MITSUBISHI
三菱電機

Changes for the Better

資料５－１

量子暗号技術の研究開発
- 最終目標にむけた取り組み-

平成16年 6月15日

三菱電機（株）、日本電気（株）、東京大学

発表者　笠原　久美雄（三菱電機）

NEC Empowered by Innovation

東京大学

目次

1. 国内外の研究開発状況（量子暗号）

2. 量子暗号技術の研究開発

3. 現状報告
   光学系、電子制御系、データ処理系

4. 最終目標にむけて

国内外の研究開発状況（量子暗号）

海外

- Geneva Univ.・・・67kmの実際の既設ファイバを用いて実施
- LM Univ.・・・・・・自由空間伝送の実験（空間23.4km）
  （LM Univ.: Ludwig-Maximilian University, Munich, Germany）
- MagiQ/Id Quantique・量子暗号プロトタイプ販売
- BBN/Harvard・・・量子暗号ネットワーク: DARPA Quantum Network

国内

- 三菱電機・・・・・システム開発（国内初システム実験成功）
  87km既存セキュリティと融合した統合量子暗号システム開発
- 東芝欧州研・・・光子検出器の研究、101km量子暗号実験
- 日本電気・・・・・低ノイズ光子検出器の開発、
  100km量子暗号実験、150km単一光子伝送実験
- 産総研・・・・・・・通信波長帯の高効率単一光子検出器の開発（10MHz）
  量子暗号実験(25.2km）、高速実験(45kbps@10km)

量子暗号技術の研究開発

研究開発項目

[期間] 2001年8月～2006年3月（5年間）

課題ア. 単一光子生成技術
課題イ. 単一光子検出技術
課題ウ. 乱数発生技術
課題エ. 量子暗号鍵配布システム技術

三菱電機担当分
（幹事会社）

エ-1. 量子暗号における安全で高効率なデータ処理技術
エ-2. 光送受信方式の高効率化技術
エ-3. 既存のセキュリティと融合した統合量子暗号システム
エ-4. 新しいスキームによる量子暗号・プロトコル方式技術

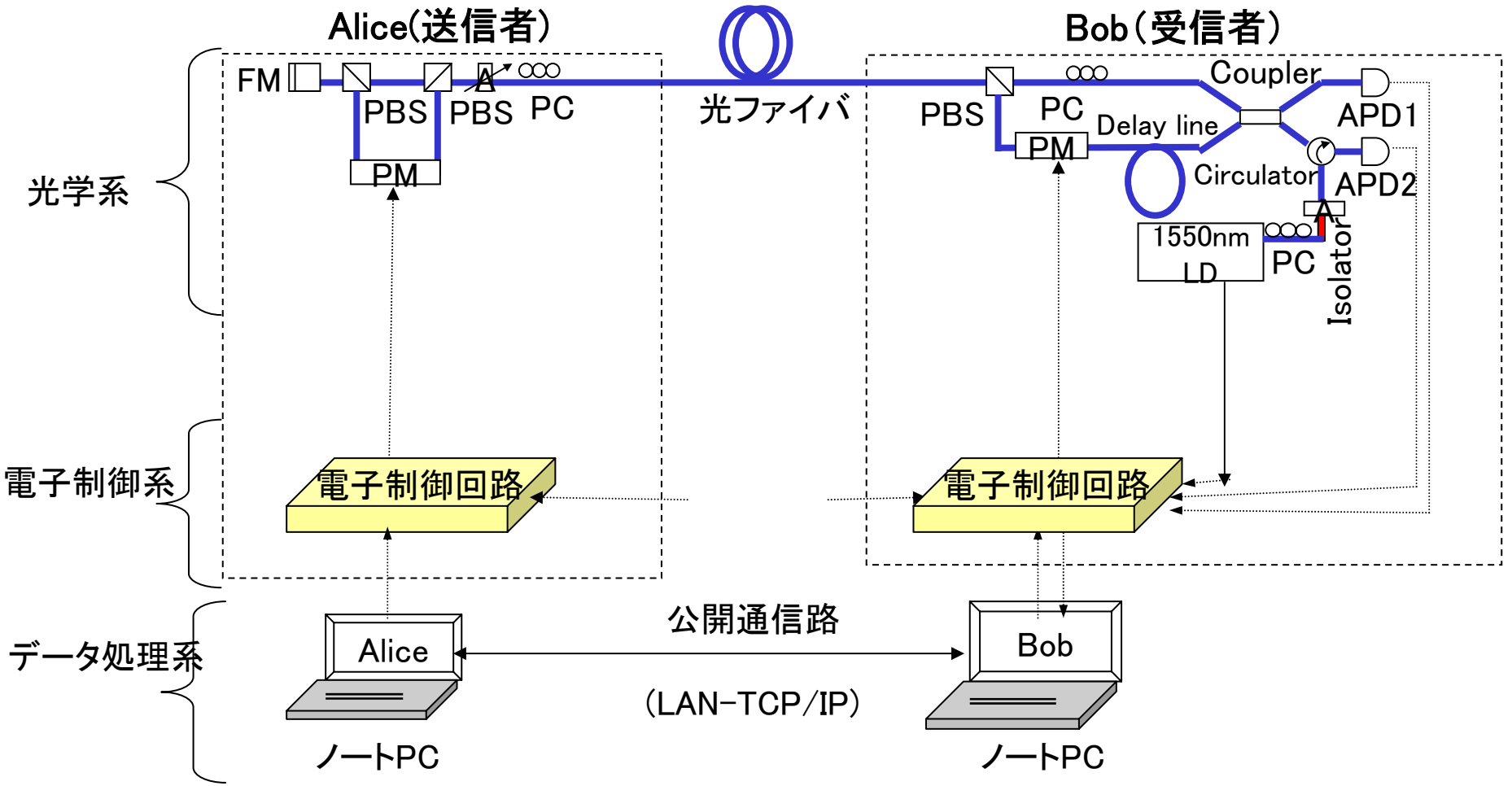
エ-5. 量子光信号変復調および位相同期技術
エ-6. モノリシック光変復調デバイス作成技術
エ-7. オンボード量子暗号システム技術
エ-8. 波長多重量子暗号ネットワーク技術

日本電気担当分

エ-9. 個人認証・誤り訂正・秘匿性増強ソフトウェア技術
エ-10.安全性解析およびマルチパーティプロトコルに関する研究

東京大学担当分

量子暗号システムの構成
（Plug&Play方式の例）



APD:Avalanche Photodiode, LD:Laser Diode, PC:Polarization Controller, PBS:Polarization Beam Splitter, PM:Phase Modulator, FM: Faraday Mirror

光学系

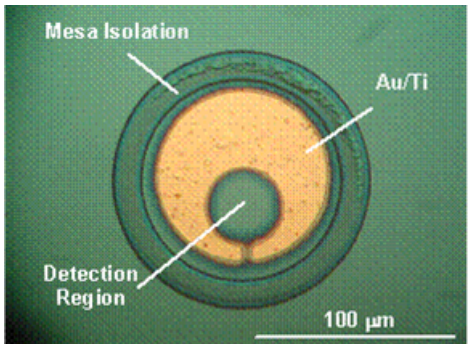
単一光子検出用デバイス（三菱電機）

量子暗号向けAPDデバイスの設計評価

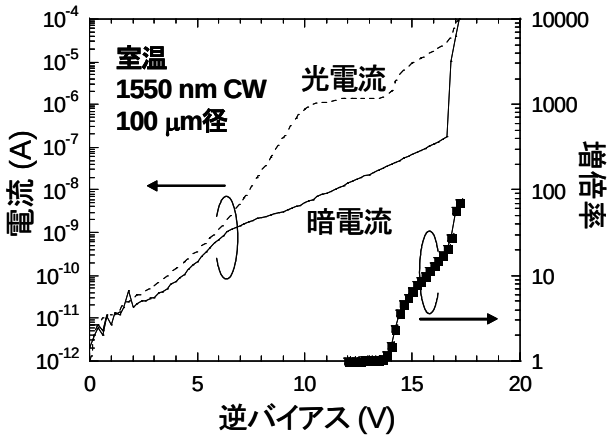
・層構造の設計

・レイアウト構造の検討

→APDデバイス開発へ



設計評価した試料（APDレイアウト構造検討）



作成した試料の
電流と増倍率の逆バイアス依存性

高性能高安定な干渉計デバイス（日本電気）

低損失PLC光遅延回路デバイス

PLC：平面光回路

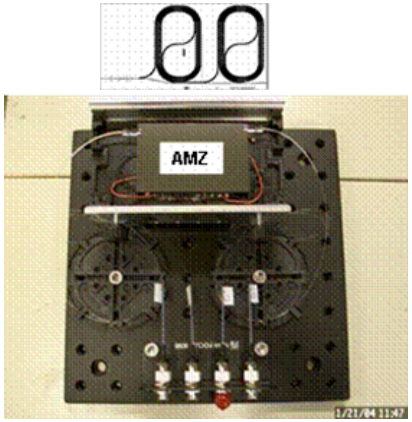
・1.75dB以下の低損失

光変調デバイス

・上記回路とLN位相変調素子を一体化

・温度制御素子を装荷して光変調デバイス試作

→ 150km 単一光子伝送実験に成功



低損失PLC光遅延回路デバイス

電子制御系

高速化対応量子暗号ハードウェア（三菱電機）

100kbpsを達成する高速量子暗号電子制御装置の開発

- 光子検出器の10MHz超の高速動作対応開発
- WDMによる光同期の実現

→ 最終年度にむけて
数百MHz動作向けの装置開発中

100kbps対応高速量子暗号装置

量子暗号プロトタイプの通信業界の展示会出展

- ITU TELECOM World 2003, Geneva 他

量子暗号装置のTELECOM World 2003 出展

データ処理系

安全で効率的な誤り訂正・秘匿性増強（三菱電機・東大の共同）

LDPC符号を用いた効率的な誤り訂正の実現

LDPC符号：Low Density Parity Check 符号

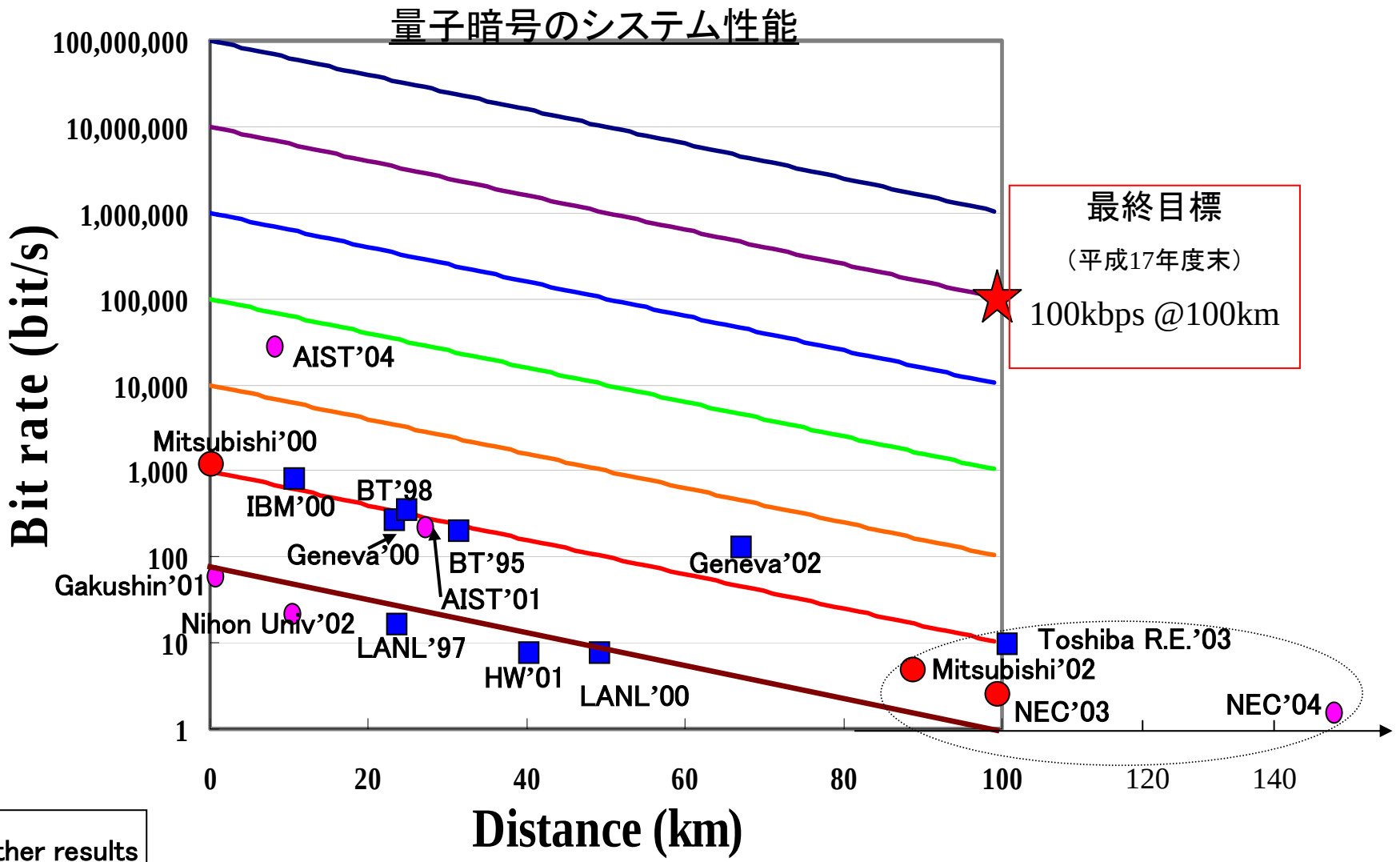
- 通信コストの低減及び（Shannon限界に近い）高効率が特徴
- 量子暗号システムでの実環境に合わせ（有限）符号長で効率設計
- 実システムに実装・評価

安全性解析・マルチパーティプロトコル（東大）

認証の実現に向けて

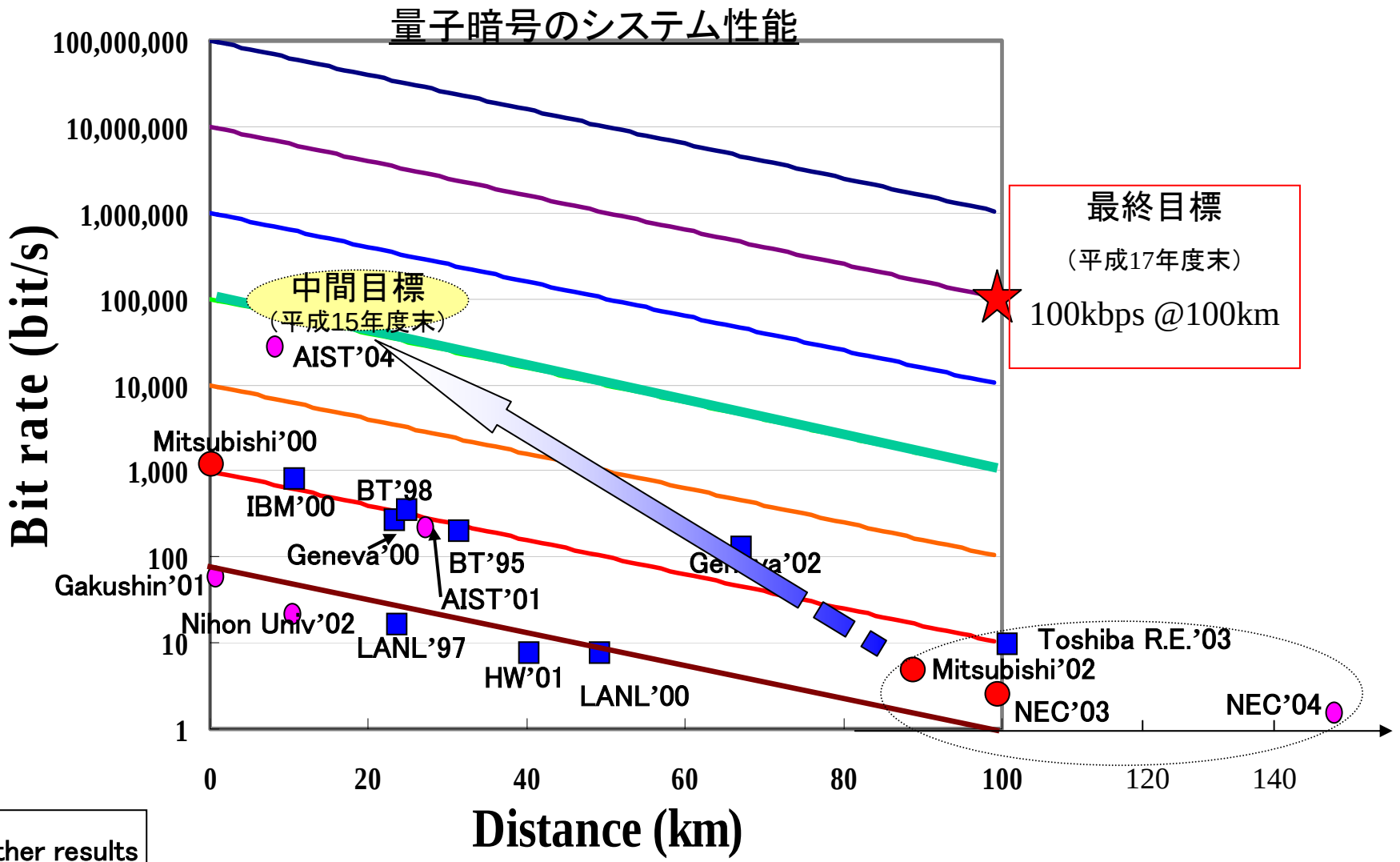
- 量子一方向性関数の存在を仮定した
  量子認証のための安全な量子ビットコミットメントの提案

最終目標にむけて



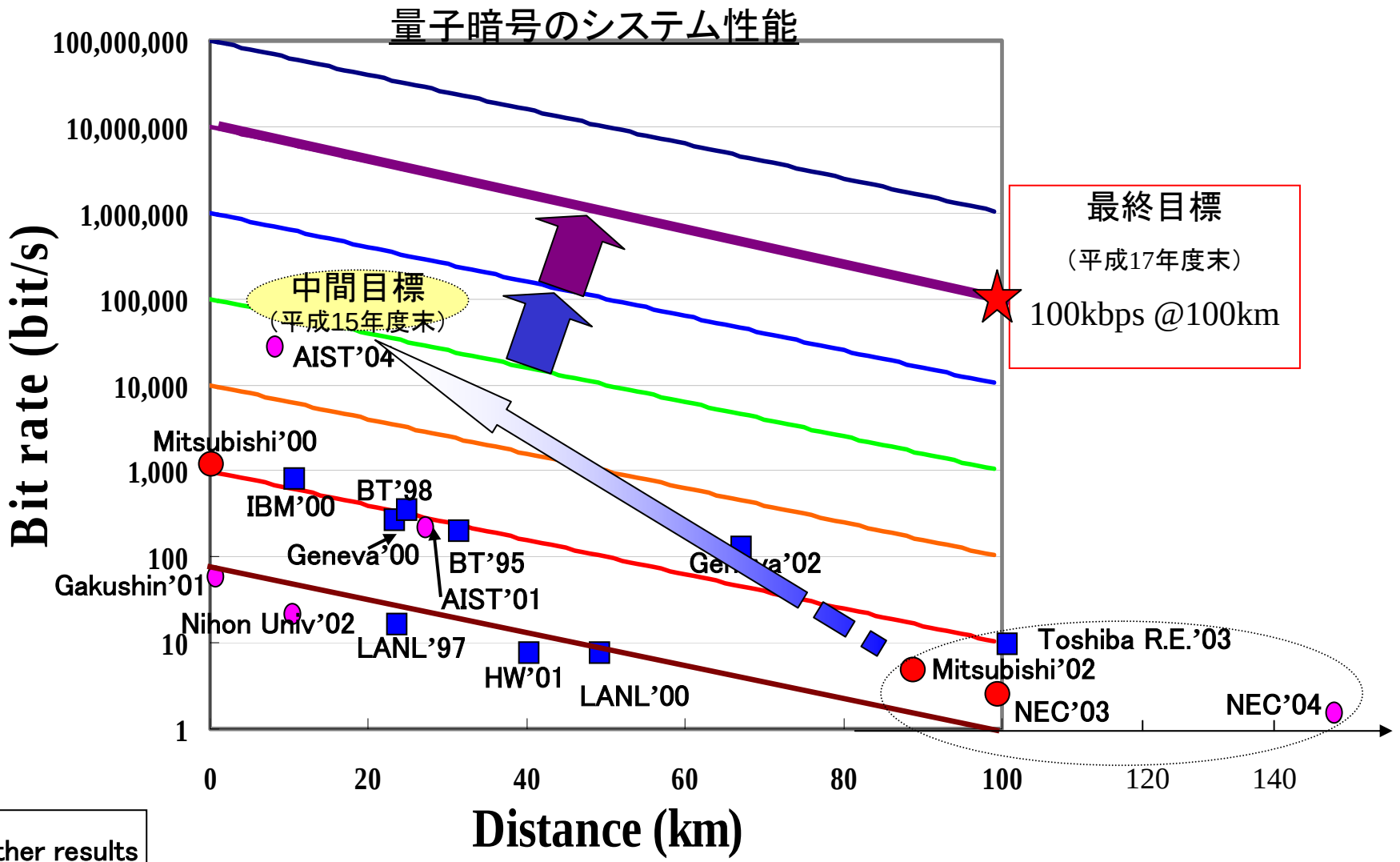
*The average photon number of Geneva'02, LANL'00 experiments are different from others(0.1)
These data are not under the same condition of laser repetition rate ν.

最終目標にむけて



*The average photon number of Geneva'02, LANL'00 experiments are different from others(0.1)
These data are not under the same condition of laser repetition rate ν.

最終目標にむけて



*The average photon number of Geneva'02, LANL'00 experiments are different from others(0.1)
These data are not under the same condition of laser repetition rate ν.