A simple, extremely large bandwidth, modulator-free QKD system

Z. Zhang$^{1,2}$, A. Locquet$^1$, P. L. Voss$^{1,2}$, P. Gallion$^3$

1. Georgia Tech.-C.N.R.S. UMI 2958, 2-3 Rue Marconi, F-57070 Metz, France
2. School of Electrical and Computer Engineering, Georgia Institute of Technology, 777 Atlantic Drive, Atlanta, Georgia 30332-0250, USA
3. Ecole Nationale Supérieure des Télécommunications (GET/Télécom Paris and C.N.R.S. LTCI), 46, rue Barrault, 75634 Paris CEDEX 13, France

A host of quantum key distribution (QKD) protocols have been proposed and built to obtain a high key refresh rate and long QKD link distance. Sophisticated key reconciliation and key distillation algorithms have also been implemented. As these systems mature, they call for the calibration and operation of more complex and expensive equipment to achieve high rates. For some applications, simplicity and low cost are paramount. For discrete variable QKD in the 1550 nm fiber transparency window, requisite photon counting technologies remain prohibitively expensive. Continuous variable QKD uses coherent detection so that efficient, inexpensive PiN photodiode detectors may be used. However, even a recent simplification requiring no modulator on the receiving side[1], will require fast modulation and driving optoelectronics and a fast stream of true random numbers for very high speed Gaussian modulation of coherent light. In this paper we propose and analyze a continuous variable QKD system that uses thermal light (or amplified spontaneous emission, or ASE) as a source of inherently Gaussian-modulated, truly random light (from an optical amplifier or an LED) and requires no modulators. This greatly simplifies experimental implementation and can lower system cost. Furthermore, it is easily scalable to higher bandwidths. On the other hand, the secrecy capacity of the system is degraded. The required optoelectronic parts are a moderately bright thermal source, a laser, and two balanced homodyne detection setups. Finally, such a system may have practical advantages for network QKD.

A schematic of the QKD system is presented in Fig. 1 (left), where Alice splits broadband thermal light. The splitter transmission coefficient for the thermal light propagating towards Alice’s detectors is $\eta$. The rest is sent to Bob. After splitting, both parts consist of a portion of the same example of a mixed state—their classical fluctuations are the same (which have a total variance $V_s$, but their quantum noise is independent. Alice and Bob synchronize their measurements to a local oscillator beam generated by a laser, and measure with total efficiencies $\eta_m$ and $\eta_c$, respectively, where $\eta_c$ includes channel propagation losses. After an alignment and channel characterization procedure, and after collecting their measurement outcomes, Alice and Bob communicate on a classical channel to perform reverse reconciliation and privacy amplification, resulting in a final secure key. We make the common assumption that Eve can replace the imperfect channel with a lossless channel and can emulate the imperfect channel by using a beamsplitter, directing the rest of the light to her apparatus where she always performs homodyne detection on the correct quadrature. The secrecy capacity for reverse reconciliation is \( \Delta I = I(A;B) - I(B;E) \). The main result for this protocol is that the mutual information, $I(A;B)$, between Alice and Bob, and $I(B;E)$, between Bob and Eve, in bits per channel use, are:

\[
I(A;B) = -\frac{1}{2} \log_2 \left( 1 - \rho_{ab}^2 \right) = \frac{1}{2} \log_2 \left[ 1 + \frac{\eta_c \eta_m (1-\eta_c) V_s^2}{(\eta_c + 1)(1-\eta_m) V_s + 1} \right],
\]

(1)

\[
I(B;E) = -\frac{1}{2} \log_2 \left( 1 - \rho_{be}^2 \right) = \frac{1}{2} \log_2 \left[ 1 + \frac{\eta_c (1-\eta_c)^2 V_s^2}{(1-\eta_m)(1-\eta_m) V_s + 1} \right].
\]

(2)

The secrecy capacity is positive for many reasonable system parameters. For fixed $\eta_c$ and $\eta_m$, one can experimentally choose $\eta_1$ to maximize the secrecy rate. The optimized secrecy rate for varying channel efficiency $\eta_c$, and 75% quantum efficiency for Alice ($\eta_m=0.75$) is plotted in Figure 1 (right), with $V_s=10$ and the vacuum variance is 1.

References