2020-01-11 第9回 Quatuo at 崇城大学

量子暗号とセキュリティの三要素: 秘匿性、完全性、可用性

三重大学
工学部 情報工学科
岩越 丈尚
iwakoshi@cs.info.mie-u.ac.jp

0-1. Information Security の三要素とは

機密性 (Confidentiality): 正規ユーザーがだけが、当該情報にアクセスできること
完全性 (Integrity): 情報が破壊、改ざん又は消去されていないこと
可用性 (Availability): 正規ユーザーが、必要時に中断なくアクセスできること
*ISO/IEC 27002 での定義 [1]

これ以外に要求される事項は下記がありますが、本日は上記の話です。
-真正性 (authenticity): ある主体が主張どおりであることを確実にすること。
-責任追跡性 (accountability): 動作主の主体まで一意に追跡できること。
-否認防止 (non-repudiation): 動作を後に否認されないように証明すること。
-信頼性 (reliability): 意図した動作及び結果に一致する特性

これと量子暗号がどう関係するか？

前半はスタンダードな量子暗号 (正確には量子鍵配送 (QKD) + One-Time Pad)、
後半は Y00 プロトコルという量子暗号について上記との関連を話します。

0-2. 発表の前に、私からのお願い

発表者は特にQKDをけなしたい訳ではありません。それどころかYOOプロトコルの安全性解析において、それまで QKD を批判的に研究したことが役に立ってます。私はこれまで下記のように書きましたが、これが真摯な思いです。

“QKDは実際に利用することが想定されている技術である．最近では，車載ネットワークや医療データベースに利用することが検討されている．しかし，もしQKDの安全性証明に本質的な問題があるならば，普及してから社会インフラに与える影響は大きい．…本研究の著者はこうした知見を量子鍵配送の安全性を評価する上で真剣に議論して頂けることを望んでいる．” [2]

“一方，QKD以外の量子暗号もいくつか発表されている．もちろん，量子力学により古典通信では不可能だった秘匿通信をQKDという形で実現できることを示唆した先人たちの基礎科学的な功績は讃えられるべきである．さらに本稿で述べた通り，QKDは物理暗号に要求される安全性とは何かという重大な課題も浮き彫りにしてくれている．しかし実用性という観点から鑑みて，QKD以外の方策も研究される価値は十分にあると思われる．そのときでも，QKDで研究された知見が生かされる可能性は十分にあると執筆者は考える．” [3]

Table of Contents (前半)

1-1. One-Time Pad の機密性と QKD (1/2)

シーザー暗号
紀元前のローマ将軍、ユリウス・カエサルが発明した暗号。アルファベットを３つずらして暗号化し、もとに戻すときはずらしたぶんだけアルファベットを戻す。

例: HELLO WORLD → KHOOR ZRUOG (3つずらしたあと)

アルファベットは26文字なので、26文字総当りで試せば解読できてしまう。

One-Time Pad (OTP) [4]
バーナムが1918年に考案した。アルファベットをずらす量を1文字ごとに完全にランダムに選択する。コンピュータは 0 と 1 でコード化するので、メッセージ X と同じ長さの 0 と 1 がランダムに続く列を鍵 K とし、暗号文 $C = X + K \bmod 2$

例: HELLO WORLD に相当する X = 1101010010100111000101010101001…
鍵 K = 0101001011010010100110101010101…
暗号文 C = 1000010001110101110001111111100…

I-2. One-Time Pad の機密性と QKD (2/2)

Shannon による証明では暗号文 $C = X + K \bmod 2$ として下記が必要条件[5]。

$$\Pr(X|C) = \Pr(X)$$

(後に等価な表現として定着したのは $H(X|C) = H(X)$)

C がわかっても、平文 X の推定に一切寄与しない。
鍵 K が一様独立分布 (IID) である場合。単に $|X| = |K|$ だけではダメ。

ではそのような鍵をどうやって共有するか？
アメリカーロシア（当時はソ連）ホットラインにかつては使用されており、実際にエージェントが運んでいた。

1984年: ベネットとブラサールが量子力学を利用して安全に鍵を送る量子鍵配送 BB84 プロトコルを発表し、これによりOTPを実現できると主張 [6]。

I-3. BB84とその Family (QKD) の安全性の定義

一般に次の形で定義される [7]。

$$\mathrm{tr}\left|\rho_{ABE}-2^{-k}I_{AB}\otimes\tau_E\right|\leq\mathrm{tr}\left|\rho_{ABE}-\zeta_{ABE}\right|+\mathrm{tr}\left|\zeta_{ABE}-2^{-k}I_{AB}\otimes\tau_E\right|\leq 2\varepsilon_{cor}+2\varepsilon_{sec}$$

$\mathrm{tr}\left|\rho_{ABE}-\zeta_{ABE}\right|\leq 2\varepsilon_{cor}$: AliceとBobとの間で鍵の誤り訂正に失敗する確率

$\mathrm{tr}\left|\zeta_{ABE}-2^{-k}I_{AB}\otimes\tau_E\right|\leq 2\varepsilon_{sec}$: AliceとBobとの間で安全な鍵抽出に失敗する確率

以上から確率 $\varepsilon_{cor}+\varepsilon_{sec}$ 以下で IID な鍵の抽出に失敗するとしている [7, etc]。

本当か？

Shor-Preskill の証明(2000年) [8] の後、Koashi の証明(2008年)により[9]、Prepare-and-Measure (PM) と Entanglement Distillation (ED) の両 QKD は等価とされている (例えば [10, 11] も)。

I-4: ED-QKD と PM-QKD の等価性で使われる論法

“Eve にわからなければ、PM-QKD と等価な仮想プロトコルを用いてもよい”

最初に Shannon’s Maxim (Kerchhoffs’ の原理) を考えましょう。

“攻撃者は秘密鍵 K 以外のすべてを知っている。”[補足 I]

↓

稼働しているのが仮想プロトコルか実プロトコルなのか Eve は知っているはず。

1. Eve にとって実プロトコルの挙動だけが重要で、実プロトコルと仮想との挙動が違えば当然、両者は物理学的にちがうプロトコルである。
2. 実/仮想どちらのプロトコルか Eve にわからないようにするには各プロトコルを確率 1/2で使い分けるべきだが、実際に使っていないからこそ仮想である。
3. 仮想プロトコルでは鍵を盗みにくいというアドバンテージがあるなら最初から Alice と Bob は仮想プロトコルを使うべき。

では本当に実/仮想プロトコルが物理学的に等価かを、具体的に計算しましょう。
ここでは Shor-Preskill が等価性を証明したとする [8] BB84 を扱います。

I-5: Prepare-and-Measure QKD への攻撃 (1/2)

ED-QKD との比較を簡単にするために次のように BB84 を少し変形 [12]。

1. Alice は IID なビット k_A に対応した2つの量子状態のコピーを用意する。
2. Alice は確率 1/2 で Z か X の基底を選択し、片方をBob に1qubitずつ送る。
3. 通信路の途中で Eve は量子メモリを準備し1qubitずつ同じユニタリ操作をする。
4. Bob は Eve の操作を受けた qubit を確率 1/2 で Z か X の基底で測定する。
5. Eveは量子メモリを測定せずひたすら同じ操作を繰り返す。
6. Alice と Bob は基底 B を公開し、一致しないものを破棄する。
7. このとき Alice と Eve も対応する量子ビットを破棄する。
8. Alice と Bob は QBER (誤り率 Q) を公開通信路で確認する。
9. さらに必要な誤り訂正方法 C を決め公開通信路上 One-Time Pad で合意する。
10. さらに必要な秘匿性増幅方法 P を公開し、最終鍵 k を得る。
11. Eve は公開情報 $S = (B, Q, C, P)$ をもとに最適測定 $M(k_E|S)$ を決める。
12. Eve は量子メモリを測定し、$k_E = k$ なら盗聴に成功。

このプロセスを式で書くと次のようになります。

I-5: Prepare-and-Measure QKD への攻撃 (1/2)

ED-QKD との比較を簡単にするために次のように BB84 を少し変形 [12]。

1. Alice は IID なビット k_A に対応した2つの量子状態のコピーを用意する。
2. Alice は確率 1/2 で Z か X の基底を選択し、片方をBob に1qubitずつ送る。
3. 通信路の途中で Eve は量子メモリを準備し1qubitずつ同じユニタリ操作をする。
4. Bob は Eve の操作を受けた qubit を確率 1/2 で Z か X の基底で測定する。
5. Eveは量子メモリを測定せずひたすら同じ操作を繰り返す。
6. Alice と Bob は基底 B を公開し、一致しないものを破棄する。
7. このとき Alice と Eve も対応する量子ビットを破棄する。
8. Alice と Bob は QBER (誤り率 Q) を公開通信路で確認する。
9. さらに必要な誤り訂正方法 C を決め公開通信路上 One-Time Pad で合意する。
10. さらに必要な秘匿性増幅方法 P を公開し、最終鍵 k を得る。
11. Eve は公開情報 $S = (B, Q, C, P)$ をもとに最適測定 $M(k_E|S)$ を決める。
12. Eve は量子メモリを測定し、$k_E = k$ なら盗聴に成功。

このプロセスを式で書くと次のようになります。

I-6: Prepare-and-Measure QKD への攻撃 (2/2)

ED-QKD との比較を簡単にするために次のように BB84 を少し変形 [12]。

1. Alice は確率 1/2 で Z か X の基底を選択し、ビット k_A に対応した2つの量子状態のコピーを用意する。
2. Alice は確率 1/2 で Z か X の基底を選択し、片方をBob に 1qubitずつ送る。
3. 通信路の途中で Eve は量子状態を盗聴し、1qubitずつ同じユニタリ操作をする。
4. Bob は Eve の操作を受けた qubit を確率 1/2 で Z か X の基底で測定する。
5. Eveは量子状態を盗聴したときに用いた操作を公開する。
6. Alice と B
7. このとき Alice と Eve も対応する量子ビットを破棄する。
8. Alice と B
9. さらに必要
10. さらに必要な秘匿性増幅方法 P を公開し、最終鍵 K を得る。

初期状態

$$|k''_A,k''_A\rangle_{AB}\otimes|l''_E\rangle_E$$

Z基底ならば $b=0$,
X基底ならば $b=1$ で Hadamard 変換

$$\left(H_A{}^b\otimes H_B{}^b\right)|k''_A,k''_A\rangle_{AB}\otimes|l''_E\rangle_E$$

Eveは b を知らずに U_{BE} を行う

$$\left(H_{AB}{}^b\otimes I_E\right)\left(I_A\otimes U_{BE}\right)\left(H_{AB}{}^b\otimes I_E\right)|k''_A,k''_A,l''_E\rangle_{ABE}=|k''_A,k''_B,k''_E\rangle_{ABE}$$

繰り返して、誤り訂正 C と秘匿性増幅 P

$$\rho_E(S,k_A)=\sum_{k''_A|k_A=f_S(k''_A)}\Pr(k''_A|S,k_A)\mathrm{tr}_{AB}|k''_A,k''_A,k''_E\rangle\langle k''_A,k''_A,k''_E|_{ABE}$$

Eve による最適測定

$$\Pr(k_E|k_A)=\mathrm{tr}[M_E(k_E|S)\,\rho_E(S,k_A)]$$

Eve にとっての平均成功率

$$\mathrm{Ex}[\Pr(k|k)]=\sum_k\Pr(k)\Pr(k|k)$$

P の性質上，$k_A=f_S(k''_A)$ は 1 対多写像であることに留意。

このプロセスを式で書くと

I-7: Prepare-and-Measure QKD への攻撃 (1/2)

$$\rho_{E}(S,k_{A})=\sum_{k''_{A}|k_{A}=f_{S}(k''_{A})}\Pr(k''_{A}|S,k_{A})\mathrm{tr}_{AB}\left|k''_{A},k''_{A},k''_{E}\right\rangle\left\langle k''_{A},k''_{A},k''_{E}\right|_{ABE}$$

Eve による最適測定

$$\Pr(k_{E}|k_{A})=\mathrm{tr}[M_{E}(k_{E}|S)\,\rho_{E}(S,k_{A})]$$

Eve にとっての平均成功率

$$\mathrm{Ex}[\Pr(k|k)]=\sum_{k}\Pr(k)\Pr(k|k)$$

P の性質上，$k_A = f_S(k_A)$は1対多写像であることに留意。

気をつけるべき点: Eve にとっての平均成功率

1. 最初に IID で k''_A を選んでも、$\Pr(k_A)$ が Eve にとって IID とは限らない。
2. 自明に $\Pr(k|k) > 2^{-|k|}$. 理由は Hashing P は $|k''_A| > |k|$ から $|k|$ への写像で、入力 $k''_E \neq k''_A$ が出力 $k_E = k$ に「偶然に衝突する確率」$> 2^{-|k|}$ だから。
3. 従って最終的な鍵ビット列は、One-Time Pad が要求する IID を満たさない。

つまり、PM-QKD で配送された鍵は完全秘匿の条件を満たし得ない。

I-8: Prepare-and-Measure QKD の数値的強度(1/2)

$$\rho_{E}(S,k_{A})=\sum_{k''_{A}|k_{A}=f_{S}(k''_{A})}\Pr(k''_{A}|S,k_{A})\mathrm{tr}_{AB}\left|k''_{A},k''_{A},k''_{E}\right\rangle\left\langle k''_{A},k''_{A},k''_{E}\right|_{ABE}$$

Eve による最適測定

$$\Pr(k_{E}|k_{A})=\mathrm{tr}[M_{E}(k_{E}|S)\,\rho_{E}(S,k_{A})]$$

Eve にとっての平均成功率

$$\mathrm{Ex}[\Pr(k|k)]=\sum_{k}\Pr(k)\Pr(k|k)$$

P の性質上，$k_{A}=f_{S}(k_{A})$ は1対多写像であることに留意。

また、H. P. Yuen および C. Portmann の導出 [13 - 15] から常に

$$\mathrm{Ex}[\Pr(k|k)]\leq\frac{1}{2}\mathrm{tr}\left|\zeta_{ABE}-2^{-k}I_{AB}\otimes\tau_{E}\right|+2^{-k}\leq\varepsilon_{sec}+2^{-k}$$

既知の実験での最良値は $\varepsilon_{sec}=2^{-50}$ [16] なので、$k=50$ bit ならかろうじて“ほぼ IID”だが、実用上 $10^{3}<|k|<10^{6}$ とすると“IID には遠すぎる。”
鍵長は $|k|$ なのに、Eve にとって 50 bit 程度の不定性しかなく、そのくらいの鍵候補を順に試していく (つまり解読する) くらいはできてもおかしくない。

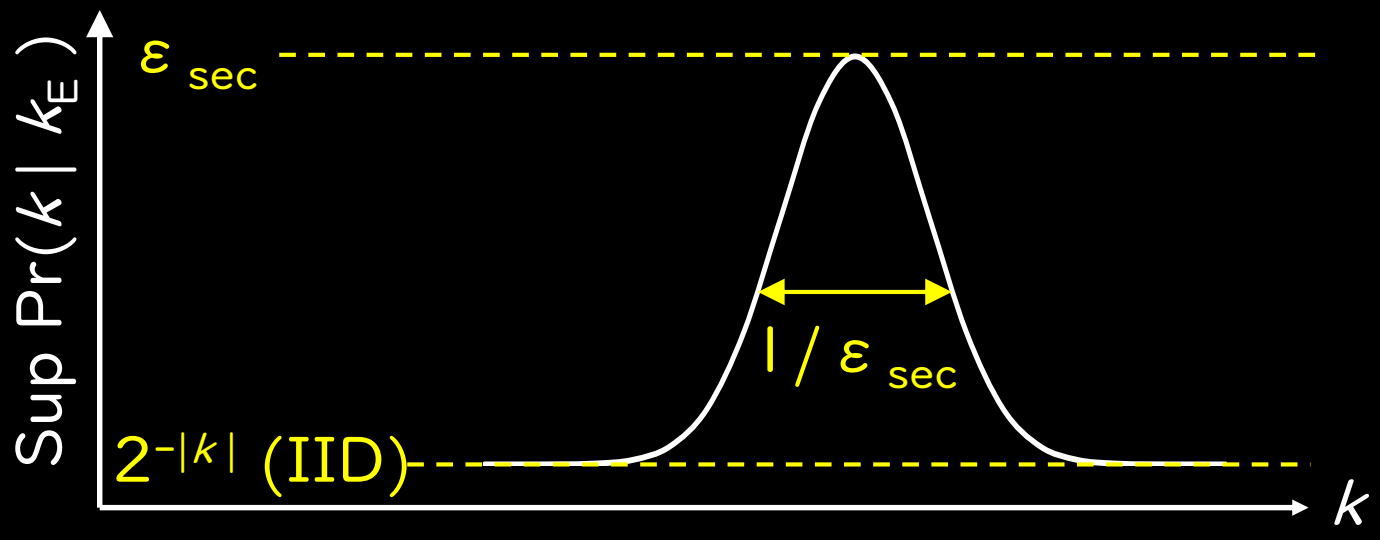
I-9: Prepare-and-Measure QKD の数値的強度 (2/2)

また、H. P. Yuen および C. Portmann の導出 [13 - 15] から常に

$$\mathrm{Ex}[\Pr(k|k)] \leq \frac{1}{2}\mathrm{tr}\left|\zeta_{ABE} - 2^{-k} I_{AB} \otimes \tau_E\right| + 2^{-k} \leq \varepsilon_{sec} + 2^{-k}$$

既知の実験での最良値は $\varepsilon_{sec} = 2^{-50}$ [16] なので、$k = 50$ bit なら “ほぼ IID” だが、実用上 $10^3 < |k| < 10^6$ とすると “IID には遠すぎる。”
鍵長は $|k|$ なのに、Eve にとって 50 bit 程度の不定性しかなく、そのくらいの鍵候補を高確率のものから試して平文候補を探索するくらいはできてもおかしくない。

図示すると例えばこんな感じ。



QKD の安全性を主張するには
ε_{sec} をさらに小さくし、かつ
ε_{sec} がどの程度 $2^{-|k|}$ に近いか、
という実験値が必要。[補足2]

I-10: Entanglement-Distillation QKD への攻撃 (1/2)

BB84 と等価とされた Modified Lo-Chau Protocol を示す[9]。

1. Alice は CSS コードで符号化された量子エンタングルメントを用意する。
2. Alice は一方を保存し、片方に確率1/2でHadamard 変換して Bob に送る。
3. 通信路の途中で Eve は量子メモリを準備し1qubitずつ同じユニタリ操作をする。
4. Bob は Eve の操作を受けた qubit を測定せず保存する。
5. Alice は Hadamard 変換した qubit を公開し、Bob に同じ変換を施させる。
6. Eve は何らかの操作を自分の量子メモリに施す。
7. Alice と Bob は Z 誤り率と X 誤り率を公開通信路で確認する。
8. Aliceは CSS コードを公開し、量子誤り訂正を施す。
9. Alice と Bob は誤り訂正後の量子状態を CSS コード化前に戻す。
10. Alice と Bob は上記で得られた最大エンタングル状態を測定しkを得る。
11. Eve は公開情報 S = (Hadamard, CSS) をもとに最適測定 $M(k_E|S)$を決める。
12. Eve は量子メモリを測定し、$k_E = k$なら盗聴に成功。

このプロセスを式で書くと次のようになります。

I-11: Entanglement-Distillation QKD への攻撃 (2/2)

BB84 と等価とされた Modified Lo-Chau Protocol を示す[11]。

初期状態 [補足3]

$$\left|k''_A, k''_A\right\rangle_{AB} \otimes \left|l''_E\right\rangle_E$$

1. [illegible] コードで符号化された量子ビットを用意する。
2. Alice は一方を保存し、片方に確率 1/2 で Hadamard 変換して Bob に送る。
3. 通信路の途中で Eve は量子メモリを [illegible] ずつ同じユニタリ操作をする。
4. Bob は Eve の操作を受けた qubit を測定せずに保存する。
5. Alice は H [illegible] 施させる。
6. Eve は何 [illegible]
7. Alice と Bob は Z 誤り率と X 誤り率を公開通信路で確認する。
8. Alice は [illegible]
9. Alice と [illegible] 測定し [illegible] を得る。
10. Alice と Bob は上記で得られた最大エラー [illegible] 状態を測定しを得る。
11. Eve は公開情報 S = (Hadamard, CSS, [illegible] 最適測定 $M(E|S)$ を構成する。
12. Eve は量子メモリを測定し、$k_E = k$ なら盗聴に成功。

このプロセスを式で書くと次 [illegible]

$$\frac{1}{2}\mathrm{tr}\left|\zeta_{ABE} - 2^{-k} I_{AB} \otimes \tau_E\right| \le \varepsilon_{sec}$$

Z基底ならば $b=0$,
X基底ならば $b=1$ で Hadamard 変換

$$\left(H_A{}^b \otimes H_B{}^b\right)\left|k''_A, k''_A\right\rangle_{AB} \otimes \left|l''_E\right\rangle_E$$

Eve は b を知らずに U_{BE} を行う

$$\left(H_{AB}{}^b \otimes I_E\right)\left(I_A \otimes U_{BE}\right)\left(H_{AB}{}^b \otimes I_E\right)\left|k''_A, k''_A, l''_E\right\rangle_{ABE} = \left|k''_A, k''_B, k''_E\right\rangle_{ABE}$$

Z誤り率とX誤り率を (e_Z, e_X) とする。

$$\rho_E(S) = \sum_{(e_Z,e_X)} \Pr((e_Z,e_X)|S)\,\mathrm{tr}_{AB}\left|(e_Z,e_X)\right\rangle\left\langle(e_Z,e_X)\right|_{AB} \otimes \left|k''_E\right\rangle\left\langle k''_E\right|_E$$

$\Pr((0,0)|S) \ge 1-\varepsilon_{sec}$ のとき
Alice-Bob の鍵が Eve にとって完全に
IID にはならない確率 (Eve の成功確率)

I-12: PM-QKD と ED-QKD の物理学的相違

PM-QKD におけるEve にとっての平均成功率

$$\mathrm{Ex}[\Pr(k|k)] = \sum_k \Pr(k)\Pr(k|k)$$

また、H. P. Yuen および C. Portmann の導出 [13 - 15] から常に

$$\mathrm{Ex}[\Pr(k|k)] \le \frac{1}{2}\mathrm{tr}\left|\zeta_{ABE} - 2^{-k} I_{AB} \otimes \tau_E\right| + 2^{-k} \le \varepsilon_{sec} + 2^{-k}$$

Eve の鍵は Alice-Bob の鍵と決して独立にはならず $\varepsilon_{sec} \sim 2^{-|k|}$ で Almost-IID。

ED-QKD におけるEve にとっての平均成功率 [12]

$$\mathrm{Ex}[\Pr(k|k)] \le \frac{1}{2}\mathrm{tr}\left|\zeta_{ABE} - 2^{-k} I_{AB} \otimes \tau_E\right| \le \varepsilon_{sec}$$

確率 $1-\varepsilon_{sec}$ 以上で、Eve にとって Alice-Bob の鍵は IID になる。
また、確率 ε_{sec} でEveのメモリはAlice-Bobとの相互作用を残しており PM-QKD と同様の状態になっているため、Eveの盗聴成功確率は ε_{sec} よりさらに小さい。

仮想/実プロトコルの等価性を主張するならEve の視点から等価性を証明すべき

I-13:「等価である」との主張はなぜ定着したか (1/2)

2000年: Shor-Preskill の証明 [9] は、安全性評価を相互情報量で行った。
2008年: 相互情報量では安全を保証できないことが証明され、R. Renner らにより
トレース距離が導入された [8, 17]。
2008年: Koashi によりトレース距離を導入し、かつ Shor-Preskill と同じ枠組みで安全性を証明できることが示された [9]。
2012年: M. Hayashi and T. Tsurumaru により、配送量子ビットの位相誤りのみでトレース距離の上界が与えられると示される [18]。
…など。

実際、PM-QKD の検算をしてみると、最終的に Eve の盗聴成功確率に影響するのは位相誤りであることはわかる [12]。
また、トレース距離の上界が位相誤りの量で決まる、というのも正しい。
しかし、これだけでは ED-QKD と PM-QKD が物理的に等価、とはならない。

検証のため、Koashi の証明を下記に概略する [9, 12]。

I-13: 「等価である」との主張はなぜ定着したか (2/2)

Koashi の証明では [9, 12] Eve の系を知らずに上界を決められない論理的矛盾。

実際に配送された状態: $\zeta_{ABE} := \sum_{k_A,k_B} \Pr(k_A,k_B)|k_A,k_A\rangle\langle k_A,k_A| \otimes \sigma_E(k_A,k_B)$

配送されるべき理想状態: $\tau_{ABE} := \sum_k 2^{-|K|}|k,k\rangle\langle k,k| \otimes \tau_E$

Koashi による証明手順では、Shor-Preskill の手法を踏まえ、量子状態 $\tau_E := \kappa_E$ を下記不等式を満たすように選んだ。

PM-QKD 形式　$F\left(\zeta_{ABE}, |MES\rangle\langle MES|_{AB} \otimes \kappa_E\right) \le F\left(\zeta_{AB}, |MES\rangle\langle MES|_{AB}\right)$　ED-QKD 形式

でなければ下記等号を満たさないから。

$$\varepsilon_{sec} \ge \sqrt{1-F(\zeta_{AB}, |MES\rangle\langle MES|_{AB})^2} \le \sqrt{1-F(\zeta_{ABE}, |MES\rangle\langle MES|_{AB} \otimes \kappa_E)^2}$$

$$\ge \sqrt{1-F(\zeta_{ABE}, \tau_{AB} \otimes \kappa_E)^2} \ge \frac{1}{2}\mathrm{tr}|\zeta_{ABE} - \tau_{AB} \otimes \kappa_E|$$

必要条件は Eve の状態が既知であること $\kappa_E := \sum_l \Pr(\kappa_E(l))|\kappa_E(l)\rangle\langle\kappa_E(l)|$

$$\Pr(\kappa_E(l)) = \langle\kappa_E(l)|\langle MES|\zeta_{ABE}|MES\rangle|\kappa_E(l)\rangle F(\zeta_{AB}, |MES\rangle\langle MES|_{AB})^2$$

I-14: QKD の Universal Composability について

Universal Composability は「実プロトコルが理想プロトコルと互換であるため、攻撃された部分が他へ影響を及ぼさない」とする概念 (R. Canetti) [19]。

QKD でいえばどのような状況か？
「Eveが一切盗聴できない量子通信と、Eveの量子メモリが配布された鍵との相互作用を残した状態とが互換である」ことが UC の条件。

繰り返しですが、H. P. Yuen および C. Portmann の導出 [13 - 15] から常に

$$\mathrm{Ex}[\Pr(k|k)] \le \frac{1}{2}\mathrm{tr}\left|\zeta_{ABE} - 2^{-k} I_{AB} \otimes \tau_E\right| + 2^{-k} \le \varepsilon_{sec} + 2^{-k}$$

既知の実験での最良値は $\varepsilon_{sec} = 2^{-50}$ [16] なので、$k = 50$ bit ならかろうじて“ほぼ IID”だが、実用上 $10^3 < |k| < 10^6$ とすると “IID には遠すぎる。”
鍵長は $|k|$ なのに、Eve にとって 50 bit 程度の不定性しかない。

つまり PM-QKD は $\varepsilon_{sec} \sim 2^{-|k|}$ でようやく Almost-UCとなる

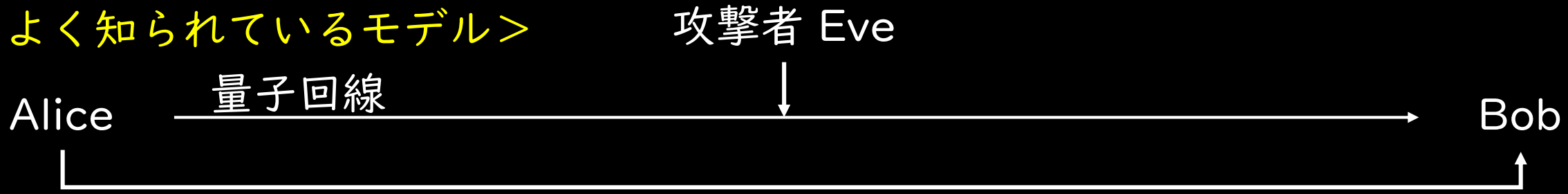
Table of Contents (前半)

2-1: QKD における情報の完全性

実は QKD は初期鍵が必要 [20]。なぜか？

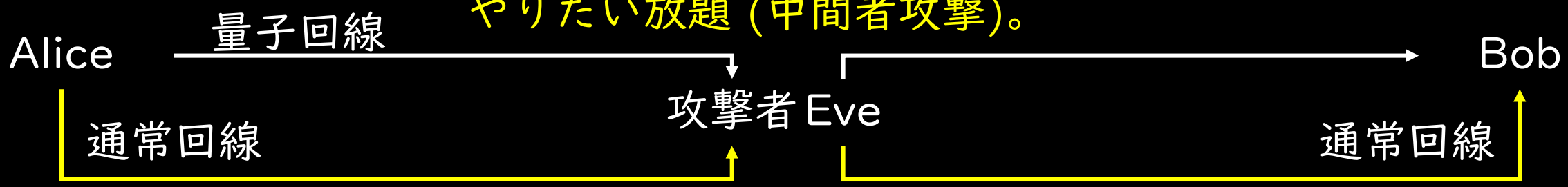
QKD では量子回線は Eve に触れられても盗聴量が反映されるので問題ないとされる。
重要なのは最終鍵を生成するための公開回線が操作されてないこと。

＜よく知られているモデル＞



通常回線 (盗聴量見積もり、秘匿性増強などに使う): 認証鍵で Eveの操作を防御

＜認証鍵なしの場合＞　Eve が「なりすまし」することで、盗聴でも改ざんでも
やりたい放題 (中間者攻撃)。



2-2: 量子インターネットでは初期鍵をどうするか(2/2)

Alice と Bob が知り合いなら、初期鍵を受け渡す方法もある。
インターネットでは次の場合もありえる。Alice は Bob の論文を入手し初めて Bob の存在を知った。Eve に知られずに Bob と通信するにはどうするか？

＜認証鍵なしの場合＞　Eve が「なりすまし」することで、盗聴でも改ざんでもやりたい放題 (中間者攻撃)。

2-2: 量子インターネットでは初期鍵をどうするか(1/2)

Alice と Bob が知り合いなら、初期鍵を受け渡す方法もある。
インターネットでは次の場合もありえる。Alice は Bob の論文を入手し初めて Bob の存在を知った。Eve に知られずに Bob と通信するにはどうするか？

＜認証鍵なしの場合＞　Eve が「なりすまし」することで、盗聴でも改ざんでもやりたい放題 (中間者攻撃)。

認証鍵をネットワーク越しに渡すことはできません。認証鍵を送った相手が Eve でないことを証明するには？ Eve に改ざんされていないことを保証するには？
現在のインターネットなら（計算量的安全な）公開鍵暗号や署名が使えますが、量子時代では Eve は無限の計算能力を持っていると仮定しています。

Stephanie Wehner (量子インターネット研究者) の現時点での考えは次の通り。

2-3: 量子インターネットでは初期鍵をどうするか(2/2)

Prof. S. Wehener: ネットワーク/計算機科学の出身で、2007年ごろから量子情報に転向、量子インターネットの実現に向けて研究している[21]。

Wehner の記事によれば [22] 、認証鍵の共有方法に下記手法が提案されている。「Eve の量子ストレージに雑音または容量の制限がある場合、認証鍵の配送は可能である [23, 24] 。」

裏返せば「Eve の計算能力に制限をもたせた場合に限って、認証鍵の配布は可能である」ということであり、無限の計算能力を持つ Eve に対して安全性を保証する、という量子ネットワークの当初の趣旨とは明らかに異なる。

(ただし将来的に、無限の計算能力を持つ Eve に対しても認証鍵を配布する方法が見つからないというわけではないと思います。反対に、見つからなければ、ネットワークの特徴であるところの見知らぬ他者とも秘匿性と完全性が保証された通信が可能という利便性は、完全に損なわれるという重要な問題です。)

2-4: Prepare-and-Measure QKD での完全性

前述したように、PM-QKD では Eve にとって鍵は IID からまだ遠すぎます。

これは何を意味するか？
配送した鍵の一部を使って認証鍵を更新すると、新しい認証鍵は IID であったはずの初期認証鍵よりも Eve にとって弱くなっているということ。
かといって更新しなければ、Eve の全数探索で初期認証鍵はいずれ破られる。

また、最終鍵の作成過程で誤り訂正方法を隠すには、前回のラウンドで配送された鍵の一部を使った OTP を用いる [9]。この OTP も 完全秘匿でないことに注意。つまり、誤り訂正手段と訂正後の鍵について何らかのヒントを Eve に与える可能性があるということです。

こうして2点間通信でさえも、PM-QKD では認証が破られる確率は時間とともに高まっていき、最終的には秘匿性も完全性も損なわれます。

このあたりの定量的評価は難解なので Yuen [25] も私も手をつけていません。

2-5: Entanglement-Distillation QKD での完全性

Prof. S. Wehener: ネットワーク/計算機科学の出身で、2007年ごろから量子情報に転向、量子インターネットの実現に向けて研究している[21]。

Wehner の記事によれば [22] 、認証鍵の共有方法に下記手法が提案されている。
「Eve の量子ストレージに雑音または容量の制限がある場合、認証鍵の配送は可能である [23, 24] 。」

認証鍵は、通信相手が Eve のなりすましでないことの証明にも使われます。
ED-QKD でも Eve が介入できない公開回線が必要なので問題は同じです。

また、Eve が IID でない鍵を入手する確率がゼロでないため、PM-QKD ほど脅威ではありませんが、認証鍵を更新するたび、その安全性は低下します。

$$\mathrm{Ex}[\Pr(k|k)] \leq \frac{1}{2}\mathrm{tr}\left|\zeta_{ABE} - 2^{-k} I_{AB} \otimes \tau_E\right| \leq \varepsilon_{sec}$$

2-6: 量子デジタル署名、量子 IPsec について

認証鍵をネットワーク越しに渡すことはできません。認証鍵を送った相手が Eve でないことを証明するには？ Eve に改ざんされていないことを保証するには？
現在のインターネットなら（計算量的安全な）公開鍵暗号や署名が使えますが、量子時代では Eve は無限の計算能力を持っていると仮定しています。

もちろん、量子デジタル署名や量子 IPsec などの手法も提案されている。

量子デジタル署名 [26 – 28]
私が知る範囲では、まず QKD インフラを使用できる前提で成り立っており、なら通信相手が認証されている状況で、Eve でないことを確認しEve の改ざんから防御された認証鍵を送る、という状況は矛盾。

量子 IPsec [29]
QKD で配送された鍵を使って IPsec を実行する、というプロトコルであり、その肝心の QKD の初期鍵の配送の解決にはならない。

Table of Contents (前半)

3-1: QKD の可用性

QKD は Eve によって引き起こされた QBER が 11% 程度を超えた場合には秘密鍵が生成できないとして最初からやり直さなければならない。

つまり Eve が 11% 以上の QBER を起こし続ける限り、正規ユーザーですら通信を開始できないという既知の問題です。よって可用性も満たせません。

では QBER < 50% まで通信可能とされる Round Robin DPS QKD [30] なら、上記のような Denial of Service (DoS) 攻撃は避けられるか？

3-2: Round Robin DPS QKD は盗聴不能か？

では QBER < 50% まで通信可能とされる Round Robin DPS QKD [30] では？

A. Saitoh [31] の計算では、パルストレイン長 $L = 4$ のとき Eve が Hadamard 演算を行うことにより、確率 3/4 で1bit の raw-key を盗むことができると判明。

任意の L に対し、確率 $p(L)$で Eve が raw-key を 1bit 盗めるとしよう。

1. Nbit の 生鍵を Eve が Alice-Bob と完全に共有する確率は $p(L)^N$。
2. Alice と Bob は 誤り訂正と秘匿性増幅を行い、最終鍵長を $N - r$にする。
3. このとき、秘匿性増幅に用いられるハッシュ関数の衝突確率（入力が不一致でも出力が偶然一致する確率）は $\Pr(k_E = k) > 2^{-(N-r)}$。
3. 上記から、Eve が鍵を入手できる確率は $> p(L)^N + 2^{-(N-r)} > 2^{-(N-r)}$。

これまでの PM-QKD での議論通り、最終鍵は最善でも Almost-IID。
さらに上記は Individual Attack という QKD では最も弱いクラスの攻撃。
ED Round Robin DPS QKD の場合は不明。試す価値はあるかもしれません。

3-3:「QKD では盗聴を検知できる」は本当か？

QKD はその量子性により当聴者の存在を検知できる、とよく聞きます。

量子通信路の QBER Q が、盗聴者不在のときには $Q = 0$ が保証されているときは上記のステートメントは正しい。

3-3:「QKD では盗聴を検知できる」は本当か？

QKD はその量子性により当聴者の存在を検知できる、とよく聞きます。

量子通信路の QBER Q が、盗聴者不在のときには $Q = 0$ が保証されているときは上記のステートメントは正しい。

Shannon の「雑音のある通信路符号化定理」を思い出しましょう。
通信路には雑音は不可避的に存在する。雑音の原因は種々あるだろうが、とにかくそれを確率現象として扱うことにより、最適な誤り訂正符号が存在し、そのときの通信路容量を計算できることを示した。

自然雑音が常にあり確率過程もわからないとき、Eve の盗聴による Q と自然雑音を Alice と Bob は区別できるか？
私がもし Eve なら、本来なら $Q = 1$, 2% 程度の回線に雑音を加え $Q = 9\%$ とし、Alice-Bob が最初の Q 測定のときにこれで妥協したあと、差分の7%を盗聴します。
物理法則以外に制約を持たない Eve が最初からいる場合はどうやって自然雑音と Eve の盗聴を区別しますか？もしご意見があれば議論させてください。

Table of Contents (後半)

4-1: Y00 プロトコルの特徴

量子暗号は QKD + OTP のみではない。Y00 プロトコルもそのひとつ。

Y00プロトコルの特徴

1. 単一光子ではなく平均光子数$|\alpha|^2 = 4 \times 10^6$個ほどの通常の通信光を使う[32]
2. 現在の光通信と同様の長距離 (1000kmでビット誤り率 $\leq 10^{-9}$は確認済み) [33]
3. 既存の光通信インフラを使用可能で既存の光中継機や光ルーターが使え、
   既存の誤り訂正符号も使用可能 [34]。特殊な量子デバイスは特に必要なし。
4. 通信速度は現在 256 Gbps まで確認ずみ [35]。1 Tbps 以上も可能？
5. 共通鍵は 256～512 bit くらいで、量子回線中で直接メッセージを伝える
6. レーザー光の量子不確定性の中に通信内容を隠すうえ、改ざん防御も可能 [36]
7. メッセージを鍵に置き換えれば鍵配送もできる[37]。
8. 安全性理論はまだ確立していない (研究中[38])。

4-2: Y00 プロトコルの原理

エンコード方式はいくつかあるが、わかりやすい位相変調 (PSK) で説明。

1. 送受信者とも256～512 bit の秘密鍵と、
   同じ疑似乱数生成器を保持

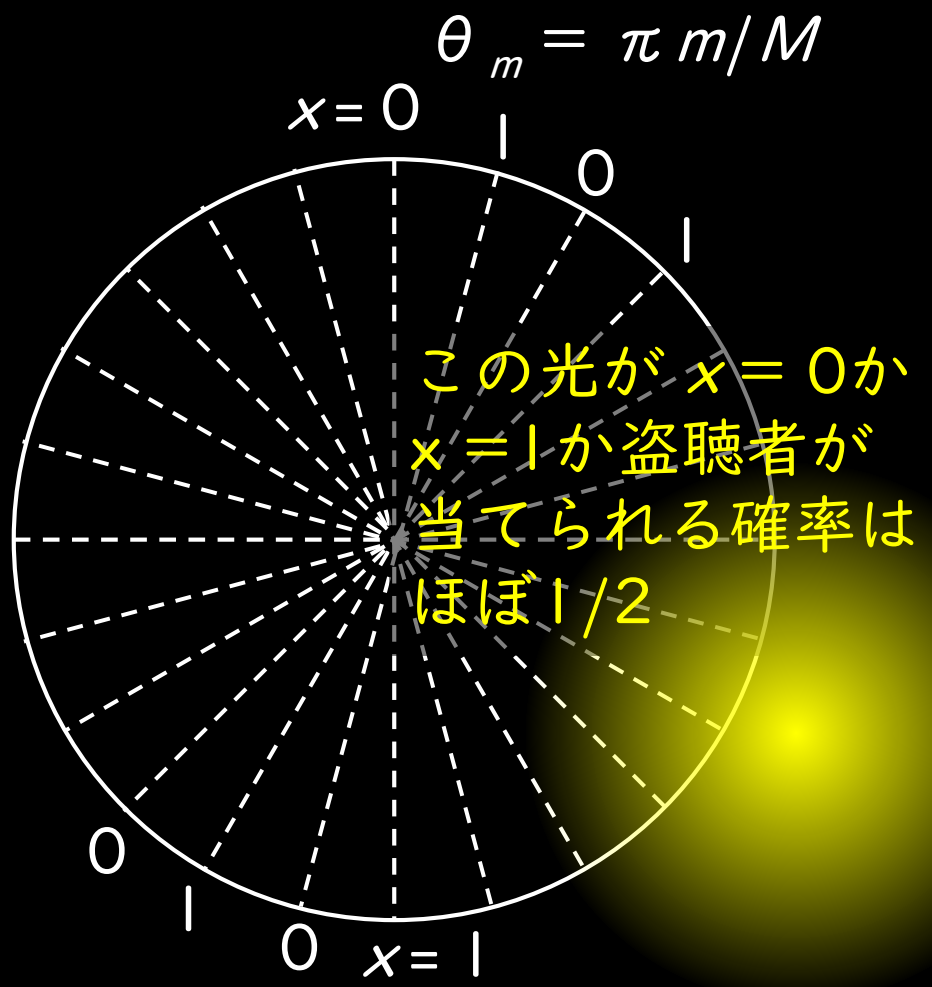
2. 擬似乱数生成器で鍵ストリームSを生成

3. Sを$\log_2 M$ bit ごとに区切って
   信号レベル$m \in \{0, 1, 2, \cdots, M-1\}$へ変換

4. メッセージビット$x \in \{0, 1\}$をエンコード
   mが偶数：$\{0,1\} \to \{|\alpha \exp[i\theta_m]\rangle, |-\alpha \exp[i\theta_m]\rangle\}$
   mが奇数：$\{0,1\} \to \{|-\alpha \exp[i\theta_m]\rangle, |\alpha \exp[i\theta_m]\rangle\}$

5. デコード時は m の偶奇で受信した光が
   どちらの$x \in \{0, 1\}$に相当するか判断

6. 盗聴者はmを知らず量子雑音の下で偶奇を判断



4-3: Wyner の盗聴モデルと比較しての安全性原理

Shannon (1949): 盗聴不能な暗号を作るには、メッセージより長い鍵が必要 [5]
Wyner (1975): もし盗聴通信路にノイズがあれば、上記条件は必要でない [39]

Wyner の仮定は自然に見えるが、盗聴通信路のノイズの量が事前にわかるか?
特に量子暗号の仮定「盗聴者には物理法則以外の制限がない」場合、不可能では?

YOO プロトコル: 設計により盗聴通信路にかかるノイズを見積もれる量子暗号。

S: 共通鍵 K から生成された疑似乱数ストリーム鍵
X: メッセージ (平文、と呼びます)
C: 正規ユーザーにとっての暗号文

正規ユーザーはノイズレスで通信: $C := X + S \mod 2$
盗聴通信路にはノイズ E がのる: $C_E := X + S + E \mod 2$

この場合、盗聴者はストリーム鍵 S の復元に成功しない。(理想的な場合)

$$H(S|C_E,X) > H(S,C_E,X) - H(C_E,X,E) = 0$$

4-3: Wyner の盗聴モデルと比較しての安全性原理

Shannon (1949): 盗聴不能な暗号を作るには、メッセージより長い鍵が必要 [5]
Wyner (1975): もし盗聴通信路にノイズがあれば、上記条件は必要でない [39]

Wyner の仮定は自然に見えるが、盗聴通信路のノイズの量が事前にわかるか?
特に量子暗号の仮定「盗聴者には物理法則以外の制限がない」場合、不可能では?

YOO プロトコル: 設計により盗聴通信路にかかるノイズを見積もれる量子暗号。

S: 共通
X: メッ
C: 正規

正規ユ
盗聴通

この場

$$H(S|C_E,X) > H(S,C_E,X) - H(C_E,X,E) = 0$$

導出は下記手順。

$$H(S|C_E,X) = H(S,C_E,X) - H(C_E,X)$$

$$H(C_E,X) \le H(C_E,X,E) \qquad \text{等号は} E = E(C_E,X) \text{のときのみ成立}$$

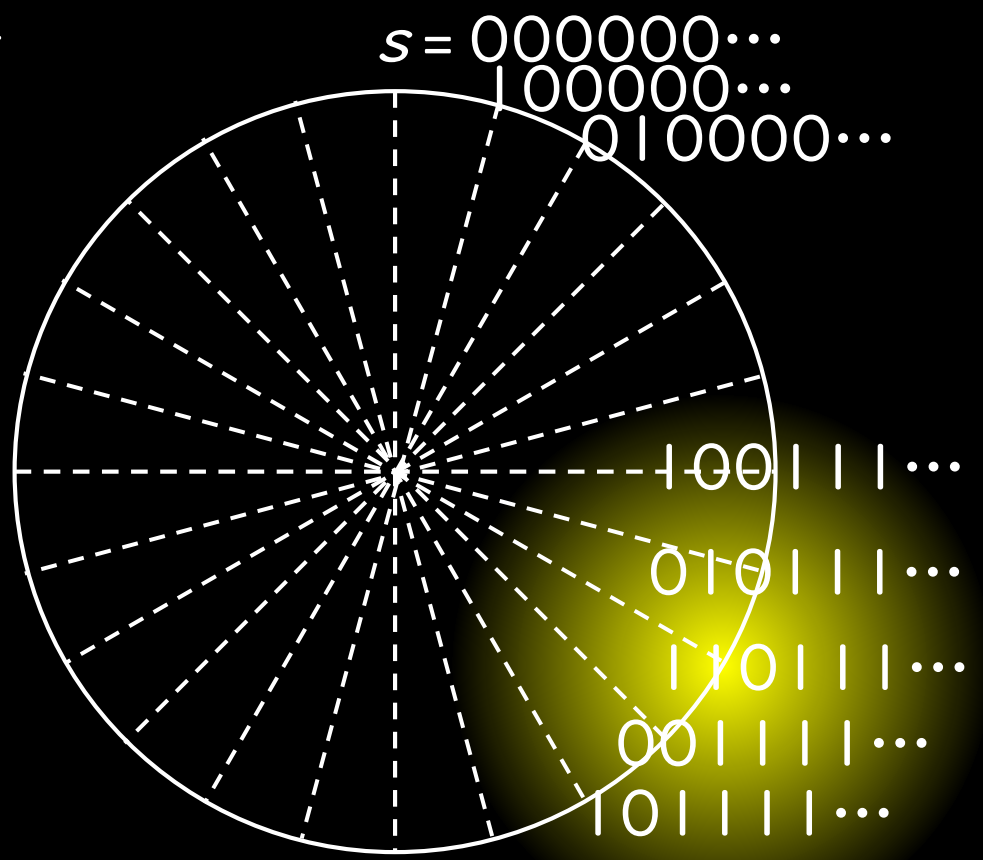
$$H(S,C_E,X,E) - H(C_E,X,E) = H(S|C_E,X,E) = 0$$

4-4: 初期型 Y00 プロトコルへの高速相関攻撃

信号レベル m の設定方法である 2, 3 のところが大きな失敗。

1. 送受信者とも256～512 bit の秘密鍵と、
   同じ線形合同法疑似乱数生成器 (LFSR) を保持
2. LFSR で疑似乱数 鍵ストリーム S を生成
3. S を $\log_2 M$ bit列 $s=(s_0, s_1, s_2, \cdots)$ に区切り
   $m = 2^0 s_0 + 2^1 s_1 + 2^2 s_2 + 2^3 s_3 + \ldots$ と設定
4. メッセージビット $x \in \{0, 1\}$ をエンコード
   mが偶数 : $\{0,1\} \to \{|\alpha \exp[i\theta_m]\rangle, |-\alpha \exp[i\theta_m]\rangle\}$
   mが奇数 : $\{0,1\} \to \{|-\alpha \exp[i\theta_m]\rangle, |\alpha \exp[i\theta_m]\rangle\}$
5. デコード時は m の偶奇で受信した光が
   どちらの $x \in \{0, 1\}$ に相当するか判断
6. 盗聴者は m を知らず量子雑音の下で偶奇を判断

$\theta_m = \pi m / M$

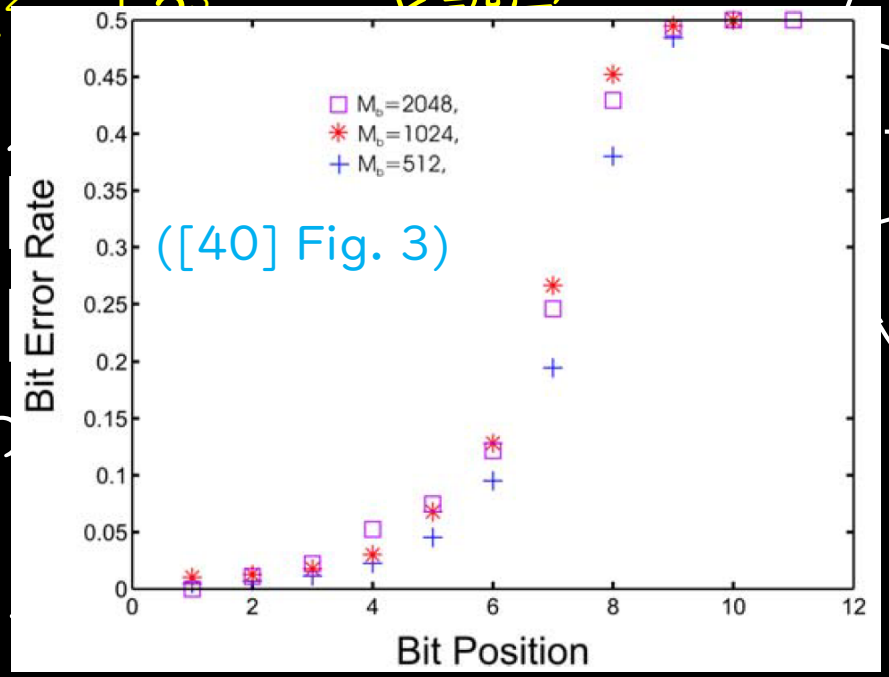


ビット列 s のほとんどは
量子雑音では隠れない

4-4: 初期型 Y00 プロトコルへの高速相関攻撃

信号レベル m の設定方法である 2, 3 のところが大きな失敗。

1. 送受信者とも256～512 bit の秘密鍵と、
   同じ線形合同法疑似乱数生成器 (LFSR) を保持
2. LFSR で疑似乱数 鍵ストリーム S を生成
3. S を $\log_2 M$ bit列 $s=(s_0, s_1, s_2, \cdots)$ に区切り
   $m = 2^0 s_0 + 2^1 s_1 + 2^2$ [illegible] と設定
4. メッセージビット
   mが偶数 : $\{0,1\} \to \{$ [illegible]
   mが奇数 : $\{0,1\} \to \{$ [illegible]
5. デコード時は m の
   どちらの $x \in \{0,$ [illegible]
6. 盗聴者は m を知ら [illegible]



$\theta_m = \pi m / M$

$s = 000000\cdots$
$100000\cdots$
$010000\cdots$
$110000\cdots$
$001000\cdots$
$101000\cdots$
$011000\cdots$
$111000\cdots$
$000100\cdots$
$100100\cdots$
$010100\cdots$
$110100\cdots$
$001100\cdots$
$101100\cdots$
$011100\cdots$
$111100\cdots$

ビット列 s のほとんどは
量子雑音では隠れない

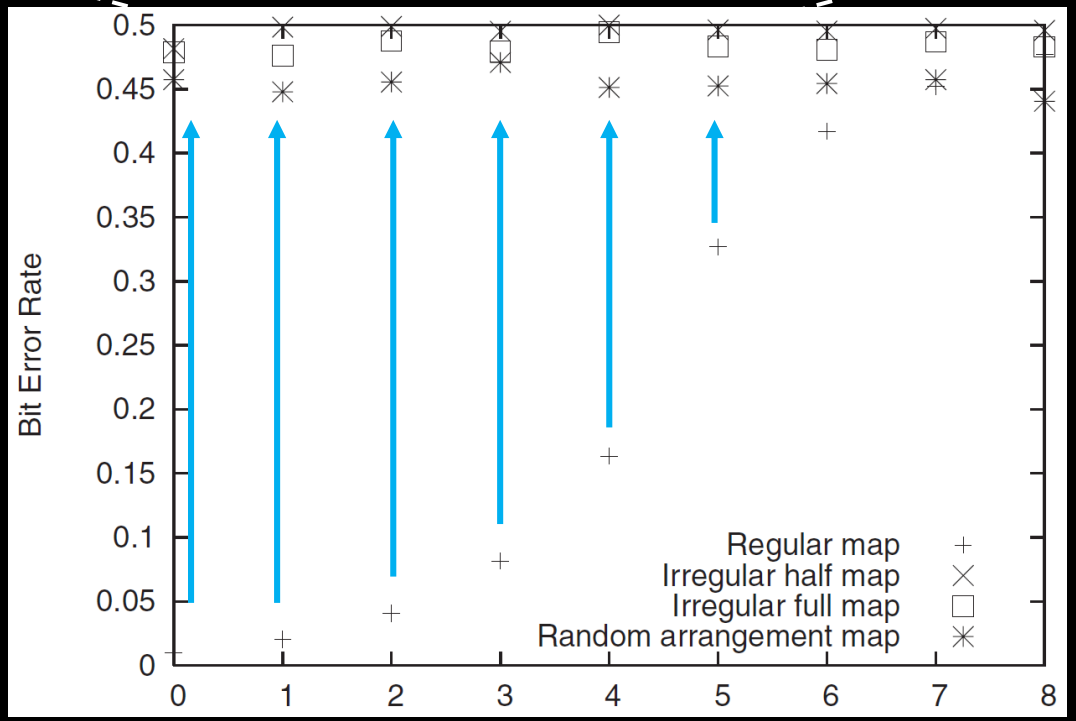
4-5: 高速相関攻撃の防御

量子雑音の効果を s 中の全てのビットに均等に割り振れば良い。[41 – 43]

1. 初期 Y00 通信機では、擬似乱数鍵 S を $\log_2 M$ bit列 $s=(s_0, s_1, s_2, \cdots)$ に区切り $m=2^0 s_0+2^1 s_1+2^2 s_2+2^3 s_3+\ldots$ とおいた

2. 改良 Y00 通信機では正則行列 R で s の順番を置換した s' から m を計算する。 $m=2^0 s'_0+2^1 s'_1+2^2 s'_2+2^3 s'_3+\ldots$

これで高速相関攻撃は防御できた。

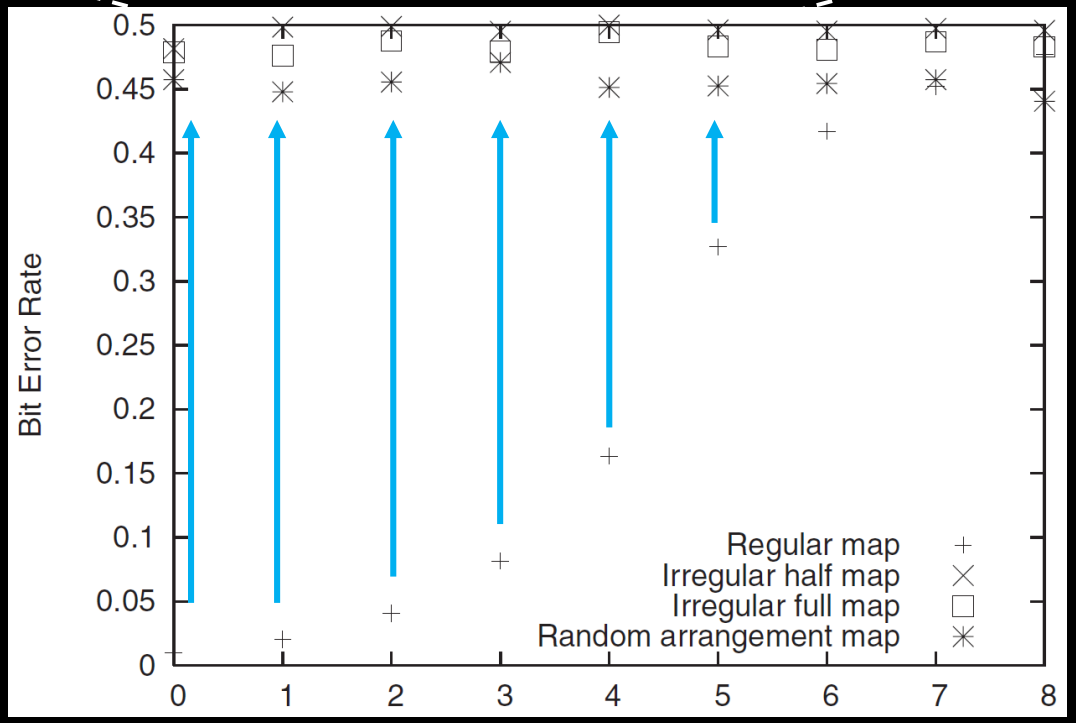


4-5: 高速相関攻撃の防御

量子雑音の効果を s 中の全てのビットに均等に割り振れば良い。[41 – 43]

1. 初期 YOO 通信機では、擬似乱数鍵 S を $\log_2 M$ bit列 $s=(s_0, s_1, s_2, \cdots)$ に区切り $m=2^0 s_0+2^1 s_1+2^2 s_2+2^3 s_3+\ldots$ とおいた

2. 改良 YOO 通信機では正則行列 R で s の順番を置換した s' から m を計算する。 $m=2^0 s'_0+2^1 s'_1+2^2 s'_2+2^3 s'_3+\ldots$



これで高速相関攻撃は防御できた。

が、受難はさらに続く。

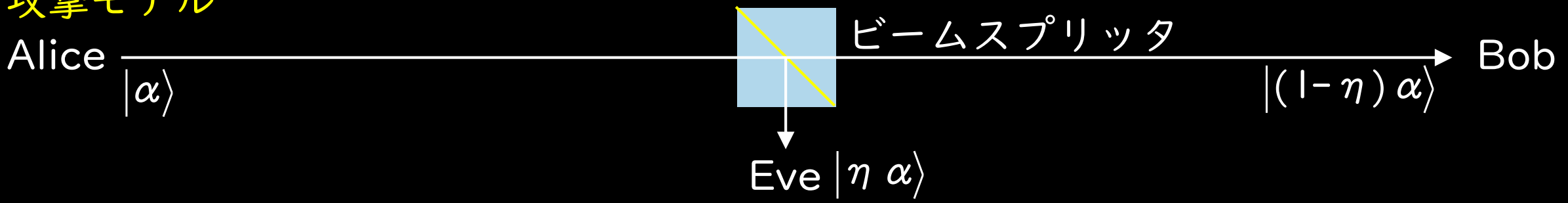
1. 上記攻撃の発見以降 YOO プロトコルは「計算量的安全」との評価が定着。
2. そもそも上記の防御は、特定の攻撃に対する防御でしかない。

4-5: 情報理論的安全な YOO 通信機の設計に向けて

講演者の着想は以下 [38]。

1. QKD と同様、攻撃者には物理法則による制約以外はないとする。
2. 通信中のメッセージが事前に手に入っていることも許す(既知平文攻撃)。
3. それでも疑似乱数鍵 S が有限時間内に確率1で判明しなければ情報理論的安全。

攻撃モデル



光を η だけビームスプリッタで盗み、攻撃開始まで量子メモリに貯め続ける
＋ Eve はすでに平文を知っている (共通鍵を探すのが狙い)

↓

量子鍵配送では集めた信号をまとめて解読に使う。
QKD で言う “Collective Attack” “Coherent Attack” に相当 [17]。
(これまでは個別信号の盗聴能力 “Individual Attack” しか考察されてない。)

4-6: Eve の最適測定のための量子信号検出理論

Eveが正しい s を得る平均失敗確率を最小にするのが量子信号検出理論 [44]

$$W(x,s) := -\Pr(s)\left|\eta\ \alpha(x,s)\right\rangle\left\langle\eta\ \alpha(x,s)\right|$$

$$\Gamma := \sum_{s\in S} M_E(s|x)W(s,x) = \sum_{s\in S} W(s,x)M_E(s|x)$$

$$\sum_{s\in S} M_E(s|x) = I$$

$$M_E(s|x)\left[W(x,s') - W(x,s)\right]M_E(s'|x) = 0$$

$$\left[W(x,s) - \Gamma\right]M_E(s|x) = M_E(s|x)\left[W(x,s) - \Gamma\right] = 0$$

$$W(x,s) - \Gamma \geq 0$$

- tr Γ = Eve の平均成功確率。

一般に上記は、有限次元ヒルベルト空間に適用されるが、YOO プロトコルの信号はコヒーレント光 (無限次元ヒルベルト空間に拡張する必要がある。)

4-7: 量子信号検出理論の無限次元空間への拡張

$$W(x,s) := -\Pr(s)\left|\eta\,\alpha(x,s)\right\rangle\left\langle\eta\,\alpha(x,s)\right|$$

$$\Gamma := \sum_{s\in S} M_{\mathrm{E}}(s|x)\mathrm{W}(s,x) = \sum_{s\in S} \mathrm{W}(s,x) M_{\mathrm{E}}(s|x)$$

$$\sum_{s\in S} M_{\mathrm{E}}(s|x) = I$$

$$M_{\mathrm{E}}(s|x)\left[W(x,s') - W(x,s)\right] M_{\mathrm{E}}(s'|x) = 0$$

$$\left[W(x,s) - \Gamma\right] M_{\mathrm{E}}(s|x) = M_{\mathrm{E}}(s|x)\left[W(x,s) - \Gamma\right] = 0$$

$$W(x,s) - \Gamma \geq 0$$

コヒーレント光の
over-completeness を応用

$$\bigotimes_{t=\mathrm{I}}^{T} \int_{\alpha(t)\in \mathrm{D(All)}} \pi^{-1} \left|\alpha(t)\right\rangle\left\langle\alpha(t)\right| \mathrm{d}\alpha(t) = \mathrm{I}$$

$$\mathrm{M_E}(s+e|x) := \bigotimes_{t=\mathrm{I}}^{T} \int_{\alpha(t)\in \mathrm{D}(s+e|x)} \pi^{-1} \left|\alpha(t)\right\rangle\left\langle\alpha(t)\right| d\alpha(t)$$

$$\bigcup_{e\in \mathrm{Set}\left[E(s|x)\right]} \mathrm{D}(s+e|x) = \mathrm{D}(s|x)$$

$$\bigcup_{s\in \mathrm{Set}(S)} \mathrm{D}(s|x) = \mathrm{D(All)}$$

$$\mathrm{D}(s+e|x) \cap \mathrm{D}(s'+e' \neq s+e|x) = \varnothing$$

$$\mathrm{M_E}(s|x) := \sum_{e\in \mathrm{Set}\left[E(s|x)\right]} \mathrm{M_E}(s+e|x)$$

4-8: セキュリティ解析結果

Y00 通信装置に使用される擬似乱数生成器の周期の最小公倍数を T_{LCM} とし、$T = N\,T_{\mathrm{LCM}}$ の間、Eve が量子メモリに信号を蓄積し一括測定したあとの推定確率[38]

$$\Pr(s|s,x) \le 1 - [1 - \Pr(s)] \exp\left[-(N/N_{\mathrm{Breach}})\ln 2\right]$$

$$1/N_{\mathrm{Breach}} := -\log_2\left[(2M)^{T_{\mathrm{LCM}}} \min_{e\in\{0,1\}^{|e|}} \Pr(e|s,x)\right]$$

$$\min_{e\in\{0,1\}^{|e|}} \Pr(e|s,x) \le (2M)^{-T_{\mathrm{LCM}}}$$

Case 1: $1/2 > (2M)^{T_{\mathrm{LCM}}} \min_{e\in\{0,1\}^{|e|}} \Pr(e|s,x) \to 0$

T_{LCM} 以内に推定確率が 1 に達する。そのような Y00 装置は情報理論的安全でない。

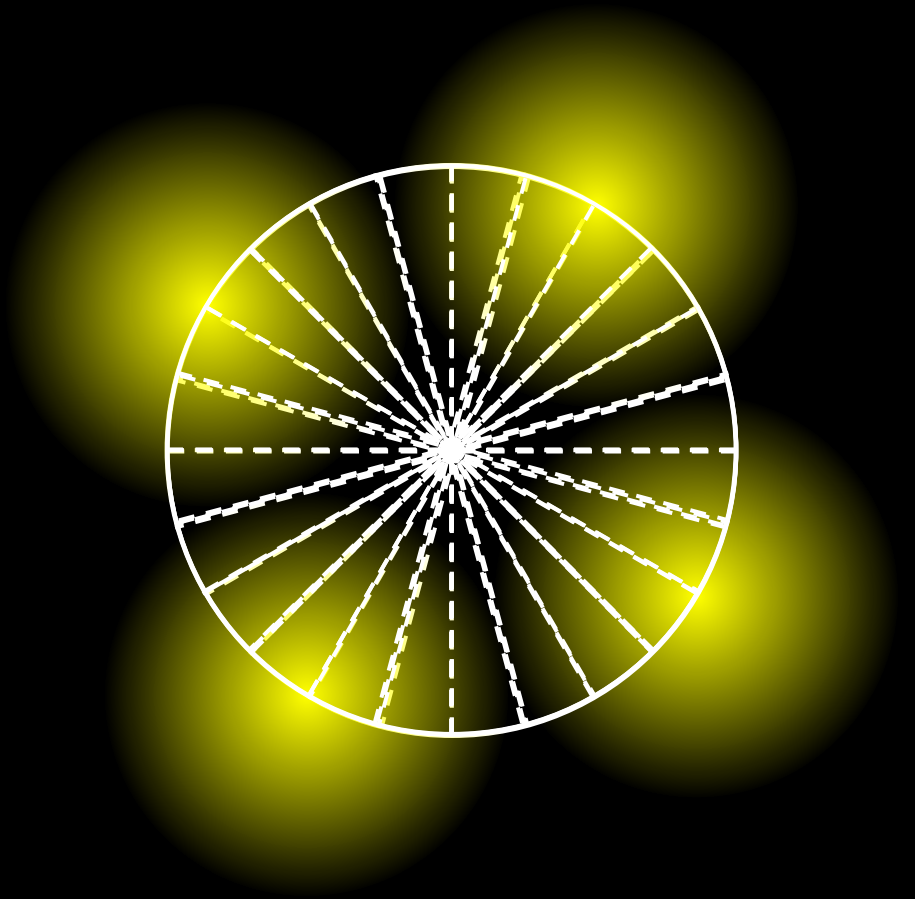
Case 2: $1 > (2M)^{T_{\mathrm{LCM}}} \min_{e\in\{0,1\}^{|e|}} \Pr(e|s,x) \ge 1/2$

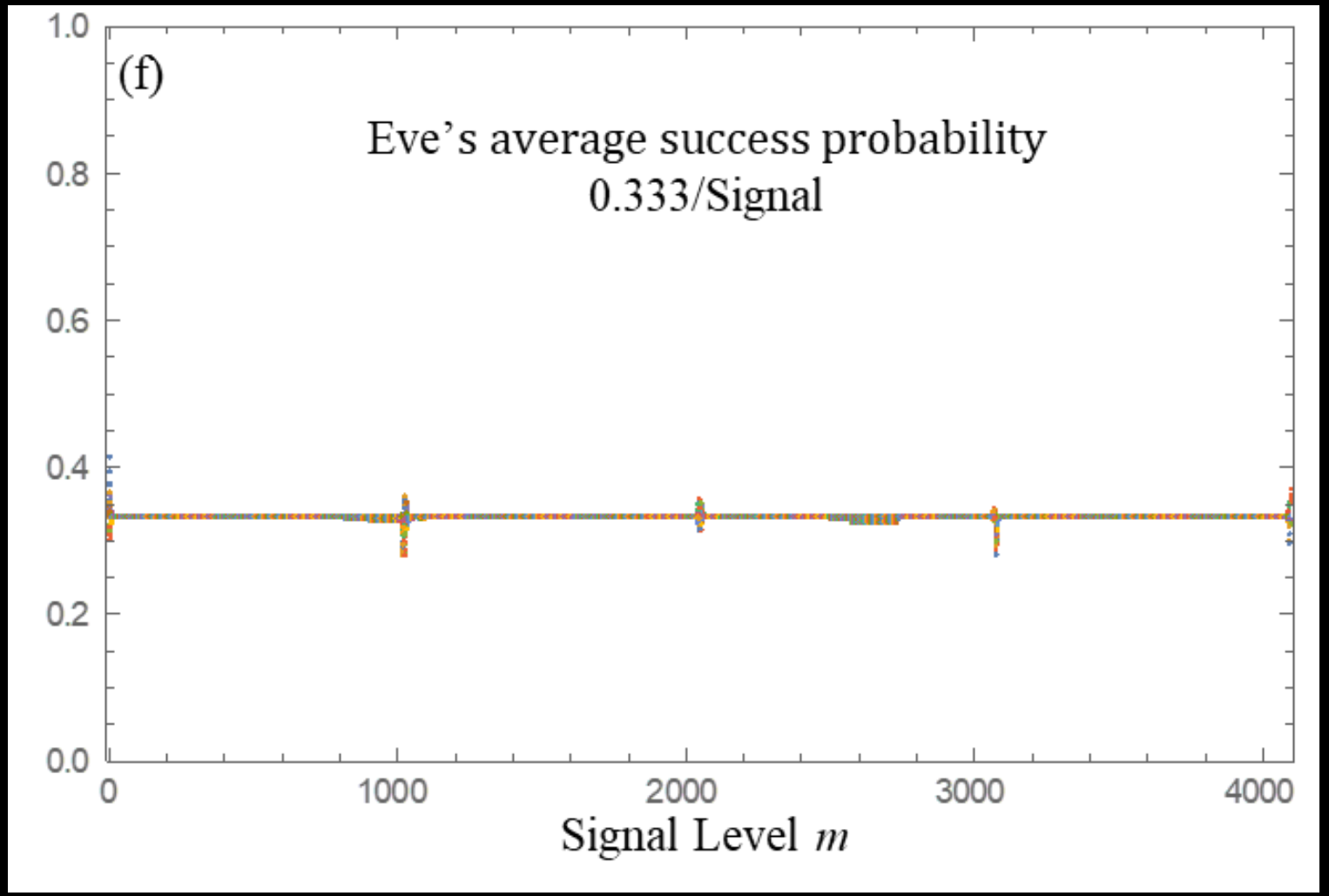
T_{LCM} 以上の時間で漸近的に推定確率が 1 に近づいていく。つまり情報理論的安全である。このとき、N_{Breach} のタイムスケールで鍵が脅威にさらされていくので、N_{Breach} を大きくとり、かつ推定確率がしきい値未満の間に新しい鍵をメッセージの代わりに送付し、鍵を更新する必要がある。

Table of Contents (後半)

5-1: Y00 における通信内容の完全性

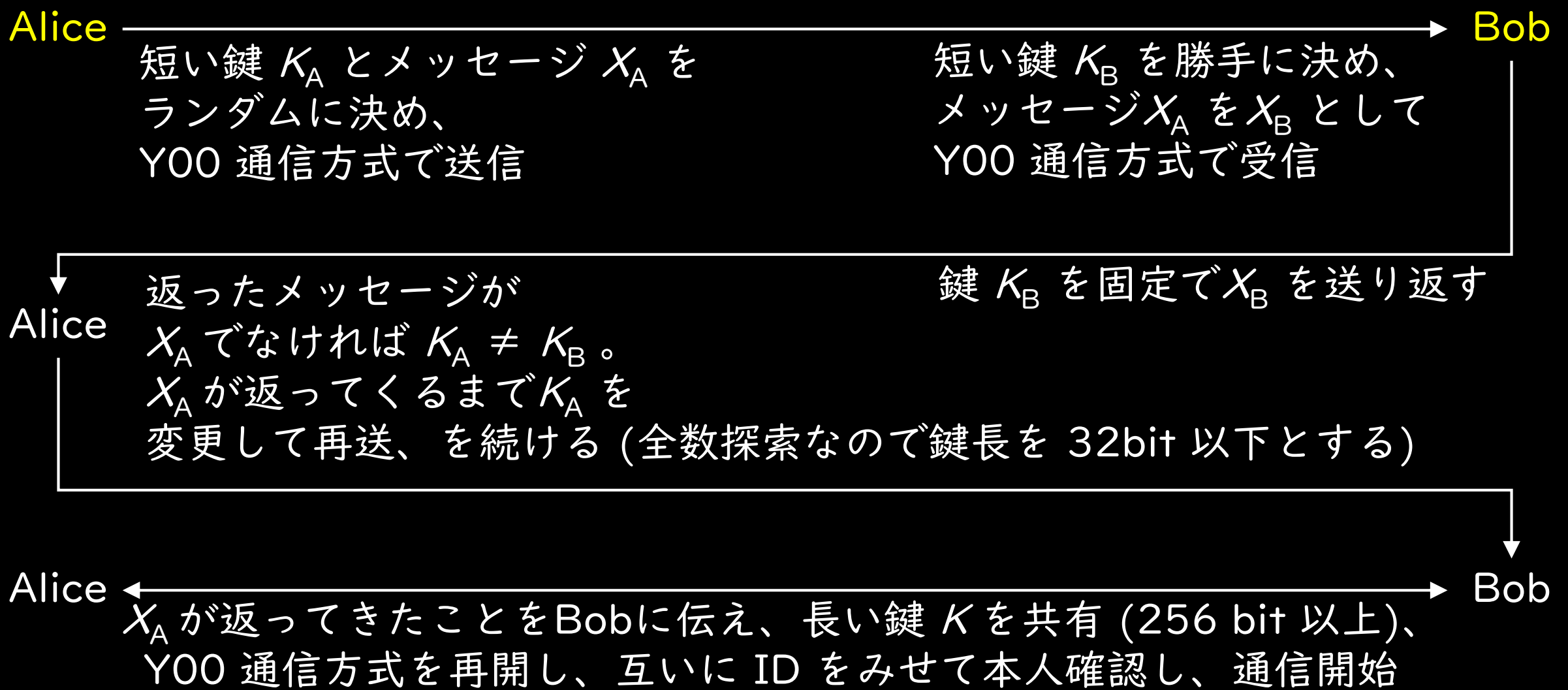
最近の論文は [36]。Y00 信号を2値から4値に変更、信号配置を擬似ランダム化。
→ Eve が内容を意図どおり改ざんしようとしても2bit あたり 2/3 の確率で失敗。
通信内容にハッシュ値をつけるだけで、改ざんがあればすぐに検知できる。





5-2: 初期鍵の配送方法案 (1/3)

YOO プロトコルは共通鍵暗号なので、もちろん初期鍵が必要。下記が配送案[36]。



5-3: 初期鍵の配送方法案 (2/3)

最後のステップは安全か？ 答えは「このままでは No」

Alice ⟷ Bob

X_A が返ってきたことをBobに伝え、長い鍵 K を共有、
YOO 通信方式を再開し、互いに ID をみせて本人確認し、通信開始

1. ID は信頼できる機関に発行してもらったものか？ (自分で作っても仕方ない)
2. ID は誰にでも知られているものであるはず (Eve も知っている)
3. ID は Eve に改変されていないか？

改ざん防御型 YOO プロトコルなら問題3はクリアできる。 1 をどうするか？

→現在のインターネットでは、Trusted Authority に発行してもらっています。
　これまでどおり活用しましょう。

5-4: 初期鍵の配送方法案 (3/3)

ID を Trusted Authority (TA) に発行してもらう

Alice → TA

短い鍵 K_A とメッセージ X_A を
ランダムに決め、
Y00 通信方式で送信

短い鍵 K_T を勝手に決め、
メッセージX_A をX_T として
Y00 通信方式で受信

鍵 K_T を固定でX_Tを送り返す

Alice

返ったメッセージが
X_A でなければ $K_A \neq K_T$。
X_A が返ってくるまでK_A を
変更して再送、を続ける

Alice ↔ TA

X_A が返ってきたことをTAに伝え、長い鍵 K を共有 (256 bit 以上)、
Y00 通信方式を再開し、Aliceは ID を TA に署名付きで発行してもらう
(情報理論的安全な署名が必要 [45-51] *量子でなくても可能)

Table of Contents (後半)

6-1: Y00 protocol の可用性 (Availability)

下記の通り、既存の光通信と互換なので可用性も当然、現在の光通信どおり。

Y00プロトコルの特徴

1. 単一光子ではなく平均光子数$|\alpha|^2 = 4\times10^6$個ほどの通常の通信光を使う[32]
2. 現在の光通信と同様の長距離 (1000kmでビット誤り率 $\leq 10^{-9}$は確認済み) [33]
3. 既存の光通信インフラを使用可能で既存の光中継機や光ルーターが使え、
   既存の誤り訂正符号も使用可能 [34]。特殊な量子デバイスは特に必要なし。
4. 通信速度は現在 256 Gbps まで確認ずみ [35]。1 Tbps 以上も可能？
5. 共通鍵は 256～512 bit くらいで、量子回線中で直接メッセージを伝える
6. レーザー光の量子不確定性の中に通信内容を隠すうえ、改ざん防御も可能 [36]
7. メッセージを鍵に置き換えれば鍵配送もできる[37]。
8. 安全性理論はまだ確立していない (研究中[38])。

Table of Contents (後半)

7-1: ファインマンの言葉をもういちど胸に刻もう

量子情報を研究されている方のほとんどが物理学系出身だと思います。私もです。

“Our freedom to doubt was born out of a struggle against authority in the early days of science. It was a very deep and strong struggle: permit us to question — to doubt — to not be sure. I think that it is important that we do not forget this struggle and thus perhaps lose what we have gained.”[52]

(初期の科学における疑うことの自由は、権威に対する長く厳しい戦いにより確立されました。それは本当に本当に厳しい戦いでした: 納得するためにではないく - 疑うために - 質問させてくれ。これはとても重要なことで、この苦難のことを忘れては、我々が今まで築き上げたものを失いかねない。); 発表者訳

R. P. Feynman

みなさん、文献を盲目的に信じずに納得するまで自分で検算してますか？

Table of Contents (後半)

8: Summary

下記、ご意見などがあれば、もちろん議論はさせてください。

1. セキュリティの三要素とは、機密性 (権限を持つ人物だけが情報にアクセスできること)、完全性 (当該情報が改ざんされていないこと)、可用性 (使うべきときに使える状態にあること) を指す。
2. Entanglement-Distillation QKD と Prepare-and-Measure QKD は等価ではない。自分で検算して Eve の盗聴成功確率を比較してみてください。
3. 少なくとも Prepare-and-Measure QKD は Universal Composability を満たさない。($\varepsilon_{sec} \sim 2^{-|k|}$ のときのみ、Almost-UC とは言える。)
4. 初期共有鍵なしで QKD をスタートする妥当な方法はまだない。
5. 量子デジタル署名などの殆どの研究はまだ、QKD がすでに動作することを前提にしており、初期鍵配送における Eve のなりすまし攻撃の防御にならない。
6. Eve が盗聴を続ける限り、QKD の可用性は保証されない。
7. そもそも盗聴検知能力は QKD にはないのでは。
8. Y00 プロトコルは通信能力は従来の光ネットワークと互換で、可用性も十分。
9. ただし安全性証明がまだ未整備。
10. 上記さえ整えば、完全性および初期鍵配送の問題も解決できる。

9-1: 参考文献

<教科書>

1. 小芦 雅斗 「量子暗号理論の展開」 saiensu.co.jp/search/?isbn=978-4-7819-9920-3 (2008)
2. 富田 章久「量子情報工学」 amazon.co.jp/dp/4627853815 (2017)
3. 結城 浩 「暗号技術入門 第3版　秘密の国のアリス」 amazon.co.jp/dp/B015643CPE (2015)
4. 広田 修 「光通信理論―量子論的基礎」 amazon.co.jp/dp/4627780605 (1985)
5. P.K. Verma, M.El RifaiKam, W.C. Chan doi.org/10.1007/978-981-10-8618-2_4 (2018)

<論文>

[1] J. Hughes & G. Cybenko, dx.doi.org/10.22215/timreview/712 (2013)
or ISO/IEC 27000:2018 https://www.iso.org/standard/73906.html (2018)
[2] T. Iwakoshi, doi.org/10.13140/RG.2.2.12625.74081 QIT33 (2015)
[3] T. Iwakoshi, doi.org/10.13140/RG.2.2.18173.77282 SCIS2017 (2017)
[4] G. S. Vernam https://google.com/patents/US1310719 (1918)
[5] C. E. Shannon, https://doi.org/10.1002/j.1538-7305.1949.tb00928.x (1949)
[6] C. H. Bennett & G. Brassard, cyberleninka.org/article/n/903792.pdf (1984)
[7] R. Koenig and R. Renner, https://doi.org/10.1103/PhysRevLett.98.140502 (2008)
[8] P.W. Shor and J. Preskill, https://doi.org/10.1103/PhysRevLett.85.441 (2000)
[9] M. Koashi, https://doi.org/10.1088/1367-2630/11/4/045018 (2008)
[10] T. Tsurumaru, https://arxiv.org/abs/1809.05479 (2018)
[11] T. Sasaki, imi.kyushu-u.ac.jp/kyodo-riyo/research_meetings/view/1 (2019)

9-2: 参考文献

<論文>

[12] T. Iwakoshi, https://doi.org/10.1117/12.2500457 (2018)
[13] H. P. Yuen, https://doi.org/10.1103/PhysRevA.82.062304 (2010)
[14] C. Portmann and R. Renner, https://arxiv.org/abs/1409.3525 (2014)
[15] T. Iwakoshi, https://doi.org/10.1117/12.2278625 (2017)
[16] H. Takesue, et al., https://doi.org/10.1038/nphoton.2015.173 (2015)
[17] R. Renner, https://doi.org/10.1142/S0219749908003256 (2008)
[18] M. Hayashi, T. Tsurumaru, https://doi.org/10.1088/1367-2630/14/9/093014 (2012).
[19] R. Canetti, https://doi.org/10.1109/SFCS.2001.959888 (2001)
[20] K. Tamaki, ieice-hbkb.org/files/S2/S2gun_05hen_01.pdf (2008)
[21] quantamagazine.org/stephanie-wehner-is-designing-a-quantum-internet-20190925/
[22] S. Wehner, D. Elkouss & R. Hanson, doi.org/10.1126/science.aam9288 P.3右 (2018)
[23] I. B. DamgÅrd, et al., https://doi.org/10.1137/060651343 (2000)
[24] S. Wehner, J. Wullschleger, https://doi.org/10.1109/TIT.2011.2177772 (2008)
[25] H. P. Yuen, https://doi.org/10.1109/ACCESS.2016.2528227 (2016)
[26] X. Xin, Z. Wanga, and Q. Yang, https://doi.org/10.1016/j.ijleo.2019.163388 (2019)
[27] X.-B. An, et al., https://doi.org/10.1364/OL.44.000139 (2019)
[28] C. Hong, J. Jang, J. Heo, H.-J. Yang, doi.org/10.1007/s11128-019-2510-4 (2020)
[29] https://www.sfc.wide.ad.jp/thesis/2009/bachelor/kurosagi-bachelor-thesis.pdf (2009)
[30] T. Sasaki, Y. Yamamot, M. Koashi, https://doi.org/10.1038/nature13303 (2014)

9-3: 参考文献

<論文>

[31] A. Saitoh, https://www.jstage.jst.go.jp/article/jpsgaiyo/71.2/0/71.2_503/_pdf (2016)
[32] O. Hirota, M. Sohma, M. Fuse, & K. Kato, doi.org/10.1103/PhysRevA.72.022335 (2005)
[33] F. Futami, et al., doi.org/10.1364/CLEO_SI.2019.SW3O.4 (2019)
[34] F. Futami, et al., doi.org/10.1364/OFC.2018.Tu2G.5 (2018)
[35] F. Futami, et al., https://doi.org/10.1364/OE.25.033338 (2017)
[36] T. Iwakoshi, https://doi.org/10.1109/ACCESS.2019.2921023 (2019)
[37] H. P. Yuen, https://doi.org/10.1109/JSTQE.2009.2025698 (2009)
[38] T. Iwakoshi, https://www.researchgate.net/publication/330956268 (2019)
[39] A. D. Wyner, doi.org/10.1002/j.1538-7305.1975.tb02040.x (1975)
[40] S. Donnet, et al., doi.org/10.1016/j.physleta.2006.04.002 (2006)
[41] M. J. Mihaljević, doi.org/10.1103/PhysRevA.75.052334 (2007)
[42] T. Shimizu, O. Hirota, & Y. Nagasako, doi.org/10.1103/PhysRevA.77.034305 (2008)
[43] K. Kato, doi.org/10.1117/12.2060631 (2014)
[44] H. P. Yuen, R. Kennedy, & M. Lax, https://doi.org/10.1109/TIT.1975.1055351 (1975)
[45] D. Chaum & S. Roijakkers, “Unconditionally secure digital signatures,” (1991)
[46] B. Pfitzmann & M. Waidner,
“Information-theoretic pseudosignatures and byzantine agreement for t ≥ n/3” (1996)
[47] G. Hanaoka, J. Shikata, Y. Zheng, & H. Imai, doi.org/10.1007/3-540-44448-3_11 (2000)
[48] J. Shikata, G. Hanaoka, Y. Zheng, & H. Imai, doi.org/10.1007/3-540-46035-7_29 (2002)

9-4: 参考文献

<論文>

[49] G. Hanaoka, et al., cis.uab.edu/yzheng/publications/files/e87-a_1_120.pdf (2004)
[50] C. M. Swanson & D. R. Stinson, doi.org/10.1515/jmc-2016-0002 (2016)
[51] R. Amiri, et al., doi.org/10.1007/978-3-319-93387-0_8 (2018)
[52] Wikiquote; Rychard Feynman, https://doi.org/10.1117/12.2500457
[53] L. Lydersen, et al. http://www.nature.com/doifinder/10.1038/nphoton.2010.214 (2010)
[54] T. Iwakoshi, http://dx.doi.org/10.24425/mms.2019.126333 (2019)

[補足1] 自由討論の時間で、質疑応答での齟齬が個人的にはクリアになったのですが、発表者の立場は Shannon's Maxim がある限り、Eve には通信手順は全て開示されているというものです。「暗号化方式の仕様は全て開示されているべき」というのは暗号学の基本で、例えば教科書３や論文 [53] を参考にされるとよいかと思います。一方で 、Eve には「実/仮想プロトコルが区別できないよう実プロトコルを設計する」という立場を堅持するなら、それはそれで私もみなさんも Eve の立場で安全性を検算してみればよいと思います。
[補足2] トレース距離の上界は、鍵長 k を短くすれば exp[(k/2)ln2] のオーダーで小さくなりますが、一方で Eve がでたらめに推定することで成功する確率の項 2^{-k} は、鍵長 k を短くするほど増加します。こうして２つの項が拮抗するところで最適な鍵削減の量が存在するというのが発表者の立場です[54]。
[補足3] CSS コードでエンコードした状態から出発するのではなく、CSSはEveの盗聴が終わったあとで決められるものだという指摘がありましたが、発表者としては、量子誤り訂正で Eve の系が孤立するならば、どっちでも良いと思います。