

<資料>

■ 論文名

Experiment of 10 Gbit/sec quantum stream cipher applicable to optical Ethernet and optical satellite link. SPIE. Proc. Vol-7465, 2009.

■ 量子情報科学と光通信ワークショップ

2009 年 8 月 10 日（月） 会場：玉川大学

招待講演：

榊裕之（東大名誉教授）、石田修（NTT 未来ネット研）、和田尚也（NICT）、久保田寛和（NTT 未来ネット研）、菊池和朗（東京大学）、川西悟基（玉川大学）、広田修（玉川大学）

■ 発表予定論文

“ 光通信量子暗号 Y-00 による準完全秘匿を持つ偵察衛星システム-Shannon 限界超越- ”

電子情報通信学会 情報セキュリティ研究会 2009 年 9 月 25 日発表予定

会場：機械振興会館（東京）

用語解説

■ Shannon 限界

1949 年に Shannon が暗号の数理的体系を構築した際に、数学的に構成可能な共通鍵暗号においてデータに対する情報理論的安全性には越えられない限界があることを証明した。その限界を Shannon 限界という。この限界のため、完全秘匿を達成する方法は通信量と同じ長さの真正乱数を一回だけ使う暗号方式である one time pad 以外存在しないことが導かれる。単一光子量子暗号は one time pad 用の鍵を量子的に配送することを目的に開発されている。

■ 量子雑音

光波は多数の光子の重ね合わせの量子状態を持ち、それを観測すると、観測値となる光電子の数が完全に不規則に出現する現象。

■ DAC

デジタル・アナログ変換器の略語。Y-00 伝送装置においてはビット伝送用の多値の基底信号の生成に用いる。