# 研究テーマ：都市圏量子鍵配送実験（1/2）

（プロジェクト番号 JGN2P-A21002）

研究機関：（独）情報通信研究機構、日本電気（株）、三菱電機（株）、日本電信電話（株）、（株）東芝（欧州研究所）、ID Quantique、All Vienna

研究の概要：

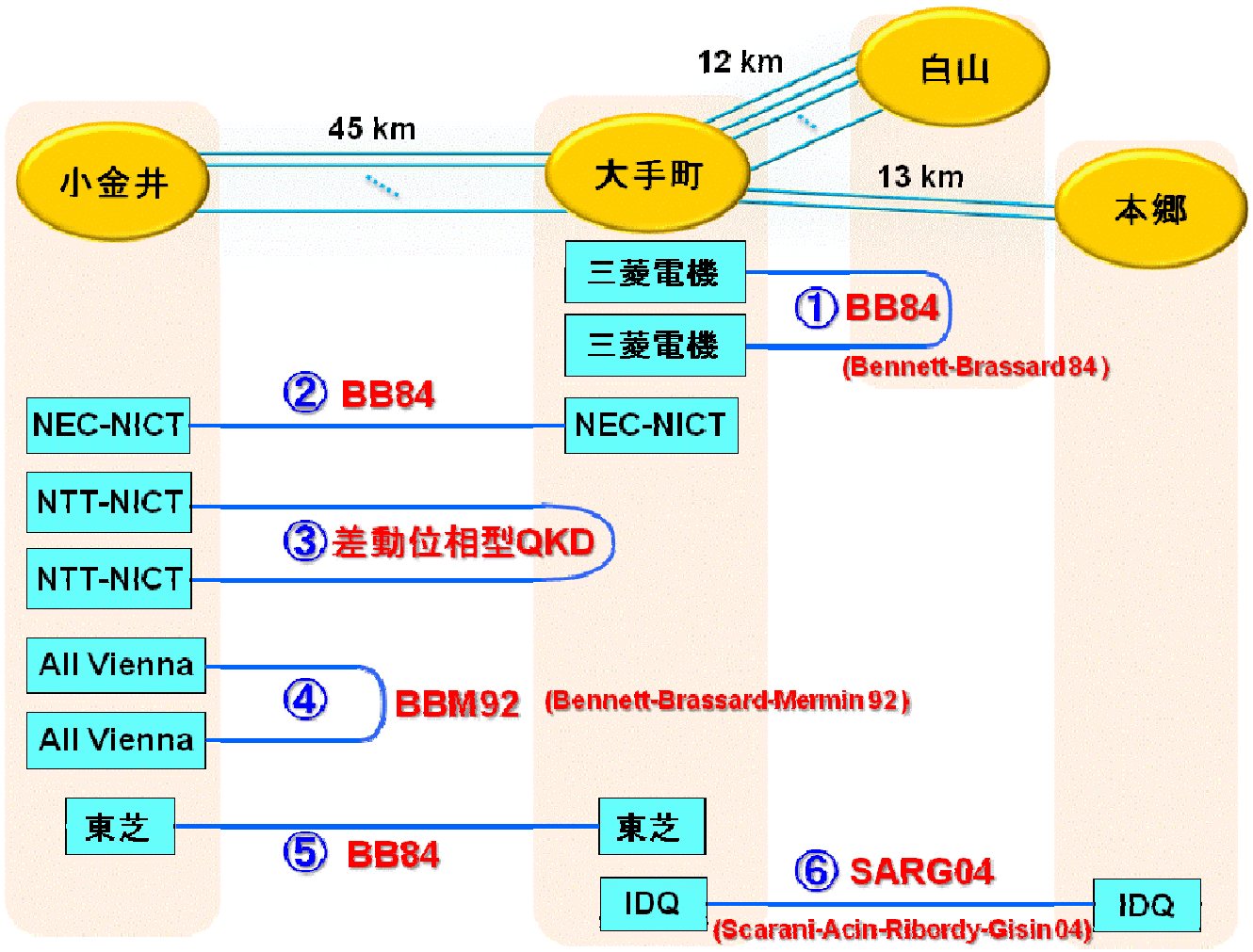
量子鍵配送（QKD）は、光の量子状態を使って絶対安全な秘密鍵を共有する技術である。その鍵を送信データと同じ長さだけ用意し、しかも1度だけ用いること（ワンタイムパッド）で完全秘匿な暗号通信を実現できる。NICT（量子ICTグループ、ナノICTグループ）、委託研究機関のNEC、三菱電機、NTT、さらに海外協力機関の東芝欧州研究所（TREL）、ID Quantique、All Vienna の連携により、JGN2plus上にQKDネットワークを構築し、相互接続試験、多地点テレビ会議システムへの適用、及び安定動作に向けた試験運用を行う。

研究の目的：

量子鍵配送は極めて高度な技術で、実用化には多くの課題があり、これまでのアメリカ国防総省や欧州連合のプロジェクトでは、音声データの暗号化が限界で、伝送距離も敷設ファイバで数10kmが限界であった。我が国では2001年からNICTの産学官連携プロジェクトにより、都市圏で完全秘匿なテレビ会議が実現できる世界最高速のQKD技術の研究開発に取り組んできた。この開発成果を用いてフィールド環境下で、完全秘匿な多地点テレビ会議システムの試験運用を行う。同時に主要な海外機関とも連携し、国際標準化に向けた相互接続試験や、盗聴攻撃の検知実験、経路切り替え動作なども実証する。

実験機器構成：

JGN2plus の 4 拠 点（大 手 町、小金井、白山、本郷)を結ぶ複数のファイバを用いて右図の①から⑥までの6つのQKD回線を構成した。赤字は用いたQKDプロトコルを示している。ネットワーク構成としては、次ページの図に示すような6つの接続ポイント、（ノード）からなり、最短1kmから最長で90kmまでカバーする都市圏のQKDネットワークになる。名称はTokyo QKD Networkである。



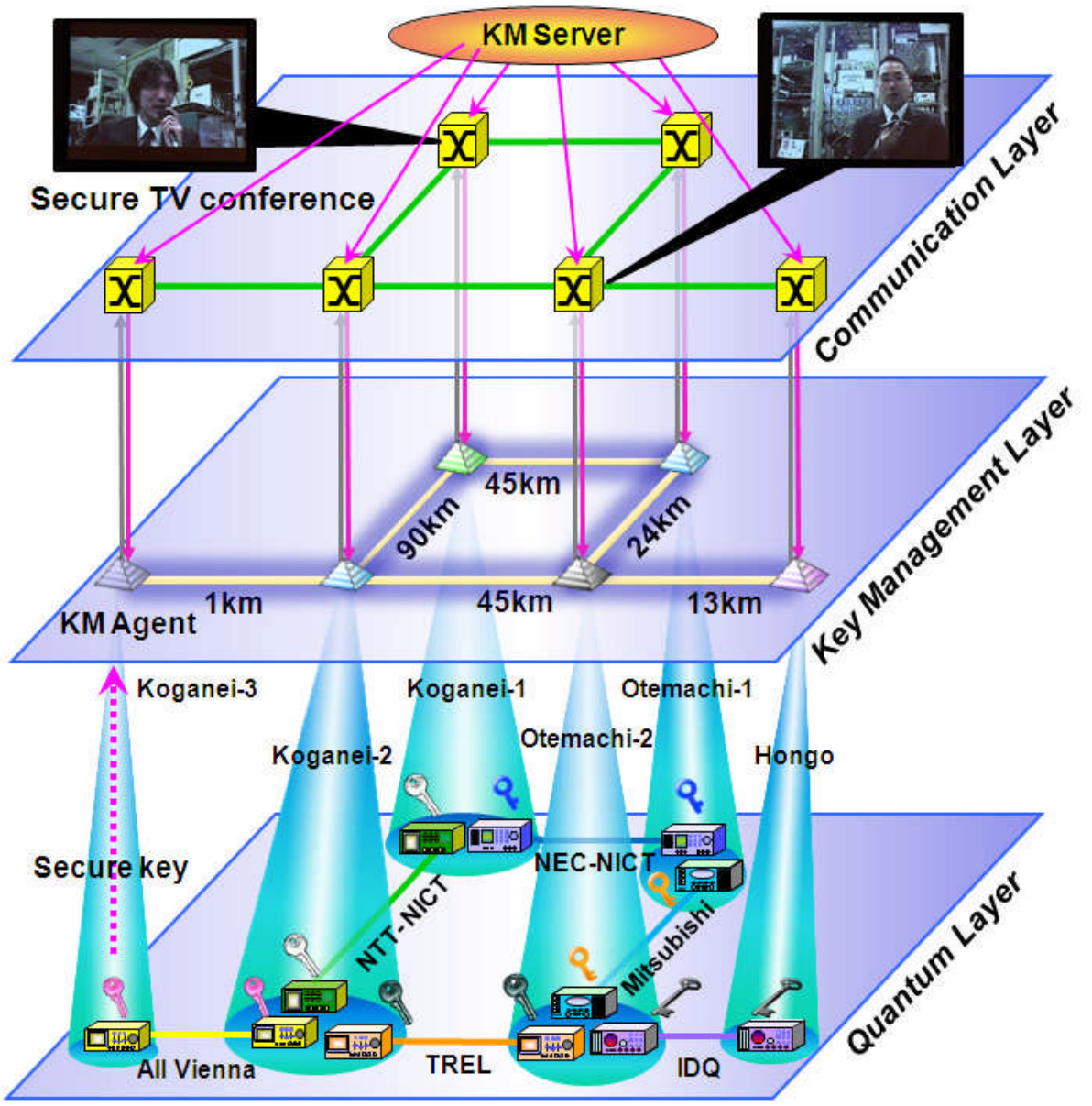
# 研究テーマ：都市圏量子鍵配送実験（2/2）

（プロジェクト番号 JGN2P－A21002）

研究機関：（独）情報通信研究機構、日本電気（株）、三菱電機（株）、日本電信電話（株）、（株）東芝（欧州研究所）、ID Quantique、All Vienna

研究開発成果：

光子の検出信号から秘密鍵を高速で蒸留するGHz動作の鍵蒸留処理エンジンを開発するとともに、極めて低雑音で高速の超伝導光子検出器を開発し、これらを統合して高速で長距離伝送可能なQKDシステムを開発した。これらの技術によって、45km圏で60～100kbpsの鍵生成速度を達成し、動画の量子暗号化に世界で初めて成功した。また、90km圏で2kbpsの性能を達成し、音声レベルの量子暗号化の長距離フィールド伝送のトップデータを叩き出した。QKDによる秘密鍵を用いたスマートフォンも開発した。




プロジェクトのアピールポイント

QKDの実利用に向けては、欧州の12カ国41機関が参加するSECOQCプロジェクトが、2008年、ウィーン市内の商用ファイバで大規模なネットワーク実証実験に成功している。当時のリンクの距離は約30kmで、鍵生成速度は1kbps程度で音声データのワンタイムパッド暗号化が限界であった。今回当プロジェクトにより、鍵生成速度は45kmの光ファイバ回線で毎秒約10万ビットと、実環境では世界最高速となった。また、SECOQCで開発された装置はもとより、日本独自の装置もネットワーク上で相互接続し、盗聴検知や経路切り替え、秘匿テレビ会議などを自在に行うためのアプリケーションインターフェースを開発した。このQKDネットワークのライブオペレーションは、10月14日に報道関係者に、さらに10月18日の国際会議UQCC2010において、研究者や省庁関係者、企業関係者に公開された。

プロジェクトの自己評価

日本と欧州のトップ機関が総力を結集して構築したTokyo QKD Networkでは、動画の完全秘匿伝送や携帯端末への応用など世界初の成果を生み出し、当該分野の発展・社会還元に向け大きな転換点を与えた。