08

Generating a common secret based on bounded observability

～Secret key distribution using broadband random light～

Abstract

Secret key distribution (SKD) is used to generate a common secret key between two legitimate users, which enables the users to communicate securely. We proposed a SKD scheme which can achieve information-theoretic security and long-distance key distribution. Our scheme is based on a property called *bounded observability,* which occurs due to the practical difficulty of completely measuring broadband random light. An implementation based on this concept has been proposed using the synchronized responses of laser systems injected with common random light with broad bandwidth, and it has been experimentally demonstrated to be possible and practicable.

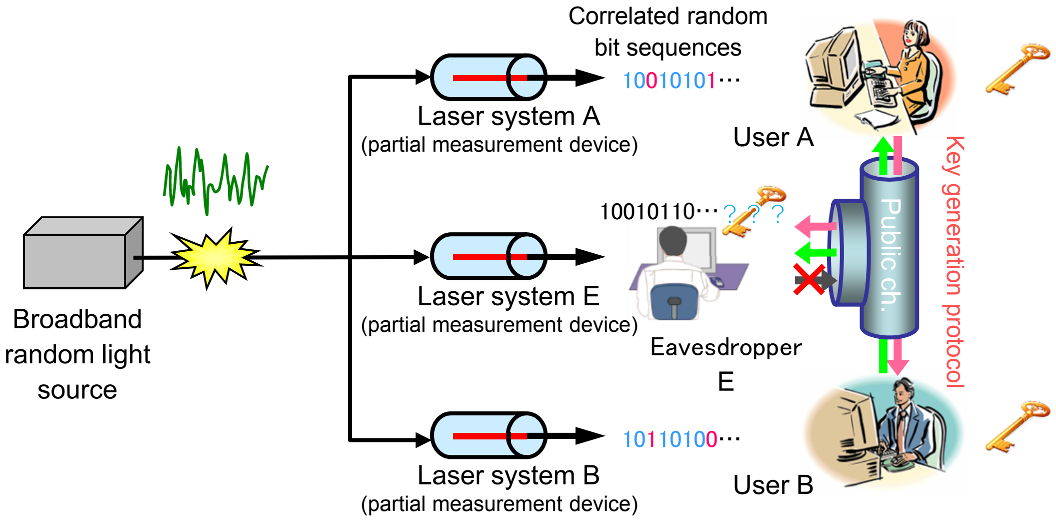
Consider a glass of water,

Complete measurement is **difficult**
(i.e. positions and velocities of all the molecules)

Partial measurement is **easy**
(e.g., temperature, volume, etc.)

Our SKD scheme uses such a difference between measurement difficulties.

We proposed an implementation of SKD using broadband random light .
Broadband random light is very difficult to measure completely.



Correlated random bit sequences

10010101…

Laser system A
(partial measurement device)

User A

10010110… ? ? ?

Laser system E
(partial measurement device)

Eavesdropper E

Public ch.

Key generation protocol

Broadband random light source

10110100…

Laser system B
(partial measurement device)

User B

Our Breakthrough: We invented a laser system realizing a huge variety of partial measurements that is suitable for generating highly secure keys.

Related work

[1] K. Yoshimura, J. Muramatsu, P. Davis, T. Harayama, H. Okumura, S. Morikatsu, H.Aida, A. Uchida, “Secure key distribution using correlated randomness in lasers driven by common random light,” *Phys. Rev. Lett.* Vol. 108, 070602, 2012.

[2] H. Koizumi, S. Morikatsu, H. Aida, T. Nozawa, I. Kakesu, A. Uchida, K. Yoshimura, J. Muramatsu, P. Davis, “Information-theoretic secure key distribution based on common random-signal induced synchronization in unidirectionally-coupled cascades of semiconductor lasers,” *Optics Express*, Vol. 21, pp. 17869-17893, 2013.

Contact

Kazuyuki Yoshimura Signal Processing Research Group, Media Information Laboratory
E-mail : yoshimura.kazuyuki{at}lab.ntt.co.jp (Please replace {at} with @)