A Novel Interactive Information Reconciliation Scheme for DV-QKD Combining Incremental Redundancy and Turbo Decoding Paradigm

F Daneshgaran[1], M Mondin[1], and F Di Stasio[2]

[1]*Electrical and Computer Engineering, California State University Los Angeles, 5151 State University Dr. , Los Angeles CA, USA. Contact Phone: +13233434480*

[2]*Electronics and Telecommunications, Politecnico di Torino, 24, C.so Duca degli Abruzzi, Turin, Italy. Contact Phone: +39011090102*

Contact Email: fdanesh@calstatela.edu

The goal of Quantum Key Distribution (QKD) is to have two parties, Alice and Bob, have an identical sequence of bits about which the amount of information, classical or quantum, obtained by Eavesdropper Eve is negligible. A key step in this process is Information Reconciliation (IR) which is tantamount to channel coding, allowing Alice and Bob to arrive at nearly identical bit sequences after error correction. For IR, the data available at Alice and Bob are on equal footing. There is no right sequence say at Alice that Bob needs to ensure his data matches, yet traditional one-way channel error-correcting codes indeed assume that the correct sequence either resides at Alice (requiring forward reconciliation) or at Bob (requiring reverse reconciliation). The first error correction algorithm proposed was indeed an interactive two-way algorithm, namely the Cascade, which uses rudimentary parity checks. This paper explores a novel interactive "Turbo" like IR for Discrete Variable (DV) QKD. There are several nuances with the proposed technique that make it different from any traditional Turbo coding and decoding strategy. We present this novel approach and show its efficacy in generating common bits with very low error probability at Alice and Bob. Our technique combines features of incremental redundancy codes and Turbo codes into a unique solution with proven performance.