Quantitative Analysis of Influence of Noise on Communication Channel, using a QKD simulator

Shinnosuke Ozawa[1], Takaaki Matsuo[1], Satoh Takahiko[1], and Rodney Van Meter[1]

[1]Keio University

Introduction

The communication security based on Diffie-Hellman key agreement [1] strongly depends on exponential classical computational complexity. This cannot be ensured anymore with quantum computing.
On the other hand, Quantum Key Distribution does not rely on computational complexity but uses physical phenomena to detect the eavesdropper.
Prior work introduced several QKD network establishment protocols (BB84[2], BBM92[3], E91[4]). Our work focuses on implementing and simulating these protocols to compare capabilities and the impact of noisy channels (bit-flip, photon loss, dark count) and eavesdropping.

$$x^y = z \mod p$$

Diffie-Hellman Key Agreement
->If we only know number pairs (x,z,p), we need so much time to derive number 'y'.

Our Research

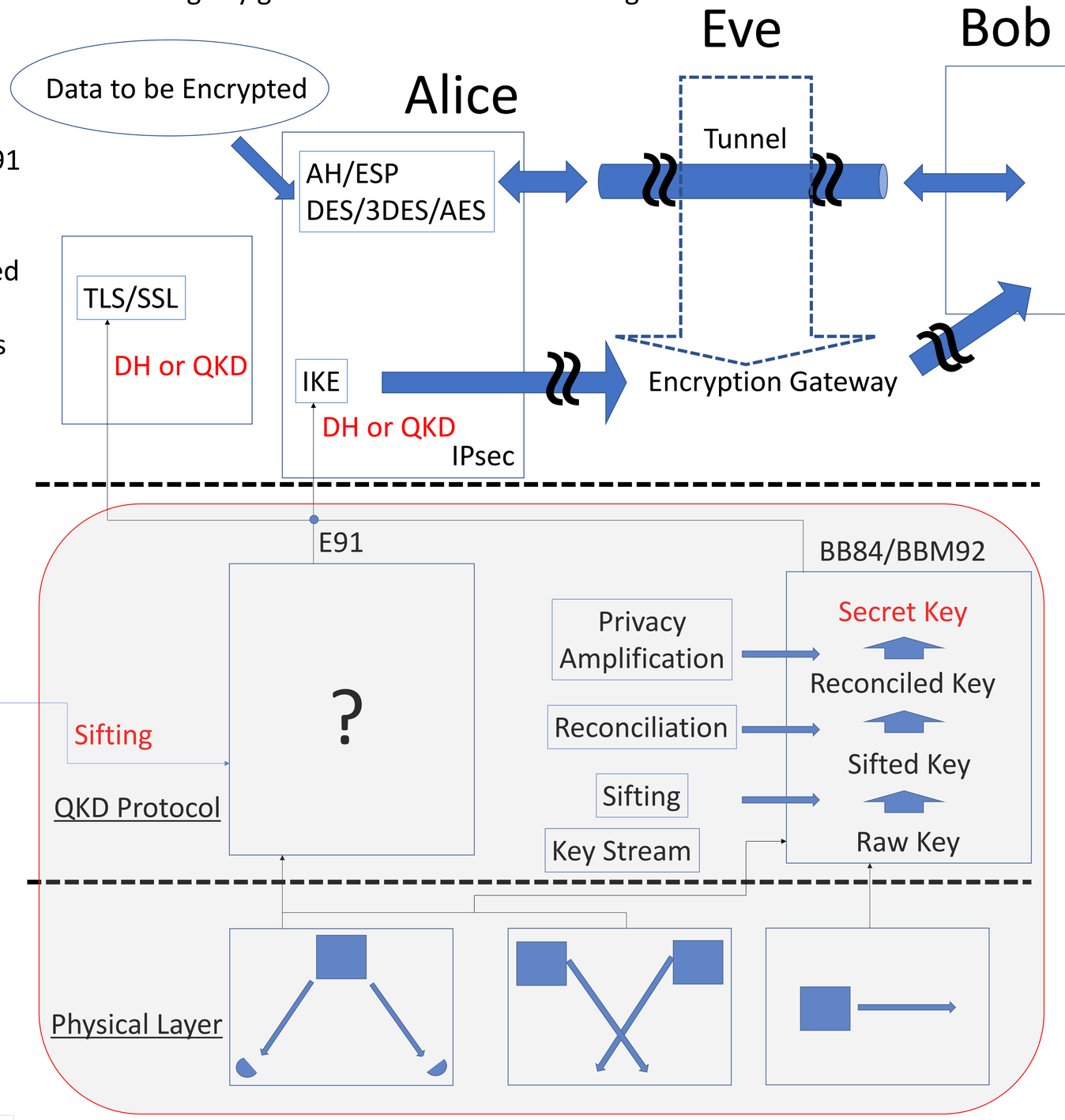
To generate shared secret key, QKD consists of some 4 step, Key stream, Sifting, Reconciliation, Privacy Amplification.
In BB84 and BBM92, the sifting step is sufficient to ensure the absence of eavesdropper. In E91 the focus is on using the CHSH inequality, yielding the S value that is sensitive to noise and eavesdropping.

Prior work on E91 have not focused on distinguishing noise from eavesdropper interference. We introduce a protocol to enable this distinction by studying the behavior of the S value. This allows us to compare the bit-rate during key generation under the three algorithms.

Work Progress

QKD networks with BB84 exist[5]. Because we don't have the way to distinguishing presence of Eve from noise, QKD network based on E91 is not yet considered practical.

We provide a protocol to distinguish eavesdropping from noise based on an S value threshold. Currently, we are implementing a network simulator for all three protocols. Using it we intend to determine this threshold and study the impact on noise.



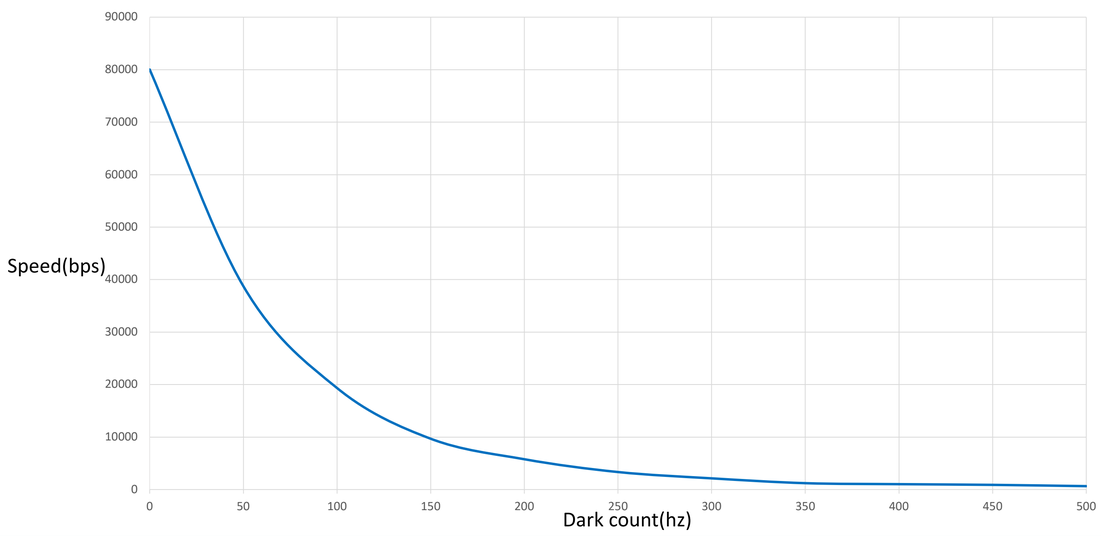
Benefits of simulator Platform
・Unified testing and development of BB84,BBm92,E91 protocols
・Examine behavior on repeater network
・Can directly test Eves strategies

CHSH Inequality

$$|E(a,b) - E(a,b') + E(a',b) + E(a',b')| = |S| \leq 2$$

a) QKD simulation

Our simulation consists of three layers.
・In the physical layer, we implement three different hardware to distribute qubits.
・In QKD protocol layer, we implement BB84, BBM92 and E91.
・The upper layer can run applications using the shared secret key



b) First experiment

We have implemented the key stream step in our BB84 simulator. In this experiment, we analyzed the influence of noise on communication channel in BB84 with a fixed bit-flip rate of 30% and 70% of bit-loss. Without dark count, communication speed is 80kbps. With increase of dark count to 500hz, communication speed down under 10bps.

[1] W.Diffie and M. E. Hellman(1976), New Directions in Cryptography, IEEE Transactions on Information Theory
[2] Charles H. Bennett and Gilles Brassaard(1984),
Quantum Cryptography: Public Key Distribution and Coin Tosing,International Conference on Computer System and Signal Processing
[3] Charles H. Bennett, Gilles Brassard, and N. David Mermin(1992), Quantum Cryptography without Bell's Theorem, Physical Review Letters
[4] Artur K. Elert(1991), Quantum cryptography based on bell's theorem, The American Physical Society
[5] Chip Elliott(2002), Building the quantum network, New Journal of Physics
[6] Alexander Ling, Matt Pelso, Ivan Marcikic, Antia Lamas-Linares and Christian Kurtsifer(2008), Experimental E91 quantum key distribution, Proc. SPCE 6903