Another Look at Symmetric Incoherent Optimal Eavesdropping against BB84

Arpita Maitra[1] and Goutam Paul[2]

[1]Indian Statistical Institute, Kolkata, India
[2]Jadavpur University, Kolkata, India

INDOCRYPT 2012, Kolkata, India.
December 10, 2012.

Outline of the talk

- Preliminaries of BB84
  - Summary of Contributions
  - Basics
  - No Cloning
  - Indistinguishability of quantum states
  - Outline of BB84
- Another Look
  - Eavesdropping
  - Comparing one- and two-bit probes
  - Comparing 4- and 6-state BB84 protocol

Contribution I

- Bruß, Phys. Rev. Lett., 1998: six-state variant of BB84 protocol.
- The mutual information between Alice (the sender) and Eve (the eavesdropper) is higher when two-bit probe is used compared to the one-bit probe.
- Hence the two-bit probe provides a stronger eavesdropping strategy.
- However, from cryptanalytic point of view, we show that Eve has the same success probability in guessing the bit transmitted by Alice in both the cases of the two-bit and the one-bit probe.
- Thus, we point out that having higher mutual information may not directly lead to obtaining higher probability in guessing the key bit.

Contribution II

- Bruß, Phys. Rev. Lett., 1998: the six-state variant of BB84 protocol is more secure than the traditional four-state BB84.
- We identify that this advantage is only achieved at the expense of communicating more qubits in the six-state protocol.
- we present different scenarios, where given the same number of qubits communicated, the security comparison of the four- and six-state protocols is evaluated carefully.

Qubit (preliminaries)

- Classical bits: $0, 1$.
- Quantum counterpart $|0\rangle, |1\rangle$.
- $|0\rangle$ can be written as $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$
- $|1\rangle$ can be written as $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$.
- Superposition of $|0\rangle, |1\rangle$: $\alpha|0\rangle + \beta|1\rangle$ can be written as $\alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$.
- $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$.

Qubit and Measurement

- A qubit:

$$\alpha|0\rangle + \beta|1\rangle,$$

$\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$.

- Measurement in $\{|0\rangle, |1\rangle\}$ basis: we will get $|0\rangle$ with probability $|\alpha|^2$, $|1\rangle$ with probability $|\beta|^2$. The original state gets destroyed.
- Example:

$$\frac{1+i}{2}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$

After measurement: we will get
$|0\rangle$ with probability $\frac{1}{2}$,
$|1\rangle$ with probability $\frac{1}{2}$.

Cloning: Possible in classical domain, not in quantum

Possible to copy a classical bit

Not possible for an unknown quantum bit

No cloning

- A result of quantum mechanics
- Not possible to create identical copies of an arbitrary unknown quantum state
- It was stated by Wootters, Zurek, and Dieks in 1982
- W. K. Wootters and W. H. Zurek. A Single Quantum Cannot be Cloned, Nature 299 (1982), pp. 802803.
- D. Dieks. Communication by EPR devices, Physics Letters A, vol. 92(6) (1982), pp. 271272.
- Huge implications in quantum computing, quantum information, quantum cryptography and related fields.

Orthogonal quantum states: distinguishable

Possible to distinguish two orthogonal states only

- Given two orthogonal states $\{|\psi\rangle, |\psi_\perp\rangle\}$, it is possible to distinguish them with certainty.
- For example,

$$\{|0\rangle, |1\rangle\};$$

$$\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$$

$$\{\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\}$$

Distinguishability of Nonorthogonal quantum states

Not possible to distinguish two nonorthogonal quantum states with certainty

- Given two nonorthogonal states $\{|\psi_0\rangle, |\psi_1\rangle\}$, it is not possible to distinguish them with probability 1.
- Example: it is given that the two states are $|0\rangle$, $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, two nonorthogonal states. Then it is not possible to exactly identify each one.

BB84 History

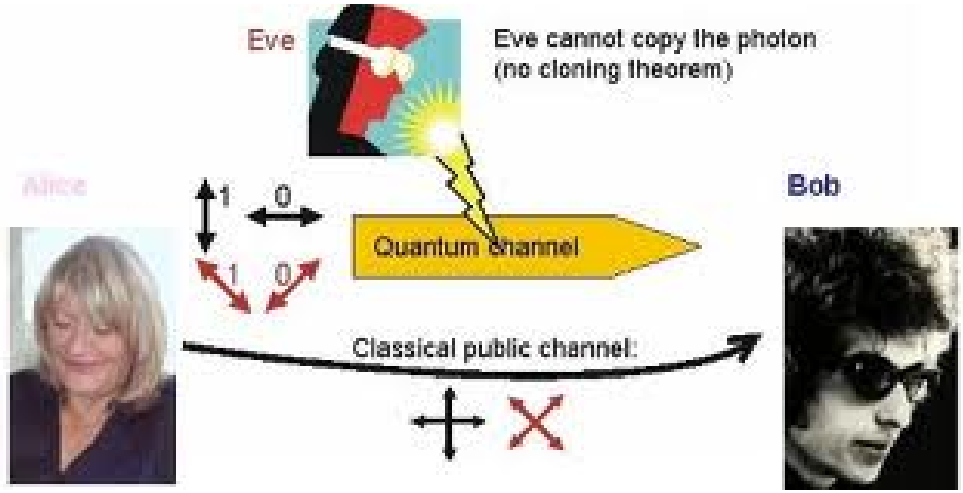
- Initiated by Charles Bennett and Gilles Brassard in 1979

  G. Brassard. Brief History of Quantum Cryptography: A Personal Perspective. [quant-ph/0604072]
- The paper was not getting accepted initially
- Finally published as Quantum Cryptography: Public key distribution and coin tossing, in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, p. 175 (1984)
- Citation: 2886 in June to 2954 in August to 3332 in November, 2012, Google Scholar
- A scheme for quantum key distribution scheme
- The first protocol in the area of quantum cryptography
- The basics of this protocol comes from the seminal concept by Wiesner.

  S. Wiesner. Conjugate Coding. Manuscript 1970, subsequently published in SIGACT News 15:1, 78–88, 1983.

BB84 (contd.)

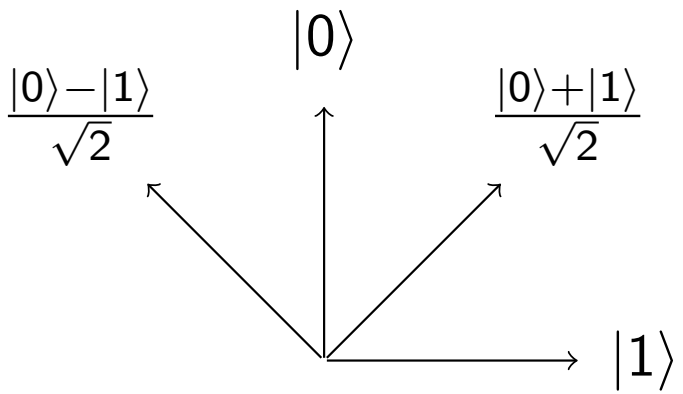
- The protocol is provably secure
- Based on no cloning theorem



- If the two states we are trying to distinguish are not orthogonal, it is not possible to distinguish them with certainty
- The protocol is a method of securely communicating a private key from Alice to Bob
- The proof comes from the quantum property that information gain is only possible at the expense of disturbing the signal

Qubits and Basis: Notations

- $+$: $\{\uparrow = |0\rangle, \rightarrow = |1\rangle\}$, i.e., Z basis
- $\times$: $\{\nearrow = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \nwarrow = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$, i.e., X basis



BB84: Basic Idea

- To transmit 0 or 1 securely.
- Choose some basis:

$$\{|0\rangle, |1\rangle\};$$

$$\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$$

$$\{\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\}$$

- Take any basis. Encode 0 to one qubit and 1 to another qubit.
- If we use only a single basis, then anybody can measure in that basis, get the information and reproduce.
- Thus Alice needs to encode randomly with more than one bases.
- Bob will also measure in random basis.
- Basis will match in a proportion of cases and from that key will be prepared.

BB84 Algorithm

- Alice chooses $(4+\delta)n$ many random data bits referred as binary string a
- Alice further chooses a random binary string b of $(4+\delta)n$ bits
- For $i = 0$ to $(4+\delta)n - 1$
  - if $a_i = 0$ and $b_i = 0$ Alice selects the qubit $|0\rangle$
  - if $a_i = 1$ and $b_i = 0$ Alice selects the qubit $|1\rangle$
  - if $a_i = 0$ and $b_i = 1$ Alice selects the qubit $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
  - if $a_i = 1$ and $b_i = 1$ Alice selects the qubit $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

BB84 Algorithm (contd.)

- Alice sends the resulting state (qubits) to Bob
- After receiving $(4+\delta)n$ many qubits Bob announces the fact and measures each qubit either in $|0\rangle, |1\rangle$ basis or in $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ basis at random
- Alice then announces b
- Bob then discards the bits where he measured the qubit in a different basis than Alice prepared and Alice also does the same thing; with high probability there are at least $2n$ bits left (not discarded) and if this does not happen then the protocol is aborted; they work with $2n$ bits

BB84 Algorithm (contd.)

- A subset of n bits are selected by Alice that will serve as checks on the interference of Eve; Alice also tells Bob which bits she actually selected
- Both Alice and Bob announce and compare the values of the n many check bits; if the number of disagreement is more than an acceptable limit then the protocol will be aborted
- Information reconciliation and privacy amplification are performed by Alice and Bob on the remaining n bits to obtain m shared key bits

Eavesdropping in Quantum Channel

- The security in the protocol is based on the fact that if one wants to distinguish two non-orthogonal quantum states, then obtaining any information is only possible at the expense of introducing disturbance in the state(s).

  - There are several works in the literature, that studied the relationship between "the amount of information obtained by Eve" and "the amount of disturbance created on the qubits that Bob receives from Alice".

Eavesdropping: Different Models

- Eve can work on each individual qubit as opposed to a set of qubits studied together
  - the first one is called the *incoherent attack*,
  - the second one is known as *coherent attack*.
- Another interesting issue in specifying the eavesdropping scenario is whether there will be equal error probability at Bob's end corresponding to different bases.
  - If this is indeed equal, then we call it *symmetric*.
  - There is also another model where this is not equal and then we call the eavesdropping model as *asymmetric*. Different error rates for different bases would be a clear indication to Alice and Bob that an eavesdropper (Eve) is interfering in the communication line.

Eavesdropping: How to interact

- Alice sends a qubit $|\mu\rangle$ to Bob and Eve lets a probe $|W\rangle$ of that interacts unitarily with $|\mu\rangle$.
- One can model it as $U(|\mu\rangle, |W\rangle) = |\tau\rangle$, where U is the unitary operator and after its application, $|\tau\rangle$ is the entangled state of the qubit that Alice sent to Bob and the probe applied by Eve.

- Eve's measurement is delayed till Alice announces the basis that has been used (i.e., by that time Bob has already measured the state).
- The probe $|W\rangle$ could be of one or two or more qubits. The most efficient model considers a two-qubit probe.

Eavesdropping (contd.)

A quantum gate is reversible. An n input, n output quantum gate can be seen as $2^n \times 2^n$ unitary matrices where the elements are complex numbers.

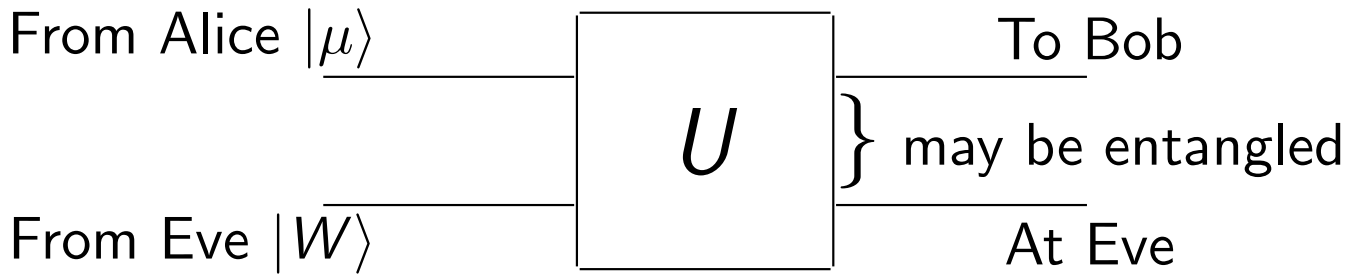


Figure: The model of Eavesdropping

Eve introduces additional qubit(s) to interact with the qubit communicated between Alice and Bob. Through interaction, $|W\rangle$ gets updated extracting some information from $|\mu\rangle$ and in the process $|\mu\rangle$ also gets modified. Thus error appears in the channel.

Eavesdropping: Exact analysis

Let D be the disturbance in the channel due to the interaction by Eve and $F = 1 - D$ be the fidelity. For the $|0\rangle, |1\rangle$ basis, i.e., the Z basis, one can write the eavesdropping interaction as

$$\begin{aligned} U(|0\rangle, |W\rangle) &= \sqrt{F}|E_{00}\rangle|0\rangle + \sqrt{D}|E_{01}\rangle|1\rangle, \\ U(|1\rangle, |W\rangle) &= \sqrt{D}|E_{10}\rangle|0\rangle + \sqrt{F}|E_{11}\rangle|1\rangle. \end{aligned} \quad (1)$$

Alice sends	Bob receives	Eve obtains	Probability
$\|0\rangle$	$\|0\rangle$	$\|E_{00}\rangle$	$F = 1 - D$
$\|0\rangle$	$\|1\rangle$	$\|E_{01}\rangle$	D
$\|1\rangle$	$\|0\rangle$	$\|E_{10}\rangle$	D
$\|1\rangle$	$\|1\rangle$	$\|E_{11}\rangle$	$F = 1 - D$

Similar equations can be written for the X basis.

BB84: 4 state vs 6 state

- Traditional BB84 uses four states $\{|0\rangle, |1\rangle\}$ and $\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$. Eavesdropping on this model was studied by Fuchs et al, 1997.
- 0 is encoded by $|0\rangle$ or $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and
  1 is encoded by $|1\rangle$ or $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.
- To obtain better security, Bruß (PRL 1998) proposed use of $\{\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\}$ too. This is referred as Y basis.
- 0 is encoded by $|0\rangle$ or $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ or $\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$.
  1 is encoded by $|1\rangle$ or $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ or $\frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$.

$|E_{ij}\rangle$'s: 4-state BB84

According to Fuchs et al, PRA 1997,

$$
\begin{aligned}
|E_{00}\rangle &= \sqrt{1-D}\frac{|00\rangle+|11\rangle}{\sqrt{2}} + \sqrt{D}\frac{|00\rangle-|11\rangle}{\sqrt{2}}, \\
|E_{01}\rangle &= \sqrt{1-D}\frac{|01\rangle+|10\rangle}{\sqrt{2}} - \sqrt{D}\frac{|01\rangle-|10\rangle}{\sqrt{2}}, \\
|E_{10}\rangle &= \sqrt{1-D}\frac{|01\rangle+|10\rangle}{\sqrt{2}} + \sqrt{D}\frac{|01\rangle-|10\rangle}{\sqrt{2}}, \\
|E_{11}\rangle &= \sqrt{1-D}\frac{|00\rangle+|11\rangle}{\sqrt{2}} - \sqrt{D}\frac{|00\rangle-|11\rangle}{\sqrt{2}}.
\end{aligned}
$$

$|E_{ij}\rangle$'s: 6-state BB84

According to Bruß, Phys. Rev. Lett., 1998

$$
\begin{aligned}
|E_{00}\rangle &= \beta|10\rangle + \sqrt{1-|\beta|^2}|01\rangle, \\
|E_{01}\rangle &= |00\rangle, \\
|E_{10}\rangle &= |11\rangle, \\
|E_{11}\rangle &= \sqrt{1-|\beta|^2}|10\rangle + \beta|01\rangle.
\end{aligned}
$$

$$
|\beta|^2 = \frac{1}{2}\left(1 + \frac{\sqrt{D(2-3D)}}{1-D}\right).
$$

one-bit vs two-bit probe

- $|E_{ij}\rangle$: Two qubits
- When one measures one-bit (the second qubit) of those, then it is called one-bit probe
- When one measures both the qubits, then it is called two-bit probe

One-bit vs two-bit probe

- For one-bit probe, Eve measures her second qubit in the bases Z or X (or Y in case of 6-state), as used by Alice.
- Similarly, for two-bit probe, Eve measures in the bases $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ when Alice and Bob use the Z basis and she measures in the basis $\{|++\rangle, |+-\rangle, |-+\rangle, |--\rangle\}$ when Alice and Bob use the X basis. Similarly, for Y basis for 6-state BB84.
- In this paper, we calculate all probabilities considering the Z basis only. Symmetry gives the same results when the X or Y basis is used.

6-state BB84: one-bit vs two-bit probe

- Bruß, Phys. Rev. Lett., 1998: six-state variant of BB84 protocol.
- The mutual information between Alice (the sender) and Eve (the eavesdropper) is higher when two-bit probe is used compared to the one-bit probe.
- Hence the two-bit probe provides a stronger eavesdropping strategy.
- However, from cryptanalytic point of view, we show that Eve has the same success probability in guessing the bit transmitted by Alice in both the cases of the two-bit and the one-bit probe.
- Thus, we point out that having higher mutual information may not directly lead to obtaining higher probability in guessing the key bit.

Optimal Success Probability of Eve

- Let A, B, V be the random variables corresponding to the bit sent by Alice, the bit received by Bob and the outcome observed by Eve due to her measurement.
- $A, B \in \{0, 1\}$, $V \in \{0, 1\}$ for one-bit probe, $V \in \{0, 1\}^2$ for two-bit probe.
- $P_{opt}(success) = \sum_{v} \max_{i} P(A = i, V = v)$
- $P(A = 0) = P(A = 1) = \frac{1}{2}$
- We need $P(A = i, V = v)$, that will be available by using $P(V = v | A = i)$

The probability table: Fuchs et al, 1997

	$V=0$	$V=1$
$A=0$	$\frac{1}{2}+\sqrt{D(1-D)}$	$\frac{1}{2}-\sqrt{D(1-D)}$
$A=1$	$\frac{1}{2}-\sqrt{D(1-D)}$	$\frac{1}{2}+\sqrt{D(1-D)}$
Marginal of V	$\frac{1}{2}$	$\frac{1}{2}$

Table: Values of $P(V=v \mid A=i)$ for the attack model of Fuchs et al, 1997.

$$\begin{aligned} P_{opt}^{4\ state}(success) &= \frac{1}{2}\left(\frac{1}{2}+\sqrt{D(1-D)}\right)+\frac{1}{2}\left(\frac{1}{2}+\sqrt{D(1-D)}\right) \\ &= \frac{1}{2}+\sqrt{D(1-D)} = f(D). \end{aligned}$$

Same success probability for two-bit probe.

The probability table: Bruß, Phys. Rev. Lett., 1998

	$V=0$	$V=1$
$A=0$	$D+(1-D)\|\beta\|^2$	$1-D-(1-D)\|\beta\|^2$
$A=1$	$1-D-(1-D)\|\beta\|^2$	$D+(1-D)\|\beta\|^2$
Marginal of V	$\frac{1}{2}$	$\frac{1}{2}$

Table: Values of $P(V=v \mid A=i)$ for one-bit probe.

	$V=00$	$V=01$	$V=10$	$V=11$
$A=0$	D	$1-D-(1-D)\|\beta\|^2$	$(1-D)\|\beta\|^2$	0
$A=1$	0	$(1-D)\|\beta\|^2$	$1-D-(1-D)\|\beta\|^2$	D
Marginal of V	$\frac{D}{2}$	$\frac{1-D}{2}$	$\frac{1-D}{2}$	$\frac{D}{2}$

Table: Values of $P(V=v \mid A=i)$ for two-bit probe.

Success probability that Eve guesses correctly the bit Alice has sent

$$\frac{1}{2}+\frac{D+\sqrt{D(2-3D)}}{2}, \text{ using } |\beta|^2=\frac{1}{2}\left(1+\frac{\sqrt{D(2-3D)}}{1-D}\right),$$

for both the cases.

Point to note

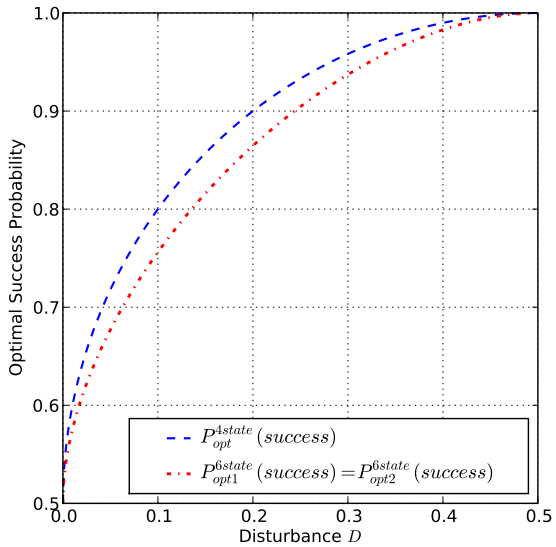
$$I_1^{AV} < I_2^{AV} < I^{AV} \text{ but}$$

$$P_{opt1}^{6\ state}(success) = P_{opt2}^{6\ state}(success) < P_{opt}^{4\ state}(success).$$

- Advantage of Eve $= P_{opt}(success) - \frac{1}{2}$. That is, $A_{opt1}^{6\ state}(D) = A_{opt2}^{6\ state}(D) < A_{opt}^{4\ state}(D)$.
- Advantage of Eve is greater in 4-state protocol than the 6-state protocol.
- Given 6-state protocol, Eve's advantage is same for both 1-bit and 2-bit probes in terms of probability.

Eavesdropping: 4- vs 6-state

- For 4-state (traditional) BB84, providing a disturbance D the eavesdropper can guess the bit correctly at a probability $\frac{1}{2} + \sqrt{D(1-D)}$ (more)
- For 6-state BB84, providing a disturbance D the eavesdropper can guess the bit correctly at a probability $\frac{1}{2} + \frac{D+\sqrt{D(2-3D)}}{2}$ (less)



BB84: 4 state vs 6 state (critical comparison)

- Bruß, Phys. Rev. Lett., 1998: the six-state variant of BB84 protocol is more secure than the traditional four-state BB84.
- We identify that this advantage is only achieved at the expense of communicating more qubits in the six-state protocol.
- For the traditional 4-state protocol, half of the states will be discarded as Bob will measure those in different basis.
- For the 6-state protocol, two third of the states will be discarded as Bob will measure them in different basis.
- we present different scenarios, where given the same number of qubits communicated, the security comparison of the four- and six-state protocols is evaluated carefully.

Fare Comparison

- We take the same values of
  1. the length of the secret key established, and
  2. the total number of qubits communicated

  in both the protocols.
- To establish a secret key of length n bits, the four state protocol must communicate around $4n$ number of qubits (in the practical scenario, the exact number is little more than $4n$) and the six state protocol must communicate around $6n$ qubits (practically little more than that).
- Therefore, in order to match the total number of bits communicated, the four state protocol may be repeated $3t$ times and the six states protocol should be repeated $2t$ times for any positive integer t.

Protocol m-BB84

Step 1. Alice and Bob run m independent instances of BB84.
(The instances may either be run sequentially,
or they may be run in parallel through separate channels).

Step 2. Suppose they establish m many n-bit secret keys, namely,
$k_1, k_2, \ldots, k_m$.

Step 3. The bit-wise XOR of m many bit strings of same length n is finally considered.

Advantage of the Adversary

Theorem

For a disturbance D in each qubit, the optimal advantages of the adversary in guessing a bit of the final key of m-BB84 are given by

$$A_{opt}^{4state}(D,m) = 2^{m-1}\left(\sqrt{D(1-D)}\right)^m, \text{ and}$$

$$A_{opt}^{6state}(D,m) = \frac{1}{2}\left(D+\sqrt{D(2-3D)}\right)^m$$

corresponding to four-state protocol and the six-state protocol respectively.

So large m kills the eavesdropper, but, as the next result shows, it increases Bob's disturbance as well.

Effective Disturbance at Bob's End

Theorem

For a disturbance D in the channel for each qubit of the individual instances of BB84, the effective disturbance perceived by Bob for each bit of the final key of m-BB84 is given by $\Delta(D, m) = \frac{1}{2} - 2^{m-1}\left(\frac{1}{2} - D\right)^m$.

As we discussed, for fare comparison, $m = 3t$ for 4-state protocol and $m = 2t$ for 6-state protocol. To keep Bob's disturbance at low level, it is practical to consider $t = 1$ only.

Scenario 1: Equal Disturbance in Each Qubit of the Individual Instances of Four-state and Six-state BB84

- Here, $D_4 = D_6 = D$, i.e., same disturbance for each individual BB84.
- For all $D \in [0, 0.5]$, $A_4(D, 1) > A_6(D, 1)$, as 4-state BB84 is less secure than 6-state BB84.
- However, we note that $A_4(D, 3) \leq A_6(D, 2)$ for $D \leq 0.27$ (up to two decimal places).
- Thus, at the expense of same number of qubits, for the range of disturbance ≤ 0.27, the four-state BB84 is more secure (as eavesdropper obtains less information) than the six-state BB84
- Greater effective disturbance is there at Bob's end for Four-state BB84, as we XOR three strings in Four-state BB84, but XOR two strings in Six-state BB84.

Scenario 2: Equal Effective Disturbance in Each Bit of the Final Key of Four-state and Six-state BB84

- We consider that Eve chooses different values of D_4 and D_6 so that the effective disturbances $\Delta(D_4, 3)$ and $\Delta(D_6, 2)$ are equal.
- We can write $\Delta(D_4, 3) = \frac{1}{2} - 2^2 \left(\frac{1}{2} - D_4\right)^3$, and $\Delta(D_6, 2) = \frac{1}{2} - 2\left(\frac{1}{2} - D_6\right)^2$.
- Equating the right hand sides and substituting $D_6 = D$, we obtain $D_4 = \frac{1}{2} - \left(\frac{1}{2}\left(\frac{1}{2} - D\right)^2\right)^{\frac{1}{3}}$.
- In this case, Eve's advantage in four-state 3-BB84 is less than in the case of six-state 2-BB84.

Scenario 3: Equal Advantages for Eve for Four-state 3-BB84 and Six-state 2-BB84

- We have $A_4(D_4, 3) = 2^2 \left(\sqrt{D_4(1-D_4)}\right)^3$, and $A_6(D_6, 2) = \frac{1}{2}\left(D_6 + \sqrt{D_6(2-3D_6)}\right)^2$.
- Equating the right hand sides and substituting $D_6 = D$, we obtain $D_4 = \frac{1}{2} - \frac{1}{2}\sqrt{1 - \left(D + \sqrt{D(2-3D)}\right)^{\frac{4}{3}}}$.
- The four-state protocol offers more (individual as well as effective) disturbance at Bob's end than the six-state one.
- Thus, Eve's advantage will be more prominent to Alice and Bob in the four-state 3-BB84 than the six-state 2-BB84.

Conclusion

- We show that both the one-bit and the two-bit probes in the six-state have the same success probability for Eve.
- We critically compare the security issues in the four and the six-state protocols when same number of qubits are used in both the cases.
- Though the theoretical results of Bruß as well as ours are correct, our results are placed from the cryptanalytic viewpoint of optimal eavesdropping and thus the interpretation is different from what claimed in Bruß's paper.


Thank You!