Title: Quantum Key Distribution Networks

Date: Jun 02, 2007 03:30 PM

URL: http://pirsa.org/07060013

Abstract: Current physical implementations of quantum key distribution (QKD) require communicating parties to be close together. We will explore methods for allowing parties separated by long distances to communicate by combining many QKD links in a network and discuss the resulting security properties.

University of Waterloo

IQC Institute for Quantum Computing

Quantum steganography

Douglas Stebila[1]
Joint work with Lana Sheridan

Institute for Quantum Computing,
University of Waterloo, Waterloo, Ontario, Canada

Saturday, June 2, 2007

[1] Supported in part by Canada's NSERC and Sun Microsystems.

What is steganography?

What is steganography?

- Steganography is the hiding of a message in a communications stream so that its presence goes undetected by anyone except the intended recipient.

What is steganography?

- Steganography is the hiding of a message in a communications stream so that its presence goes undetected by anyone except the intended recipient.
- No active or passive adversary should be able to detect that you're doing something out of the ordinary.

What is steganography?

- Steganography is the hiding of a message in a communications stream so that its presence goes undetected by anyone except the intended recipient.
- No active or passive adversary should be able to detect that you're doing something out of the ordinary.
- Steganography has been used in espionage, as a form of encryption, and in watermarking.

A sample image (Wikipedia)

A sample image (Wikipedia)

Decoding algorithm:

- Filter out everything except the lower two bits of each 8-bit colour value for each pixel.

A sample image (Wikipedia)

Decoding algorithm:

- Filter out everything except the lower two bits of each 8-bit colour value for each pixel.
- This induces a 6-bit (2 red, 2 blue, 2 green) hidden image.

A sample image (Wikipedia)

Is this cryptography?

- The security of this image hiding scheme is hard to quantify cryptographically.

Is this cryptography?

- The security of this image hiding scheme is hard to quantify cryptographically.
- If someone knows the algorithm you might be using to hide your data, then they can easily find messages just by applying the decoding algorithm to every communication they see.

Is this cryptography?

- The security of this image hiding scheme is hard to quantify cryptographically.
- If someone knows the algorithm you might be using to hide your data, then they can easily find messages just by applying the decoding algorithm to every communication they see.
- There is no secret information shared between the sender and receiver other than the knowledge of which steganographic algorithm was applied.

Is this cryptography?

- The security of this image hiding scheme is hard to quantify cryptographically.
- If someone knows the algorithm you might be using to hide your data, then they can easily find messages just by applying the decoding algorithm to every communication they see.
- There is no secret information shared between the sender and receiver other than the knowledge of which steganographic algorithm was applied.
- In cryptography, we usually have greater trust in schemes where the entire algorithm is publicly known, and only a secret key is shared between the sender and receiver.

A few definitions

- Covertext: the original messages you would expect to see in a normal communication.

A few definitions

- Covertext: the original messages you would expect to see in a normal communication.
- Stegotext: a communication with a hidden message embedded inside it.

A few definitions

- Covertext: the original messages you would expect to see in a normal communication.
- Stegotext: a communication with a hidden message embedded inside it.
- Encoding function: a function that constructs a stegotext to hide a given message.

A few definitions

- Covertext: the original messages you would expect to see in a normal communication.
- Stegotext: a communication with a hidden message embedded inside it.
- Encoding function: a function that constructs a stegotext to hide a given message.
- Decoding function: a function that recovers a hidden message from a stegotext.

An information-theoretic framework

An information-theoretic framework for steganography[2]

- Model things using probability distributions.

[2] C. Cachin. An information-theoretic model for steganography. *Information and Computation*, 192(1):41–56, July 2004. Eprint: `http://eprint.iacr.org/2000/028.pdf`

An information-theoretic framework for steganography[2]

- Model things using probability distributions.
- Let $\mathcal{C}$ be the probability distribution of covertexts.

[2] C. Cachin. An information-theoretic model for steganography. *Information and Computation*, 192(1):41–56, July 2004. Eprint: `http://eprint.iacr.org/2000/028.pdf`

An information-theoretic framework for steganography[2]

- Model things using probability distributions.
- Let $\mathcal{C}$ be the probability distribution of covertexts.
- Let $\mathcal{K}$ be the probability distribution of keys shared between the sender and the receiver.

[2] C. Cachin. An information-theoretic model for steganography. *Information and Computation*, 192(1):41–56, July 2004. Eprint: `http://eprint.iacr.org/2000/028.pdf`

An information-theoretic framework for steganography[2]

- Model things using probability distributions.
- Let $\mathcal{C}$ be the probability distribution of covertexts.
- Let $\mathcal{K}$ be the probability distribution of keys shared between the sender and the receiver.
- Let $\mathcal{M}$ be the probability distribution of messages that the sender wishes to send.

[2] C. Cachin. An information-theoretic model for steganography. *Information and Computation*, 192(1):41–56, July 2004. Eprint: `http://eprint.iacr.org/2000/028.pdf`

An information-theoretic framework for steganography[2]

- Model things using probability distributions.
- Let $\mathcal{C}$ be the probability distribution of covertexts.
- Let $\mathcal{K}$ be the probability distribution of keys shared between the sender and the receiver.
- Let $\mathcal{M}$ be the probability distribution of messages that the sender wishes to send.
- Let $E(m, k)$ be an encoding function that constructs a stegotext to encode the hidden message m under the key k.

[2] C. Cachin. An information-theoretic model for steganography. *Information and Computation*, 192(1):41–56, July 2004. Eprint: `http://eprint.iacr.org/2000/028.pdf`

An information-theoretic framework for steganography[2]

- Model things using probability distributions.
- Let $\mathcal{C}$ be the probability distribution of covertexts.
- Let $\mathcal{K}$ be the probability distribution of keys shared between the sender and the receiver.
- Let $\mathcal{M}$ be the probability distribution of messages that the sender wishes to send.
- Let $E(m, k)$ be an encoding function that constructs a stegotext to encode the hidden message m under the key k.
- Let $D(s, k)$ be a decoding function that recovers a hidden message from a stegotext s using the key k.

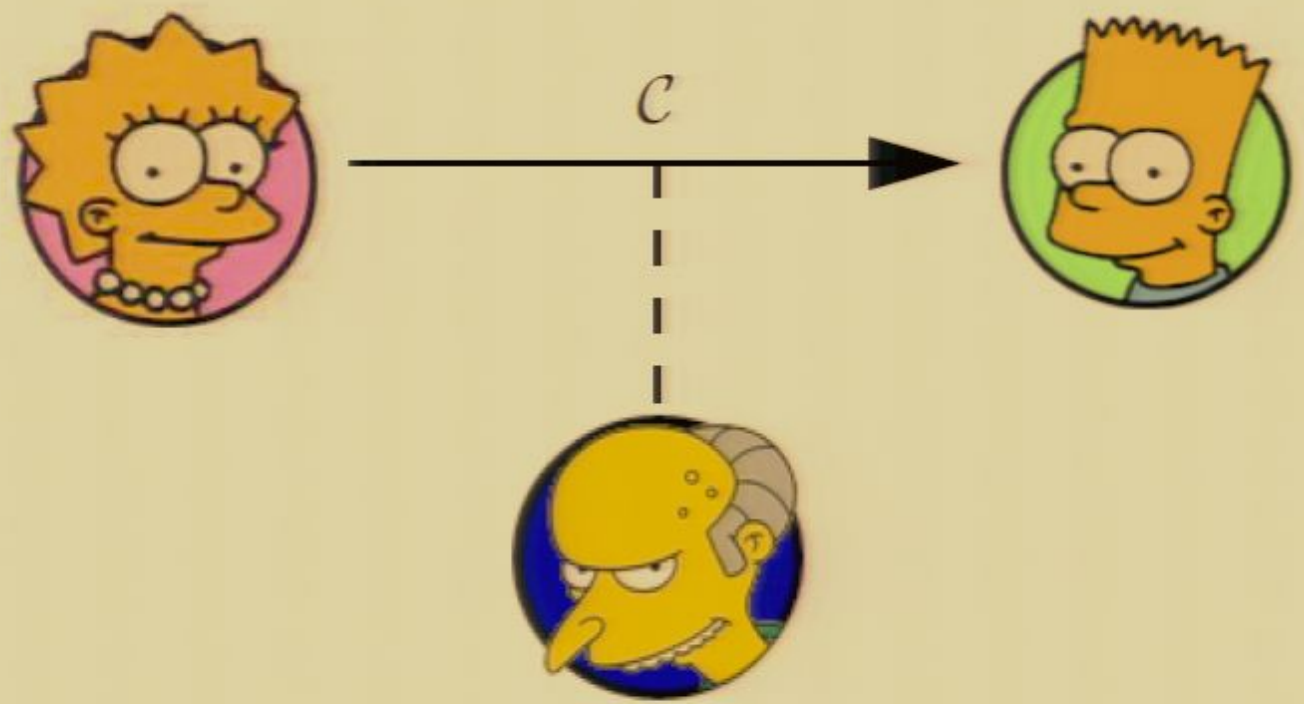
[2] C. Cachin. An information-theoretic model for steganography. *Information and Computation*, 192(1):41–56, July 2004. Eprint: `http://eprint.iacr.org/2000/028.pdf`

An information-theoretic framework for steganography[2]

- Model things using probability distributions.
- Let $\mathcal{C}$ be the probability distribution of covertexts.
- Let $\mathcal{K}$ be the probability distribution of keys shared between the sender and the receiver.
- Let $\mathcal{M}$ be the probability distribution of messages that the sender wishes to send.
- Let $E(m, k)$ be an encoding function that constructs a stegotext to encode the hidden message m under the key k.
- Let $D(s, k)$ be a decoding function that recovers a hidden message from a stegotext s using the key k.
- Let $\mathcal{S}$ be probability distribution of stegotexts created by E using messages $\mathcal{M}$ and keys $\mathcal{K}$.

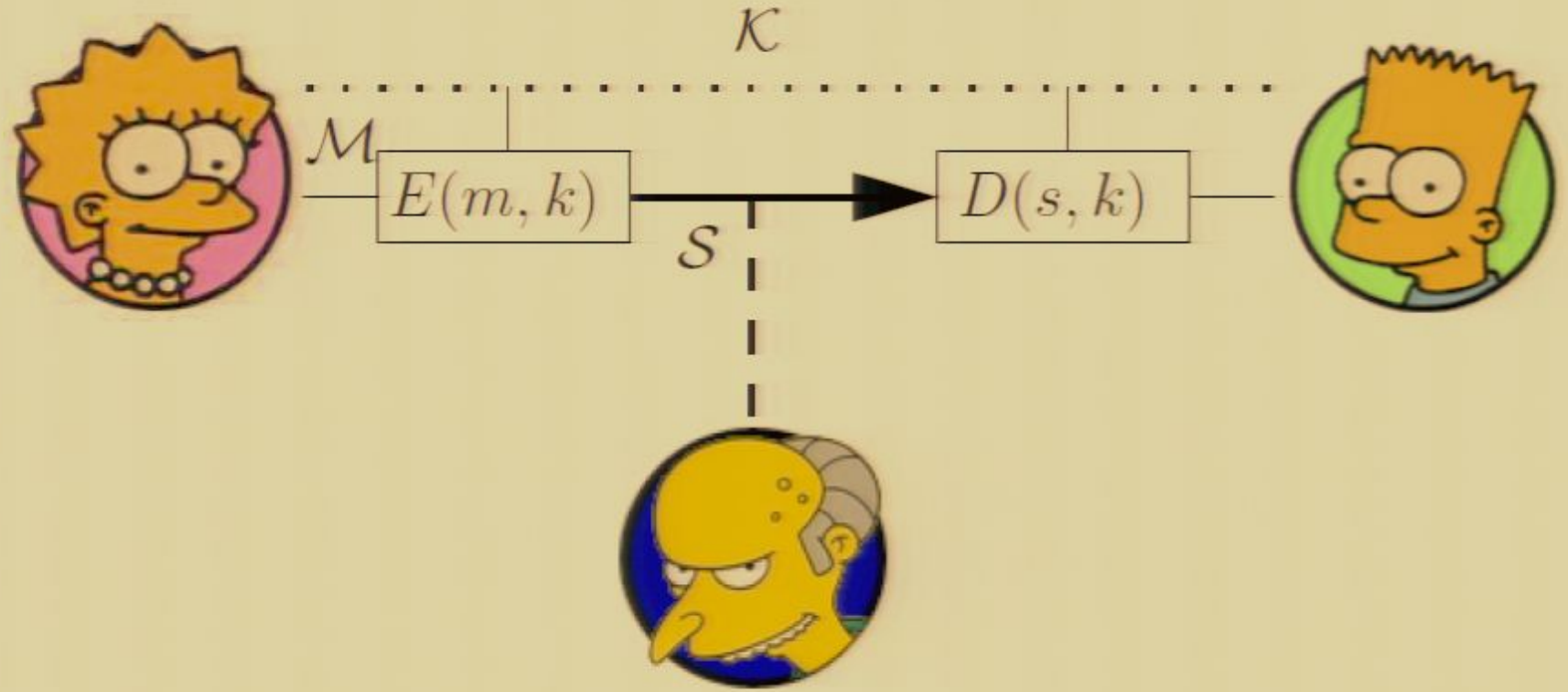
[2] C. Cachin. An information-theoretic model for steganography. *Information and Computation*, 192(1):41–56, July 2004. Eprint: `http://eprint.iacr.org/2000/028.pdf`

Normal communication



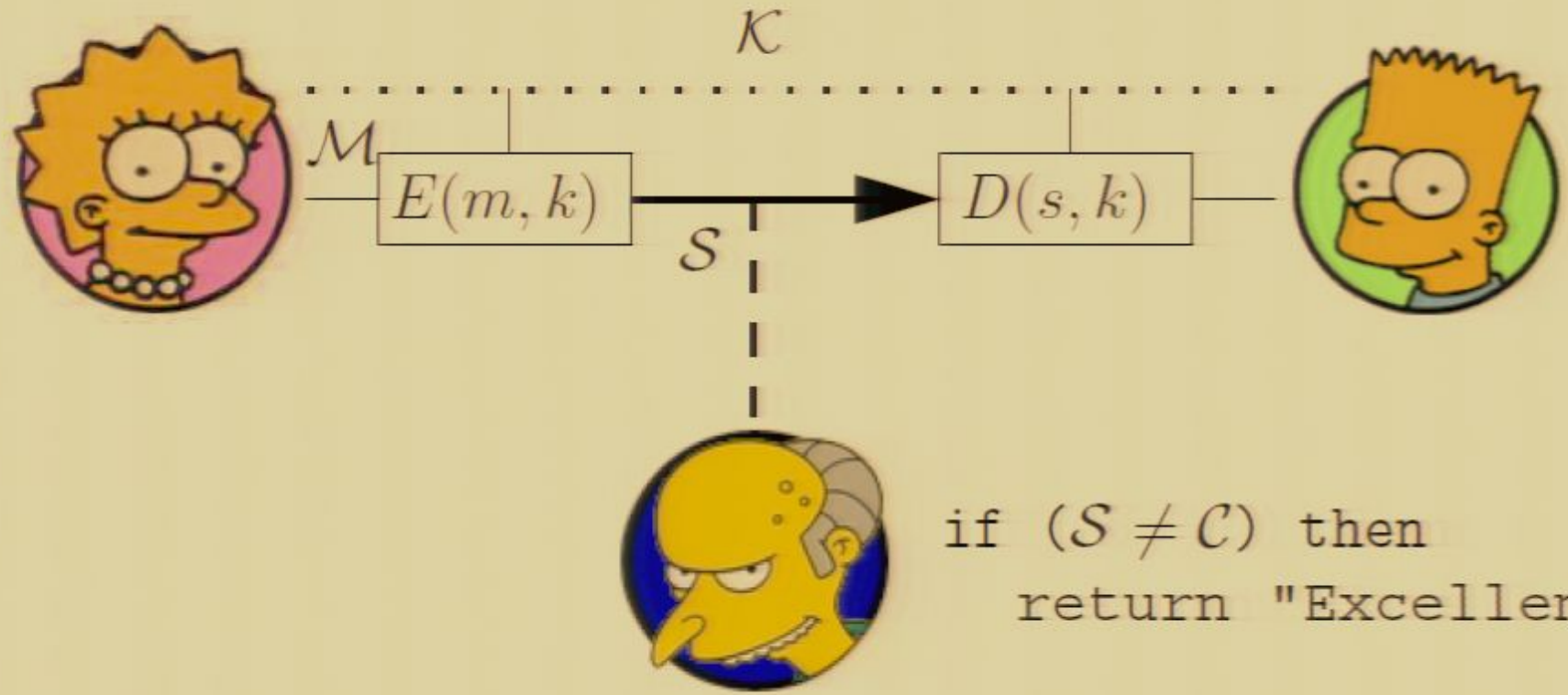
Eavesdropper sees communication distributed according to covertext distribution $\mathcal{C}$.

Steganographic communication



Eavesdropper sees communication distributed according to stegotext distribution $\mathcal{S}$.

Steganographic communication



Eavesdropper sees communication distributed according to stegotext distribution $\mathcal{S}$.

Security: relative entropy of probability distributions

- To keep an eavesdropper unaware of whether steganographic communication is occurring or not, we wish for $\mathcal{S}$ and $\mathcal{C}$ to be indistinguishable.

Security: relative entropy of probability distributions

- To keep an eavesdropper unaware of whether steganographic communication is occurring or not, we wish for $\mathcal{S}$ and $\mathcal{C}$ to be indistinguishable.
- The relative entropy $\mathcal{D}(\mathcal{A}||\mathcal{B})$ between two probability distributions $\mathcal{A}$ and $\mathcal{B}$ both on sets $\mathcal{T}$

Security: relative entropy of probability distributions

- To keep an eavesdropper unaware of whether steganographic communication is occurring or not, we wish for $\mathcal{S}$ and $\mathcal{C}$ to be indistinguishable.
- The relative entropy $\mathcal{D}(\mathcal{A}||\mathcal{B})$ between two probability distributions $\mathcal{A}$ and $\mathcal{B}$ both on sets $\mathcal{T}$ is

$$\mathcal{D}(\mathcal{A}||\mathcal{B}) = \sum_{t \in \mathcal{T}} \mathbb{P}(\mathcal{A} = t) \log_2 \left(\frac{\mathbb{P}(\mathcal{A} = t)}{\mathbb{P}(\mathcal{B} = t)} \right)$$

(with $0 \log \frac{0}{0} = 0$ and $p \log \frac{p}{0} = \infty$ for $p > 0$).

Security: relative entropy of probability distributions

- To keep an eavesdropper unaware of whether steganographic communication is occurring or not, we wish for $\mathcal{S}$ and $\mathcal{C}$ to be indistinguishable.
- The relative entropy $\mathcal{D}(\mathcal{A}||\mathcal{B})$ between two probability distributions $\mathcal{A}$ and $\mathcal{B}$ both on sets $\mathcal{T}$ is

$$\mathcal{D}(\mathcal{A}||\mathcal{B}) = \sum_{t\in\mathcal{T}} \mathbb{P}(\mathcal{A}=t)\log_2\left(\frac{\mathbb{P}(\mathcal{A}=t)}{\mathbb{P}(\mathcal{B}=t)}\right)$$

  (with $0\log\frac{0}{0}=0$ and $p\log\frac{p}{0}=\infty$ for $p>0$).
- $\mathcal{A}=\mathcal{B}$ if and only if $\mathcal{D}(\mathcal{A}||\mathcal{B})=0$. The relative entropy is always non-negative, although it is not symmetric and hence not a true distance measure.

Security: relative entropy of probability distributions

- The relative entropy describes, in some sense, how well two probability distributions can be distinguished having observed outputs from one of them.

Security: relative entropy of probability distributions

- The relative entropy describes, in some sense, how well two probability distributions can be distinguished having observed outputs from one of them.
- A stegosystem is perfectly secure against passive adversaries if $\mathcal{D}(\mathcal{C}||\mathcal{S}) = 0$.

Security: relative entropy of probability distributions

- The relative entropy describes, in some sense, how well two probability distributions can be distinguished having observed outputs from one of them.
- A stegosystem is perfectly secure against passive adversaries if $\mathcal{D}(\mathcal{C}||\mathcal{S}) = 0$.
- A stegosystem is ϵ-secure against passive adversaries if $\mathcal{D}(\mathcal{C}||\mathcal{S}) \leq \epsilon$.

Information rate

- In addition to being secure, we want a stegosystem to also communicate some information.

Information rate

- In addition to being secure, we want a stegosystem to also communicate some information.
- Let $\mathcal{M}'$ be the probability distribution of messages decoded by the recipient based on key distribution $\mathcal{K}$ and sender message distribution $\mathcal{M}$.

Information rate

- In addition to being secure, we want a stegosystem to also communicate some information.
- Let $\mathcal{M}'$ be the probability distribution of messages decoded by the recipient based on key distribution $\mathcal{K}$ and sender message distribution $\mathcal{M}$.
- The information rate of a stegosystem is given by the mutual information $I(\mathcal{M}'; \mathcal{M})$.

Information rate

- In addition to being secure, we want a stegosystem to also communicate some information.
- Let $\mathcal{M}'$ be the probability distribution of messages decoded by the recipient based on key distribution $\mathcal{K}$ and sender message distribution $\mathcal{M}$.
- The information rate of a stegosystem is given by the mutual information $I(\mathcal{M}'; \mathcal{M})$.
- We want the information rate to be greater than 0, typically bounded away from 0.

Classical example: one-time pad

- The one-time pad can be used to create a stegosystem if the covertext and key distributions are uniform.

Classical example: one-time pad

- The one-time pad can be used to create a stegosystem if the covertext and key distributions are uniform.
- Covertexts $\mathcal{C}$: uniform distribution on $\{0,1\}^n$

Classical example: one-time pad

- The one-time pad can be used to create a stegosystem if the covertext and key distributions are uniform.

- Covertexts $\mathcal{C}$: uniform distribution on $\{0,1\}^n$
- Keys $\mathcal{K}$: uniform distribution on $\{0,1\}^n$

Classical example: one-time pad

- The one-time pad can be used to create a stegosystem if the covertext and key distributions are uniform.

- Covertexts $\mathcal{C}$: uniform distribution on $\{0,1\}^n$
- Keys $\mathcal{K}$: uniform distribution on $\{0,1\}^n$
- Messages $\mathcal{M}$: any distribution on $\{0,1\}^n$

Classical example: one-time pad

- The one-time pad can be used to create a stegosystem if the covertext and key distributions are uniform.

- Covertexts $\mathcal{C}$: uniform distribution on $\{0,1\}^n$
- Keys $\mathcal{K}$: uniform distribution on $\{0,1\}^n$
- Messages $\mathcal{M}$: any distribution on $\{0,1\}^n$
- Encoding $E(m,k) = m \oplus k$
- Decoding $D(s,k) = s \oplus k$

Classical example: one-time pad

Claim: The one-time pad stegosystem with uniform covertext and key distributions is perfectly secure and has information rate 1.

Classical example: one-time pad

Claim: The one-time pad stegosystem with uniform covertext and key distributions is perfectly secure and has information rate 1.

Proof:

- **Secure**: Since $\mathcal{K}$ is uniformly distributed, so too is $\mathcal{K} \oplus \mathcal{M}$ for any probability distribution $\mathcal{M}$ on $\{0,1\}^n$.

Classical example: one-time pad

Claim: The one-time pad stegosystem with uniform covertext and key distributions is perfectly secure and has information rate 1.

Proof:

- **Secure**: Since $\mathcal{K}$ is uniformly distributed, so too is $\mathcal{K} \oplus \mathcal{M}$ for any probability distribution $\mathcal{M}$ on $\{0,1\}^n$.
- So $\mathcal{S}$ is uniformly distributed. Thus $\mathcal{S} = \mathcal{C}$, so $\mathcal{D}(\mathcal{S}||\mathcal{C}) = 0$ and the scheme is perfectly secure.

Classical example: one-time pad

Claim: The one-time pad stegosystem with uniform covertext and key distributions is perfectly secure and has information rate 1.

Proof:

- **Secure**: Since $\mathcal{K}$ is uniformly distributed, so too is $\mathcal{K} \oplus \mathcal{M}$ for any probability distribution $\mathcal{M}$ on $\{0,1\}^n$.
- So $\mathcal{S}$ is uniformly distributed. Thus $\mathcal{S} = \mathcal{C}$, so $\mathcal{D}(\mathcal{S}||\mathcal{C}) = 0$ and the scheme is perfectly secure.
- **Decoding**: $D(E(m,k),k) = (m \oplus k) \oplus k = m$.

Classical example: one-time pad

Claim: The one-time pad stegosystem with uniform covertext and key distributions is perfectly secure and has information rate 1.

Proof:

- **Secure**: Since $\mathcal{K}$ is uniformly distributed, so too is $\mathcal{K} \oplus \mathcal{M}$ for any probability distribution $\mathcal{M}$ on $\{0,1\}^n$.
- So $\mathcal{S}$ is uniformly distributed. Thus $\mathcal{S} = \mathcal{C}$, so $\mathcal{D}(\mathcal{S}||\mathcal{C}) = 0$ and the scheme is perfectly secure.
- **Decoding**: $D(E(m,k),k) = (m \oplus k) \oplus k = m$.
- So $\mathcal{M}' = \mathcal{M}$. Thus the information rate is n.

Classical example: one-time pad

- The one-time pad can be used to create a stegosystem if the covertext and key distributions are uniform.

- Covertexts $\mathcal{C}$: uniform distribution on $\{0,1\}^n$
- Keys $\mathcal{K}$: uniform distribution on $\{0,1\}^n$
- Messages $\mathcal{M}$: any distribution on $\{0,1\}^n$
- Encoding $E(m,k) = m \oplus k$
- Decoding $D(s,k) = s \oplus k$

Classical example: one-time pad

Claim: The one-time pad stegosystem with uniform covertext and key distributions is perfectly secure and has information rate 1.

Classical example: one-time pad

Claim: The one-time pad stegosystem with uniform covertext and key distributions is perfectly secure and has information rate 1.

Proof:

- **Secure**: Since $\mathcal{K}$ is uniformly distributed, so too is $\mathcal{K} \oplus \mathcal{M}$ for any probability distribution $\mathcal{M}$ on $\{0,1\}^n$.
- So $\mathcal{S}$ is uniformly distributed. Thus $\mathcal{S} = \mathcal{C}$, so $\mathcal{D}(\mathcal{S}||\mathcal{C}) = 0$ and the scheme is perfectly secure.
- **Decoding**: $D(E(m,k),k) = (m \oplus k) \oplus k = m$.

Classical example: one-time pad

Claim: The one-time pad stegosystem with uniform covertext and key distributions is perfectly secure and has information rate 1.

Proof:

- **Secure**: Since $\mathcal{K}$ is uniformly distributed, so too is $\mathcal{K} \oplus \mathcal{M}$ for any probability distribution $\mathcal{M}$ on $\{0,1\}^n$.
- So $\mathcal{S}$ is uniformly distributed. Thus $\mathcal{S} = \mathcal{C}$, so $\mathcal{D}(\mathcal{S}||\mathcal{C}) = 0$ and the scheme is perfectly secure.
- **Decoding**: $D(E(m,k),k) = (m \oplus k) \oplus k = m$.
- So $\mathcal{M}' = \mathcal{M}$. Thus the information rate is n.

Quantum steganography

Quantum steganography framework

- Covertext and stegotext are quantum states, keys and messages are still classical.

Quantum steganography framework

- Covertext and stegotext are quantum states, keys and messages are still classical.
- Let $\mathcal{C}$ be the probability distribution of covertext quantum states, with density matrix $\rho_{\mathcal{C}}$.

Quantum steganography framework

- Covertext and stegotext are quantum states, keys and messages are still classical.
- Let $\mathcal{C}$ be the probability distribution of covertext quantum states, with density matrix $\rho_{\mathcal{C}}$.
- Keys $\mathcal{K}$ and messages $\mathcal{M}$ as before.

Quantum steganography framework

- Covertext and stegotext are quantum states, keys and messages are still classical.
- Let $\mathcal{C}$ be the probability distribution of covertext quantum states, with density matrix $\rho_{\mathcal{C}}$.
- Keys $\mathcal{K}$ and messages $\mathcal{M}$ as before.
- Let $E(m, k)$ be an encoding function that constructs a stegotext quantum state that encodes the hidden message m under the key k.

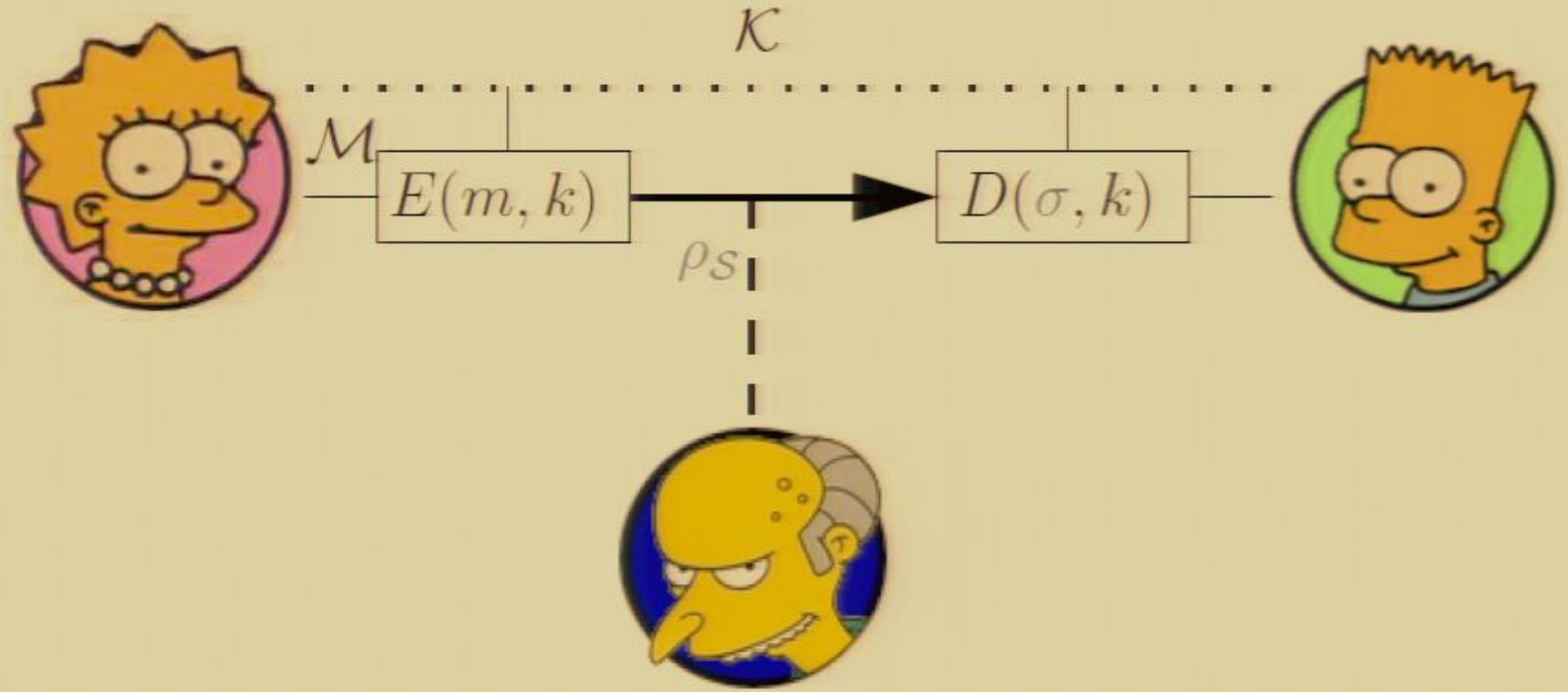
Quantum steganography framework

- Covertext and stegotext are quantum states, keys and messages are still classical.
- Let $\mathcal{C}$ be the probability distribution of covertext quantum states, with density matrix $\rho_{\mathcal{C}}$.
- Keys $\mathcal{K}$ and messages $\mathcal{M}$ as before.
- Let $E(m, k)$ be an encoding function that constructs a stegotext quantum state that encodes the hidden message m under the key k.
- Let $D(\sigma, k)$ be a decoding function that recovers a hidden message from a stegotext quantum state σ using the key k.

Quantum steganography framework

- Covertext and stegotext are quantum states, keys and messages are still classical.
- Let $\mathcal{C}$ be the probability distribution of covertext quantum states, with density matrix $\rho_{\mathcal{C}}$.
- Keys $\mathcal{K}$ and messages $\mathcal{M}$ as before.
- Let $E(m, k)$ be an encoding function that constructs a stegotext quantum state that encodes the hidden message m under the key k.
- Let $D(\sigma, k)$ be a decoding function that recovers a hidden message from a stegotext quantum state σ using the key k.
- Let $\mathcal{S}$ be probability distribution of stegotext quantum states created by E using messages $\mathcal{M}$ and keys $\mathcal{K}$, with density matrix $\rho_{\mathcal{S}}$.

Steganographic communication



Eavesdropper sees communication distributed according to stegotext mixed state ρ_S.

Security: quantum relative entropy

- To keep an eavesdropper unaware of whether steganographic communication is occurring or not, we wish for ρ_S and ρ_C to be indistinguishable.

Security: quantum relative entropy

- To keep an eavesdropper unaware of whether steganographic communication is occurring or not, we wish for ρ_S and ρ_C to be indistinguishable.
- The quantum relative entropy $S(\rho||\sigma)$ between two mixed states ρ and σ

Security: quantum relative entropy

- To keep an eavesdropper unaware of whether steganographic communication is occurring or not, we wish for ρ_S and ρ_C to be indistinguishable.
- The quantum relative entropy $S(\rho||\sigma)$ between two mixed states ρ and σ is

$$S(\rho||\sigma) = \mathrm{Tr}(\rho(\log\rho - \log\sigma))$$

(with $S(\rho||\sigma) = \infty$ if the support of ρ is not contained in the support of σ).

Security: quantum relative entropy

- To keep an eavesdropper unaware of whether steganographic communication is occurring or not, we wish for ρ_S and ρ_C to be indistinguishable.
- The quantum relative entropy $S(\rho||\sigma)$ between two mixed states ρ and σ is

$$S(\rho||\sigma) = \mathrm{Tr}(\rho(\log\rho - \log\sigma))$$

(with $S(\rho||\sigma) = \infty$ if the support of ρ is not contained in the support of σ).

- $\rho = \sigma$ if and only if $S(\rho||\sigma) = 0$. The relative entropy is always non-negative, although it is not symmetric and hence not a true distance measure.

Security: quantum relative entropy

- The quantum relative entropy describes, in some sense, how well two mixed states can be distinguished.

Security: quantum relative entropy

- The quantum relative entropy describes, in some sense, how well two mixed states can be distinguished.
- More precisely, the quantum relative entropy describes the classical relative entropy of the two classical probability distributions resulting from POVM measurements, maximized over all POVMs, in the limit.

Security: quantum relative entropy

- The quantum relative entropy describes, in some sense, how well two mixed states can be distinguished.
- More precisely, the quantum relative entropy describes the classical relative entropy of the two classical probability distributions resulting from POVM measurements, maximized over all POVMs, in the limit.

- A quantum stegosystem is perfectly secure against passive adversaries if $S(\rho_{\mathcal{C}}||\rho_{\mathcal{S}}) = 0$.

Security: quantum relative entropy

- The quantum relative entropy describes, in some sense, how well two mixed states can be distinguished.
- More precisely, the quantum relative entropy describes the classical relative entropy of the two classical probability distributions resulting from POVM measurements, maximized over all POVMs, in the limit.

- A quantum stegosystem is perfectly secure against passive adversaries if $S(\rho_{\mathcal{C}}||\rho_{\mathcal{S}}) = 0$.
- A quantum stegosystem is ϵ-secure against passive adversaries if $S(\rho_{\mathcal{C}}||\rho_{\mathcal{S}}) \leq \epsilon$.

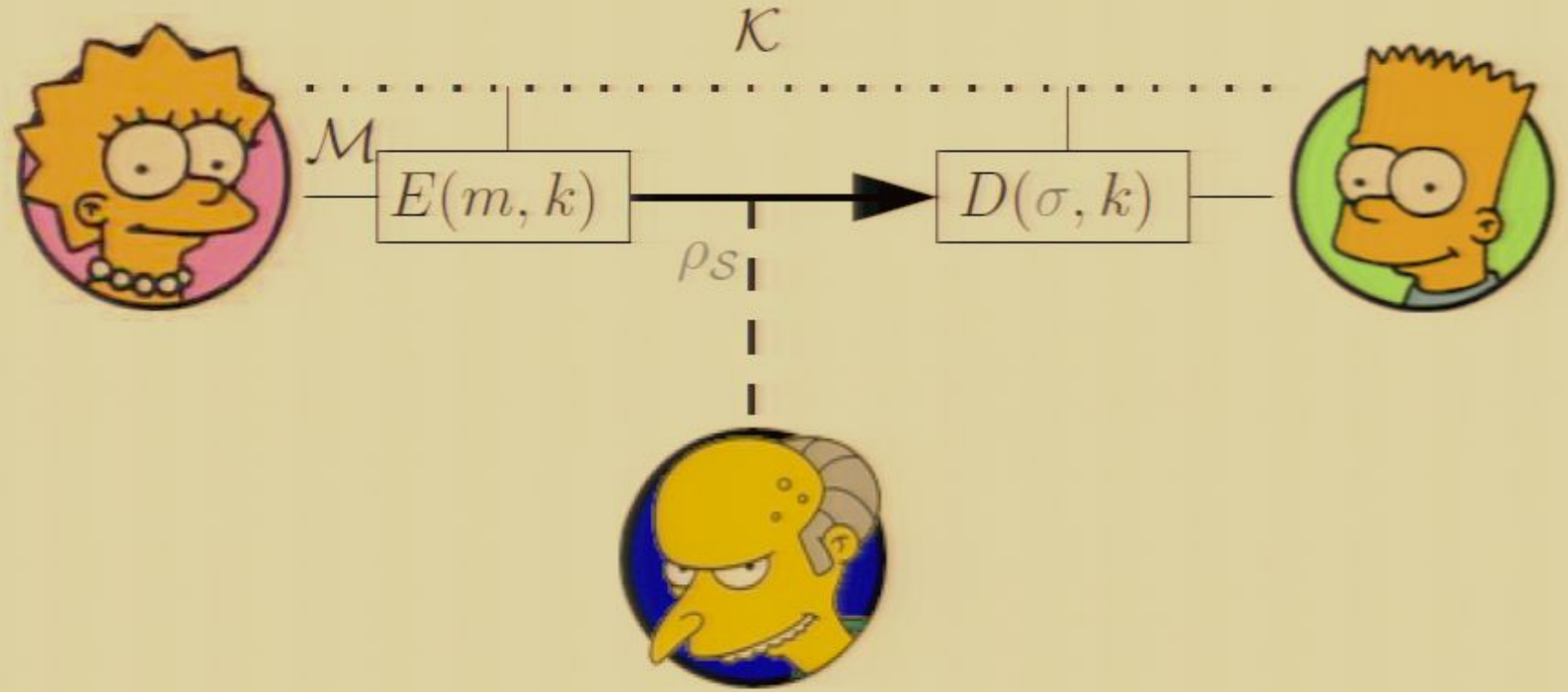
Security: quantum relative entropy

- To keep an eavesdropper unaware of whether steganographic communication is occurring or not, we wish for ρ_S and ρ_C to be indistinguishable.
- The quantum relative entropy $S(\rho||\sigma)$ between two mixed states ρ and σ

Quantum steganography framework

- Covertext and stegotext are quantum states, keys and messages are still classical.
- Let $\mathcal{C}$ be the probability distribution of covertext quantum states, with density matrix $\rho_{\mathcal{C}}$.
- Keys $\mathcal{K}$ and messages $\mathcal{M}$ as before.
- Let $E(m, k)$ be an encoding function that constructs a stegotext quantum state that encodes the hidden message m under the key k.
- Let $D(\sigma, k)$ be a decoding function that recovers a hidden message from a stegotext quantum state σ using the key k.
- Let $\mathcal{S}$ be probability distribution of stegotext quantum states created by E using messages $\mathcal{M}$ and keys $\mathcal{K}$, with density matrix $\rho_{\mathcal{S}}$.

Steganographic communication



Eavesdropper sees communication distributed according to stegotext mixed state ρ_S.

Security: quantum relative entropy

- To keep an eavesdropper unaware of whether steganographic communication is occurring or not, we wish for ρ_S and ρ_C to be indistinguishable.
- The quantum relative entropy $S(\rho||\sigma)$ between two mixed states ρ and σ is

$$S(\rho||\sigma) = \mathrm{Tr}(\rho(\log\rho - \log\sigma))$$

(with $S(\rho||\sigma) = \infty$ if the support of ρ is not contained in the support of σ).

Security: quantum relative entropy

- The quantum relative entropy describes, in some sense, how well two mixed states can be distinguished.

Security: quantum relative entropy

- The quantum relative entropy describes, in some sense, how well two mixed states can be distinguished.
- More precisely, the quantum relative entropy describes the classical relative entropy of the two classical probability distributions resulting from POVM measurements, maximized over all POVMs, in the limit.

- A quantum stegosystem is perfectly secure against passive adversaries if $S(\rho_{\mathcal{C}}||\rho_{\mathcal{S}}) = 0$.

Security: quantum relative entropy

- The quantum relative entropy describes, in some sense, how well two mixed states can be distinguished.
- More precisely, the quantum relative entropy describes the classical relative entropy of the two classical probability distributions resulting from POVM measurements, maximized over all POVMs, in the limit.

- A quantum stegosystem is perfectly secure against passive adversaries if $S(\rho_{\mathcal{C}}||\rho_{\mathcal{S}}) = 0$.
- A quantum stegosystem is ϵ-secure against passive adversaries if $S(\rho_{\mathcal{C}}||\rho_{\mathcal{S}}) \leq \epsilon$.

Security: quantum relative entropy

- The quantum relative entropy describes, in some sense, how well two mixed states can be distinguished.
- More precisely, the quantum relative entropy describes the classical relative entropy of the two classical probability distributions resulting from POVM measurements, maximized over all POVMs, in the limit.

- A quantum stegosystem is perfectly secure against passive adversaries if $S(\rho_{\mathcal{C}}||\rho_{\mathcal{S}}) = 0$.
- A quantum stegosystem is ϵ-secure against passive adversaries if $S(\rho_{\mathcal{C}}||\rho_{\mathcal{S}}) \leq \epsilon$.

- We can use the same definition of information rate as in the classical case.

BB84 quantum key distribution

- In the BB84 quantum key distribution protocol, the quantum states sent across the wire are generated as follows:

BB84 quantum key distribution

- In the BB84 quantum key distribution protocol, the quantum states sent across the wire are generated as follows:
- Choose a, b uniformly at random from $\{0, 1\}$.

BB84 quantum key distribution

- In the BB84 quantum key distribution protocol, the quantum states sent across the wire are generated as follows:
- Choose a, b uniformly at random from $\{0, 1\}$.
- Construct the state $|\psi\rangle = H^a|b\rangle$, where H is the Hadamard matrix.

BB84 quantum key distribution

- In the BB84 quantum key distribution protocol, the quantum states sent across the wire are generated as follows:
- Choose a, b uniformly at random from $\{0, 1\}$.
- Construct the state $|\psi\rangle = H^a|b\rangle$, where H is the Hadamard matrix.
- Each of the following states will be constructed with probability $\frac{1}{4}$:

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

BB84 quantum key distribution

- In the BB84 quantum key distribution protocol, the quantum states sent across the wire are generated as follows:
- Choose a, b uniformly at random from $\{0, 1\}$.
- Construct the state $|\psi\rangle = H^a|b\rangle$, where H is the Hadamard matrix.
- Each of the following states will be constructed with probability $\frac{1}{4}$:

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

- The mixed state for the probability distribution of states generated in this manner is the totally mixed state:

$$\rho_{\mathrm{BB84}} = \frac{1}{2}I = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$$

Quantum example: BB84-like with uniform $\mathcal{K}$ and $\mathcal{M}$

- Idea: encode the message in a BB84 basis.

Quantum example: BB84-like with uniform $\mathcal{K}$ and $\mathcal{M}$

- Idea: encode the message in a BB84 basis.
- Covertexts $\rho_{\mathcal{C}} = \rho_{\mathrm{BB84}}$: totally mixed state

Quantum example: BB84-like with uniform $\mathcal{K}$ and $\mathcal{M}$

- Idea: encode the message in a BB84 basis.
- Covertexts $\rho_{\mathcal{C}} = \rho_{\mathrm{BB84}}$: totally mixed state
- Keys $\mathcal{K}$: uniform distribution on $\{0, 1\}$

Quantum example: BB84-like with uniform $\mathcal{K}$ and $\mathcal{M}$

- Idea: encode the message in a BB84 basis.
- Covertexts $\rho_{\mathcal{C}} = \rho_{\mathrm{BB84}}$: totally mixed state
- Keys $\mathcal{K}$: uniform distribution on $\{0, 1\}$
- Messages $\mathcal{M}$: uniform distribution on $\{0, 1\}$

Quantum example: BB84-like with uniform $\mathcal{K}$ and $\mathcal{M}$

- Idea: encode the message in a BB84 basis.
- Covertexts $\rho_{\mathcal{C}} = \rho_{\mathrm{BB84}}$: totally mixed state
- Keys $\mathcal{K}$: uniform distribution on $\{0, 1\}$
- Messages $\mathcal{M}$: uniform distribution on $\{0, 1\}$
- Encoding $E(m, k) = H^k|m\rangle$
- Decoding $D(\sigma, k) =$ measure $H^k \sigma H^{k\dagger}$ in the computational basis

Quantum example: BB84-like with uniform $\mathcal{K}$ and $\mathcal{M}$

- Since $\mathcal{K}$ and $\mathcal{M}$ are uniform, trivially the stegotexts and covertexts have the same distribution: $\rho_{\mathcal{S}} = \rho_{\mathrm{BB84}} = \rho_{\mathcal{C}}$.

Quantum example: BB84-like with uniform $\mathcal{K}$ and $\mathcal{M}$

- Since $\mathcal{K}$ and $\mathcal{M}$ are uniform, trivially the stegotexts and covertexts have the same distribution: $\rho_{\mathcal{S}} = \rho_{\mathrm{BB84}} = \rho_{\mathcal{C}}$.
- Thus the stegosystem is perfectly secure.

Quantum example: BB84-like with uniform $\mathcal{K}$ and $\mathcal{M}$

- Since $\mathcal{K}$ and $\mathcal{M}$ are uniform, trivially the stegotexts and covertexts have the same distribution: $\rho_{\mathcal{S}} = \rho_{\mathrm{BB84}} = \rho_{\mathcal{C}}$.
- Thus the stegosystem is perfectly secure.
- Assuming a perfect quantum channel, the decoding operation will recover the original message with certainty, so the information rate is 1.

Quantum example: BB84-like with uniform $\mathcal{K}$ and $\mathcal{M}$

- Since $\mathcal{K}$ and $\mathcal{M}$ are uniform, trivially the stegotexts and covertexts have the same distribution: $\rho_{\mathcal{S}} = \rho_{\mathrm{BB84}} = \rho_{\mathcal{C}}$.
- Thus the stegosystem is perfectly secure.
- Assuming a perfect quantum channel, the decoding operation will recover the original message with certainty, so the information rate is 1.

- However, this only holds for uniform message distributions.

Quantum example: BB84-like with uniform $\mathcal{K}$ and $\mathcal{M}$

- Since $\mathcal{K}$ and $\mathcal{M}$ are uniform, trivially the stegotexts and covertexts have the same distribution: $\rho_{\mathcal{S}} = \rho_{\mathrm{BB84}} = \rho_{\mathcal{C}}$.
- Thus the stegosystem is perfectly secure.
- Assuming a perfect quantum channel, the decoding operation will recover the original message with certainty, so the information rate is 1.

- However, this only holds for uniform message distributions.
- If $\mathcal{M}$ is not uniform, then in general $\rho_{\mathcal{S}}$ will not be ρ_{BB84}.

Quantum example: BB84-like with uniform $\mathcal{K}$ and $\mathcal{M}$

- Since $\mathcal{K}$ and $\mathcal{M}$ are uniform, trivially the stegotexts and covertexts have the same distribution: $\rho_{\mathcal{S}} = \rho_{\mathrm{BB84}} = \rho_{\mathcal{C}}$.
- Thus the stegosystem is perfectly secure.
- Assuming a perfect quantum channel, the decoding operation will recover the original message with certainty, so the information rate is 1.

- However, this only holds for uniform message distributions.
- If $\mathcal{M}$ is not uniform, then in general $\rho_{\mathcal{S}}$ will not be ρ_{BB84}.
- We may know the message distribution is not uniform, or we may in fact not know the message distribution *a priori*.

Quantum example: BB84-like with uniform $\mathcal{K}$ and $\mathcal{M}$

- Since $\mathcal{K}$ and $\mathcal{M}$ are uniform, trivially the stegotexts and covertexts have the same distribution: $\rho_{\mathcal{S}} = \rho_{\mathrm{BB84}} = \rho_{\mathcal{C}}$.
- Thus the stegosystem is perfectly secure.
- Assuming a perfect quantum channel, the decoding operation will recover the original message with certainty, so the information rate is 1.

- However, this only holds for uniform message distributions.
- If $\mathcal{M}$ is not uniform, then in general $\rho_{\mathcal{S}}$ will not be ρ_{BB84}.
- We may know the message distribution is not uniform, or we may in fact not know the message distribution *a priori*.
- In either case, this scheme won't be perfectly secure.

Quantum example: BB84-like with uniform $\mathcal{K}$

- Idea: use the message to choose the BB84 basis.

Quantum example: BB84-like with uniform $\mathcal{K}$

- Idea: use the message to choose the BB84 basis.
- Covertexts $\rho_{\mathcal{C}} = \rho_{\mathrm{BB84}}$: totally mixed state
- Keys $\mathcal{K}$: uniform distribution on $\{0, 1\}$
- Messages $\mathcal{M}$: any distribution on $\{0, 1\}$

Quantum example: BB84-like with uniform $\mathcal{K}$

- Idea: use the message to choose the BB84 basis.
- Covertexts $\rho_{\mathcal{C}} = \rho_{\mathrm{BB84}}$: totally mixed state
- Keys $\mathcal{K}$: uniform distribution on $\{0, 1\}$
- Messages $\mathcal{M}$: any distribution on $\{0, 1\}$
- Encoding $E(m, k) = H^m|k\rangle$
- Decoding $D(\sigma, k)$ (more complicated: recipient uses knowledge of key to help determine if he got the right basis or not)

Quantum example: BB84-like with uniform $\mathcal{K}$

- Regardless of the message distribution $\mathcal{M}$, the stegotexts and covertexts have the same distribution: $\rho_{\mathcal{S}} = \rho_{\mathrm{BB84}} = \rho_{\mathcal{C}}$.

Quantum example: BB84-like with uniform $\mathcal{K}$

- Regardless of the message distribution $\mathcal{M}$, the stegotexts and covertexts have the same distribution: $\rho_{\mathcal{S}} = \rho_{\mathrm{BB84}} = \rho_{\mathcal{C}}$.
- Thus the stegosystem is perfectly secure.

Quantum example: BB84-like with uniform $\mathcal{K}$

- Regardless of the message distribution $\mathcal{M}$, the stegotexts and covertexts have the same distribution: $\rho_{\mathcal{S}} = \rho_{\mathrm{BB84}} = \rho_{\mathcal{C}}$.
- Thus the stegosystem is perfectly secure.
- However, we now have some decoding errors because the receiver doesn't always know what basis to measure in.

Quantum example: BB84-like with uniform $\mathcal{K}$

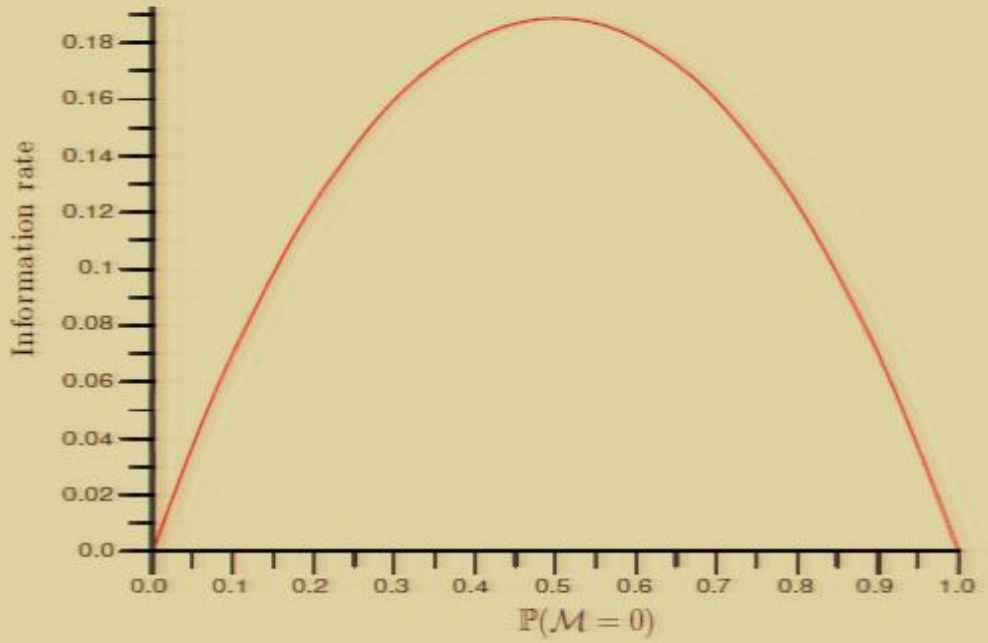
- Regardless of the message distribution $\mathcal{M}$, the stegotexts and covertexts have the same distribution: $\rho_{\mathcal{S}} = \rho_{\mathrm{BB84}} = \rho_{\mathcal{C}}$.
- Thus the stegosystem is perfectly secure.
- However, we now have some decoding errors because the receiver doesn't always know what basis to measure in.
- We have a decoding scheme that gives a probability of error in decoding of $\frac{1}{4}$ for all message distributions $\mathcal{M}$.

Quantum example: BB84-like with uniform $\mathcal{K}$

- The information rate for this scheme is

$$h\left(\frac{1}{4}+\frac{1}{2}\mathbb{P}(\mathcal{M}=0)\right)-h\left(\frac{3}{4}\right)$$

where $h(x)=-x\log_2(x)+(1-x)\log_2(1-x)$.



Summary

Protocol	Message Distribution	Security	Information Rate
Classical one-time pad	any	perfect	1
Quantum $H^k\|m\rangle$	uniform	perfect	1
Quantum $H^m\|k\rangle$	any	perfect	< 0.2

Future work

- Investigate the security of steganography when combined with classical communication in a full QKD protocol.

Summary

Protocol	Message Distribution	Security	Information Rate
Classical one-time pad	any	perfect	1
Quantum $H^k\|m\rangle$	uniform	perfect	1
Quantum $H^m\|k\rangle$	any	perfect	< 0.2

Future work

- Investigate the security of steganography when combined with classical communication in a full QKD protocol.

Future work

- Investigate the security of steganography when combined with classical communication in a full QKD protocol.
- Find quantum steganography schemes with better information rates.

Future work

- Investigate the security of steganography when combined with classical communication in a full QKD protocol.
- Find quantum steganography schemes with better information rates.
- Find quantum steganography schemes for other covertext distributions, e.g., the six-state protocol, the 3-state protocol, or other quantum communication scenarios.