研究テーマ：超伝導光子検出器を用いた量子鍵配送（1/2）

（プロジェクト番号　JGN2-A18029）

研究機関：（独）情報通信研究機構、新世代ネットワーク研究センター

日本電気（株）ナノエレクトニクス研究所、システムプラットフォーム研究所

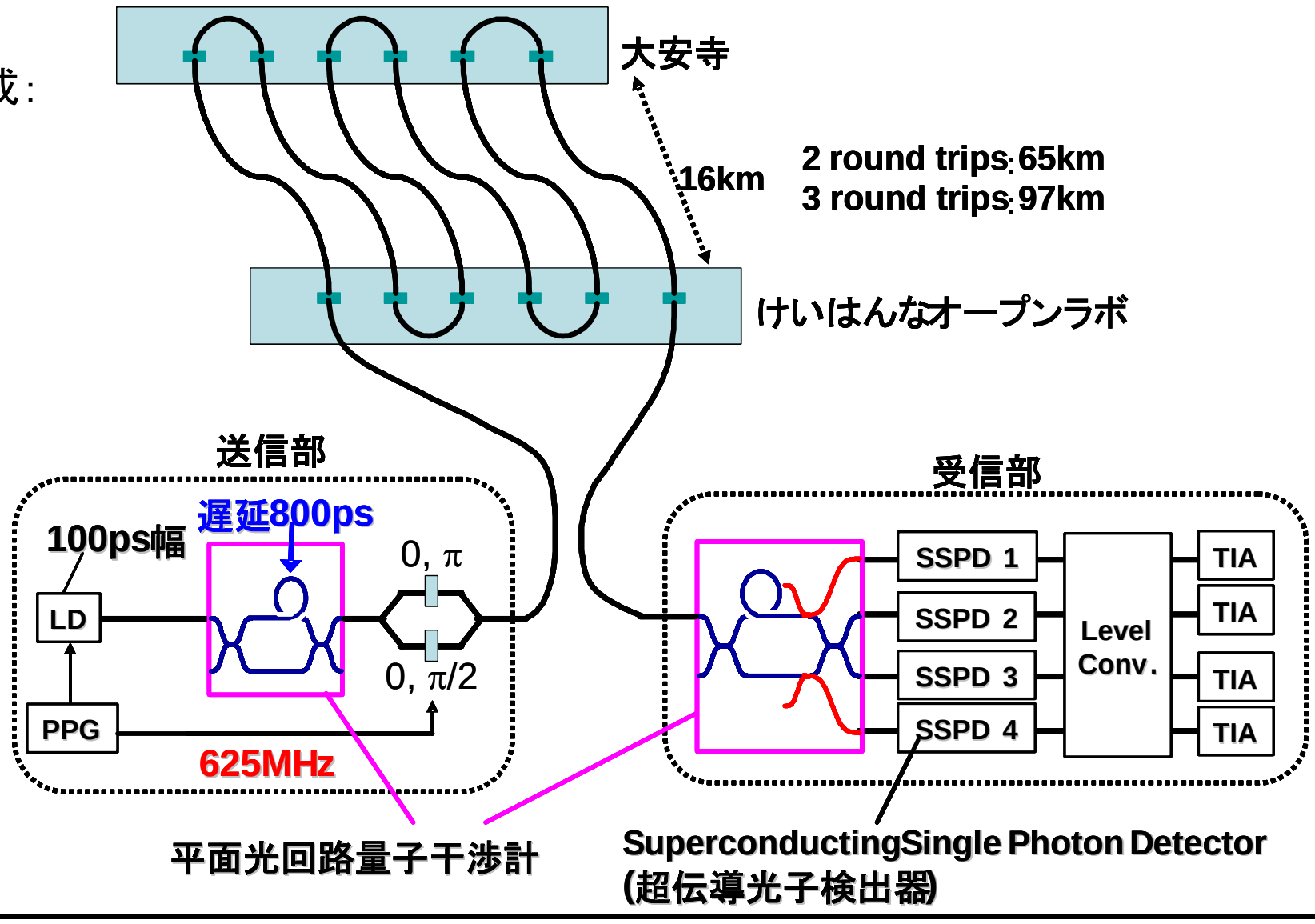
研究の概要：

究極の暗号技術である量子暗号を都市圏ネットワークで実用化するために、超伝導素子に基づく最新の光子検出技術と、平面光回路量子干渉計を組み込んだ単一方向伝送型量子鍵配送システムを組み合わせて、量子鍵の安全性及び生成速度向上をフィールド試験において実証する。

研究の目的：

従来の計算量的安全性に基づく暗号が常に解読の脅威にさらされているのに対して、量子暗号は物理法則に基づき無条件安全性を保証する。しかし、その実装には光子を制御する高度な技術が要求される。特に光子検出器の不完全性が暗号性能を直接制限する。これまで主に InGaAs APD が用いられてきたが、雑音が大きく実用化にはまだ大きな隔たりがある。2006 年以降、米国国立ロスアラモス研究所や国立標準技術研究所が低雑音の超伝導光子検出器を用いて、Bennett-Brassard 84 プロトコルによる室内 100km での秘密鍵生成に成功した。しかし、クロック同期も Rb 発振器や室内の電気ケーブルで済ますなど高速化、フィールドファイバへの適用に大きな課題を残している。当該プロジェクトでは、最新の超伝導光子検出器と平面光回路量子干渉計を用いて単一方向伝送型量子鍵配送システムを開発し、更なる性能改善をフィールドファイバ伝送において実証する。

実験機器構成：



研究テーマ：超伝導光子検出器を用いた量子鍵配送（2/2）

（プロジェクト番号　JGN2- A18029）

研究機関：（独）情報通信研究機構、新世代ネットワーク研究センター

日本電気（株）ナノエレクトニクス研究所、システムプラットフォーム研究所

研究開発成果：

現在最高の安全性を保証する「おとり信号付きBennett-Brassard84プロトコル」を用いてフィールド100km圏で従来比10倍の鍵生成速度を達成した。

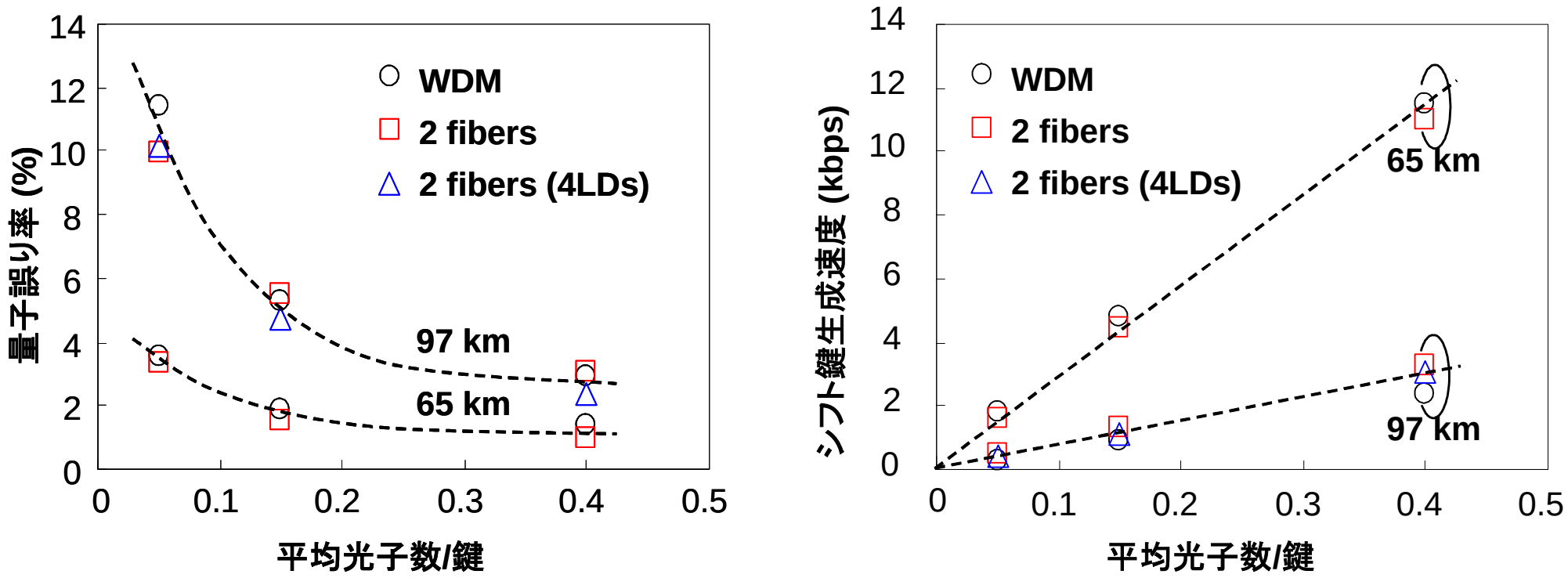


図1　左：量子誤り率−平均光子数特性
右：シフト鍵生成速度−平均光子数特性

プロジェクトのアピールポイント

フィールド環境下で長距離化・高速化かつ安定化を実現するため

・平面光回路量子干渉計

・ゲーティング動作が不要な低雑音の超伝導光子検出器

という独自の最新デバイス技術と

・量子信号とクロック用古典信号の波長分割多重による同一ファイバ伝送

という実用的なクロック同期方式を組み合わせた。クロック周波数は、625MHz で従来比10 倍。最終秘密鍵の蒸留では、従来の符号長無限大を仮定した外挿解析を超え、

・有限符号長での実際的な安全性解析を可能にする独自の評価理論

を用いて、最も実用に近い安全性保証を提示した。

プロジェクトの自己評価

本成果により単一方向伝送型量子鍵配送システムの一般環境下での有用性が実証され、今後の都市圏ネットワークへの展開や標準化を進める上で大きなマイルストーンとなる。今後、政府安全保障レベルの量子鍵配送システムの実現、さらに装置の小型化・低コスト化を進め、金融など民生展開にも取り組んでゆく。