ON THE NATURE AND CLAIMS OF QUANTUM KEY DISTRIBUTION (QKD)

Horace P. Yuen

Department of Electrical Engineering and Computer Science
Department of Physics and Astronomy
Northwestern University
Evanston Il. 60208
Email: yuen@eecs.northwestern.edu

Main Points and Outline of This Talk

1. **Contrast between conventional cryptography and QKD**
2. **Basic cryptographic primitives and associated concepts**
3. **QKD protocols, their security analysis and claims assuming model is complete and correct**
4. **Claims versus Facts of QKD protocols**
5. **Some historical claims on QKD protocols**
6. **Need for alternative security approach to QKD protocols**

WHY QKD?

—as an engineering goal apart from justifying physics research

- **Information theoretic security (ITS)**

  — not available in conventional cryptography since public-key (RSA) has complexity-based security
- **Rigorously provable security**

  — again compared to complexity-based one with no provable example except one-time pad
- **High quantitative security level— security parameter**

Catch:

- **Very inefficient in principle**
- **Not compatible with existing infrastructure**
- **The above 3 points on "why" are NOT TRUE in reality**

BASIC CRYPTOGRAPHIC FUNCTIONS

- **Encryption (for Privacy)**

data sequence

(plaintext)

$$\begin{tikzcd} x_i \arrow[r] & \oplus \arrow[r] & y_i = x_i \oplus k_i \\ & k_i \arrow[u] & \end{tikzcd}$$

all binary $\{0,1\}$

running key sequence

OTP

one-time pad

k_i **uniformly random**

$$p(0) = p(1) = \frac{1}{2}$$

$$p(x_i \mid y_i) = \frac{1}{2}$$

no "information"

of any kind

only when k_i **used once**

still problem of message

integrity—altered by Eve

- **Key Distribution**
- **Message Authentication**

Assertion 1: The key from QKD is declared by different groups to be “perfect”, “unconditionally secure”, “absolutely secure”, or “perfect with a high probability”.

Fact 1: The QKD key is imperfect with 100% probability and the deviation from perfect (uniform random bits to Eve) is huge.

Assertion 2: QKD has information-theoretic security (ITS) for encryption that classical cryptography cannot have other than one-time pad (OTP).

Fact 2: Classical Noise cryptography also has ITS.

Classical symmetric-key expansion also has ITS, and is the more proper comparison with QKD than public-key technique.

What is Unconditional Security

- In classical cryptography it often refers to information-theoretic (ITS) — an intrinsic uncertainty, usually taken to be that of a uniformly random bit sequence — in contrast with complexity-based security (CBS) — many trials needed to find the correct answer.
- In QKD it is defined (Mayers 2001) to be ITS with a security parameter Λ, such that as $\Lambda \to \infty$ perfect security (or uniform randomness) can be obtained asymptotically.
- Proven CBS becomes ITS under a fixed resource constraint — say if only m trials are allowed among M possibilities that need to be tried one by one, the probability of success is $\frac{m}{M}$.

Assertion 3: QKD is provably secure but classical cryptography is not other than OTP.

Fact 3: QKD is definitely not proved secure even when the security claim is restricted to what is claimed to have been rigorously proved.

Assertion 4: The QKD key K from concrete protocol has adequate security level.

Fact 4: Even single-photon BB84 has only been shown in theory to be capable of generating an imperfect K that has very poor operational security guarantee.

Assertion 5: QKD is necessary for key distribution when public-key method such as RSA becomes insecure.

Fact 5: Classical symmetric key distribution is available.

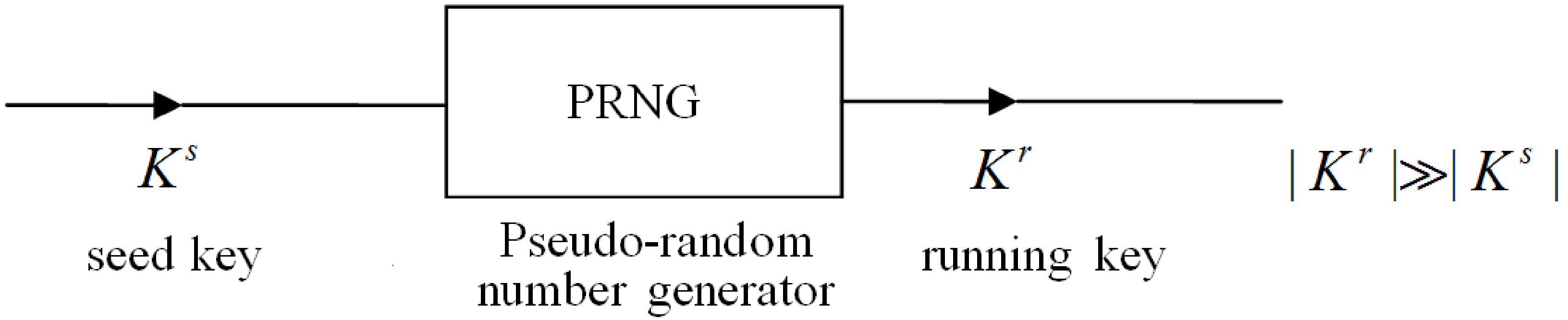
Assertion 6: The numerous previous erroneous claims on QKD are natural in the development of a subject.

Fact 6: No rigorously proved unconditional security claim was ever made in conventional cryptography that turned out wrong.

Importance of Quantitative Security Lever are Operational Meaning

- **Since security is not perfect and there is no security parameter, the actual available quantitative security level is crucial for evaluating a QKD protocol**
- **Thus, it is totally misleading to characterize a QKD protocol as “unconditionally secure” or “information-theoretically” secure without a quantitative level with corresponding key rate.**
- **The empirical security guarantee of any QKD security criterion must be spelled out in terms of its operational probabilistic meaning and Eve’s error rate.**

SYMMETRIC KEY EXPANSION ALSO HAS ITS



Additive Stream Cipher — one-time pad (OTP)

(block cipher similar)

X	**data stream**	x_i	**plaintext**
K^r	**key stream**	k_i^r	
Y	**encryption**	$y_i = x_i \oplus k_i^r$	**ciphertext**

Shannon Limit $H(X \mid Y) \leq H(K^s)$

ATTACKS ON PRIVACY

- ☐ **Ciphertext-only attack—**

  estimate X **from** Y **only**

  OTP with uniform $K^r \Rightarrow p(x_i \mid y_i) = p(x_i)$

- ☐ **Known-plaintext attack (KPA)—**

  $X = X_1 \| X_2$ X_1 **known to Eve**

  $Y = Y_1 \| Y_2$ Y **always known to Eve**

  $Y = X \oplus K$ **Eve knows** K_1 → **gets at** K_2 **from key correlation**

  → **gets at** X_2 **from** Y_2 **and** K_2

✧ **Note that when** X **is uniform to Eve,** K **is totally hidden**

And the ITS of X **is exactly that of** K **from PRNG or QKD**

COMPARISON OF QKD WITH PRNG

- **When X is uniform to Eve, PRNG gives adequate security for privacy for reasonable K^s**

  ⟹ QKD only needed for KPA

  (Yuen, PRA 82, 062304, 2010 and more to come)
- **Only complexity based security for PRNG under KPA but QKD has ITS**
- **Clear that security is a quantitative question (not just qualitative)**

  —Level of ITS
- **Criterion and its operational meaning through probabilities and error rates**

EVE'S ATTACK AND KEY ESTIMATE

- **With her probe she has state ρ_E^k depending on actual possible key value k that A and B finally generate**
- **With her side information and measurement result y_E she obtains the conditional probability distribution** $P(y_E \mid k)$
- **From Bayes rule she generates the whole distribution** $P(k \mid y_E)$ **of correctly estimating** k

  → **generally** $P(k^* \mid K_1 = k_1)$ $K^* \subseteq K_2$

  under KPA with $K = K_1 \sqcup K_2$

Information Theoretic Security (ITS) in Cryptography — current typical

① **Uniform key U for one-time pad**

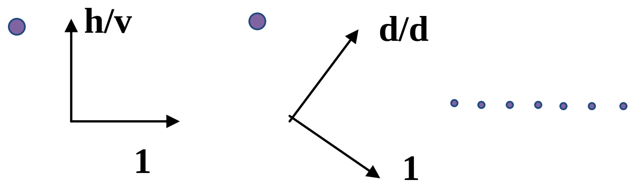
② **Mutual information criterion $I_E \equiv I(K;X_E)$ on Eve's information about K**

③ **Statistical distance criterion $\delta_E \equiv \delta(K;U)$ between Eve's estimate of K and U — equivalent to I_E classically, but not quantum mechanically**

④ **Probability of impersonation and substitution in message authentication**

→ only Eve's success probability and bit error rate (BER) has operational significance

BB84 Protocol (ideal single-photon)



(1) A sends a sequence of qubits with random h/v or d/d basis on which a data bit is modulated.

(2) B randomly measures on h/v or d/d, the openly announced matching basis ones are retained.

(3) A portion of the agreed basis qubits are used to measure the quantum bit error rate (QBER).

(4) If QBER is below a design threshold, the data bits in the rest of the agreed basis qubits give the sifted key K''.

(5) Error correction on K'' is applied to yield the privacy amplification input K' with output K the generated key.

Information Theoretic Security (ITS) in Cryptography — Operational

- **For Privacy and Key Generation**

  Eve's success probabilities: $K_2^* \subseteq K_2$

  $P(k_2^* \mid K_1 = k_1)$ $K = K_1 \sqcup K_2$

  — ciphertext only and known-plaintext attacks included
- **Eve's bit error rate even when sequence estimate fails**
- **Message authentication impersonation and substitution probabilities**

  —— Quantum Case:

  reduces to classical upon measurement but with quantum probe till measurement

General QKD Security Proof Approach in Literature

(1) **Choose a single-number security criterion, usually a trace distance d or an accessible mutual information I_E;**

(2) **For a designed QBER bound Eve's relevant information on the sifted key K'' under an arbitrary attack;**

(3) **Use such bound on K'' as input to PAC and bound d for the final output key K;**

(4) **Subtract the ECC information leak $leak_{EC}$ to Eve from K**

$$leak_{EC} = f \cdot |K| \cdot h(QBER) \qquad h(\cdot)$$ **binary entropy function**

to yield the net generated key;

(5) **d is defined with uniform a priori distribution on PAC input K' which is the ECC output.**

MUTUAL INFORMATION AND SECURITY PARMETER — classical and quantum

- **Eve's mutual (accessible) information on** K **(** K^r **)**

  QKD (PRNG)

  $$I_E \equiv H(K) - H(K \mid E)$$

  whatever information Eve can get

- **Early (before 2004) QKD security proofs: below a threshold key rate**

  $I_E \to 0$ **as** $n \to \infty$ **,** $|K| = n$

- **Unconditional Security in QKD**

  Security criterion $\to 0$ **(perfect) as security parameter** $s \to \infty$

  (Mayers 2001 and earlier)

  Under any attack consistent with the laws of physics

  — Contrast with perfect security

OPERATIONAL ITS

- **Eve gets an entire distribution on estimate of** K

  $P_1 \geq \cdots \geq P_N$ $N = 2^n$ **for** N **possible values of the** n**-bit** K

  With P_1 **her maximum probability of correctly estimating the whole** K

  $\longrightarrow \bar{P}_1$ **when averaged over the a priori distribution of** K
- **Any single-number criterion is just a constraint on** $\{P_i\}$
- **Generally under KPA with known** X_1 **in OTP use of** K**, Eve has the distribution** $P(k^* \mid K_1 = k_1)$ $K^* \subseteq K_2$
- **Even when estimating wrong, her bit error rate (BER) should be sufficiently small**

  —equivalent to knowing non-uniform a priori $P(k)$

NATURE OF QKD KEY

- ☐ **NO Security parameter since $|K|$ is not a security parameter**
- ☐ **Possible that** **（App I, 2009 IEEE）**

  $I_E \sim 2^{-(\lambda n - \log n)}$ **&** $P_1 = 2^{-\lambda n}$ **for**

  $I_E / n \leq 2^{-\lambda n}$ **which is merely a constraint on Eve's** $\{P_i\}$

  Thus, $I_E \to 0$ **as** $n \to \infty$ **for any constant** $\lambda > 0$

  but K **is far from perfect since** $P_1 = 2^{-n}$ **for a uniform key**
- ☐ **Quality of an imperfect key with** $\{P_i\}$ **must be compared to a uniform key** $\{\frac{1}{N}\}$
- ☐ **Quantitative level important,** $\lambda << 1$ **for QKD key**

  It is the (exponential) rate $I_E \to 0$ **that limits key quality**

CHANGE OF CRITERION IN QKD

- **The phenomenon of quantum information locking shows that under an I_E constraint, it is not ruled out that knowing $\log n$ bits of data in a KPA would reveal the entire n-bit K**
- **Change to trace distance criterion d, a quantum generalization of the classical statistical distance $\delta(P,Q)$ between two distribution P and Q, $0 \le \delta \le 1$,**

$$\delta(P,Q) \equiv \frac{1}{2}\sum_i | P_i - Q_i |$$

- **Measure quality of key K by $\delta_E \equiv \delta(P(k),U(k))$ where $P(k)$ is Eve's distribution on K and $U(k)$ the uniform distribution**
- **Most other single-number criteria are equivalent to d**

WRONG INTERPRETATION OF δ AND d

- Since 2004, δ is incorrectly interpreted as the maximum probability that P is different from Q, i.e., δ_E is the maximum probability that $P(k)$ is different from $U(k)$, which implies d is the maximum probability that the generated QKD key K is not perfect

  (for such explicit statement in many papers, see ref.[25] in the above cited PRA paper)
- Error pointed out since 2009 (App II, IEEE J. Sel. Top. Quantum Electron 15, 1630, 2009) but persists to date
- Error has huge consequences on the usefulness of a QKD key

Qualitative Difference Between Wrong and Correct Interpretation of the Trace Distance Criterion d

- **Wrong interpretation of $d=\varepsilon$:**

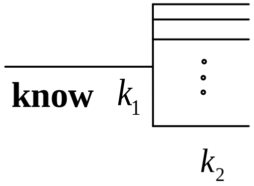
fraction $\underbrace{U,\cdots,U}_{1-\varepsilon},\underbrace{K^{\vartheta},\cdots K^{\vartheta}}_{\varepsilon}$ K^{ϑ} **an imperfect key** $\neq U$

- **Correct interpretation:**

key K **has** $p(K)\neq U$ **with probability** $=1$

- **Under known-plaintext attack (KPA):**

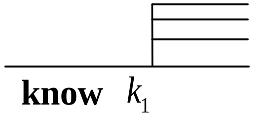
wrong interpretation



all k_2 **uniform for**

$K=U$ **with probability** $1-\varepsilon$

correct interpretation



possible some k_2 **are fixed by**

k_1 **or strongly calculated with**

k_1 **(for** K **with) probability** $=1$**)**

CLAIM ON QKD KEY IN LITERATURE

- **The generated key K is “ε-secure”, $d \le \varepsilon$**

$$d \equiv \frac{1}{2}\sum_{k}\left\| p_0(k)\rho_E^k - \frac{1}{N}\rho_E \right\|_1$$

- **An ε-secure key K is interpreted to be “ε-uniform”, that K is uniform with a probability $\ge 1-\varepsilon$**
- **Many quotes on such claim in many papers can be found in ref.[25] of Yuen, PRA 82, 062304 (2010)**
- **It yields the general claim in technical and popular literature that the QKD generated K is “perfect”, etc.**

- **R. Renner and R. Konig, Lecture Notes on Computer Science, vol. 3378, 407-425, 2005: Universally Composable Privacy Amplification Against Quantum Adversaries (p.414)**

  "it follows from (5) and Lemma 1 that the real and the ideal setting can be considered to be identical with probability at least $1-\varepsilon$."

  "ideal setting where S is replaced by a perfect key U which is uniformly distributed and independent of ρ."

- **R. Konig, R. Renner, A. Bariska, and U. Maurer, Phys. Rev. Lett. 98, 140502 (2007): Small Accessible Quantum Information Does Not Imply Security (p.140502-3)**

  "ε-security has an intuitive interpretation: with probability at least $1-\varepsilon$, the key S can be considered identical to a perfectly secure key U, i.e., U is uniformly distributed and independent of the adversary's information."

- J. Muller-Quade and R. Renner, New J. Phys. 11, 085006 (2009): Composability in quantum cryptography (p.5)

  "Intuitively, the parameter ε can be understood as the maximum failure probability of the protocol P^{real}, i.e the maximum probability that P^{real} deviates from the behavior of the ideal protocol P^{ideal}."

- V. Scarani, etc., Rev. Mod. Phys. 81, 1301 (2009): The security of practical quantum key distribution (p.1310)

  "In this definition, the parameter ε has a clear interpretation as the maximum failure probability of the process of key extraction."

Problem Even under the Wrong Interpretation of an ε-Secure key as an ε-Uniform Key

- Quantitatively the d level becomes $d^{1/2}$ upon application of Markov Inequality for individual guarantee since d is a (privacy amplification code) PAC-average
- This is devastating given there is no security parameter Λ in QKD protocols for which security can be made arbitrarily perfect as $\Lambda \to \infty$, and the best single-photon BB84 protocol gives no net key generation for $d \sim 10^{-14}$ ($d^{1/2} \sim 10^{-7}$)
- Quantitatively security level way too low for application to message authentication (which is a major cryptographic task as important as privacy)
- Cannot rectify the lack of mathematically correct security quantification with error correction and privacy amplification

Serious Problem of Quantitative Security Level Even Under Wrong Interpretation

- **Key may be totally identified by Eve with (failure) probability $\sim \varepsilon$**
- **After Markov Inequality,** $\varepsilon \to \varepsilon^{1/2}$
- **Theoretical single-photon BB84** $\varepsilon > 10^{-14} \to 10^{-7}$

  Experimental BB84 $\varepsilon \sim 10^{-9} \to 10^{-5}$
- **If 100 QKD rounds per second is carried out, one day $\to 10^{7}$ rounds. So, much higher demand on ε for repeated QKD rounds**

  —— that is why one may need a much longer key than 64 bits against many uses in cryptography

Achievable Security level in QKD

- For single-photon BB84 in theory, exchange of key rates and security $d \le \varepsilon$ levels plotted in 2012. Nat. Commun., with

  $|K| \sim 0$ for $d \sim 10^{-14}$ (such d is a double average)

- Recent experimental claims on achievable $\varepsilon \sim 10^{-9}$
- Effective $\varepsilon \sim d^{1/2}$ under wrong interpretation of d

  $\longrightarrow 10^{-7}$ in theory at best, 10^{-5} in experiments

- Effective $\varepsilon \sim d^{1/3}$ under correct interpretation of d

  $\longrightarrow 10^{-5}$ in theory at best, 10^{-3} in experiments

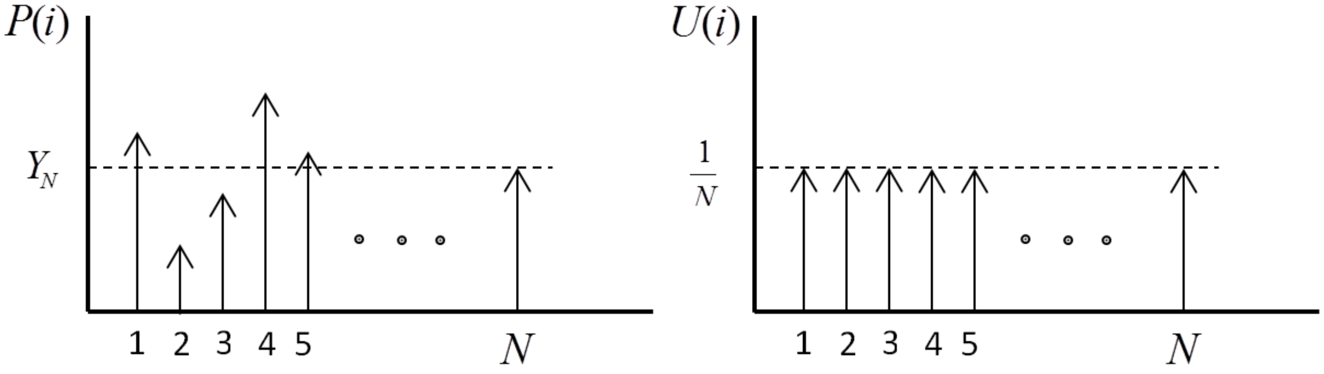
- Thus security guarantee is very poor, especially for 10^{7} rounds in one day of just 100 rounds per second

BUT an ε-secure Key Is NOT ε-uniform

- d **reduces to a** K**-average statistical distance** δ_E **between Eve's** P_i **and uniform** U_i

$$\delta_E = \frac{1}{2}\sum_i |P_i - U_i| \qquad i \in \overline{1-N}, \quad N = 2^n$$

- **N possible bit sequences for an** n**-bit** K**,** $\delta_E \le \varepsilon$



- **Thus, there is no sense that** $K = U$ **with probability** $\ge 1-\varepsilon$**,** $K \ne U$ **with probability one in general**

Wrong interpretation of an ε-secure key as an ε-uniform key from Wrong interpretation of δ_E

Lemma 1 (of Renner and Konig above and R. Konig, U. Maurer and R.Renner, IEEE Tran. Inform. Theory 5, pp.2381-2401,2005):

For any two distribution P, Q for two random variable X, X', there exists a joint distribution $P_{XX'}$ that gives P, Q as marginal with

$$P[X \neq X'] = \delta(P,Q)$$

Problems: ① **No cause for such joint distribution other than independent $P_{XX'} = P_X \cdot P_{X'}$ with $P[X \neq X'] = 1 - \frac{1}{N}$**

② **Needs "for every", "there exists" not enough**

③ **It does not imply ε -uniform even if such a joint distribution is in force -- just get marginals**

See arXiv: 1210.2804v2, 1310.0842v2 and references cited therein

Wrong Interpretation of an ε-secure key as an ε-uniform Key from indistinguishability

- ☐ **Interpret $d \sim \delta_E$ as the distinguishability probability**

  —— the maximum probability that the real and the ideal situations can be distinguished

  Phys. Rev. A 81, 012318 (2010)

- ☐ **Problems:**

  ① **forget additive $\frac{1}{2}+\varepsilon$ for binary decision probability**

  ② **Eve makes an N-ary decision to get at the value k, or 2^m-ary decision to get at an m-bit subset of K**

Why Isn't indistinguishability from δ_E adequate in Classical Cryptography

① **Use in Public-key probabilistic encryption—**

fine for next bit prediction, which does not cover Eve's M -ary estimation of $m>2$ subsets of K, $M=2^m$

② **Use in bounded storage model--**

1) again does not cover M -ary decision

2) does not cover known-plaintext attack

3) such model has a security parameter in contrast to QKD

③ δ_E **not important at all in the practice of classical cryptography**

In particular the above two theoretical model results never implemented due to inefficiency

Condition for Wrong Interpretation to Hold

- **Possible decomposition**

  $P(k) = (1-\lambda)U(k) + \lambda P'(k)$ **for another distribution** $P'(k)$

- **Impossible for** $\lambda = \delta_E$
- **True if and only if**

  $$\frac{1-\lambda}{N} \le P(k) \le \lambda + \frac{1-\lambda}{N}$$ **for all** k

  So that $P(k)$ **is nearly uniform for each** k

  BUT $d \gg 1/N$ **in QKD** ε**-secure key, thus this condition**

  cannot be satisfied in general under $d \le \varepsilon$

General Operational Security Signification of $d \le \varepsilon$ or $\delta_E \le \varepsilon$

- **For whole K estimation in ciphertext-only attack,**

  $P_1 \le \frac{1}{N} + \varepsilon$ **bound can be achieved**

  P_1 **Eve's optimal probability of getting the whole K**

- **Under known-plaintext attack,**

  $$\overline{P}_1(K_2^* \mid K_1) \le 2^{-|K_2^*|} + \varepsilon \qquad K_2^* \subseteq K_2 \qquad K = K_1 \coprod K_2$$

after averaging over K_1 and K_2^*

— **may approach 1 for some specific k_1, k_2^***

POSSIBLE SECURITY BREACH UNDER $d \le \varepsilon$

- d would reduce to δ_E when Eve measures on her probe, $d \le \varepsilon$ becomes $\delta_E \le \varepsilon$
- Eve's $P_1 \ge \cdots P_N$ may take the form $P_1 = \frac{1}{N} + \varepsilon$ with rest of $P_j \ge 0$, $j \in \overline{2-N}$, so that $\delta_E = \frac{1}{2}\sum_i | P_i - \frac{1}{N} | = \varepsilon$
- Thus the whole key may be compromised with Eve's secure probability P_1 of estimating whole K correctly, $P_1 = \frac{1}{N} + \varepsilon$
- It is the job of a security proof to rule out such breach with a high probability, or simply rule out when probability not applicable.
- K with $\varepsilon \sim 10^{-9}$, 10^{-14} (before individual guarantee) compared to $2^{-\frac{|K|}{3.3}} \sim 10^{-2000}$ for $K = U$

Key Distribution

- Get two users A and B to have a common secret key K^s (or K), problem of agent identification.
- In standard cryptography it is done via a key distribution center (KDC), can use asymmetric (public key) distribution via public key certificates or symmetric (private key) distribution in which the KDC knows how to decrypt — only security advantage of public key is when KDC is compromised.
- Symmetric key distribution (or even key expansion) also has information-theoretic (ITS) and fresh key generation.
- QKD and public key also have agent identification problem.

Message Authentication (data integrity)

- **Can be complexity based but ITS ones possible.**
- **Use of a keyed hash family to generate an authentication tag**

  K^h **, message** m **, tag** $t = h(m)$

  Criterion: Eve's success probability P **in**

  Impersonation attack —

  given m **find** t **so that** $t = h(m)$ **for proper** h

  Substitution attack —

  given $h(m_1) = t_1$ **and** m_2 **find** $t_2 = h(m_2)$

  For both attacks, $P \leq \varepsilon$ **in an** $\varepsilon - ASU_2$ **family of hash function**
- $\varepsilon \geq 1/|T|$**,** $|T|$ **tag bit length**

  So the tag length $|T|$ **is a security parameter since the bound can be achieved with equality**

ITS LIMIT OF QKD KEY USED FOR MESSAGE AUTHENTICATION

- ☐ $\varepsilon - ASU_2$ **family of hash function**

  key K^h **, Message** m **and Tag** t $\rightarrow t = h(m)$

  then for substitution attack (given $h(m_1) = t_1$ **and** m_2 **find** $h(m_2) = t_2$ **)**

  Eve's success probability P **bounded by** ε

- ☐ **Always** $\varepsilon \geq \frac{1}{|T|}$ **for tag bit length** $|T|$

- ☐ **For** $d \leq \varepsilon'$ **of the QKD key** K^h **,**

  $P \leq \varepsilon + \varepsilon' \cdot 2^{|T|}$ **can go to** 1 **, may be achieved for some** t

  $\overline{P} \leq \varepsilon + \varepsilon'$ **average over** t

  arXiv: 1303.0210

* $\varepsilon + \varepsilon'$ **cannot be lowered with longer** $|T|$ **or** $|K^h|$

- ☐ **Need** $d \sim 10^{-20}$ **for individual guarantee to reach a common** $|T| = 64$

- ☐ **Worse in multiple uses of hash function with OTP tags**

  — $\overline{P} \leq \varepsilon + m\varepsilon''$ **for** m **uses** $d \leq \varepsilon''$ **for** K^t

  arXiv: 1202.1229

- ☐ **No security parameter for MAC with use of QKD** $\varepsilon -$ **key**

SEVERE QKD LIMIT ON MESSAGE AUTHENTICATION

- **Message authentication more common place and necessary than encryption for privacy**
- **Eve success probability can achieve** $\overline{P} \le \varepsilon + m\varepsilon'$
  $\varepsilon - ASU_2$ **family** $d \le \varepsilon'$ m **uses**
- **Even for one use security cannot be improved beyond** $\varepsilon + \varepsilon'$ **with longer** $|T|$ **or hash family size**
- **Already need effective** $d \sim 10^{-20}$ **for individual guarantee to reach a common 64 bit tag which, after effective** $(\varepsilon')^{1/3}$ **and** $|T|^{1/2}$ **are taken into account, is 100 orders of magnitude beyond current experiment and 90 orders of magnitude beyond theoretic single-photon BB84.**

History of Error Correction Leak in QKD

① **Cascade— a random leak in a complicated nonlinear random situation, wrong leak estimate**

(2006 QCMC paper)

② **Neglected in early "unconditional security" proof papers**

③ **Formula** $leak_{EC} = f \cdot n \cdot h(Q)$ $Q = QBER$**,** $n = |K|$**,** $1 \le f \le 2$

is used with no justification spelled out

④ **Even covering the error correcting code by uniform bits not sufficient since structure of code openly known**

arXiv: 1310.0892

— problem even just under collective attack

Importance of Accounting for Eve’s ECC Information

- Say if ECC corrects 20% error for one-way single-photon BB84 and QBER threshold is 18%, all Eve’s errors would be corrected too from her single qubit probes

  $\longrightarrow$ a quantitative issue of what Eve may correct
- If ECC is one-time padded with a uniform key, still ECC structure may reveal information to Eve

  $\longrightarrow$ again quantitative issue, also unsolved problem of ε –secure imperfect key
- Need to bound $\overline{P}_1(K')$ (equivalently $H_{\min}(K')$) for the ECC output K' which is the PAC input

PROBLEM OF $leak_{EC}$

- **No (valid) justification ever given for any $leak_{EC}$ formula for any reconciliation procedure**
- **Commonly used $leak_{EC} = f \cdot n \cdot h(Q)$, $1 \leq f \leq 2$, Q users' QBER clearly arbitrary for finite protocol**
- **Asymptotic $n \to \infty$ with $f = 1$ only applicable to a constant channel, not applicable to joint attacks, also requires padding the parity digits of a linear ECC with uniform key bits — no known guarantee for an $\varepsilon -$key**
- **More discussions and problems are given in arXiv: 1205.3820**
- **Much worse as follows, even just for collective attacks**

Why Bounding $H_{\min}(K'')$ and Use $leak_{EC}$ Cannot be correct

- **The ECC output K' has a $\overline{P}_1(K')$ or $H_{\min}(K')$ which is different from its input $H_{\min}(K'')$**
- **Even if Eve knows nothing about ECC, her actual $\overline{P}_1(k')$ would change from use of ECC given whatever attack strategy she chooses**
- **But Eve in fact knows at least what set of ECC the actual ECC is chosen from, with $\rho_E^{k''} \xrightarrow{ECC} \rho_E^{k'} \longrightarrow \overline{P}_1(K')$ averaged over all ECC**
- **Thus the explicit ECC structure must be accounted for in quantitative security proof**

LIMITATION OF PRIVACY AMPLIFICATION

- **The $H_{\min}(K')=l$ on the input K' to PAC limits the number of uniform key bits that can in principle be obtained to l bits**
  - **—— simple proof from $\overline{P}_1(K')$ cannot be lowered from a deterministic transformation**
- **Generally no security parameter in QKD —— always exchange of key rate and security level from $\overline{P}_1$ consideration**
- **Same situation for $\varepsilon-$smooth generalization of an $\varepsilon-$secure key — quantitative limits similarly severe**

Current Security Proof Approach

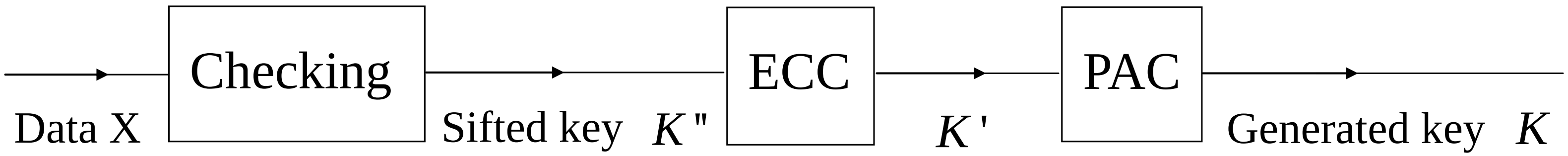
① For sifted key K'', bound Eve's $\overline{P}_1(K'')$ (equivalently minimum entropy) for Eve's probe state $\rho_E(K'')$ under the QBER threshold Q.

② Consider K'' the input to ECC as also the input K' to PAC and subtract $leak_{EC}$.

The Correct Security Proof Approach

①' For sifted key K'' with ECC structure or a specific ECC known to Eve, $\rho_E(K'') \rightarrow \rho_E(K')$, bound $\overline{P}_1(K')$ for any of Eve's probe state $\rho_E(K'')$ under Q.

Required QKD Security Analysis But Not Followed



Data X

Checking

Sifted key K''

ECC

K'

PAC

Generated key K

① **Need Eve's optimum error probability (or equivalently minimum entropy) $\overline{P}_1(K')$ to guarantee trace distance criterion d on K**

② **Typically bound $\overline{P}_1(K'')$ from data checking**

③ **Need to bound $\overline{P}_1(K')$ for given class of (or a specific) ECC from K'' with ECC knowledge, $\overline{P}_1(K'')$ not relevant**

Problems of Current General Security Approach (I)

(1) **The a priori distribution $P_0(K'')$ for K'' the ECC input is not uniform and can vary widely**

(2) **Eve (or the objective) a priori distribution $P_0(K')$ needed for the $H_m(K')$ bound that enters the PAC is not uniform, and in fact cannot be estimated without incorporating the ECC (specific or structure) known to Eve**

(3) **The a priori distribution $P_0(K)$ for the output key K cannot be determined without specific (or structure) PAC and ECC known to Eve**

(4) **So it is wrong to take $P_0(K'')$ and $P_0(K)$ as uniform as done in the literature**

Problems of Current General Security Approach (II)

(1) **The Eve's probe state $\rho_E^{k''}$ is transformed to $\rho_E^{k'}$ upon knowing specific or structure of ECC;**

(2) **Eve's probe state $\rho_E^{k'}$ is correctly transformed to ρ_E^{k} from the Quantum leftover Hash Lemma;**

(3) **However, need all possible $\rho_E^{k''}$ under QBER threshold to all possible ρ_E^{k} — cannot chop off at $\rho_E^{k''}$ by $H_{\min}(K'')$ and jump to PAC output**

(4) **Even when ECC is covered by true OTP (with U), still**

$$\rho_E^{k'} = \sum_i p_i \rho_E^i \qquad\qquad p_i = i \text{ th ECC probability}$$

where ρ_E^i is $\rho_E^{k'}$ under the i th ECC

Correct General Approach and Major Problems

- **For** $d \le \varepsilon$**,** $d \equiv \frac{1}{2}\sum_k \left\| p_0(k)\rho_E^k - \frac{1}{N}\rho_E \right\|_1$**,** k **the value of the PAC output** K **, need to bound** $\overline{P}_1(K')$ **or equivalently** $H_m(K')$ **from** ρ_E^k**,** k' **value of the PAC input** K' **= ECC output** K'
- **So need to deal with all possible a priori distribution** $p_0(k'') \to p_0(k') \to p_0(k)$ **and Eve's probe state** $\rho_E^{k''} \to \rho_E^{k'}$ **for the sifted key** K'' **given QBER threshold** Q
- **In particular the specific ECC, or its general structure when covered by uniform key bits, needs to be incorporated in** $\rho_E^{k''} \to \rho_E^{k'}$

Privacy Amplification from Leftover Hash Lemma

- **Sifted key** $K'' \longrightarrow$ **ECC output** $K' \longrightarrow$ **final key** K

  a priori distribution $p_0(K'') \longrightarrow p_0(K') \longrightarrow p_0(K)$

  Eve's probe state $\rho_E^{k''} \xrightarrow{ECC} \rho_E^{k'} \xrightarrow{PAC} \rho_E^{k}$

  $H_{\min}(K') \equiv -\log \overline{P}_1(K')$

  $\overline{P}_1(K')$ — **Eve's averaged optimum probability of getting** K' **from** $\rho_E^{k'}$

- **Let** f **be chosen randomly from a proper set of hash functions from** m **-bit** K' **to** n **-bit** K**,** $m > n$ **and let** $n \le H_{\min}(K') - 2\log\frac{1}{\varepsilon}$

  Then averaged over f **we have** $d \le \varepsilon$**,**

$$d \equiv \frac{1}{2}\sum_k \left\| p_0(k)\rho_E^k - \frac{1}{2^n}\rho_E \right\|_1, \quad \rho_E \equiv \sum_k p_0(k)\rho_E^k, \quad k = f(k')$$

- **Clear that need ECC output state** $\rho_E^{k'}$ **and a priori distribution** $p_0(k'')$ **to yield PAC input state** $\rho_E^{k'}$ **and a priori distribution** $p_0(k')$ **for obtaining PAC output state** ρ_E^{k} **and a priori distribution** $p_0(k)$

Some History of the Main Erroneous Claims on QKD Security in the Theory Literature

① Security claim was made since the 1990's but the problem of known-plaintext attack on the use of the QKD generated key K was not addressed till 2004.

② Security claim was made for concrete systems on the basis of qubit results while total breach of security occurs in actual higher dimensional Hilbert spaces without further processing.

③ Use Eve's accessible information as security criterion since the beginning, its inadequacy not pointed out till 2007.

④ The length of K is erroneously taken to be a security parameter since the beginning.

⑤ No operational security guarantee on K has even been spelled out properly till arXiv: 1205.5056.

⑥ Incorrect use of channel mutual information against active attacks.

Some History of the Main Erroneous Claims on QKD

⑦ **The security meaning of the trace distance criterion d given for many years in many papers is incorrect as pointed out since 2009, but such misleading claims persist to date.**

⑧ **The theoretical and realizable levels of d from QKD protocols are totally inadequate for security, but the contrary is maintained to date.**

⑨ **Absolute or perfect security (with a high probability) is claimed for systems that are totally breached by detector blinding attacks.**

⑩ **Classical instead of qubit counting in general security proofs.**

⑪ **Numerous errors of a physical or mathematical nature on security proofs are made to claim security, including those associated with the effects of loss, decoy states, etc., and in CV-QKD also.**

⑫ **Whole security approach from sifted key K'' to error corrected key K' to final key K incorrectly carried out.**

Some Erroneous QKD Security Claims in the Experiment Literature
— other than reliance on incorrect theories

① **Give results with key rates but no security level, which are not proper cryptographic results**

② **Rely on theories whose validity have never been claimed to cover the systems being implemented**

③ **Short cuts on various protocol features affecting security but not treated**

Major QKD Security Problem Neglected (but unconditional security claimed)

- **Many of Eve’s attacks not covered in security proofs, especially in the lossy case and the multi-photon source case**
- **The problem of bounding $\overline{P}_1(K')$, or equivalently the minimum entropy at the output of error correction which is the input of privacy amplification**
- **Operational security guarantee from security criterion**
- **Completeness of cryptosystem model for security analysis**

Inadequacy of Proofs Against Collective Attack

- **Collective attack— Eve has identical probe on every qubit**
- **One can readily bound $\overline{P}_1(K')$ under collective attack, with or without decoy states**

① **No need for Eve to entangle to launch a joint attack outside the class of collective attack**

— just use individual qubit probes on a portion of the qubits

Such attacks may give Eve a lot more information than that allowed by collective attacks

② **"Proofs" that collective attack is optimum are not valid; in fact in the presence of loss Eve can significantly bias the a prior distribution of effective (detected) qubits**

③ **Still need $\overline{P}_1(K')$ for the ECC output or PAC input**

SECURITY IN THE PRESENCE OF LOSS

- **No proof ever offered on why loss only affects throughput but not security for single-photon sources**
- **However, loss clearly affects information-disturbance tradeoff since Eve can delete some disturbance she does not want upon a probabilistic measurement attack similar to approximate probabilistic cloning**
- **An example of the above breach is B92 in loss, which shows a general security proof is necessary in a proper general loss formulation including all Eve's possible attacks**
- **Post-detection selection by Eve in loss never taken into account**

Major Security Proof Problem of Multi-Photon Source

- **Eve knows for sure a portion of K'' from (generalized) photon-number splitting attack**

  arXiv: 1207.6985

- **Hence:**

  Cannot separate ECC input and output due to the matching of ECC structure to Eve's known qubits

  — need $\overline{P}_1(K')$ directly from K''

  (In fact same problem under general probe)

- **Analysis of Decoy States performance needs $\overline{P}_1(K')$ for PAC input, not just $\overline{P}_1(K'')$**

Problems of CV-QKD

① **Incorrect use of mutual information criterion under heterodyne attack**

② **Incorrect estimate of error correction leak**

③ **Lack of robustness for system parameter uncertainly and fluctuation**

④ **Lack of False Alarm security analysis for such serious lack of robustness**

False Alarm and Denial of Service

① **Weak QKD signals prone to jamming**

② **False alarm rate (never treated in literature) may be too high— added inefficiency when protocol aborted with no Eve presence due to lack of robustness**

③ **Eve can consume the users' key bits by her stronger attacks— users need to spend many key bits for protocol execution, and Eve may gain a lot more information when passed by users (again never studied)**

Security Proof and Model Completeness

- **Security cannot be established experimentally**
- **need to rigorously prove security for specific model**

  — or else no difference from classical cryptography
- **Special quantum hacking weakness for (weak-signal) QKD which is not present in classical mathematical cryptography or (strong-signal) KCQ or classical noise cryptography**

Problems of Measurement-Device-Independent QKD

① Give asymptotic key generation rate with no security level attached, but such key rate is meaningless, especially given there is no security parameter for the cryptosystem

② Such key rate was allegedly derived only for CSS code for (some unknown) error correction and privacy amplification codes, not for any concrete protocol or experimental system

③ Many physical issues not accounted for properly, including those associated with system loss and use of decoy states

④ Does not answer any of the criticisms described in this talk, at best just avoids use of single-photon detectors

Special Weakness of QKD (BB84 type information-disturbance tradeoff protocols)

Need weak signal to sense disturbance, which gives rise to numerous problems:

1) inefficiency, especially susceptible to loss

2) lack or robustness and sensitivity to imperfection and nonideal disturbance

3) infrastructure incompatible

4) false-alarm and information leak from stronger attacks

5) open to quantum hacking

6) numerical security gap to adequate quantitative level appears unbridgeable

SUMMARY OF QKD SECURITY SITUATION

- **Even if derivation valid, the generated QKD key has poor quantitative security guarantee that renders it unsuitable for the high security situation it is intended**
  - **rigorous proof needed or else standard cryptography would do**
- **Many major steps in the security proofs are not validly deduced contrary to claims; especially serious in error correction**

- **Issue of model completeness not present in other crypto systems**
- **Inefficiency, lack of robustness, infrastructure incompatibility**

References

Some relevant QKD papers and my criticisms

can be traced from

① **arXiv: 1210.2804**

② **arXiv: 1310.0842**