16th Optics and Quantum Electronics Conference (7. 8~9, 1999)

Fluctuation을 이용한 key의 전달

Key distribution using fluctuation

Ajung Kim
SAIT, Digital Communication Lab.
Ajung@ sait.samsung.co.kr

As communication systems and networks have been widely installed, system security and reliability have become issues of great importance. The advent of the quantum computer[1] with the ability of massive parallelism and storing superpositions of numbers has been a threat to conventional cryptosystems. Unlike the classical cryptography, quantum cryptographic systems[2],[3] devise new ways of attaining secure optical communications against an adversary. A drawback of the classical cryptosystem is that it can always be monitored without the legitimate users being aware of any eavesdropping taking place. Quantum cryptographic systems are also vulnerable to eavesdropping, but they provide ways to detect the extent of eavesdropping.

Extending the concept of quantum noise exploited in quantum cryptography to the classical noise region, another cryptosystem based on fluctuations can be supposed. It has a wider range of implementations and the sources of noise employed are omnipresent. However, the level of signals used in plausible system design for the noise cryptosystem as well as the quantum cryptosystem is estimated to be low for security compliance, which results in low transmission rate and system susceptibility to device noises as trade-offs.

With this protocol, a legitimate user, say B, uses signals susceptible to additive noise and can avoid the pitfall of erroneous decisions by accepting the measurement results beyond a threshold value, while an eavesdropper, E, ends up with a higher error rate and results uncorrelated to B. Detecting test factors, as criteria to estimate the degree of eavesdropping, is proposed as well.

In simple implementation with the use of additive white Gaussian noise (AWGN), the performance can be analyzed for various signal keyings and cryptofunctions. Fig.1 shows error rates[4] of E and B in noise cryptographic sysytems using detector's AWGN as a function of SNR. The dashed line refers to Babe's error rate with a threshold $\theta = 0.7\sqrt{E}$, and the dotted line does to $\theta = 1.1\sqrt{E}$.

In implementation of these cryptosystems in LANs, code division multiplexing is considered a promising candidate for multi-access networks. Estimates can be evaluated on the number of divisions multiplexed, which is limited by intermodulations between multiplexed channels. Fig.2