1

Title: Secret key distribution using correlated randomness in lasers

測れない光で秘密ができる

～レーザの相関ランダム現象を利用した秘密鍵配送～

どんな研究？

二人の正規ユーザ間で、盗聴者には推測できない秘密鍵を共有する方式の研究です。提案方式では、高速に変化するランダム光の完全測定が難しいことを利用します。共通ランダム光注入により同期するレーザを用いて実装されます。情報理論とレーザ物理の融合により実現できました。

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しているため、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。また量子暗号では非常に弱い光を利用するため、長距離伝送には不向きでした。提案技術は、盗聴者の計算能力によらない安全性と長距離伝送を実現します。

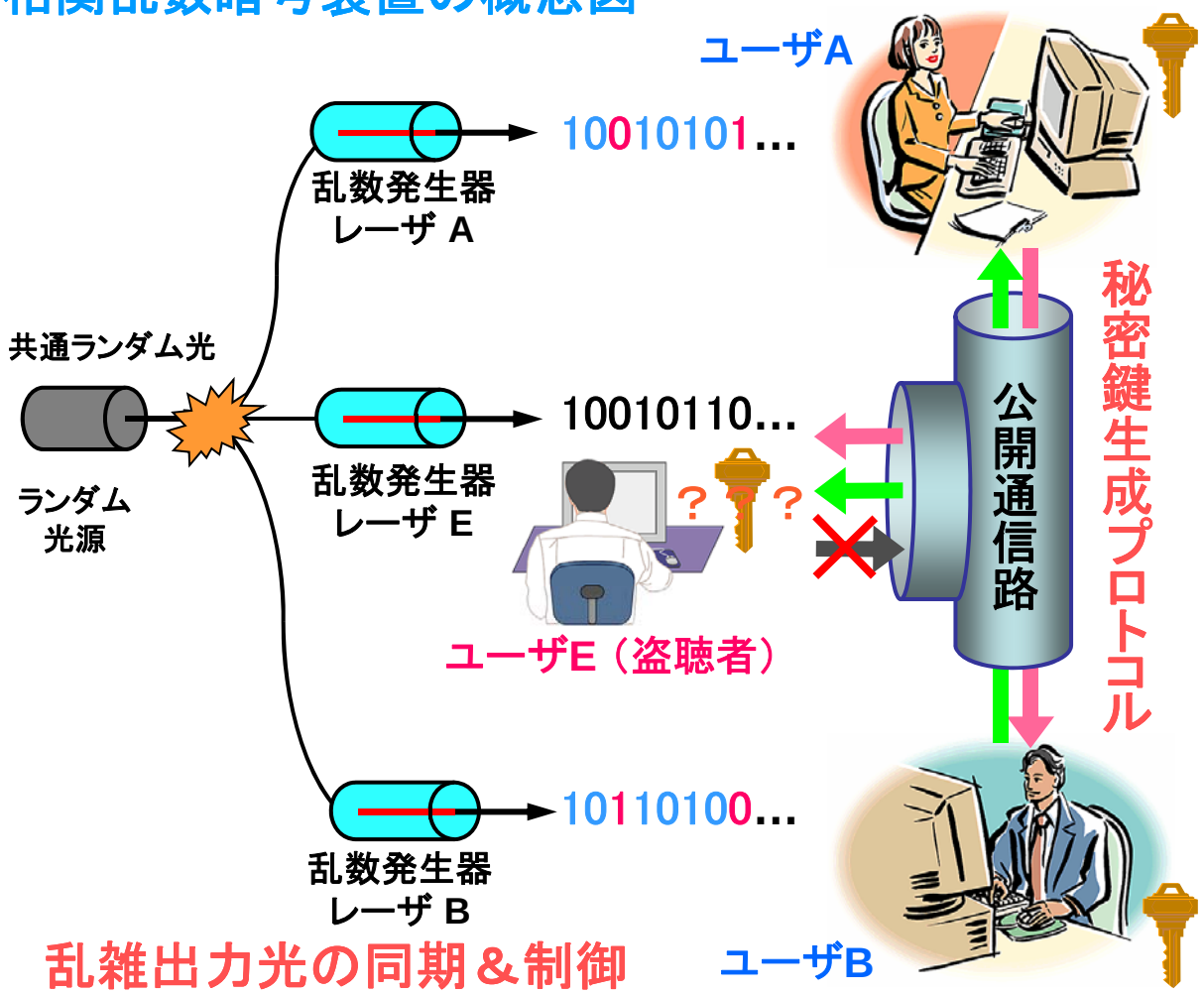
どんな風に役立つ？

・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

相関乱数暗号装置の概念図



関連文献

[1] J. Muramatsu, K. Yoshimura, and P. Davis., “Information theoretic security based on bounded observability,” Lecture Notes on Computer Science (LNCS), vol. 5973, pp. 128-139, Springer, 2010.

[2] K. Yoshimura, J. Muramatsu, P. Davis, T. Harayama, H. Okumura, S. Morikatsu, H. Aida, and A. Uchida, “Secure key distribution using randomness in lasers driven by common random light,” Physical Review Letters, vol. 108, 070602, Feb. 2012.

連 絡 先

村松純 (Jun Muramatsu)　メディア情報研究部 信号処理研究グループ

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