$ where

$$|m_\alpha^{(0)}\rangle = \frac{|0\rangle + e^{i\alpha}\,|1\rangle}{\sqrt{2}} \tag{1}$$

$$|m_\alpha^{(1)}\rangle = \frac{|0\rangle - e^{i\alpha}\,|1\rangle}{\sqrt{2}}, \tag{2}$$

  where $\alpha = 0, \frac{\pi}{2}, \frac{\pi}{4}$. The measurement bases of Alice and Bob are randomly and independently varied.

- **Selecting the testing set:** For photon pairs selected for the test we relabel them with the index $t$ and define the selected set as $\mathbf{T} = \{t | t \in [1, 2, ...N_{ent}]\}$. Alice then exchanges $\mathbf{T}$ with Bob. The table below shows how the values of $x_t$ and $y_t$ are mapped to the actions to be taken in the phases that follow.

| $x_t$ | $y_t$ | Action |
|---|---|---|
| 2 | 1 | Kept for estimating the channel parameter |
| 0 | 0 | Kept for CHSH game |
| 0 | 1 | Kept for CHSH game |
| 1 | 0 | Kept for CHSH game |
| 1 | 1 | Kept for CHSH game |

- **Checking the violation of Bells Inequality:** We want to estimate the probability of winning the CHSH game to measure the entanglement of Alice and Bob's photons:

$$P_{CHSH} = Pr\left(x_t \cdot y_t = a_t \oplus b_t\right),$$

  A pre-set noise tolerance parameter $\delta$ is introduced so that the protocol will abort if $P_{CHSH} \leqslant cos^2\left(\frac{\pi}{8}\right) - \delta$.

- **Estimating the channel parameter:** Alice and Bob estimate the fraction of erroneous bits, $\hat{p}$, when $x_t = 2, y_t = 1$. The protocol will abort if $\hat{p} \leqslant \delta$. When the estimation is complete, Alice and Bob discard the exchanged bits.

- **Key sifting:** Alice and Bob exchange all the choices of $x_i$ and $y_i$ which are not yet publicly revealed and save the measurement outcome of each photon pair to the raw key only if $x_i = y_i$.

- **Reconciliation:** Alice and Bob agree on an LDPC matrix $H$ generated by some algorithm (e.g. the Progressive Edge Growth algorithm[4]).Alice applies this matrix on her key string, and sends $H$ and her syndrome to Bob. Then, Bob adopts an LDPC decoding algorithm to reconcile his key string.

- **Privacy Amplification:** For the reconciled string, Alice and Bob use a Toeplitz matrix as a 2-universal hash function (e.g. see [**?**]) where the block length is $N'$, and the number of rows of the Toeplitz matrix is calculated via $L = (1 - H_2(\hat{p})) \cdot N'$, and where $H_2(\cdot)$ is the binary entropy function.

## Main Results

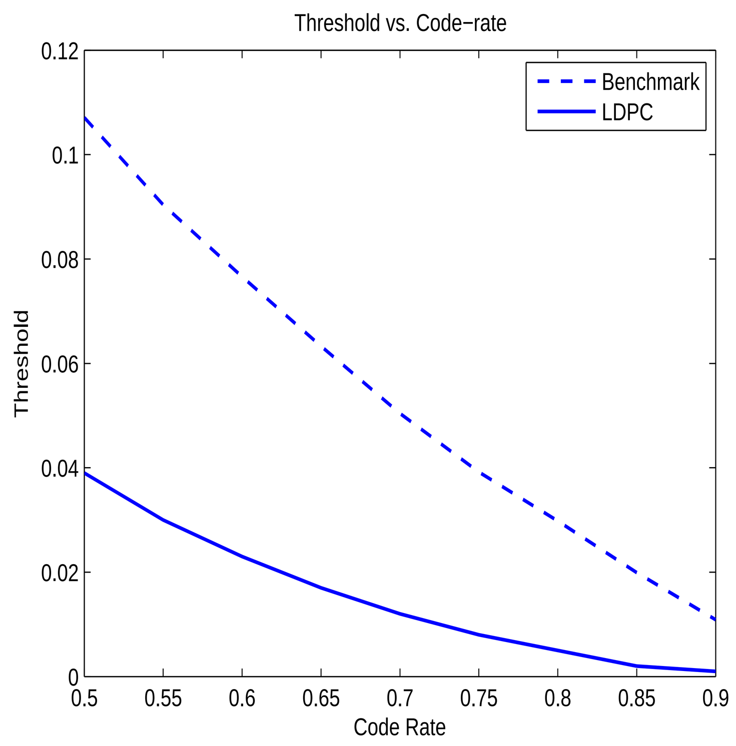


Figure 1: The threshold of the 2400 block length LDPC code used in this work compared to benchmark capacity-approaching irregular LDPC codes.

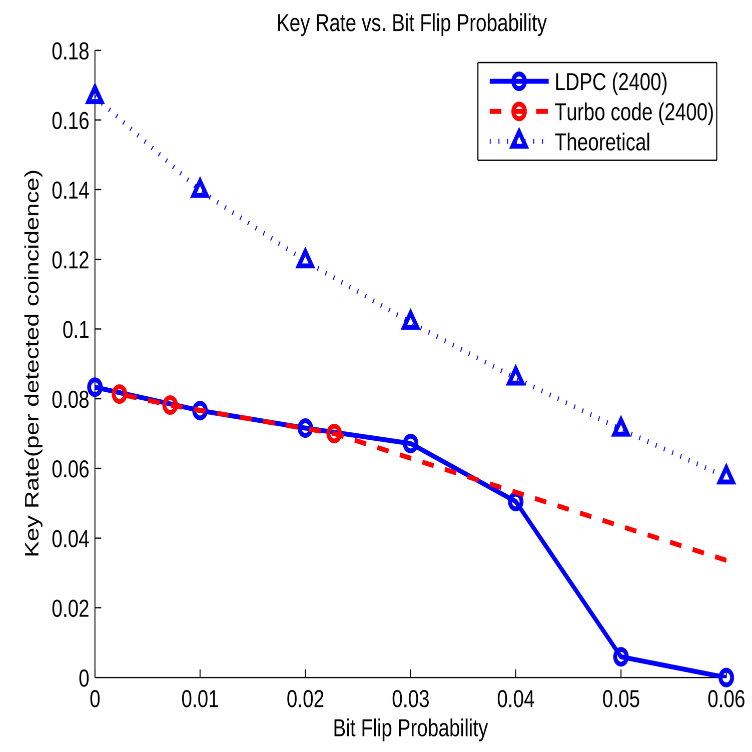


Figure 2: The key rate for one-half rate codes. A value of $k = 0.5$ is assumed. The blue (solid) line represents the LDPC code, while the red (dashed) line is a turbo code with the same rate. The block lengths for both codes used in the simulation is 2400. The dotted line is a standard entanglement-based QKD key rate calculated.

- **Potential rate-adaptive reconciliation schemes (Fig. 1)** We note that in any practical implementation of a satellite-based QKD protocol, rate-adaptive reconciliation from some Mother code is appealing. In this paper, puncturing technique in [3] is applied to increase the code rate from 0.5 to 0.9. Over a wide range of code rates derived from our Mother code, the thresholds for our 2400 block length LDPC code is over a factor of two smaller than those for a capacity achieving code.

- **LDPC vs. Turbo code (Fig. 2)** LDPC code has a slightly better performance at the low bit-flip errors, although the turbo code does show better performance at higher bit-flip probabilities (better threshold performance).

- **Performance reduction when using short codes (Fig. 2)** We simply investigate the impact our state-of-the-art short-block length codes have on reductions of the system throughput relative to optimal capacity.

## Conclusion

- Due to the short time span available for satellite-to-ground station detections, the use of short-length codes for the key reconciliation phase of space-based QKD may be required.
- We outline how short-block length LDPC and turbo codes may be able to provide reconciliation solutions for the satellite-based DI-QKD system.
- Future work should consider the improvement of decoding performance of the short LDPC codes and the neglect of finite signalling in the security aspects of our derived key rates.

## References

[1] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.- Y. Liu, B. Li, H. Dai et al., "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 11401144, 2017.

[2] U. Vazirani and T. Vidick, "Fully device-independent quantum key distribution," *Physical Review Letters*, vol. 113, no. 14, p. 140501, 2014.

[3] D. Elkouss, J. Martinez, D. Lancho, and V. Martin, "Rate compatible protocol for information reconciliation: An application to QKD," *Information Theory*, *IEEE Information Theory Workshop on*, pp. 15, 2010.

[4] X.-Y. Hu, E. Eleftheriou, and D.-M. Arnold, "Progressive edge-growth Tanner graphs," in *Globecom 01*, vol. 2. IEEE, 2001, pp. 9951001.