＜資料＞

【背景】BB84 量子鍵配送の安全性保証原理の変遷過程は以下のようになっている。(表１)

第一世代 (不確定性原理)：(a)完全な理想モデル（完全単一光子源、損失のない通信路、理想的な単一光子受信）の時の安全性は不確定性原理による信号への反作用によって、盗聴者を検知する。検知を受けて、全てを棄却し、通信を止めることによって安全性は保証される。(b) しかし以下のような問題が発生した：完全理想モデルは実現不可能である。

第二世代 (相互情報量評価)：(a) 物理的に実現可能なモデル（現実モデル）では、不確定性原理による信号の反作用なのか雑音などによる変化なのか識別できない。これらの 2 つの効果を盗聴者へ漏れる情報の量として評価し、盗聴者への相互情報量が極めて小さいなら、無条件安全と定義した。ここでは不確定性原理は主役ではなく、安全性は誤り訂正符号や秘密増幅符号の能力に依存する。(b) しかし、以下のような問題が発生した：盗聴者への相互情報量をいくら小さくしても、BB84 によって配送された鍵による One time pad 暗号(鍵使い捨て暗号)などの安全性が保証できない事例が発見された。

第三世代 (識別不可能性評価)：(a) BB84 で配送された鍵の系列としての乱数性を保証すれば、相互情報量による評価の欠点が解消されるという理論が提案され、その乱数性の識別評価誤差が極めて小さいなら無条件安全と定義された。(b) しかし、以下のような問題が発生した：識別評価誤差が有限の数値（ゼロではない）のとき、その値が暗号学的にどのような意味があるのか不明。プロトコルが失敗する確率であるとの解釈があるが、失敗の確率という概念は暗号学的な安全性を意味しない。

第四世代 (鍵推定成功確率評価)：暗号学的に安全性を評価する方法として、BB84 で配送された鍵の推定成功確率が Northwestern 大学と玉川大学によって導入された。これは情報理論的安全性の原点である Shannon の概念の自然な一般化であり最終的評価基準となる。

表１　BB84安全性保証原理の変遷

	モデル	安全性評価法	安全性保証法	有効性
第一世代 1984- 1995年	完全理想モデル **•単一光子源、無損失、無雑音** **•単一光子検出**	不確定性原理or 量子非複製定理	•鍵廃棄処分 •通信停止	○
第二世代 1996- 2006年	現実モデル **•単一光子源、損失、雑音** **•光子検出**	送信者・盗聴者 の相互情報量評価	•符号能力 誤り訂正 秘密増幅	✖
第三世代 2007- 2009年	現実モデル **•単一光子源、損失、雑音** **•光子検出**	識別不可能性評価	•符号能力 誤り訂正 秘密増幅	✖
第四世代 2010年-	現実モデル **•単一光子源、損失、雑音** **•光子検出**	盗聴者の 鍵推定成功確率評価	•符号能力 誤り訂正 秘密増幅	○

第三世代評価法で現実モデルのBB84は安全であるように見えたが、同じモデルを第四世代評価法で評価すれば無条件安全性を達成できない事が証明される。
結果として、安全性が保証されたBB84は実現不可能となる。