08

Secret key distribution using broadband random light

“観測の限界”が秘密をつくる

～広帯域ランダム光の観測困難性を利用した秘密鍵配送～

どんな研究

二人のユーザ間で、盗聴者には推測できない秘密鍵を共有する**鍵配送方式**の研究です。提案方式では、高速に変化するランダム光の完全測定は難しく、一方で部分的な測定は容易であることを利用します。ランダム光注入で同期するレーザを、部分測定器として用い実装されます。

どこが凄い

公開鍵暗号は盗聴者の計算能力の限界を仮定するため、暗号文が記録されれば将来に解読されてしまうかもしれません。また量子暗号では、長距離伝送は現状においては困難です。提案技術は、盗聴者の計算能力に依らない**将来に渡る安全性**と**長距離伝送**の両立を実現します。

目指す未来

・将来に解読される心配のないセキュア通信

・大陸を結び、大陸を横断する長距離セキュア通信

・既存の光ファイバ網をそのまま利用できるセキュア通信

容器内の水について、

完全測定（全ての水分子の位置・速度）は**困難**

しかし、

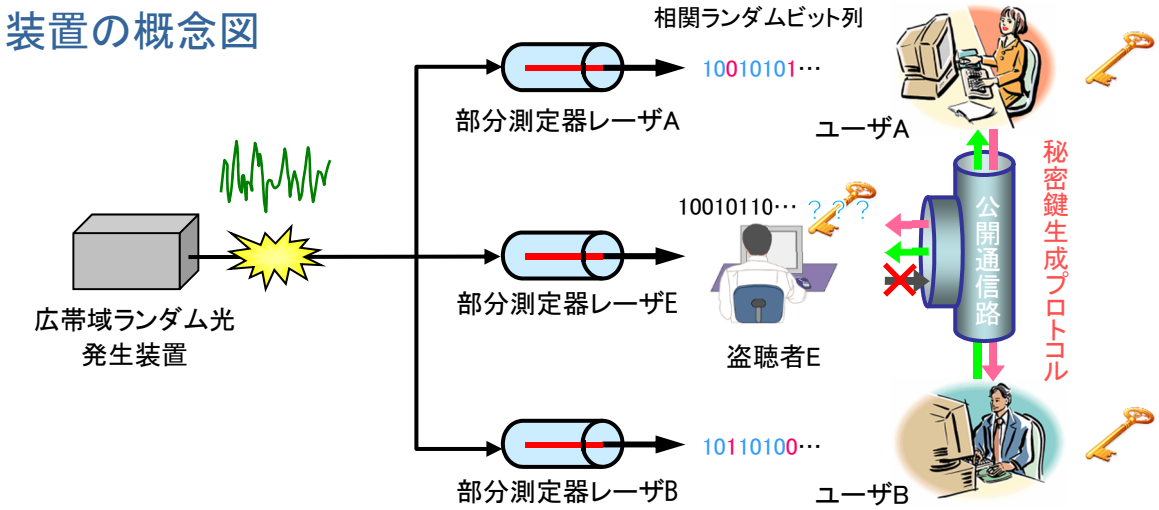
部分測定（例えば、温度、体積 etc.）は**容易**

測定難易度の差を利用して秘密鍵を共有する方式を提案

高速変動するランダム光（完全測定は困難）を利用して本方式を実装

実装のためには、膨大な種類の部分測定法を用意することが重要！

装置の概念図



成果：レーザを組合わせて多種の部分測定を実現する手法を提案＆実験実証

関連文献

[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.

連 絡 先

吉村 和之 (Kazuyuki Yoshimura)　メディア情報研究部 信号処理研究グループ

E-mail: yoshimura.kazuyuki{at}lab.ntt.co.jp ({at}の部分を@に置き換えてください)