Closing all loopholes in quantum devices

Connor Behan

February 25, 2015

The problem

Alice

Bob

The problem

Alice

Any classical communication between them can be intercepted by an intruder with the right type of wire or antenna.

Bob

The problem

Alice

Any classical communication between them can be intercepted by an intruder with the right type of wire or antenna.

Bob

	Plain	Encrypted
Classical	Trivially insecure	Secure if the pair already knows a secret key
Quantum	Self-destructs upon measurement if the data is randomized	Desired solution

Basic cryptography

Message:	100110101010101110010
Key:	010110110001101011001
Result:	110000011011000101011

Basic cryptography

Message:	100110101010101110010
Key:	010110110001101011001
Result:	110000011011000101011

- Bob reconstructs Alice's message with the same operation.

Basic cryptography

Message:	10011010101010111 0010
Key:	01011011000110101 1001
Result:	11000001101100010 1011

- Bob reconstructs Alice's message with the same operation.
- This "one time pad" is perfect the first time, vulnerable to pattern recognition after.

Basic cryptography

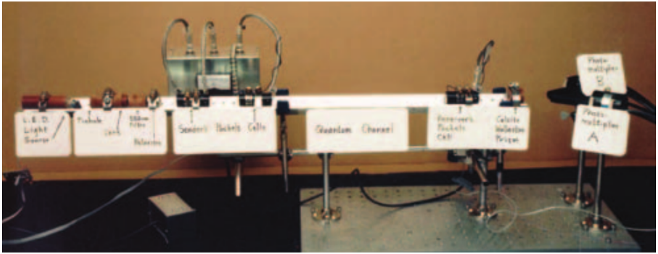
Message:	10011010101010111001 0
Key:	01011011000110101100 1
Result:	11000001101100010101 1

- Bob reconstructs Alice's message with the same operation.
- This "one time pad" is perfect the first time, vulnerable to pattern recognition after.
- Quantum key distribution is the problem that must be solved.

Basic cryptography

Message:	10011010101011110010
Key:	01011011000110101001
Result:	11000001101100101011

- Bob reconstructs Alice's message with the same operation.
- This "one time pad" is perfect the first time, vulnerable to pattern recognition after.
- Quantum key distribution is the problem that must be solved.



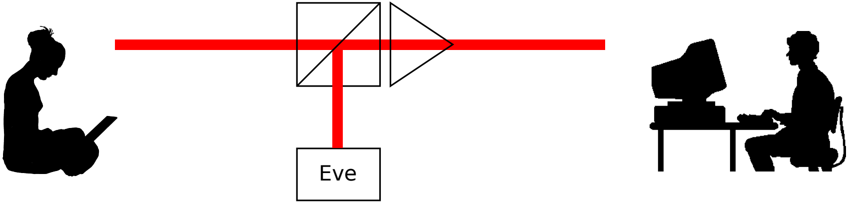
[J Cryptol **5**, 2–38, 1992]

The BB84 protocol

Developed by Bennett and Brassard in 1984.

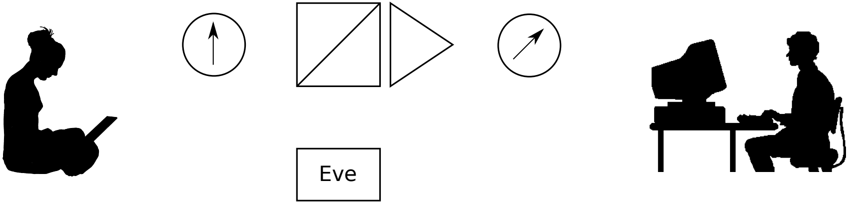
The BB84 protocol

Developed by Bennett and Brassard in 1984.



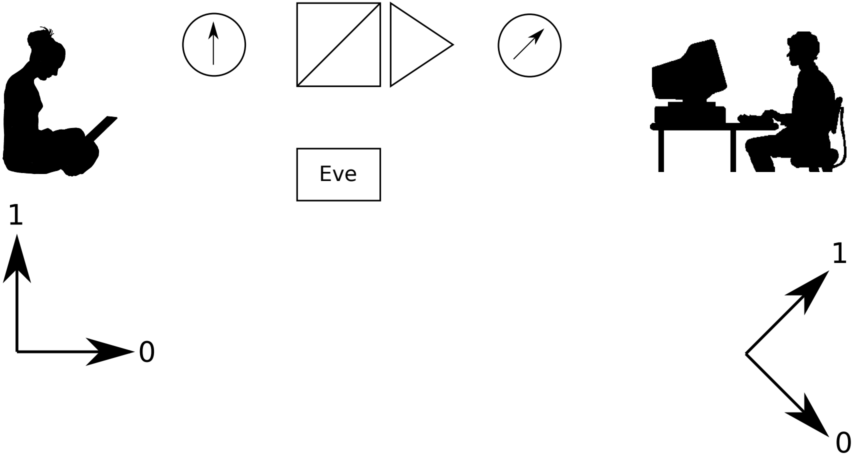
The BB84 protocol

Developed by Bennett and Brassard in 1984.



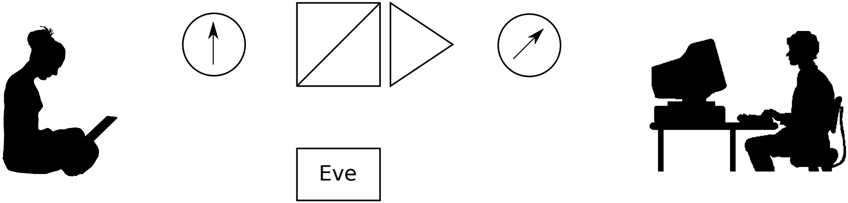
The BB84 protocol

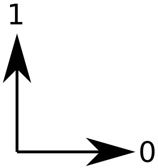
Developed by Bennett and Brassard in 1984.



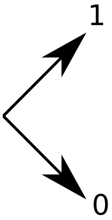
The BB84 protocol

Developed by Bennett and Brassard in 1984.





1. Alice encodes with a random basis.
2. Bob measures with a random basis.
3. After all transfers, Alice and Bob publically reveal basis choices.
4. When choices agree, they check agreement on a subset of data.
5. Data not revealed becomes the key.



The BB84 protocol

Eve chooses a different basis $\frac{1}{2}$ of the time. Each time she causes disagreement with probability $\frac{1}{2}$.

The BB84 protocol

Eve chooses a different basis $\frac{1}{2}$ of the time. Each time she causes disagreement with probability $\frac{1}{2}$. This has been used to safeguard the 2007 Swiss election.

The BB84 protocol

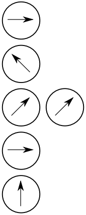
Eve chooses a different basis $\frac{1}{2}$ of the time. Each time she causes disagreement with probability $\frac{1}{2}$. This has been used to safeguard the 2007 Swiss election.

Imperfect devices have allowed their QKD systems to be defeated.

The BB84 protocol

Eve chooses a different basis $\frac{1}{2}$ of the time. Each time she causes disagreement with probability $\frac{1}{2}$. This has been used to safeguard the 2007 Swiss election.

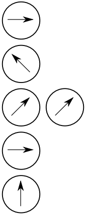
Imperfect devices have allowed their QKD systems to be defeated.



The BB84 protocol

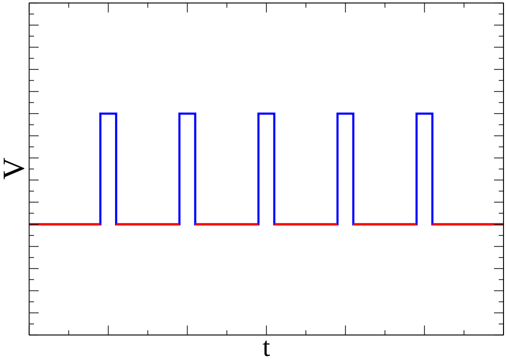
Eve chooses a different basis $\frac{1}{2}$ of the time. Each time she causes disagreement with probability $\frac{1}{2}$. This has been used to safeguard the 2007 Swiss election.

Imperfect devices have allowed their QKD systems to be defeated.

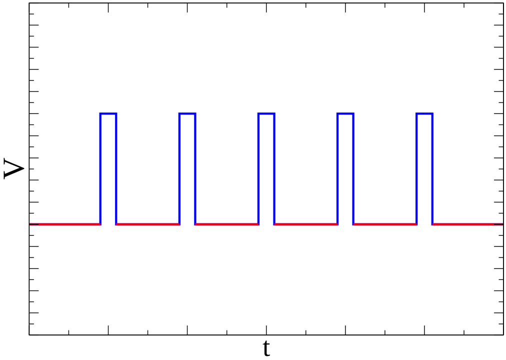


When two photons accidentally arrive, Eve can pass one along, store the other and wait to learn the right basis [PhysRevA **51**, 1863–1869, 1995].

Hacking avalanche photodiodes



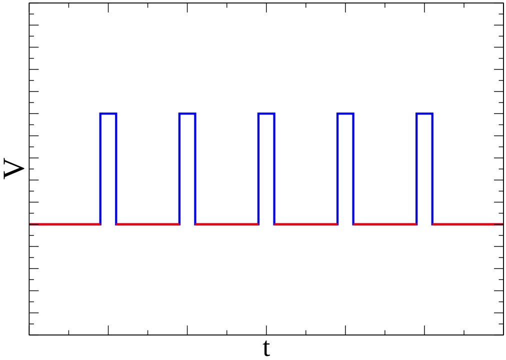
Hacking avalanche photodiodes



Above the breakdown, detectors are very sensitive and click for single photons.

Otherwise they respond linearly and only click for light above power P_0.

Hacking avalanche photodiodes



Above the breakdown, detectors are very sensitive and click for single photons.

Otherwise they respond linearly and only click for light above power P_0.

If Bob's APD is ever in linear mode (*e.g.* the quench after Alice's photon), Eve can use blinding to keep it this way.

Hacking avalanche photodiodes

1. Eve chooses bases and measures bits as they come.
2. She retransmits a beam just above P_0 to Bob when his detector is linear.
3. If their bases agree, Bob sees the same as Eve. Otherwise he thinks event was dropped.
4. Eve has whatever bits Alice tells Bob to keep.
5. No intrusion is detected because checking is only done when Alice, Bob and Eve share a basis.

Hacking avalanche photodiodes

1. Eve chooses bases and measures bits as they come.
2. She retransmits a beam just above P_0 to Bob when his detector is linear.
3. If their bases agree, Bob sees the same as Eve. Otherwise he thinks event was dropped.
4. Eve has whatever bits Alice tells Bob to keep.
5. No intrusion is detected because checking is only done when Alice, Bob and Eve share a basis.

Protocols immune to weaknesses in the device are possible with device independent QKD.

Hacking avalanche photodiodes

1. Eve chooses bases and measures bits as they come.
2. She retransmits a beam just above P_0 to Bob when his detector is linear.
3. If their bases agree, Bob sees the same as Eve. Otherwise he thinks event was dropped.
4. Eve has whatever bits Alice tells Bob to keep.
5. No intrusion is detected because checking is only done when Alice, Bob and Eve share a basis.

Protocols immune to weaknesses in the device are possible with device independent QKD.
Vazirani and Vidick have developed the most robust one to date [PRL **113**, 140501, 2014].

QKD with entanglement

QKD with entanglement

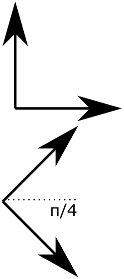
$$\rightarrow |\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \leftarrow$$

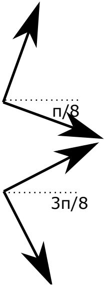
QKD with entanglement

$$\rightarrow |\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \leftarrow$$

QKD with entanglement

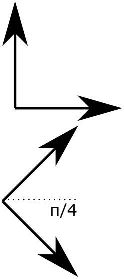
$$\rightarrow |\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \leftarrow$$



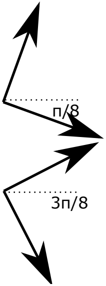


QKD with entanglement

$$\rightarrow |\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \leftarrow$$



Alice uses input $x_i \in \{0, 1\}$ to decide on basis for output a_i.
Bob uses input $y_i \in \{0, 1\}$ to decide on basis for output b_i.
If outputs saturate the Bell inequality, nothing else can be entangled with the system [PRL **67**, 661–663, 1991].



QKD with entanglement

For $(x, y) = (0, 0)$, if Alice gets a 0, project onto $\cos\left(\frac{\pi}{8}\right)\langle 0| + \sin\left(\frac{\pi}{8}\right)\langle 1|$.

QKD with entanglement

For $(x, y) = (0, 0)$, if Alice gets a 0, project onto $\cos\left(\frac{\pi}{8}\right)\langle 0| + \sin\left(\frac{\pi}{8}\right)\langle 1|$.

$$P(\mathrm{same}) = \cos^2\left(\frac{\pi}{8}\right)$$

QKD with entanglement

For $(x, y) = (0, 0)$, if Alice gets a 0, project onto $\cos\left(\frac{\pi}{8}\right)\langle 0| + \sin\left(\frac{\pi}{8}\right)\langle 1|$.

$$P(\mathrm{same}) = \cos^2\left(\frac{\pi}{8}\right)$$

For $(x, y) = (0, 1)$, if Alice gets a 0, project onto $\cos\left(\frac{3\pi}{8}\right)\langle 0| + \sin\left(\frac{3\pi}{8}\right)\langle 1|$.

$$P(\mathrm{different}) = 1 - \cos^2\left(\frac{3\pi}{8}\right)$$

QKD with entanglement

For $(x, y) = (0, 0)$, if Alice gets a 0, project onto $\cos\left(\frac{\pi}{8}\right)\langle 0| + \sin\left(\frac{\pi}{8}\right)\langle 1|$.

$$P(\text{same}) = \cos^2\left(\frac{\pi}{8}\right)$$

For $(x, y) = (0, 1)$, if Alice gets a 0, project onto $\cos\left(\frac{3\pi}{8}\right)\langle 0| + \sin\left(\frac{3\pi}{8}\right)\langle 1|$.

$$P(\text{different}) = 1 - \cos^2\left(\frac{3\pi}{8}\right)$$

In a fraction of "Bell rounds" B, Alice and Bob should check if $a_i \oplus b_i = x_i \wedge y_i$ is satisfied $\cos^2\left(\frac{\pi}{8}\right)$ of the time.

QKD with entanglement

For $(x, y) = (0, 0)$, if Alice gets a 0, project onto $\cos\left(\frac{\pi}{8}\right)\langle 0| + \sin\left(\frac{\pi}{8}\right)\langle 1|$.

$$P(\mathrm{same}) = \cos^2\left(\frac{\pi}{8}\right)$$

For $(x, y) = (0, 1)$, if Alice gets a 0, project onto $\cos\left(\frac{3\pi}{8}\right)\langle 0| + \sin\left(\frac{3\pi}{8}\right)\langle 1|$.

$$P(\mathrm{different}) = 1 - \cos^2\left(\frac{3\pi}{8}\right)$$

In a fraction of "Bell rounds" B, Alice and Bob should check if $a_i \oplus b_i = x_i \wedge y_i$ is satisfied $\cos^2\left(\frac{\pi}{8}\right)$ of the time. To form a key, "Check rounds" C have Alice use the $\frac{3\pi}{8}$ basis.

QKD with entanglement

For $(x, y) = (0, 0)$, if Alice gets a 0, project onto $\cos\left(\frac{\pi}{8}\right)\langle 0| + \sin\left(\frac{\pi}{8}\right)\langle 1|$.

$$P(\text{same}) = \cos^2\left(\frac{\pi}{8}\right)$$

For $(x, y) = (0, 1)$, if Alice gets a 0, project onto $\cos\left(\frac{3\pi}{8}\right)\langle 0| + \sin\left(\frac{3\pi}{8}\right)\langle 1|$.

$$P(\text{different}) = 1 - \cos^2\left(\frac{3\pi}{8}\right)$$

In a fraction of "Bell rounds" B, Alice and Bob should check if $a_i \oplus b_i = x_i \wedge y_i$ is satisfied $\cos^2\left(\frac{\pi}{8}\right)$ of the time. To form a key, "Check rounds" C have Alice use the $\frac{3\pi}{8}$ basis.

$$\left|\left|\rho_{KE} - \rho_{\not K} \otimes \rho_E\right|\right| < \epsilon$$

$$\rho_{\not K} = diag\left(\frac{1}{2^{|K|}}, \ldots, \frac{1}{2^{|K|}}\right)$$

Privacy amplification

If they notice a Bell discrepancy, Alice and Bob must shorten their key to reduce Eve's knowledge.

Privacy amplification

If they notice a Bell discrepancy, Alice and Bob must shorten their key to reduce Eve's knowledge. A non-uniform

$$X \in \{0,1\}^p, \qquad P(X = X') \leq \frac{1}{2^q}$$

has $H_{min}(X) = q$.

Privacy amplification

If they notice a Bell discrepancy, Alice and Bob must shorten their key to reduce Eve's knowledge. A non-uniform

$$X \in \{0,1\}^p, \qquad P(X = X') \leq \frac{1}{2^q}$$

has $H_{min}(X) = q$. A hash function acts as $f : \{0,1\}^p \to \{0,1\}^r$.

Privacy amplification

If they notice a Bell discrepancy, Alice and Bob must shorten their key to reduce Eve's knowledge. A non-uniform

$$X \in \{0,1\}^p, \qquad P(X = X') \leq \frac{1}{2^q}$$

has $H_{min}(X) = q$. A hash function acts as $f : \{0,1\}^p \to \{0,1\}^r$. A family of 2^s such functions is parwise-universal if for all $x \neq x'$, at most $\frac{1}{2^r}$ of the functions satisfy $f(x) = f(x')$.

Privacy amplification

If they notice a Bell discrepancy, Alice and Bob must shorten their key to reduce Eve's knowledge. A non-uniform

$$X \in \{0,1\}^p, \qquad P(X = X') \leq \frac{1}{2^q}$$

has $H_{min}(X) = q$. A hash function acts as $f : \{0,1\}^p \to \{0,1\}^r$. A family of 2^s such functions is parwise-universal if for all $x \neq x'$, at most $\frac{1}{2^r}$ of the functions satisfy $f(x) = f(x')$. Example:

x	1	2	$\dots$	2^r	$2^r + 1$	$\dots$	2^{r+1}
$f_1(x)$	1	2	$\dots$	2^r	1	$\dots$	2^r
$f_2(x)$	2^r	1	$\dots$	$2^r - 1$	1	$\dots$	2^r
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$f_{2^r}(x)$	2	3	$\dots$	1	1	$\dots$	2^r

Privacy amplification

Leftover Hash Lemma

Supposed we have 2^s *pairwise universal hash-functions that output* r *bit strings. If* $r \leq H_{min}(X) - 2\log_2\left(\frac{1}{\epsilon}\right)$ *and the functions are chosen uniformly,* $(F, F(X))$ *is* ϵ *away from the uniform distribution on* $r + s$ *bits.*

Privacy amplification

Leftover Hash Lemma

Supposed we have 2^s pairwise universal hash-functions that output r bit strings. If $r \le H_{min}(X) - 2\log_2\left(\frac{1}{\epsilon}\right)$ and the functions are chosen uniformly, $(F, F(X))$ is ϵ away from the uniform distribution on $r+s$ bits.

Proof.

$$
\begin{aligned}
P((F,F(X)) &= (F',F'(X'))) = P(F=F')P(F(X)=F(X')) \\
&= P(F=F')\left[P(X=X') + \frac{1}{2^r}\right] \\
&\le \frac{1}{2^s}\left[\frac{1}{2^q} + \frac{1}{2^r}\right] \\
&= \frac{1}{2^{r+s}}\left[\frac{1}{2^{q-r}} + 1\right] \\
&\le \frac{1}{2^{r+s}}\left[\epsilon^2 + 1\right]
\end{aligned}
$$

Information reconciliation

Alice and Bob pick and communicate a hash function after the measurements but they might apply it to different keys.

Information reconciliation

Alice and Bob pick and communicate a hash function after the measurements but they might apply it to different keys.

1. Alice sends Bob an l bit hash of her key X.
2. Bob sees if his key Y hashes to the same value.
3. If not, he modifies it to some $\hat{X}$ in the support of the Y marginal distribution.

Information reconciliation

Alice and Bob pick and communicate a hash function after the measurements but they might apply it to different keys.

1. Alice sends Bob an l bit hash of her key X.
2. Bob sees if his key Y hashes to the same value.
3. If not, he modifies it to some $\hat{X}$ in the support of the Y marginal distribution.

$$\begin{aligned} P(\hat{X} \neq X) &= |supp(Y)|\, P(F(\hat{X}) = F(X)) \\ &= |supp(Y)|\, \frac{1}{2^l} \\ &\leq \epsilon \end{aligned}$$

Information reconciliation

Alice and Bob pick and communicate a hash function after the measurements but they might apply it to different keys.

1. Alice sends Bob an l bit hash of her key X.
2. Bob sees if his key Y hashes to the same value.
3. If not, he modifies it to some $\hat{X}$ in the support of the Y marginal distribution.

$$\begin{aligned} P(\hat{X} \neq X) &= |supp(Y)|\, P(F(\hat{X}) = F(X)) \\ &= |supp(Y)|\, \frac{1}{2^l} \\ &\leq \epsilon \end{aligned}$$

This says that $l = H_{max}(Y) + \log_2\left(\frac{1}{\epsilon}\right)$.

Information reconciliation

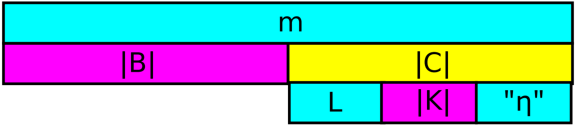
Alice and Bob pick and communicate a hash function after the measurements but they might apply it to different keys.

1. Alice sends Bob an l bit hash of her key X.
2. Bob sees if his key Y hashes to the same value.
3. If not, he modifies it to some $\hat{X}$ in the support of the Y marginal distribution.

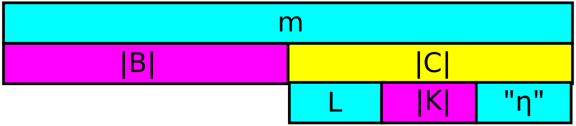
$$\begin{aligned} P(\hat{X} \neq X) &= |supp(Y)|\, P(F(\hat{X}) = F(X)) \\ &= |supp(Y)|\, \frac{1}{2^l} \\ &\leq \epsilon \end{aligned}$$

This says that $l = H_{max}(Y) + \log_2\left(\frac{1}{\epsilon}\right)$. Think of the UNIX program `md5sum`.

Key length with noise

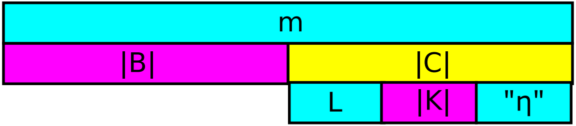


Key length with noise



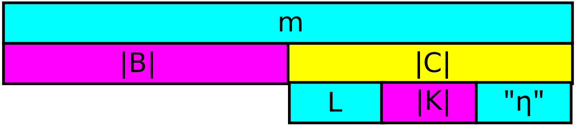
The noise η is defined as the difference between the Bell success probability and $\cos^2\left(\frac{\pi}{8}\right)$.

Key length with noise



The noise η is defined as the difference between the Bell success probability and $\cos^2\left(\frac{\pi}{8}\right)$. Vazirani and Vidick's bound uses the binary entropy $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$.

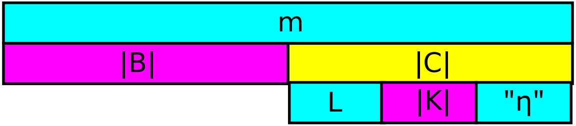
Key length with noise



The noise η is defined as the difference between the Bell success probability and $\cos^2\left(\frac{\pi}{8}\right)$. Vazirani and Vidick's bound uses the binary entropy $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$.

$$|K| = H^{\epsilon}_{min}(B_C|E) - l - O\left(\log_2\left(\frac{1}{\epsilon}\right)\right) \qquad \Big| \ \text{PA}$$

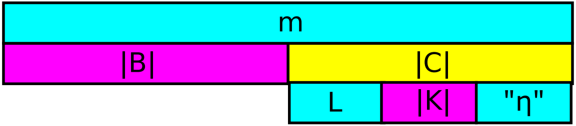
Key length with noise



The noise η is defined as the difference between the Bell success probability and $\cos^2\left(\frac{\pi}{8}\right)$. Vazirani and Vidick's bound uses the binary entropy $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$.

$$\begin{array}{l|l} |K| = H^{\epsilon}_{min}(B_C|E) - l - O\left(\log_2\left(\frac{1}{\epsilon}\right)\right) & \text{PA} \\ |K| \geq H^{\epsilon}_{min}(B_C|E) - H^{\epsilon}_{max}(B_C|A_C) - O\left(\log_2\left(\frac{1}{\epsilon}\right)\right) & \text{IR} \end{array}$$

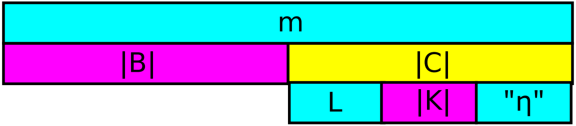
Key length with noise



The noise η is defined as the difference between the Bell success probability and $\cos^2\left(\frac{\pi}{8}\right)$. Vazirani and Vidick's bound uses the binary entropy $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$.

$$
\begin{array}{l|l}
|K| = H^{\epsilon}_{min}(B_C|E) - l - O\left(\log_2\left(\frac{1}{\epsilon}\right)\right) & \text{PA} \\
|K| \geq H^{\epsilon}_{min}(B_C|E) - H^{\epsilon}_{max}(B_C|A_C) - O\left(\log_2\left(\frac{1}{\epsilon}\right)\right) & \text{IR} \\
|K| \geq H^{\epsilon}_{min}(B_C|E) - H\left(\frac{11}{10}\eta\right)|C| - O\left(\log_2\left(\frac{1}{\epsilon}\right)\right) & \text{Noise estimate}
\end{array}
$$

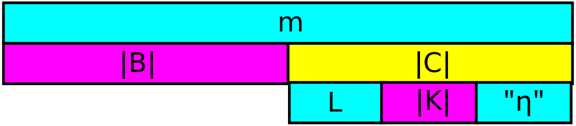
Key length with noise



The noise η is defined as the difference between the Bell success probability and $\cos^2\left(\frac{\pi}{8}\right)$. Vazirani and Vidick's bound uses the binary entropy $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$.

$$
\begin{array}{l|l}
|K| = H^{\epsilon}_{min}(B_C|E) - l - O\left(\log_2\left(\frac{1}{\epsilon}\right)\right) & \text{PA} \\
|K| \geq H^{\epsilon}_{min}(B_C|E) - H^{\epsilon}_{max}(B_C|A_C) - O\left(\log_2\left(\frac{1}{\epsilon}\right)\right) & \text{IR} \\
|K| \geq H^{\epsilon}_{min}(B_C|E) - H\left(\frac{11}{10}\eta\right)|C| - O\left(\log_2\left(\frac{1}{\epsilon}\right)\right) & \text{Noise estimate} \\
|K| \geq \kappa(\eta)|C| - H\left(\frac{11}{10}\eta\right)|C| - O\left(\log_2\left(\frac{1}{\epsilon}\right)\right) & \text{Rest of the paper}
\end{array}
$$

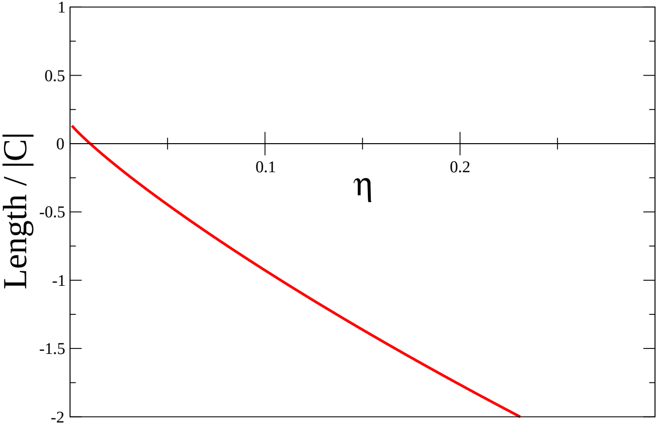
Key length with noise



The noise η is defined as the difference between the Bell success probability and $\cos^2\left(\frac{\pi}{8}\right)$. Vazirani and Vidick's bound uses the binary entropy $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$.

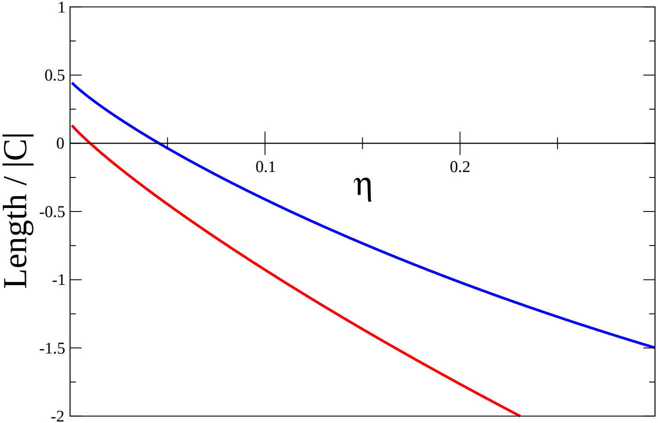
$$
\begin{array}{l|l}
|K| = H^{\epsilon}_{min}(B_C|E) - l - O\left(\log_2\left(\frac{1}{\epsilon}\right)\right) & \text{PA} \\
|K| \geq H^{\epsilon}_{min}(B_C|E) - H^{\epsilon}_{max}(B_C|A_C) - O\left(\log_2\left(\frac{1}{\epsilon}\right)\right) & \text{IR} \\
|K| \geq H^{\epsilon}_{min}(B_C|E) - H\left(\frac{11}{10}\eta\right)|C| - O\left(\log_2\left(\frac{1}{\epsilon}\right)\right) & \text{Noise estimate} \\
|K| \geq \kappa(\eta)|C| - H\left(\frac{11}{10}\eta\right)|C| - O\left(\log_2\left(\frac{1}{\epsilon}\right)\right) & \text{Rest of the paper} \\
|K| \geq \left[\kappa(\eta) - H\left(\frac{11}{10}\eta\right) - O\left(\frac{1}{m}\log_2\left(\frac{1}{\epsilon}\right)\right)\right]|C| & \text{Since } |C| \approx \frac{m}{6}
\end{array}
$$

Key length with noise



$$\kappa(\eta) = \frac{\sqrt{2} - 1}{4 \log 2} - \frac{4}{\log 2}\eta$$

Key length with noise



$$\kappa(\eta) > \frac{\sqrt{2}-1}{4\log 2} - \frac{4}{\log 2}\eta$$

$$\kappa(\eta) = -\frac{11}{3}\log_2\left(\frac{11}{12} + \frac{2}{3}\eta\right)$$

"A pair of entangled photons is like a pair of hippies who are spiritually in tune with one another but not voicing coherent opinions about anything."

—Charles Bennett