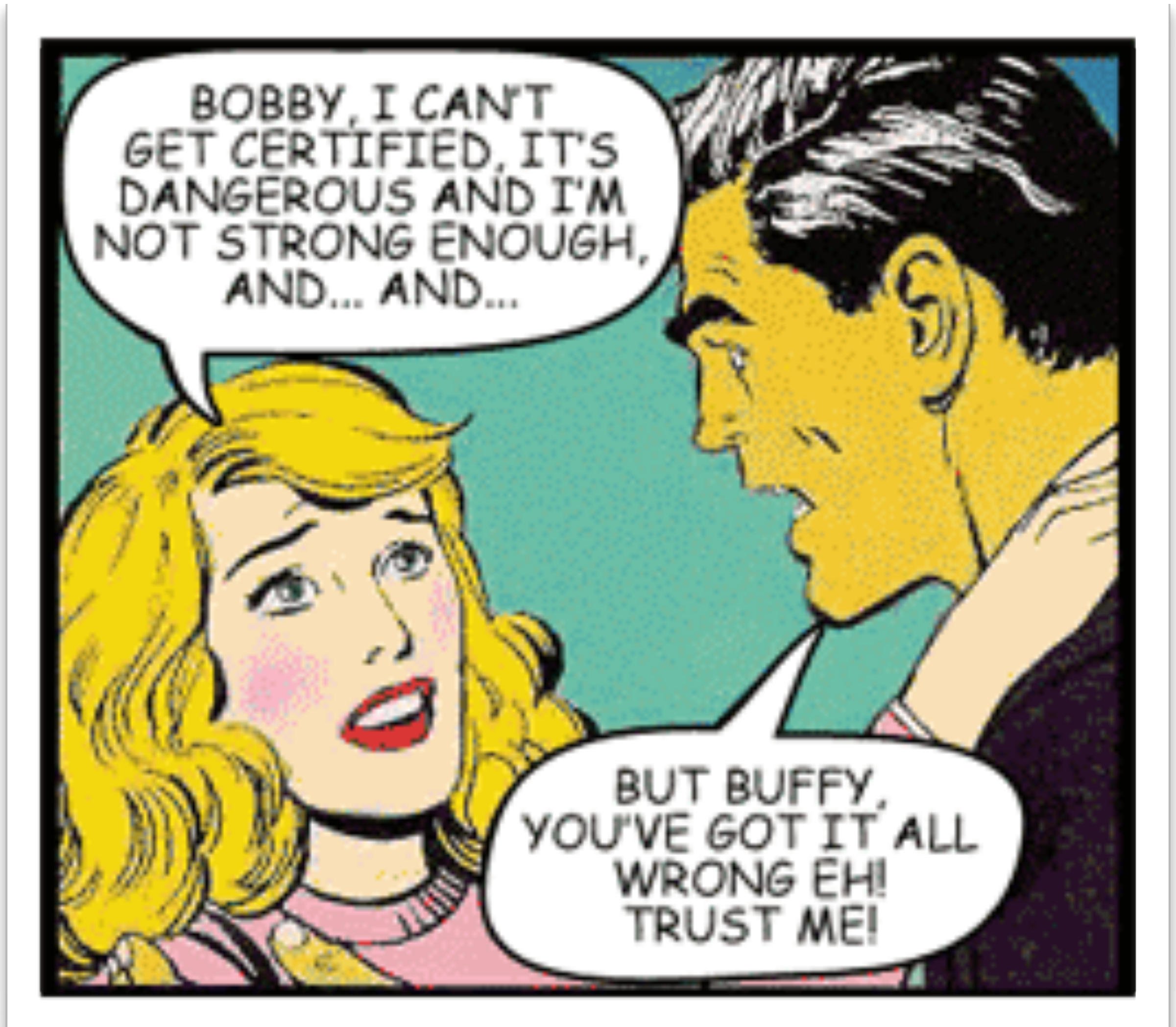


Quantum Cryptography with Local Bell Tests

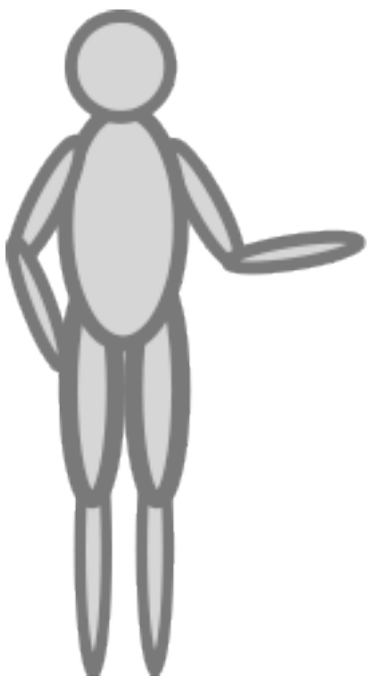
Charles Ci Wen Lim, Christopher Portmann, Marco Tomamichel, Renato Renner and Nicolas Gisin

A project between University of Geneva and ETH Zurich

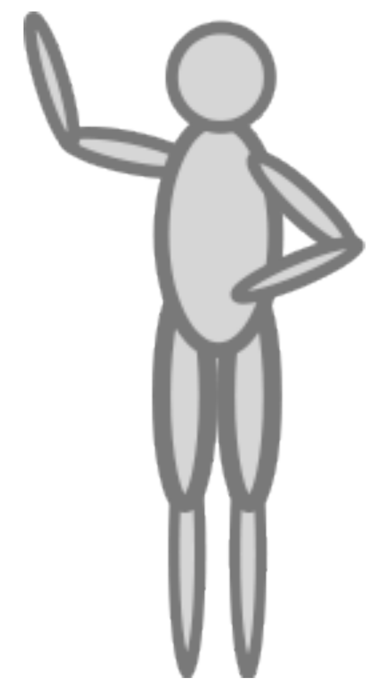
Inception

Bennett and Brassard 1984

Alice

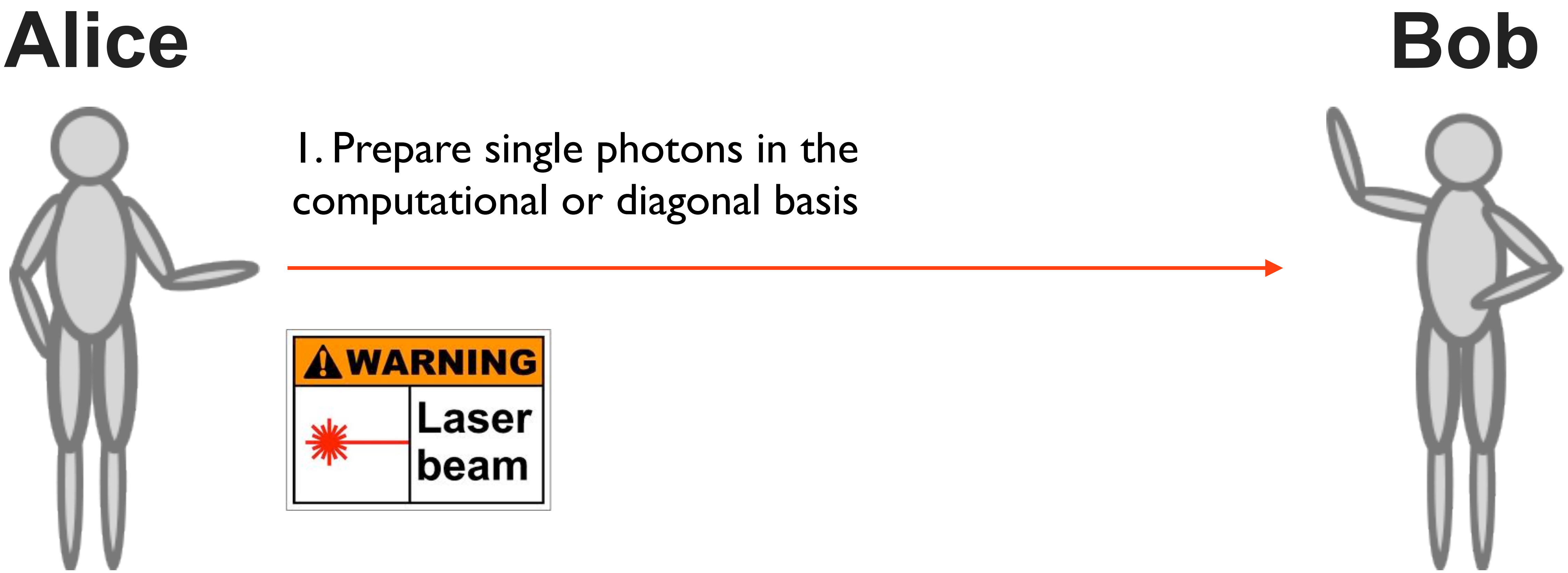


Bob



Inception

Bennett and Brassard 1984

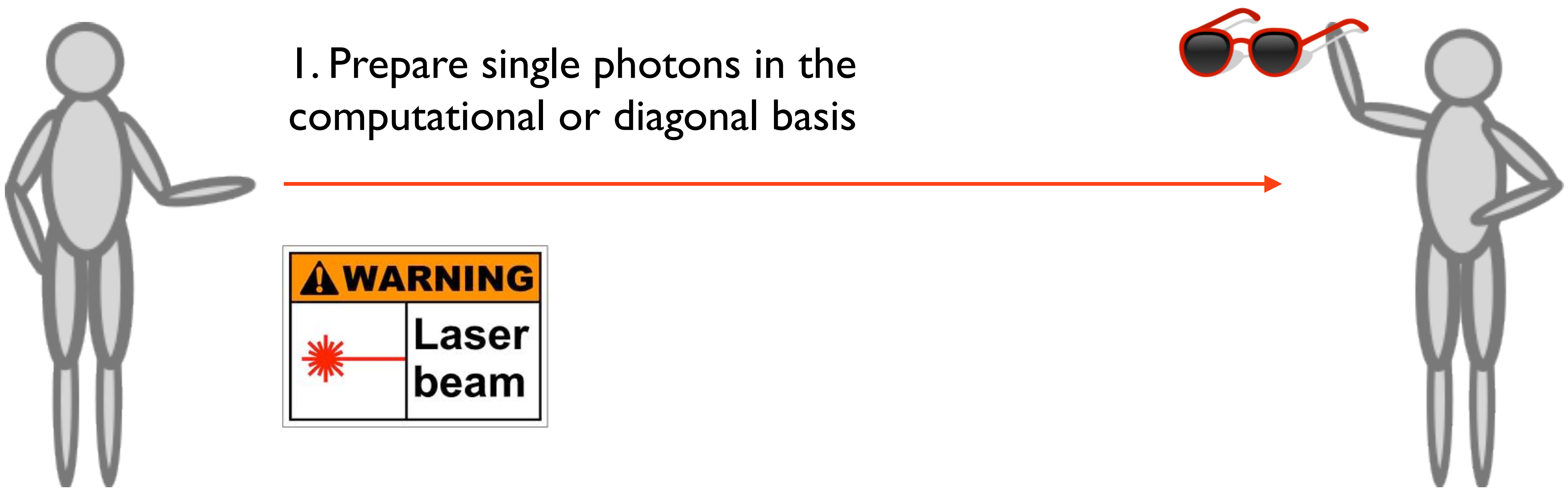


Inception

Bennett and Brassard 1984

Alice **Bob**

1. Prepare single photons in the computational or diagonal basis



2. Measures them in the computational or diagonal basis

Experiment done in QCRYPT Conference Dinner 2011

At the age of reconciliation of the GAP between theory and practice....

At the age of reconciliation of the GAP between theory and practice....

arXiv.org > quant-ph > arXiv:quant-ph/0212066

Search

Quantum Physics

Security of quantum key distribution with imperfect devices

Daniel Gottesman, Hoi-Kwong Lo, Norbert Lütkenhaus, John Preskill

(Submitted on 11 Dec 2002 (v1), last revised 3 Sep 2004 (this version, v3))

We prove the security of the Bennett-Brassard (BB84) quantum key distribution protocol in the case where the source and detector are under the limited control of an adversary. Our proof applies when both the source and the detector have small basis-dependent flaws, as is typical in practical implementations of the protocol. We derive a general lower bound on the asymptotic key generation rate for weakly basis-dependent eavesdropping attacks, and also estimate the rate in some special cases: sources that emit weak coherent states with random phases, detectors with basis-dependent efficiency, and misaligned sources and detectors.

At the age of reconciliation of the GAP between theory and practice....

arXiv.org > quant-ph > arXiv:quant-ph/0212066

arXiv.org > quant-ph > arXiv:quant-ph/0411004

Quantum Physics

Decoy State Quantum Key Distribution

Hoi-Kwong Lo, Xiongfeng Ma, Kai Chen (Center for Quantum Information and Quantum Control, University of Toronto)

(Submitted on 31 Oct 2004 (v1), last revised 12 May 2005 (this version, v4))

There has been much interest in quantum key distribution. Experimentally, quantum key distribution over 150 km of commercial Telecom fibers has been successfully performed. The crucial issue in quantum key distribution is its security. Unfortunately, all recent experiments are, in principle, insecure due to real-life imperfections. Here, we propose a method that can for the first time make most of those experiments secure by using essentially the same hardware. Our method is to use decoy states to detect eavesdropping attacks. As a consequence, we have the best of both worlds--enjoying unconditional security guaranteed by the fundamental laws of physics and yet dramatically surpassing even some of the best experimental performances reported in the literature.

At the age of reconciliation of the GAP between theory and practice....

arXiv.org > quant-ph > arXiv:quant-ph/0212066

arXiv.org > quant-ph > arXiv:quant-ph/0411004

arXiv.org > quant-ph > arXiv:0708.0709

Quantum Physics

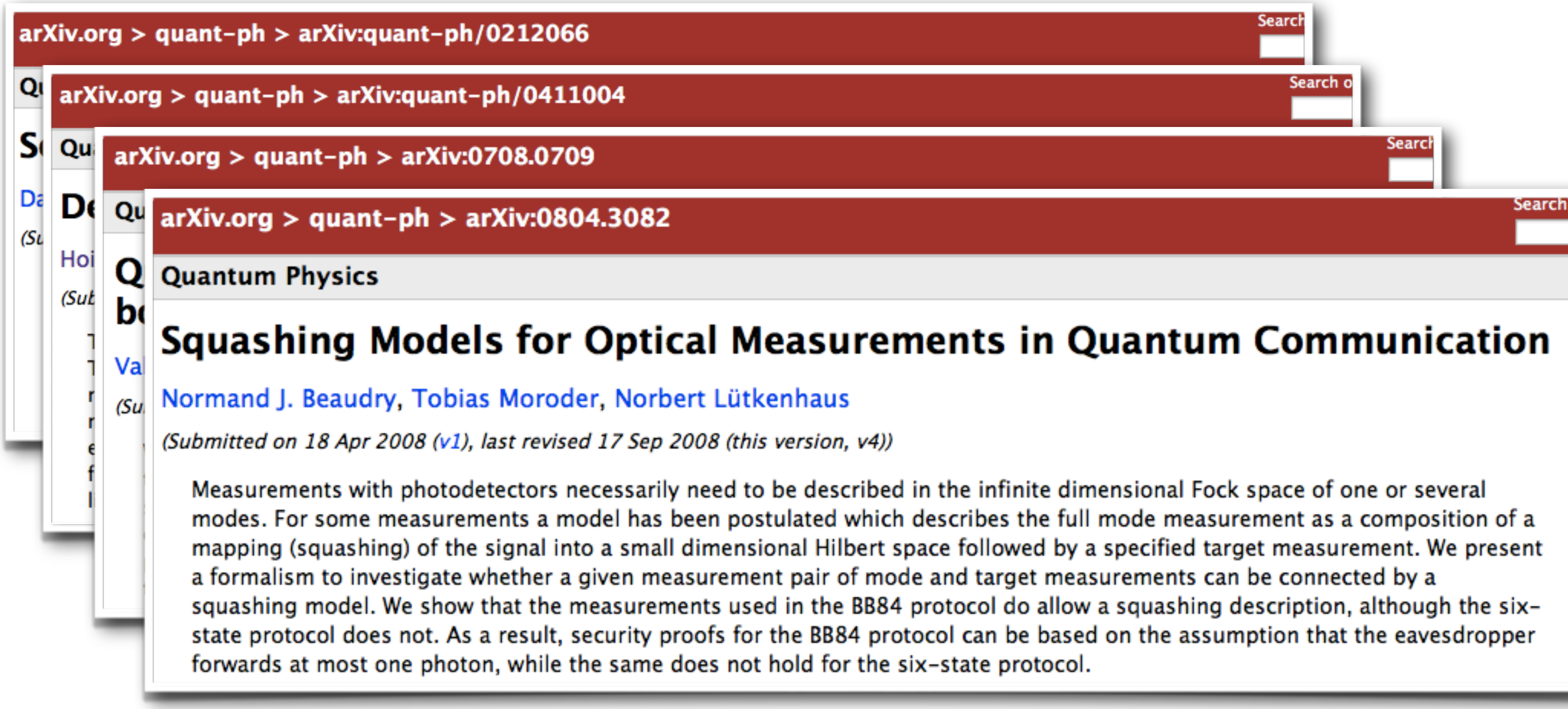
Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way post-processing

Valerio Scarani, Renato Renner

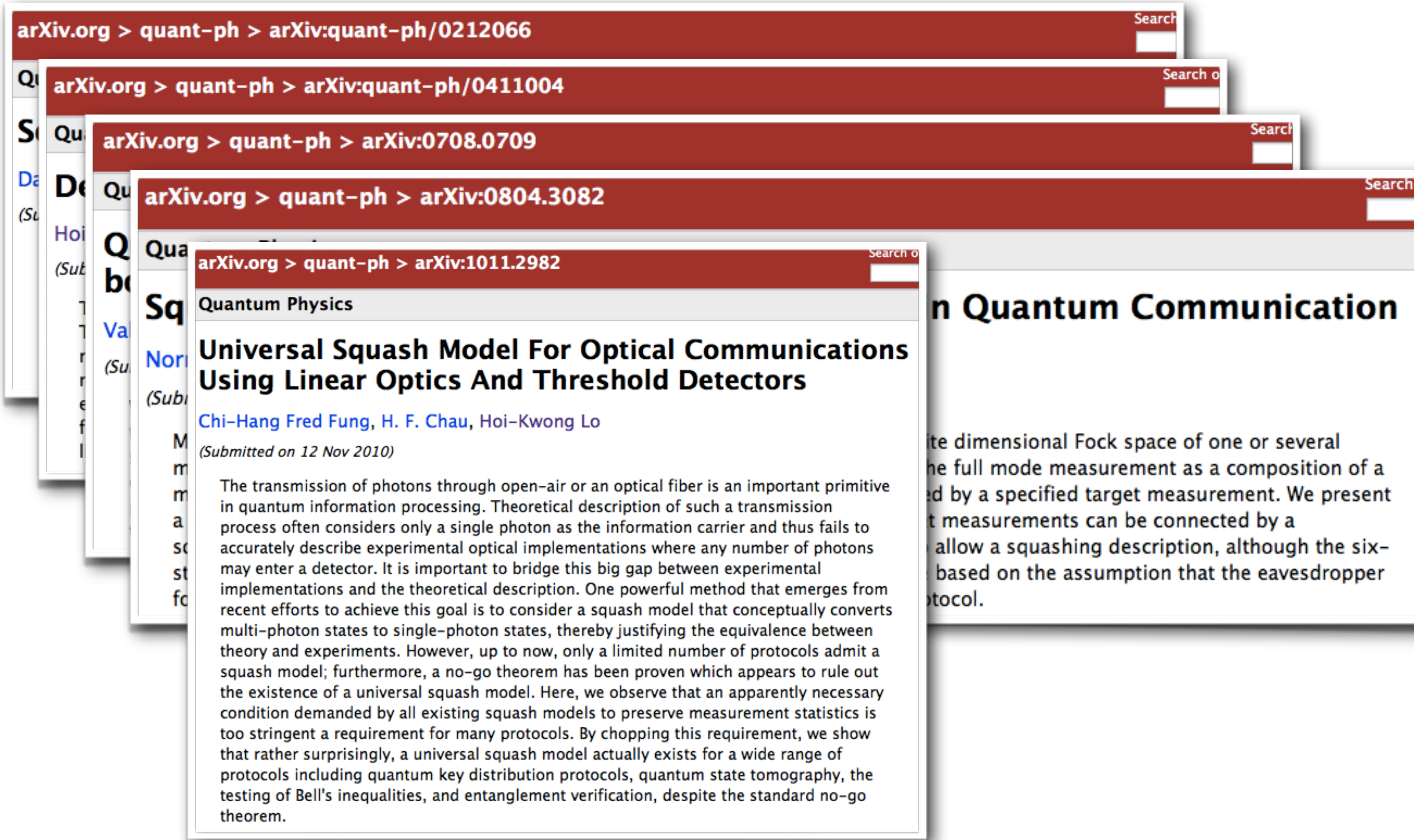
(Submitted on 6 Aug 2007 (v1), last revised 1 Jun 2008 (this version, v2))

We derive a bound for the security of QKD with finite resources under one-way post-processing, based on a definition of security that is composable and has an operational meaning. While our proof relies on the assumption of collective attacks, unconditional security follows immediately for standard protocols like Bennett-Brassard 1984 and six-states. For single-qubit implementations of such protocols, we find that the secret key rate becomes positive when at least N\sim 10^5 signals are exchanged and processed. For any other discrete-variable protocol, unconditional security can be obtained using the exponential de Finetti theorem, but the additional overhead leads to very pessimistic estimates.

At the age of reconciliation of the GAP between theory and practice....



At the age of reconciliation of the GAP between theory and practice....



arXiv.org > quant-ph > arXiv:1011.2982

Quantum Physics

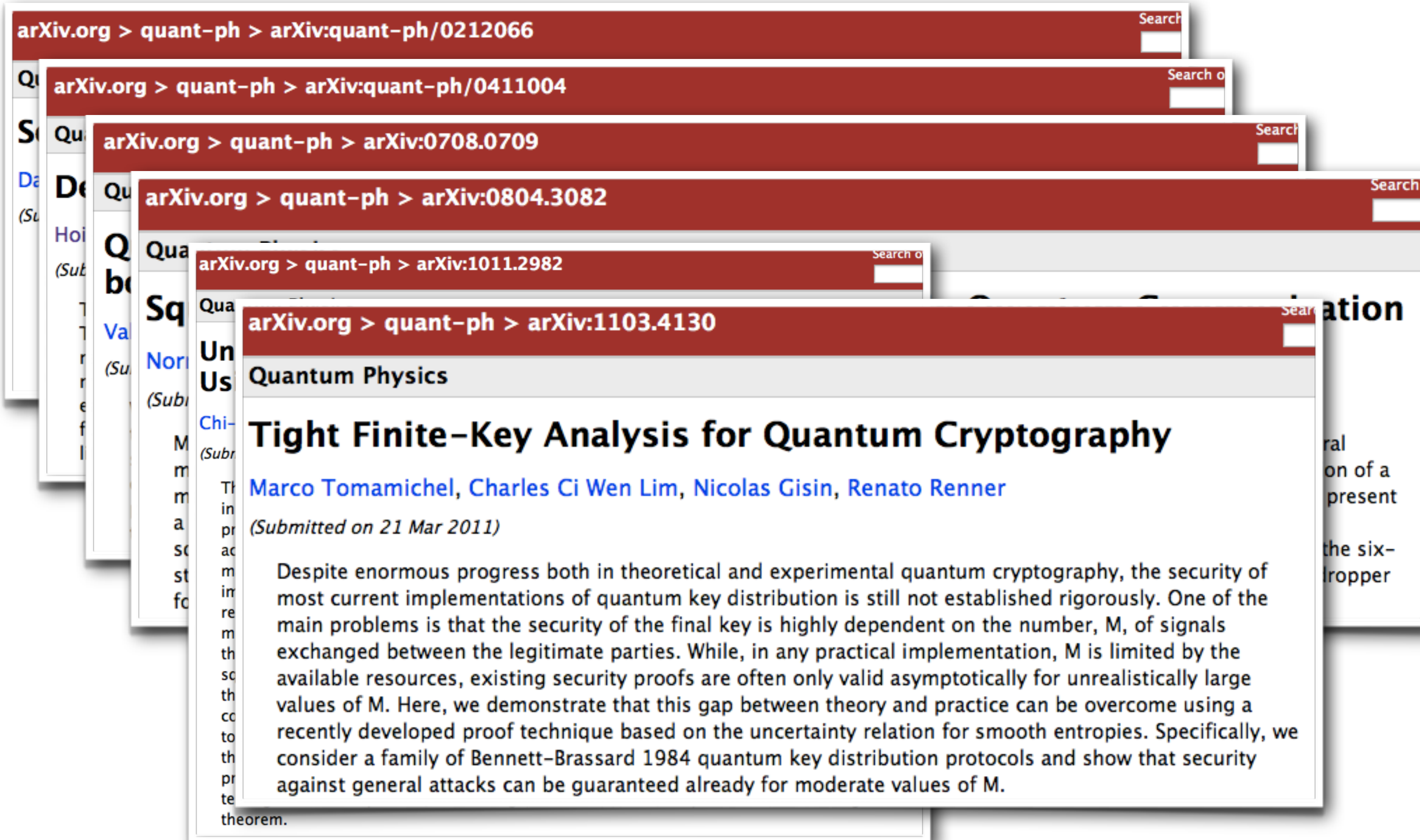
Universal Squash Model For Optical Communications Using Linear Optics And Threshold Detectors

Chi-Hang Fred Fung, H. F. Chau, Hoi-Kwong Lo

(Submitted on 12 Nov 2010)

The transmission of photons through open-air or an optical fiber is an important primitive in quantum information processing. Theoretical description of such a transmission process often considers only a single photon as the information carrier and thus fails to accurately describe experimental optical implementations where any number of photons may enter a detector. It is important to bridge this big gap between experimental implementations and the theoretical description. One powerful method that emerges from recent efforts to achieve this goal is to consider a squash model that conceptually converts multi-photon states to single-photon states, thereby justifying the equivalence between theory and experiments. However, up to now, only a limited number of protocols admit a squash model; furthermore, a no-go theorem has been proven which appears to rule out the existence of a universal squash model. Here, we observe that an apparently necessary condition demanded by all existing squash models to preserve measurement statistics is too stringent a requirement for many protocols. By chopping this requirement, we show that rather surprisingly, a universal squash model actually exists for a wide range of protocols including quantum key distribution protocols, quantum state tomography, the testing of Bell's inequalities, and entanglement verification, despite the standard no-go theorem.

At the age of reconciliation of the GAP between theory and practice....



arXiv.org > quant-ph > arXiv:quant-ph/0212066

arXiv.org > quant-ph > arXiv:quant-ph/0411004

arXiv.org > quant-ph > arXiv:0708.0709

arXiv.org > quant-ph > arXiv:0804.3082

arXiv.org > quant-ph > arXiv:1011.2982

arXiv.org > quant-ph > arXiv:1103.4130

Quantum Physics

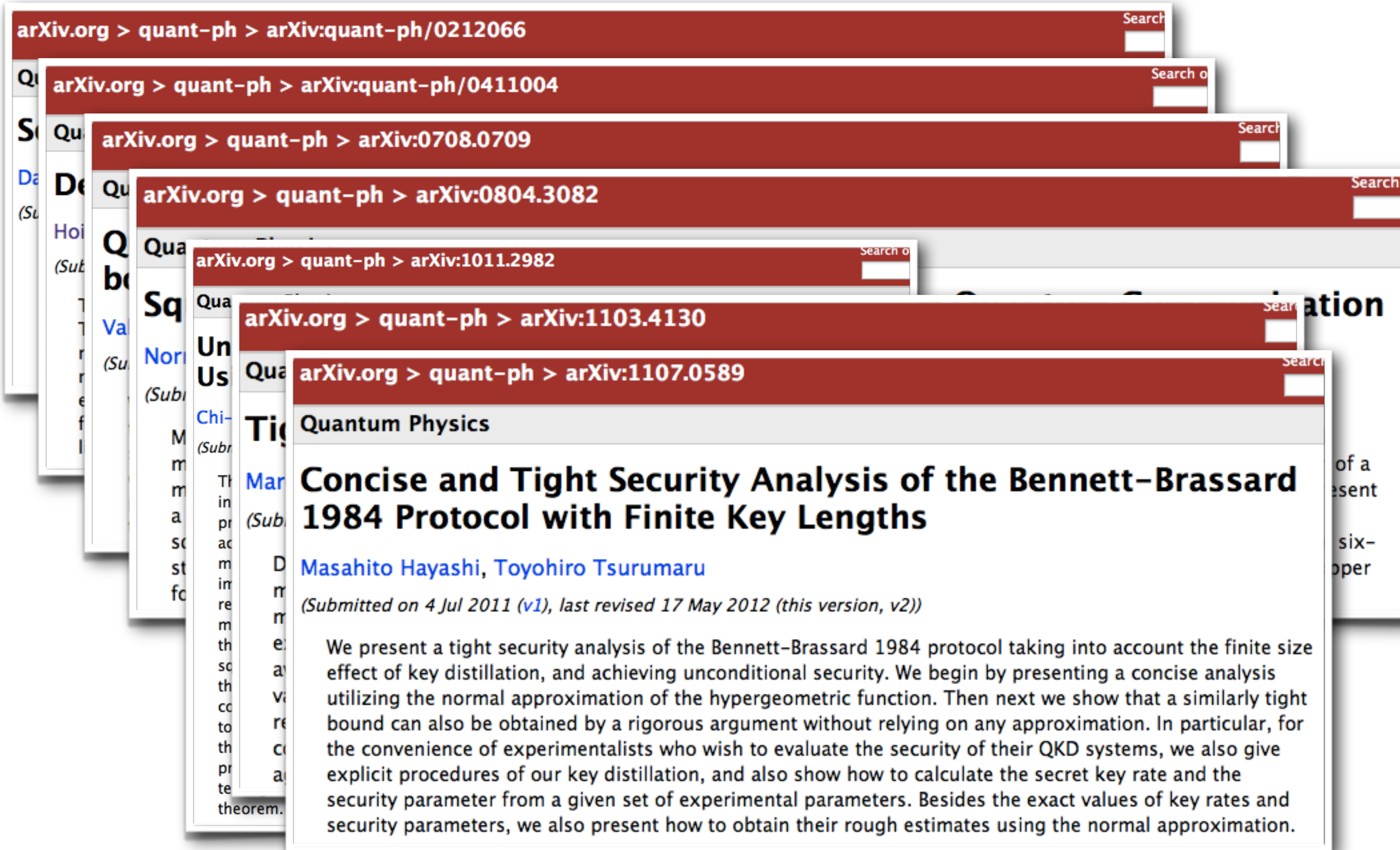
Tight Finite-Key Analysis for Quantum Cryptography

Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, Renato Renner

(Submitted on 21 Mar 2011)

Despite enormous progress both in theoretical and experimental quantum cryptography, the security of most current implementations of quantum key distribution is still not established rigorously. One of the main problems is that the security of the final key is highly dependent on the number, M, of signals exchanged between the legitimate parties. While, in any practical implementation, M is limited by the available resources, existing security proofs are often only valid asymptotically for unrealistically large values of M. Here, we demonstrate that this gap between theory and practice can be overcome using a recently developed proof technique based on the uncertainty relation for smooth entropies. Specifically, we consider a family of Bennett-Brassard 1984 quantum key distribution protocols and show that security against general attacks can be guaranteed already for moderate values of M.

At the age of reconciliation of the GAP between theory and practice....


arXiv.org > quant-ph > arXiv:quant-ph/0212066

arXiv.org > quant-ph > arXiv:quant-ph/0411004

arXiv.org > quant-ph > arXiv:0708.0709

arXiv.org > quant-ph > arXiv:0804.3082

arXiv.org > quant-ph > arXiv:1011.2982

arXiv.org > quant-ph > arXiv:1103.4130

arXiv.org > quant-ph > arXiv:1107.0589

Quantum Physics

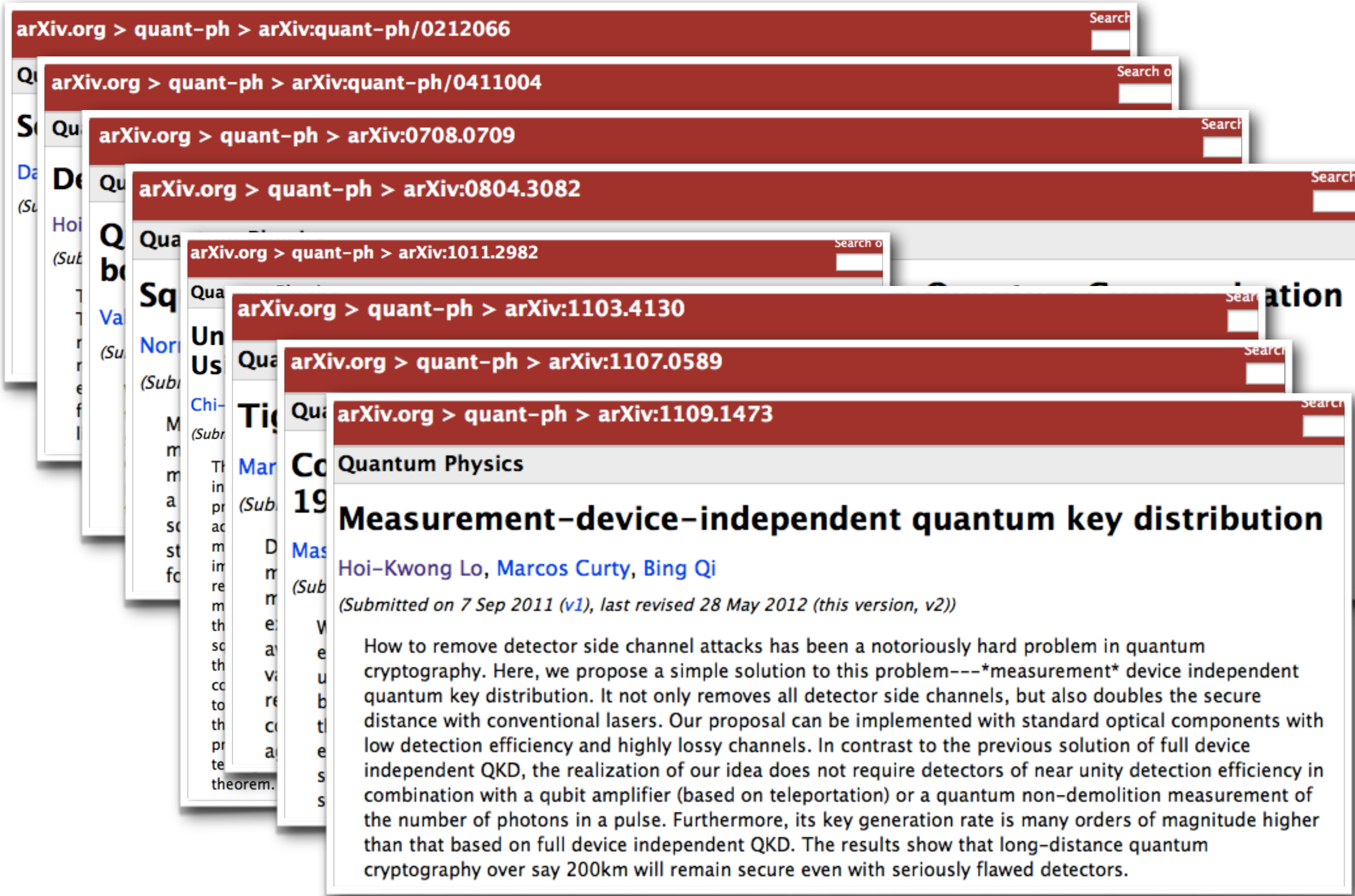
Concise and Tight Security Analysis of the Bennett-Brassard 1984 Protocol with Finite Key Lengths

Masahito Hayashi, Toyohiro Tsurumaru

(Submitted on 4 Jul 2011 (v1), last revised 17 May 2012 (this version, v2))

We present a tight security analysis of the Bennett-Brassard 1984 protocol taking into account the finite size effect of key distillation, and achieving unconditional security. We begin by presenting a concise analysis utilizing the normal approximation of the hypergeometric function. Then next we show that a similarly tight bound can also be obtained by a rigorous argument without relying on any approximation. In particular, for the convenience of experimentalists who wish to evaluate the security of their QKD systems, we also give explicit procedures of our key distillation, and also show how to calculate the secret key rate and the security parameter from a given set of experimental parameters. Besides the exact values of key rates and security parameters, we also present how to obtain their rough estimates using the normal approximation.

At the age of reconciliation of the GAP between theory and practice....



arXiv.org > quant-ph > arXiv:quant-ph/0212066

arXiv.org > quant-ph > arXiv:quant-ph/0411004

arXiv.org > quant-ph > arXiv:0708.0709

arXiv.org > quant-ph > arXiv:0804.3082

arXiv.org > quant-ph > arXiv:1011.2982

arXiv.org > quant-ph > arXiv:1103.4130

arXiv.org > quant-ph > arXiv:1107.0589

arXiv.org > quant-ph > arXiv:1109.1473

Quantum Physics

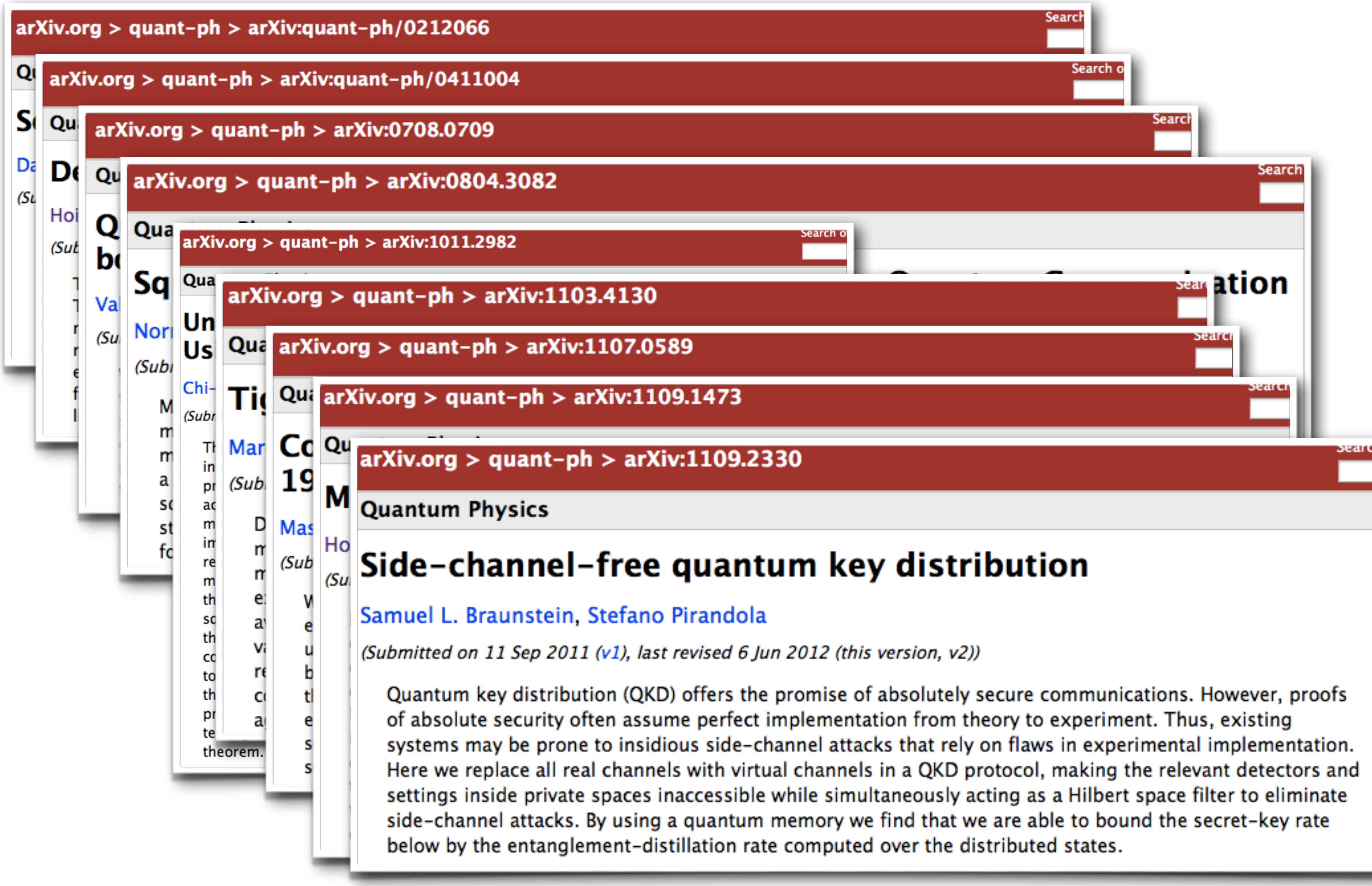
Measurement-device-independent quantum key distribution

Hoi-Kwong Lo, Marcos Curty, Bing Qi

(Submitted on 7 Sep 2011 (v1), last revised 28 May 2012 (this version, v2))

How to remove detector side channel attacks has been a notoriously hard problem in quantum cryptography. Here, we propose a simple solution to this problem---*measurement* device independent quantum key distribution. It not only removes all detector side channels, but also doubles the secure distance with conventional lasers. Our proposal can be implemented with standard optical components with low detection efficiency and highly lossy channels. In contrast to the previous solution of full device independent QKD, the realization of our idea does not require detectors of near unity detection efficiency in combination with a qubit amplifier (based on teleportation) or a quantum non-demolition measurement of the number of photons in a pulse. Furthermore, its key generation rate is many orders of magnitude higher than that based on full device independent QKD. The results show that long-distance quantum cryptography over say 200km will remain secure even with seriously flawed detectors.

At the age of reconciliation of the GAP between theory and practice....

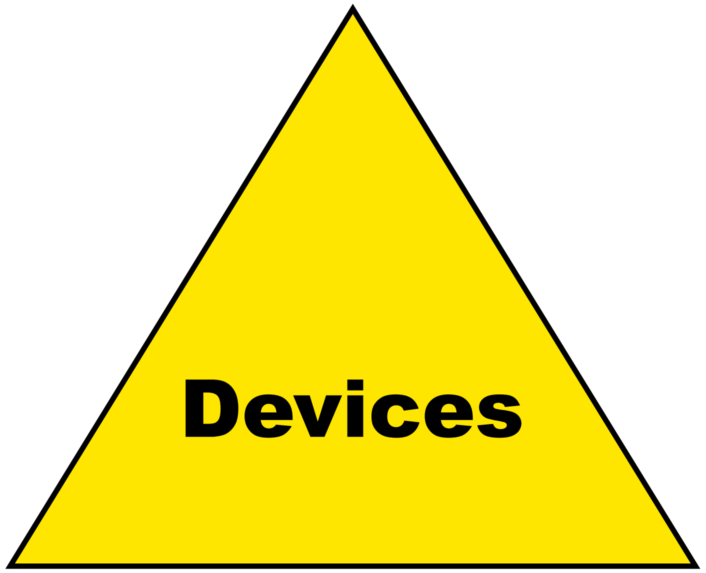


Motivation

Towards a framework for **practical** quantum cryptography

Motivation

Towards a framework for **practical** quantum cryptography

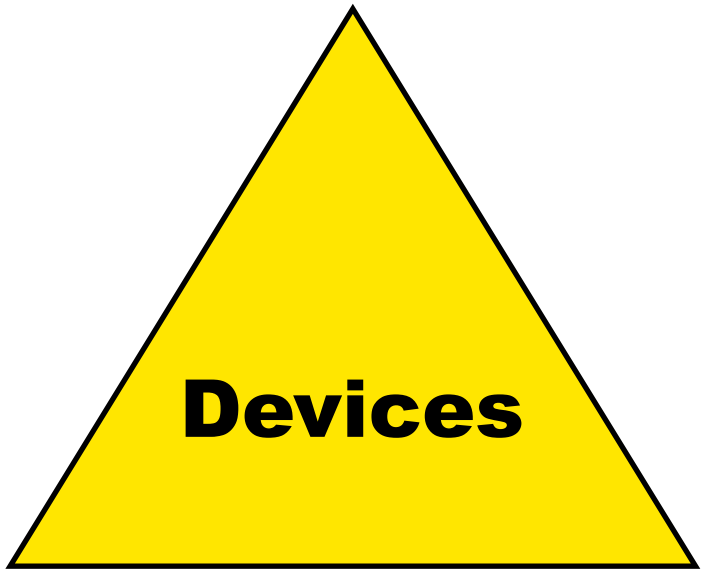


Motivation

Towards a framework for **practical** quantum cryptography

Discrepancies

- Imperfect Devices
- Side-Channels

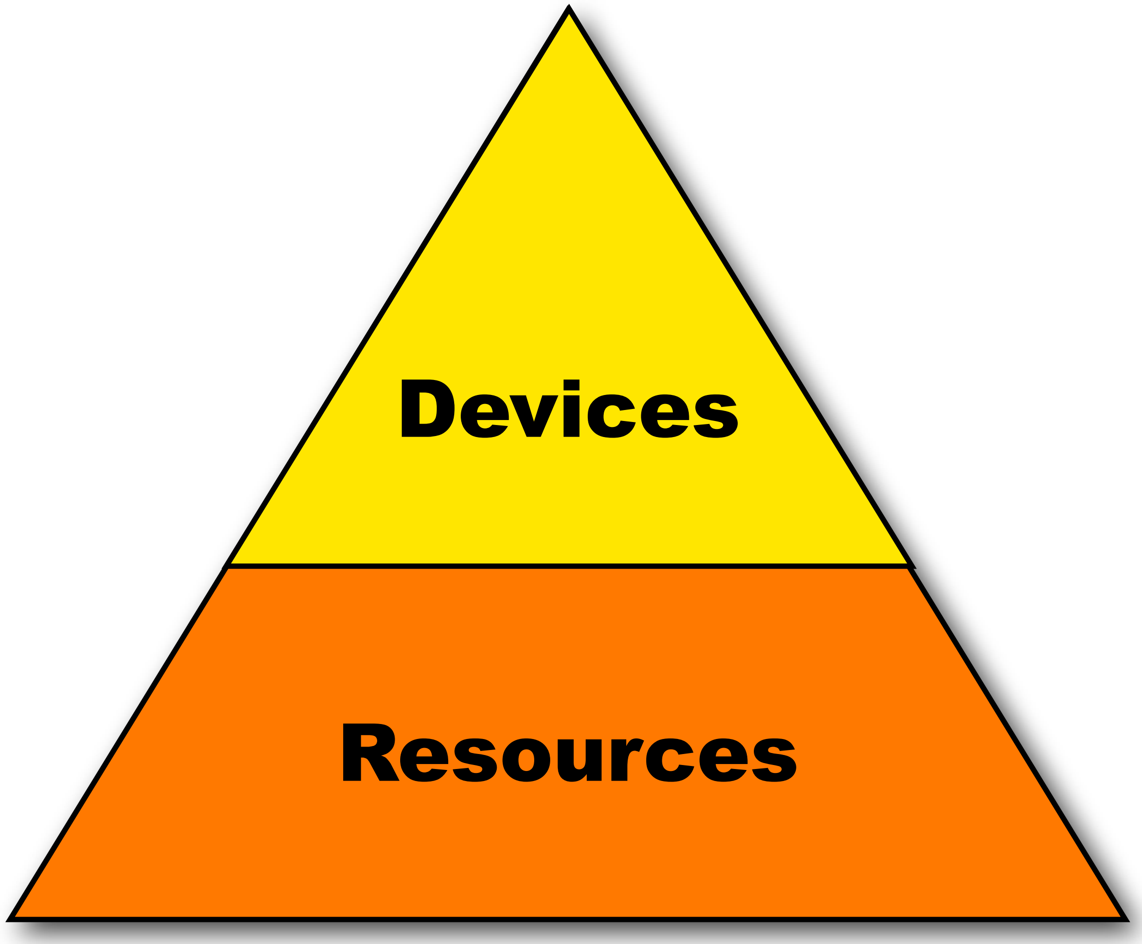


Motivation

Towards a framework for **practical** quantum cryptography

Discrepancies

- Imperfect Devices
- Side-Channels

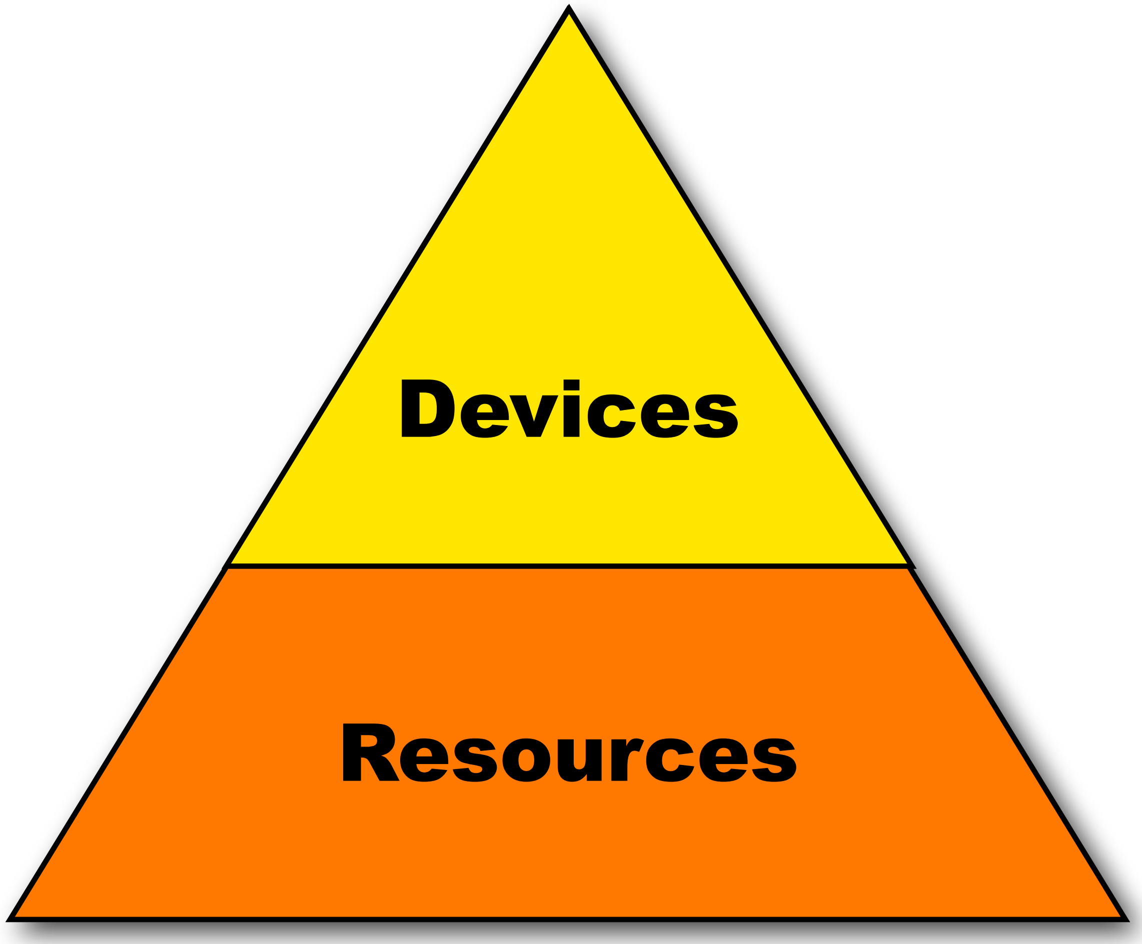


Motivation

Towards a framework for **practical** quantum cryptography

Discrepancies

- Imperfect Devices
- Side-Channels

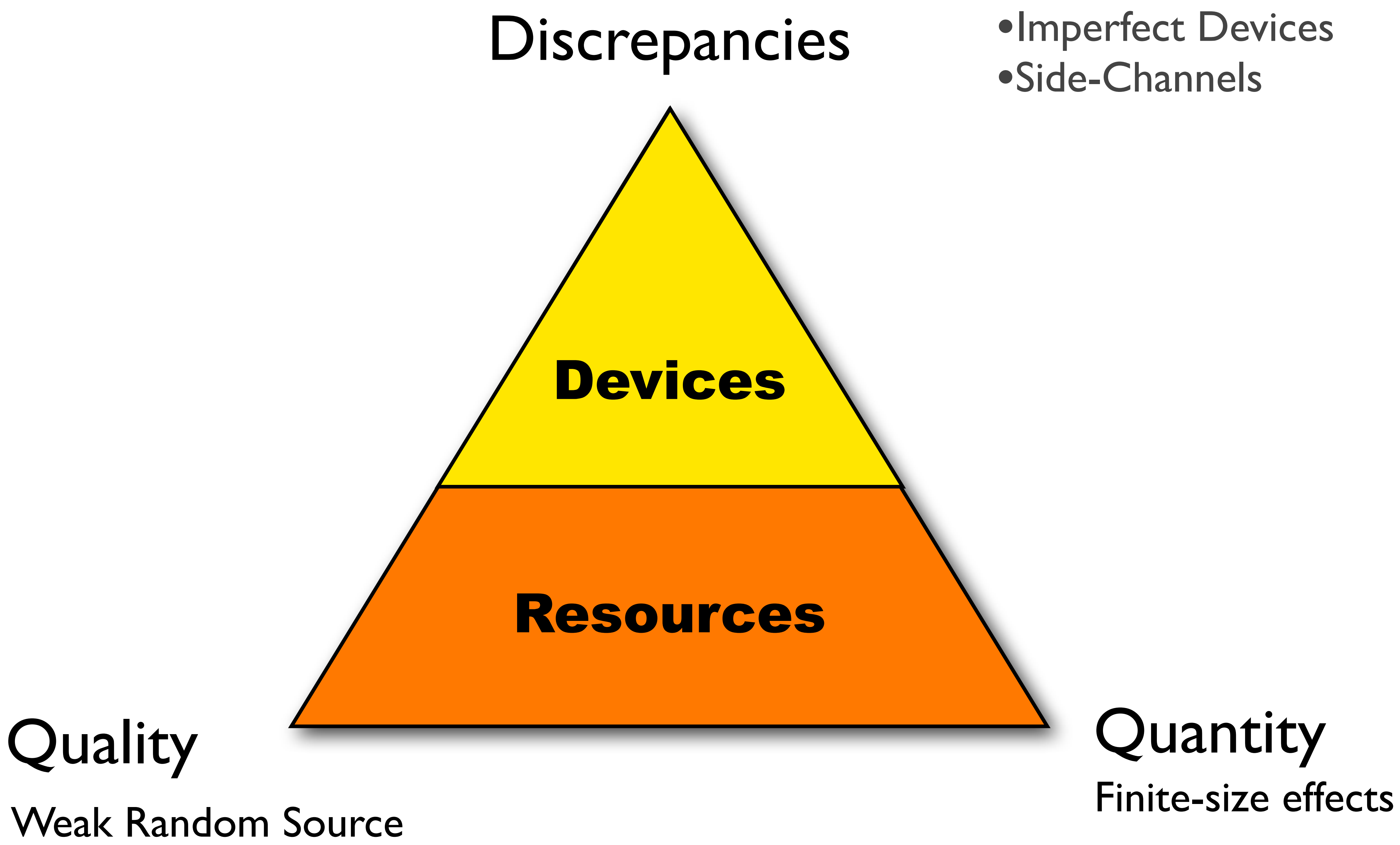


Quality

Weak Random Source

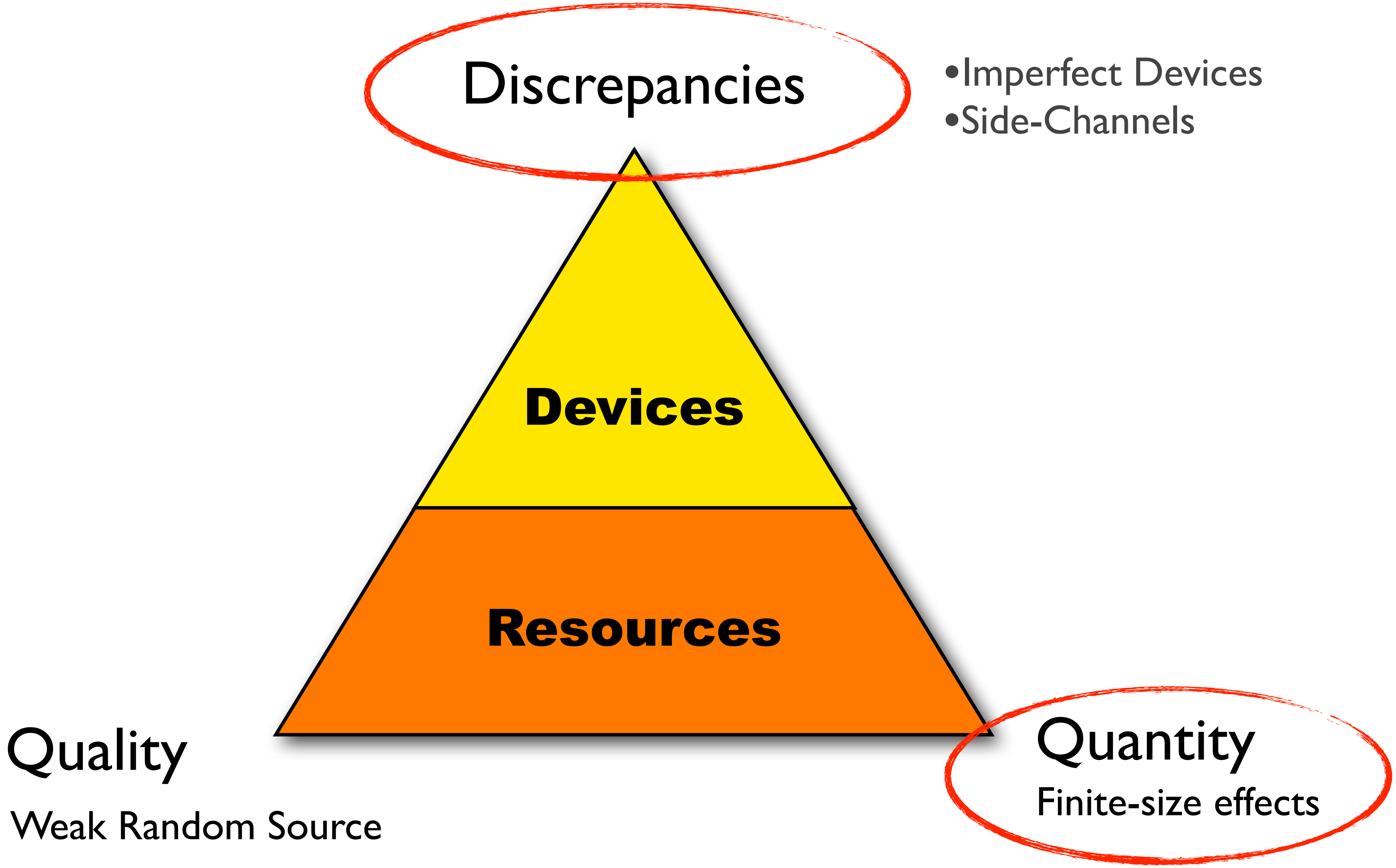
Motivation

Towards a framework for **practical** quantum cryptography



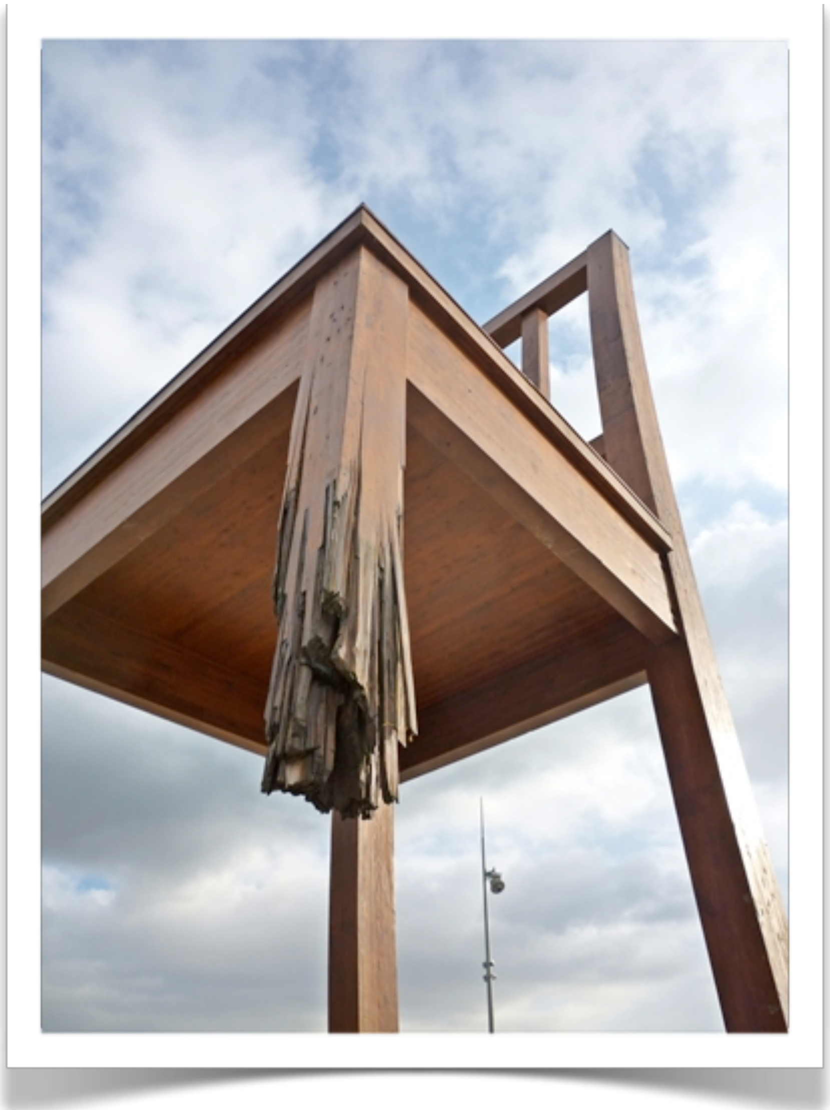
Motivation

Towards a framework for **practical** quantum cryptography



Imperfect devices

In reality, most practical devices do not conform to the required theoretical models.

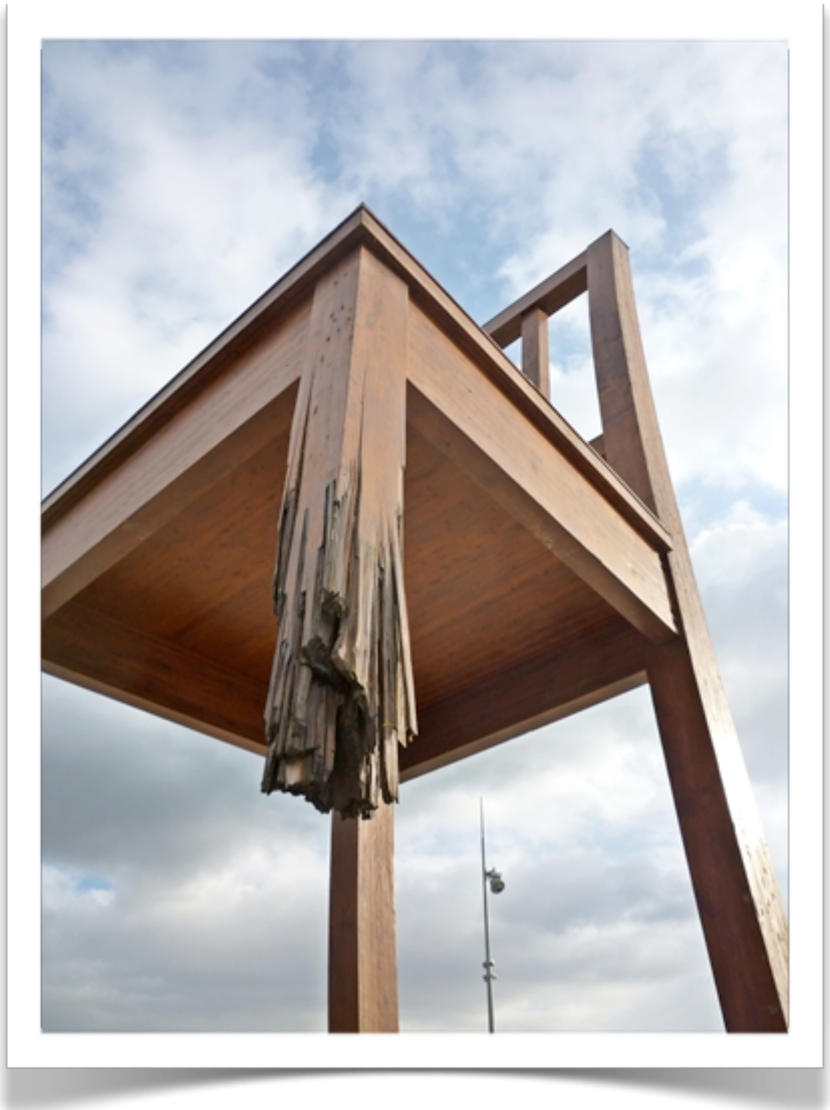


Imperfect devices

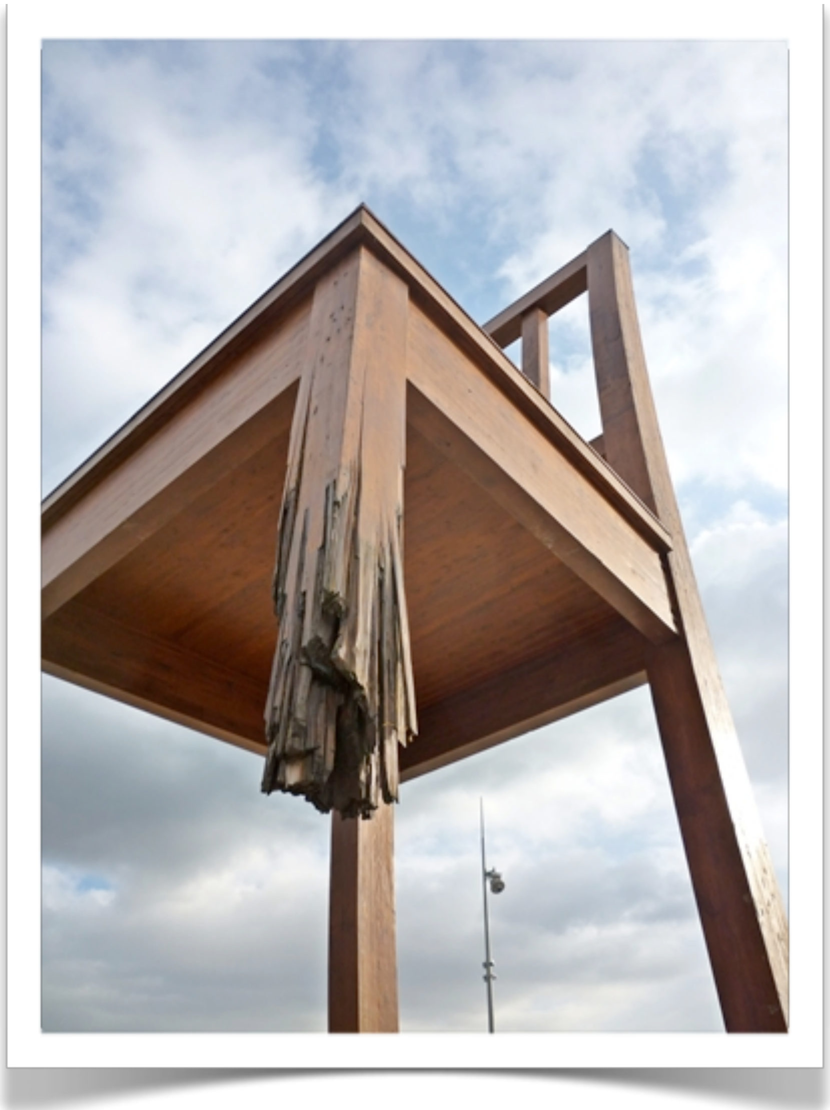
In reality, most practical devices do not conform to the required theoretical models.

However, if we know where an imperfect is, then we can measure it and include it in the security proof.

Examples: Basis mis-alignment, basis leakage, etc.



Imperfect devices



In reality, most practical devices do not conform to the required theoretical models.

However, if we know where an imperfect is, then we can measure it and include it in the security proof.

Examples: Basis mis-alignment, basis leakage, etc.

In the case of basis leakage, we have to give this additional information to the adversary,

$$K_{\mathrm{rate}} = 1 - \mathrm{h}_2(e_{\mathrm{phase}}) - \mathrm{h}_2(e_{\mathrm{bit}})$$

$$e_{\mathrm{phase}} \leq e_{\mathrm{X}} + 4\Gamma + 4\sqrt{\Gamma e_{\mathrm{X}}}$$

where Γ parameterizes the basis leakage.

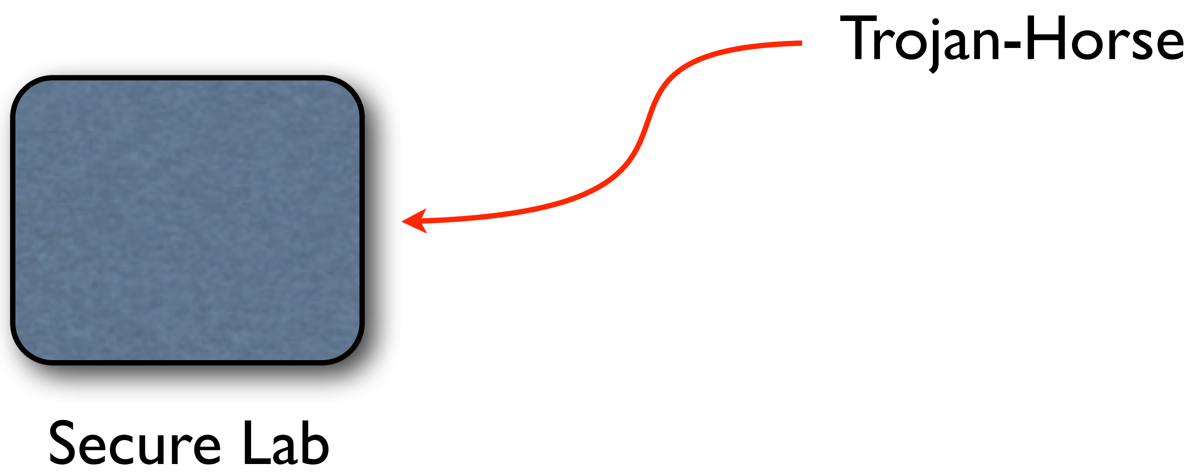
For more details, refer to the works of Lo and Preskill (2007) and Gottesman *et al* (2004).

Hidden Side-Channels

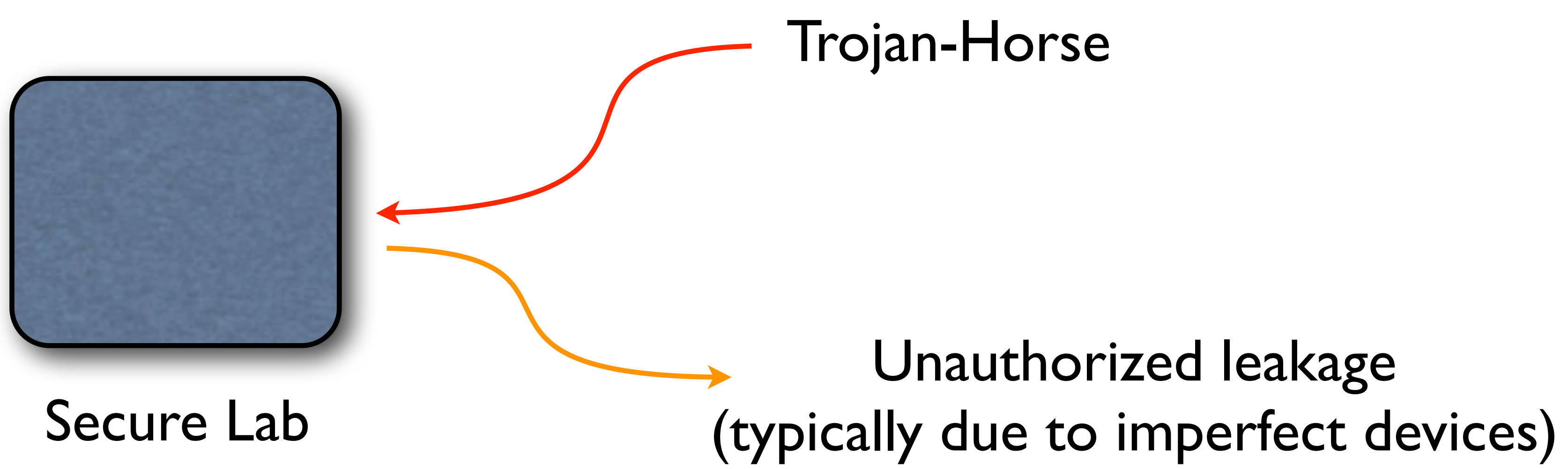
Hidden Side-Channels

Secure Lab

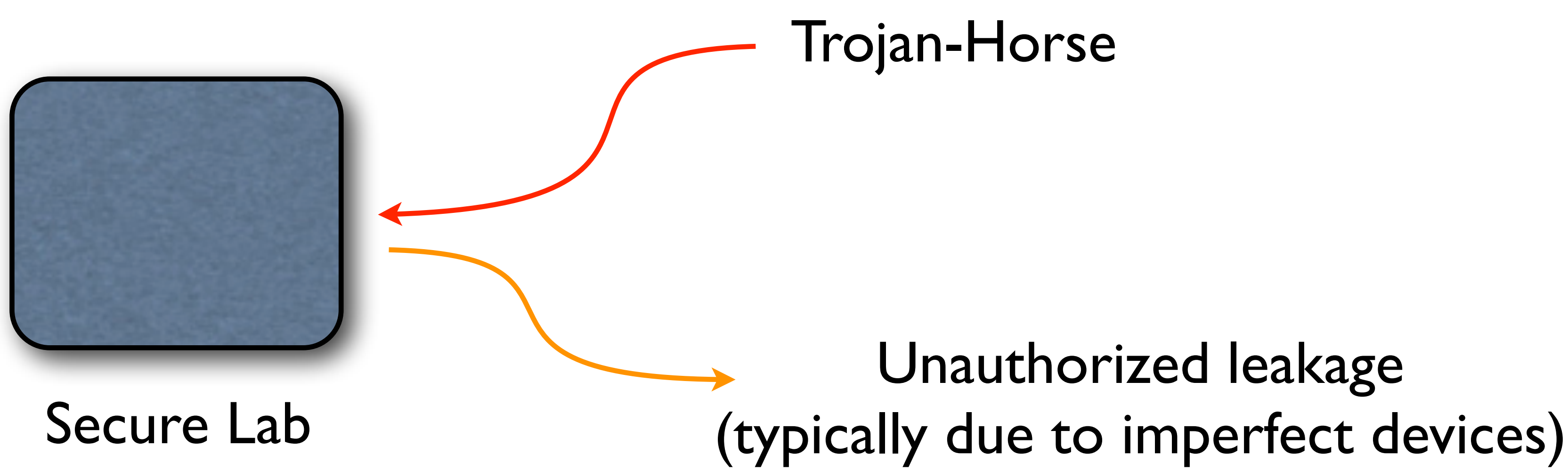
Hidden Side-Channels



Hidden Side-Channels



Hidden Side-Channels



Basically, these are the channels which are not considered in the protocol tests.

Asymptotic Limit

Pre-existing security proofs are obtained under the assumption that Alice and Bob exchange an infinite number of signals. Then, it is possible to obtain the secret key rate, e.g., for the BB84 protocol

$$K_{\mathrm{rate}} = 1 - \mathrm{h}_2(e_{\mathrm{phase}}) - \mathrm{h}_2(e_{\mathrm{bit}})$$

Asymptotic Limit

Pre-existing security proofs are obtained under the assumption that Alice and Bob exchange an infinite number of signals. Then, it is possible to obtain the secret key rate, e.g., for the BB84 protocol

$$K_{\text{rate}} = 1 - \mathrm{h}_2(e_{\text{phase}}) - \mathrm{h}_2(e_{\text{bit}})$$

To correct for the finite key size, **the basic idea is to give all the statistic fluctuations to the adversary**, i.e.,

$$\hat{K}_{\text{rate}} \approx 1 - \mathrm{h}_2(e_{\text{phase}} + \Delta e_{\text{phase}}) - \mathrm{h}_2(e_{\text{bit}} + \Delta e_{\text{bit}})$$

Asymptotic Limit

Pre-existing security proofs are obtained under the assumption that Alice and Bob exchange an infinite number of signals. Then, it is possible to obtain the secret key rate, e.g., for the BB84 protocol

$$K_{\mathrm{rate}} = 1 - \mathrm{h}_2(e_{\mathrm{phase}}) - \mathrm{h}_2(e_{\mathrm{bit}})$$

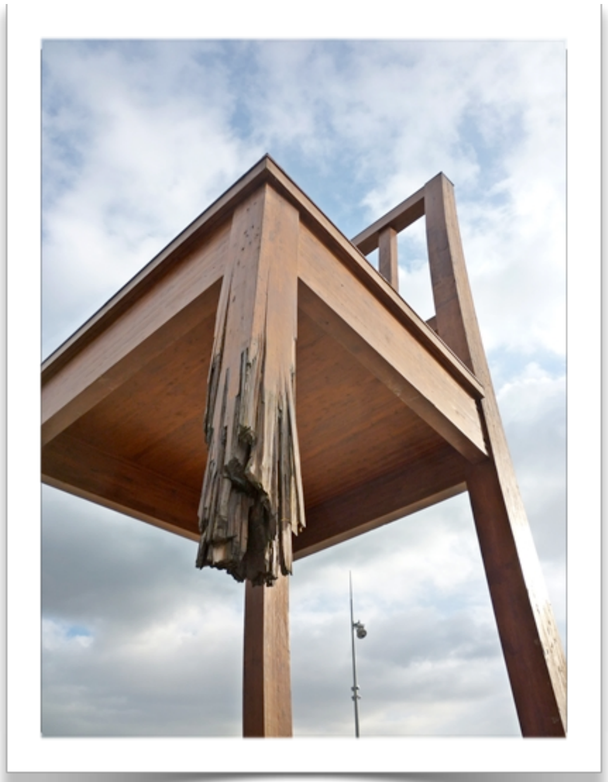
To correct for the finite key size, **the basic idea is to give all the statistic fluctuations to the adversary**, i.e.,

$$\hat{K}_{\mathrm{rate}} \approx 1 - \mathrm{h}_2(e_{\mathrm{phase}} + \Delta e_{\mathrm{phase}}) - \mathrm{h}_2(e_{\mathrm{bit}} + \Delta e_{\mathrm{bit}})$$

However, most of the finite-key security proofs assume that the devices are perfect.

Brute force approach

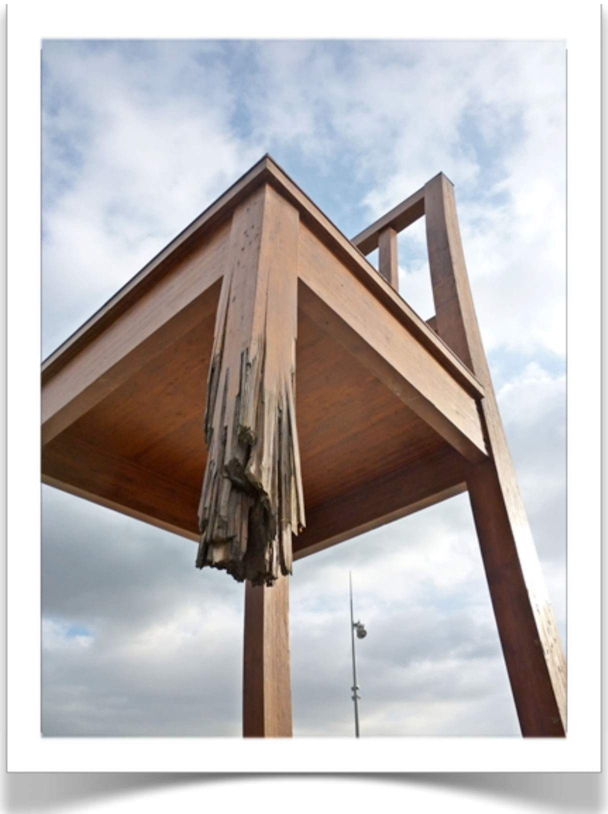
Brute force approach



Devices are **imperfect** w.r.t the theoretical models used in the proof.

Hidden Side-Channels

Brute force approach



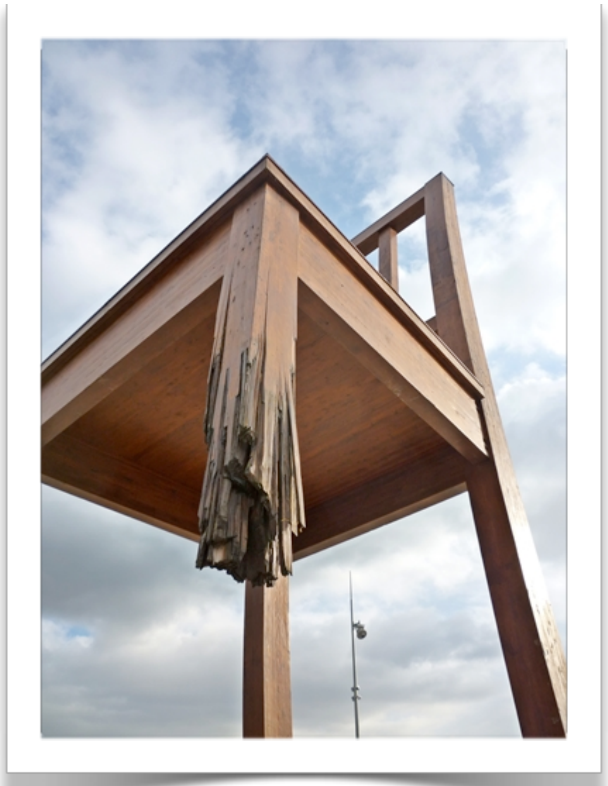
Devices are **imperfect** w.r.t the theoretical models used in the proof.

Hidden Side-Channels

Step 1:
a complete characterization of the devices

Brute force approach

Hidden Side-Channels

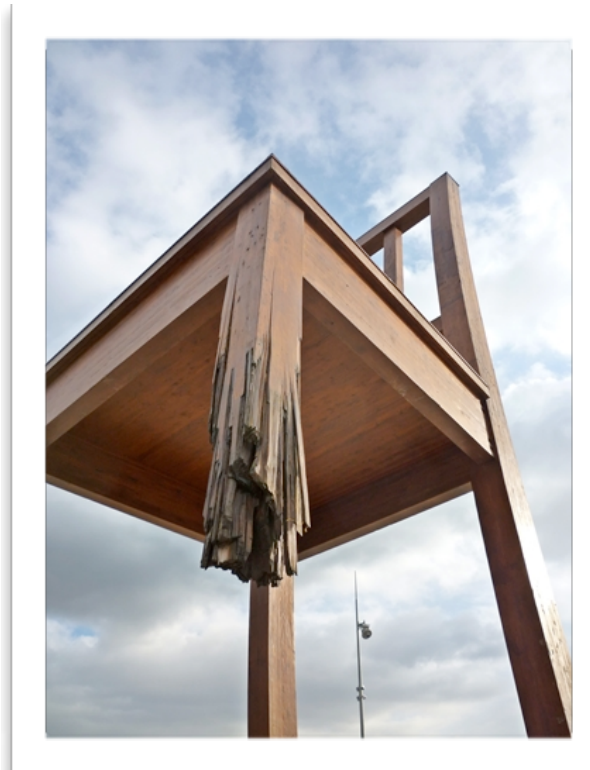


Devices are **imperfect** w.r.t the theoretical models used in the proof.

Step 1:
a complete characterization of the devices

Step 2:
Put all the parameters into the security proof

Brute force approach



Devices are **imperfect** w.r.t the theoretical models used in the proof.

Hidden Side-Channels

Step 1:
a complete characterization of the devices

Step 2:
Put all the parameters into the security proof

Step 3:
Add in all the statistical fluctuations

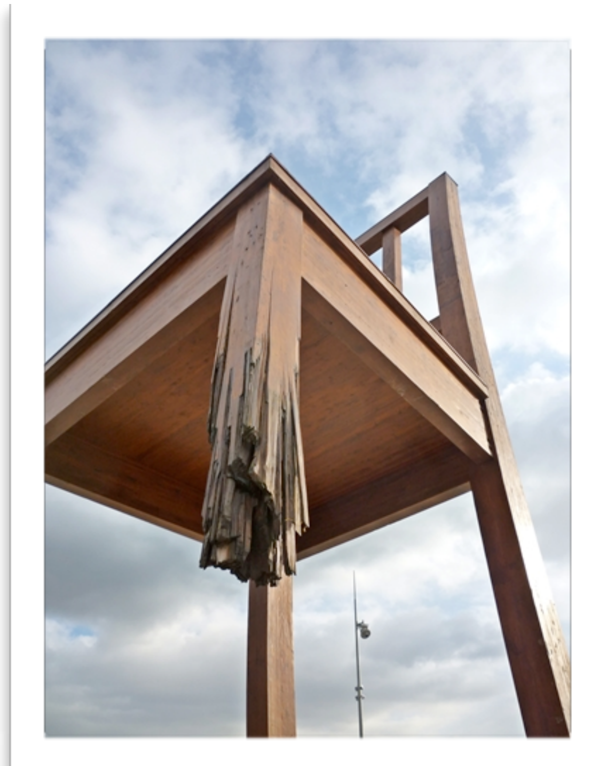
Most pre-existing proofs are valid only in the **asymptotic limit**

Brute force approach

What happens next?

Step 3:
Add in all the statistical fluctuations

Most pre-existing proofs are valid only in the **asymptotic limit**



Devices are **imperfect** w.r.t the theoretical models used in the proof.

Hidden Side-Channels

Step 1:
a complete characterization of the devices

Step 2:
Put all the parameters into the security proof

Brute force approach

Although it appears possible to attain such a security proof, one can imagine....

Brute force approach

Although it appears possible to attain such a security proof, one can imagine....

Disadvantages:

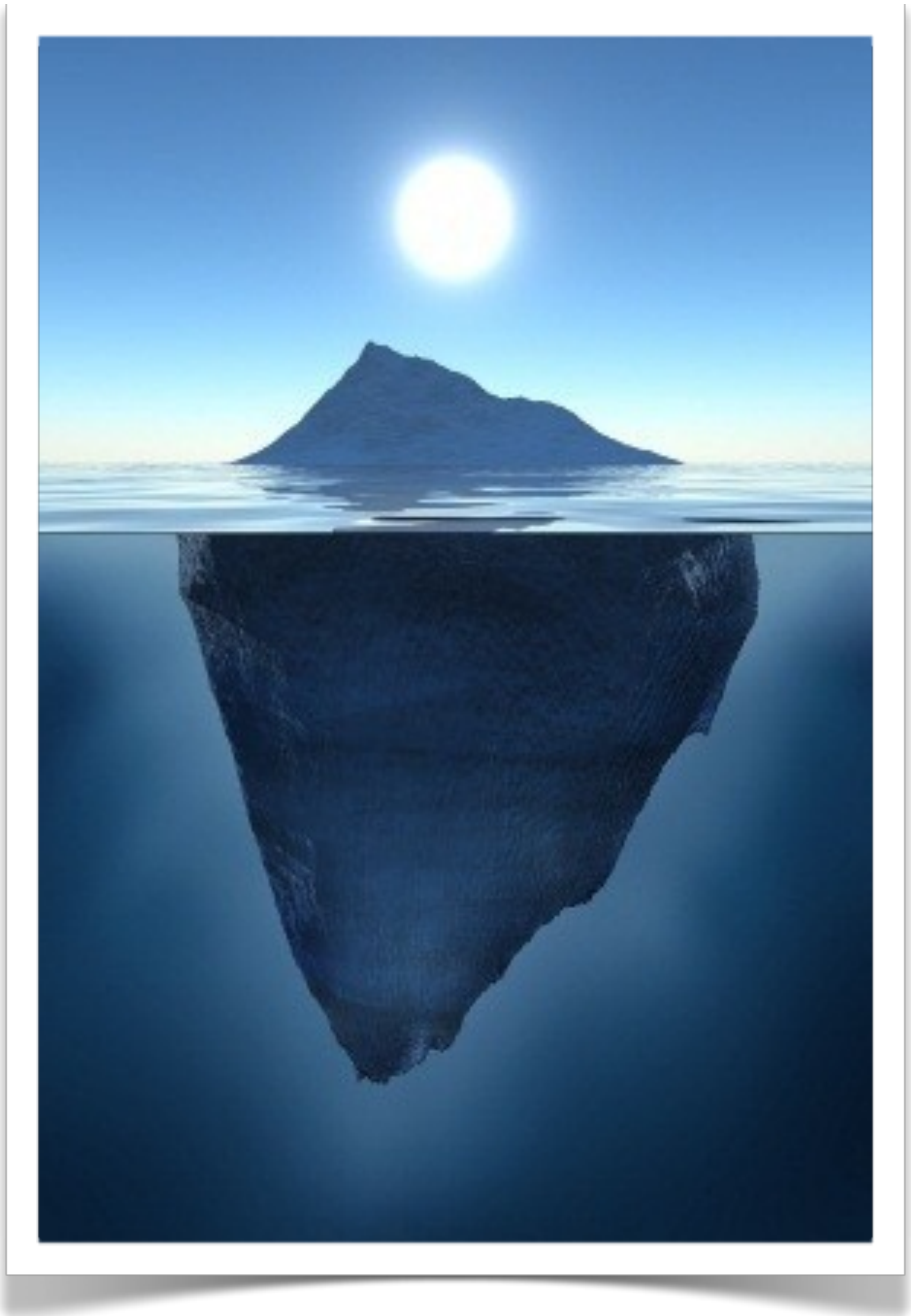
- Very likely to require a large amount of signals
- Cumbersome
- Requires more local randomness for parameter estimation phase
- Difficult to identify the entire set of discrepancies

Brute force approach

Although it appears possible to attain such a security proof, one can imagine....

Disadvantages:

- Very likely to require a large amount of signals
- Cumbersome
- Requires more local randomness for parameter estimation phase
- Difficult to identify the entire set of discrepancies



An iceberg in QKD

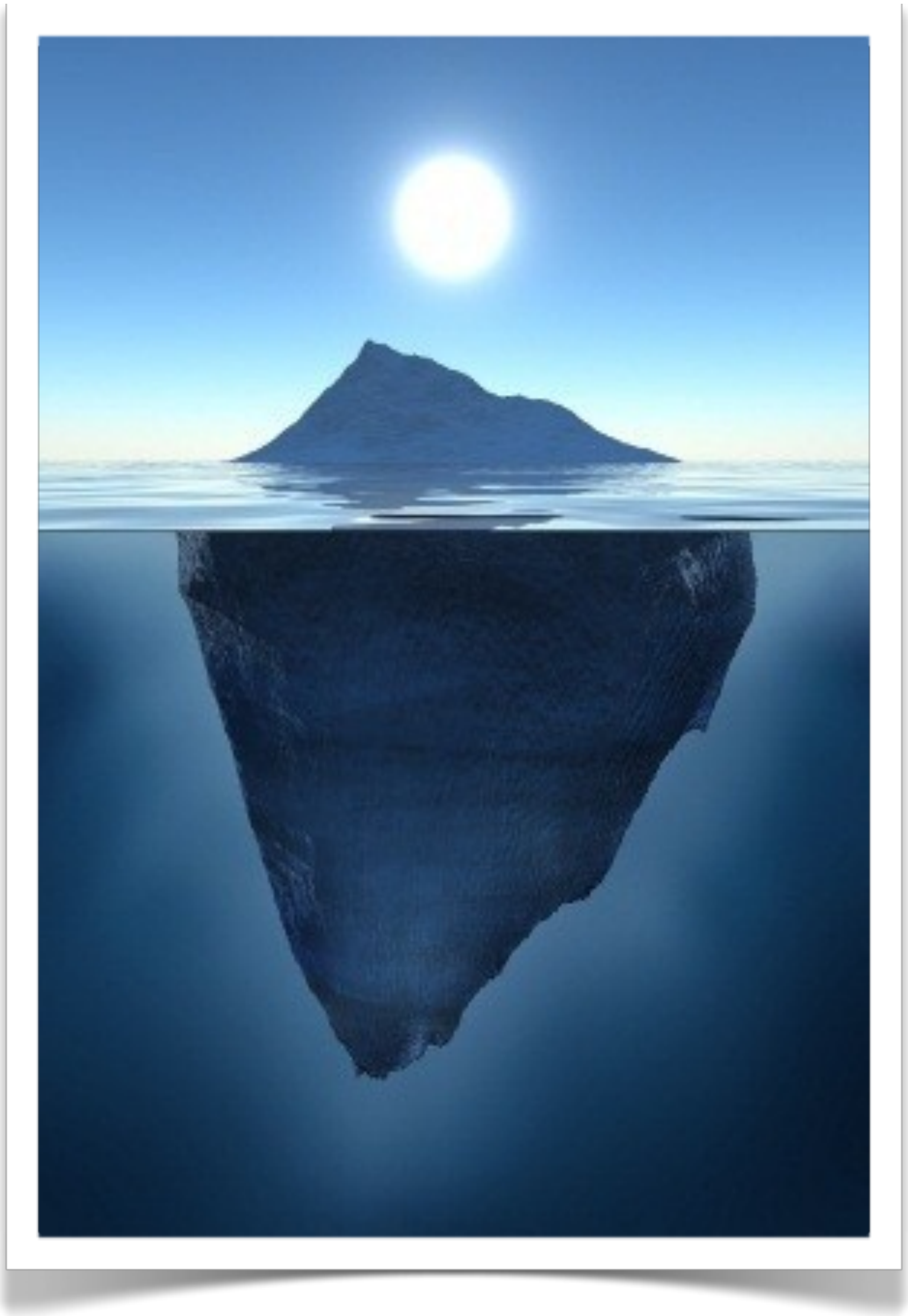
Brute force approach

Although it appears possible to attain such a security proof, one can imagine....

Disadvantages:

- Very likely to require a large amount of signals
- Cumbersome
- Requires more local randomness for parameter estimation phase
- Difficult to identify the entire set of discrepancies

Need an alternative method!!!



An iceberg in QKD

Building a clean approach

Building a clean approach

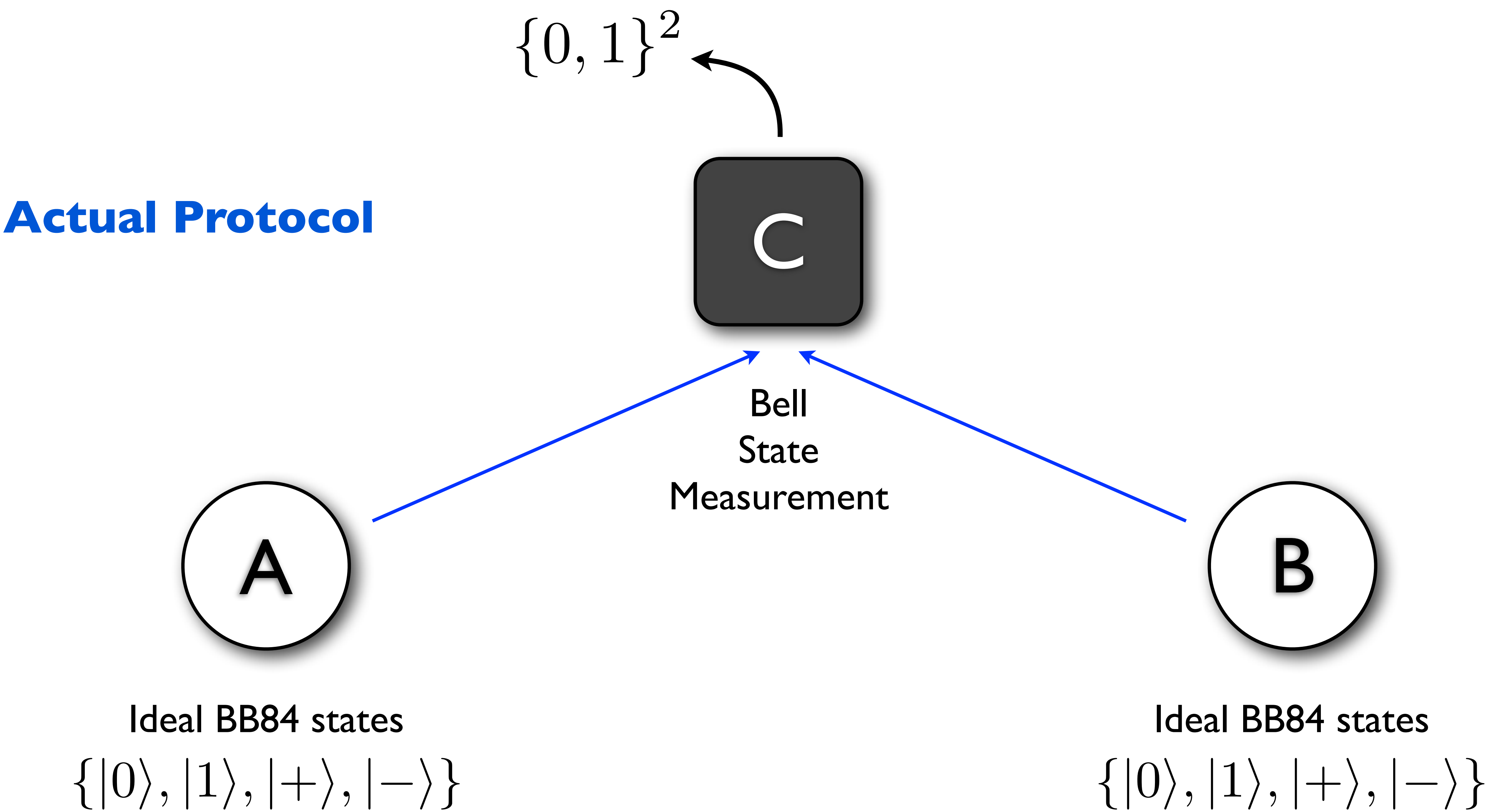
First, tackle the Trojan-horse attacks via the idea of Time-reversed EPR scheme

Biham, Huttner and Mor (1996) and Inamori (2005)

Building a clean approach

First, tackle the Trojan-horse attacks via the idea of Time-reversed EPR scheme

Biham, Huttner and Mor (1996) and Inamori (2005)

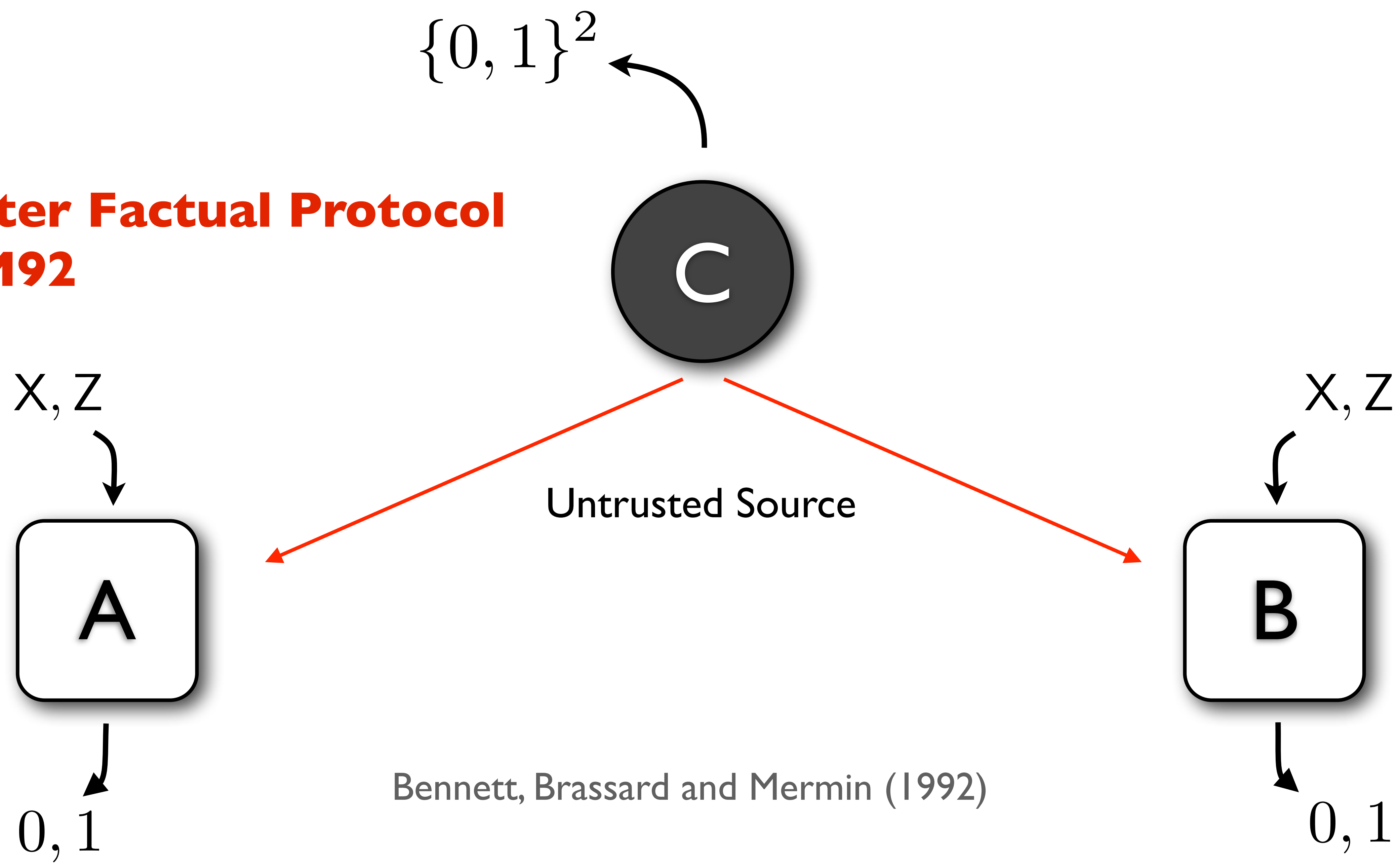


Building a clean approach

First, tackle the Trojan-horse attacks via the idea of Time-reversed EPR scheme

Biham, Huttner and Mor (1996) and Inamori (2005)

Counter Factual Protocol
=BBM92

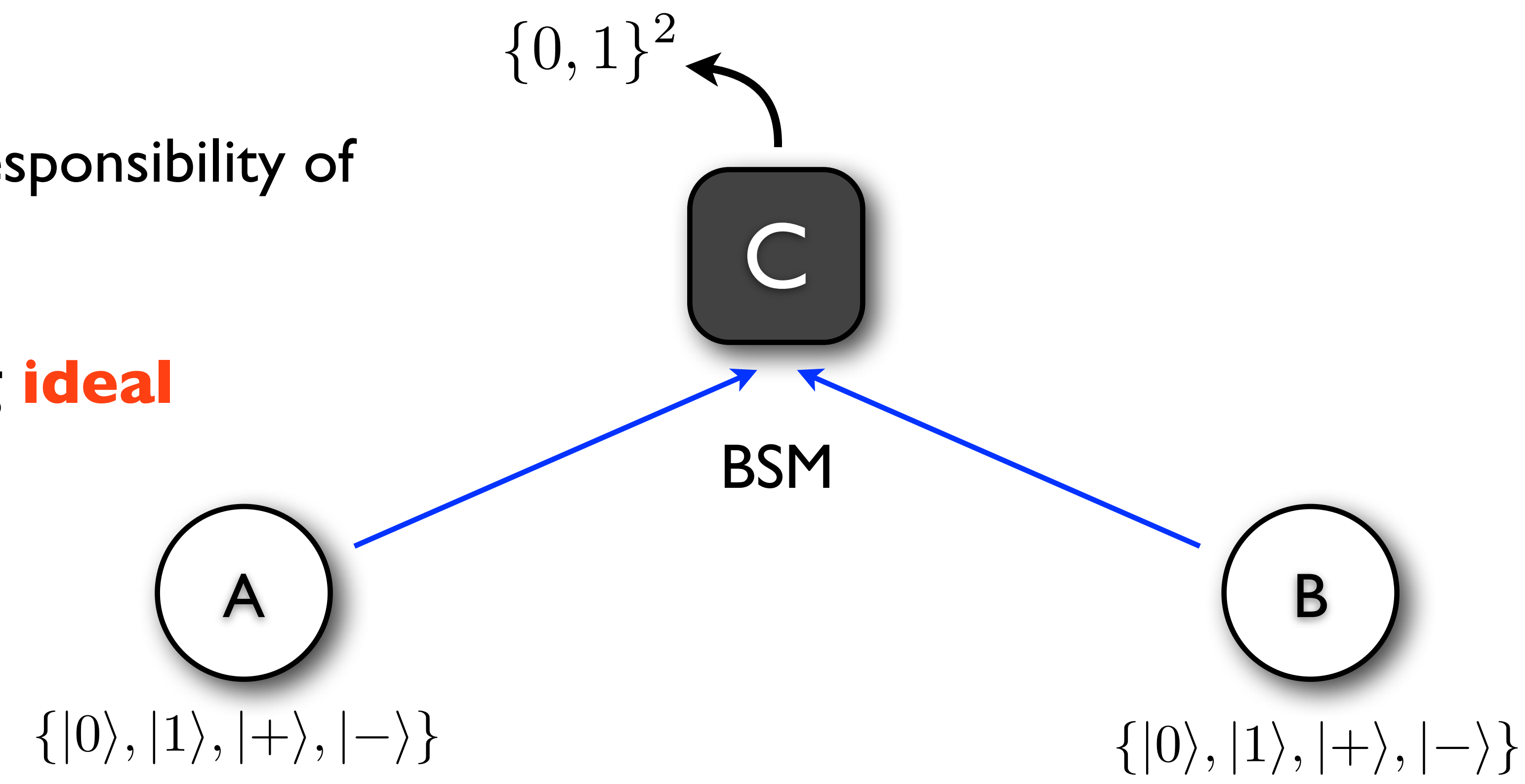


Bennett, Brassard and Mermin (1992)

Building a clean approach

In this picture, one does not have the responsibility of the detectors.

But Alice and Bob are still using ideal devices.

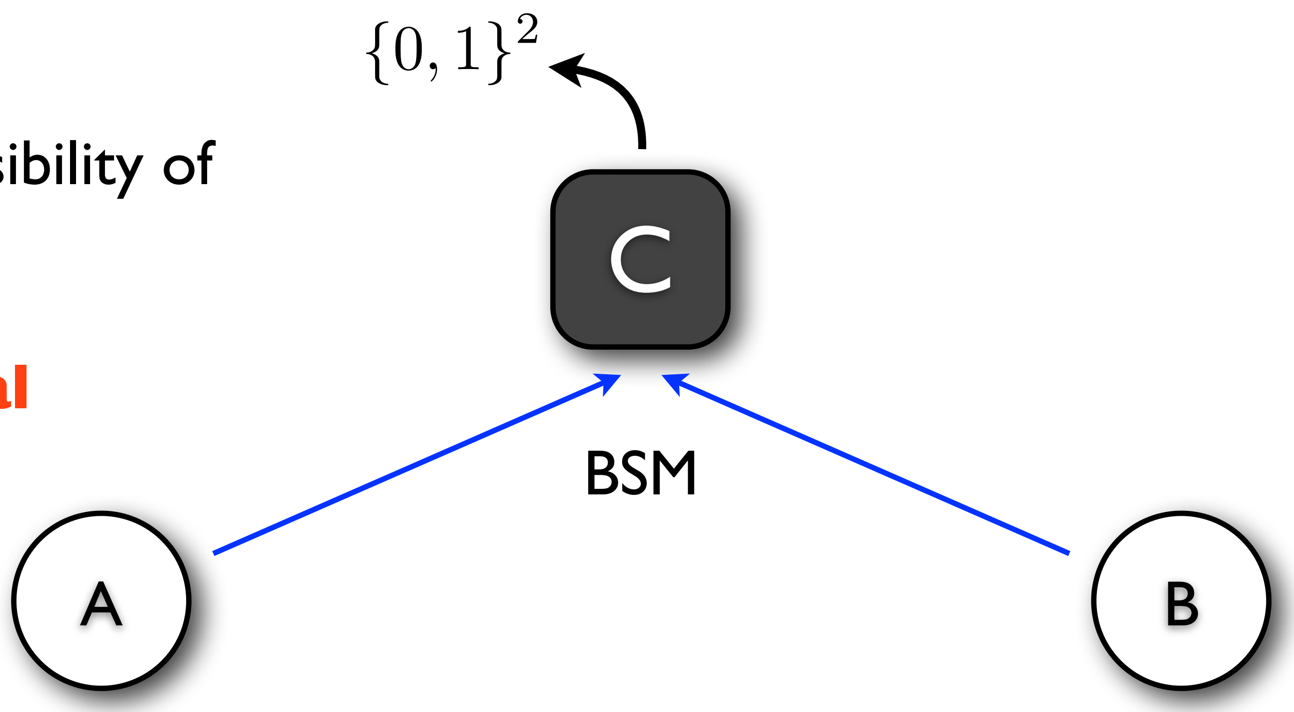


Building a clean approach

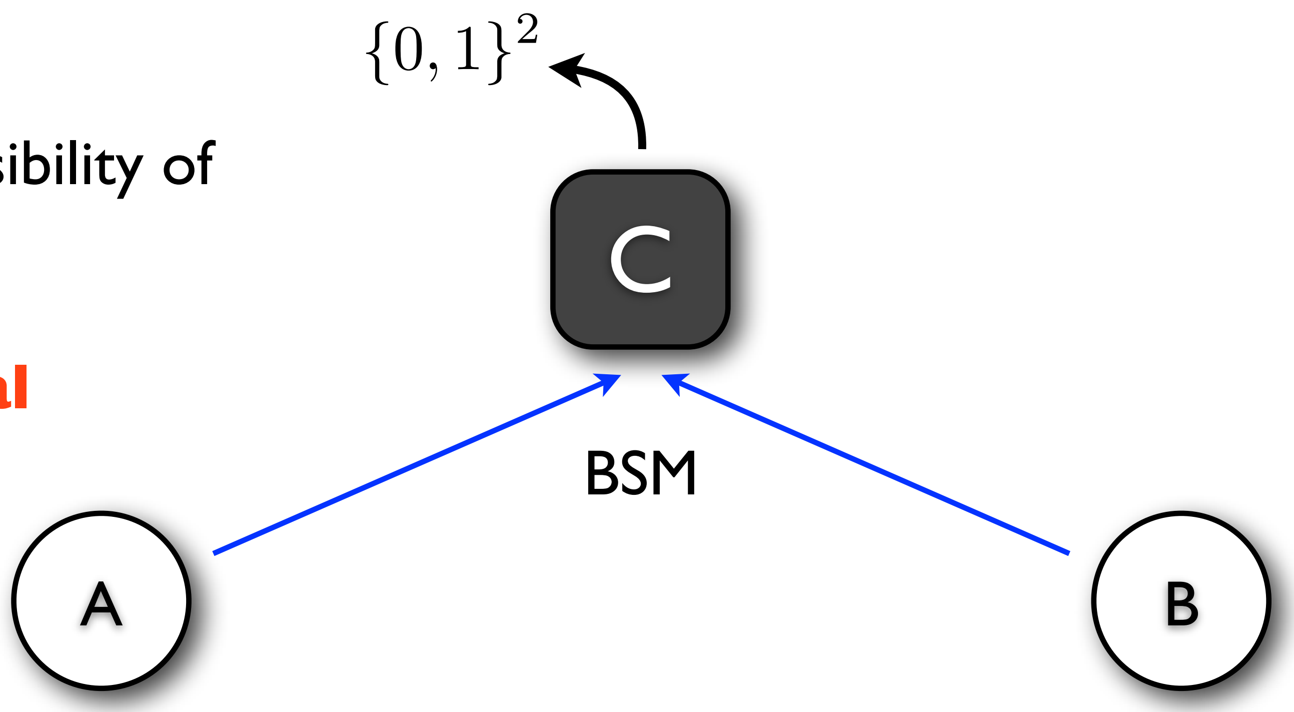
In this picture, one does not have the responsibility of the detectors.

But Alice and Bob are still using ideal devices.

Lo, Curty and Qi (2012) and Braunstein and Pirandola (2012)



Building a clean approach



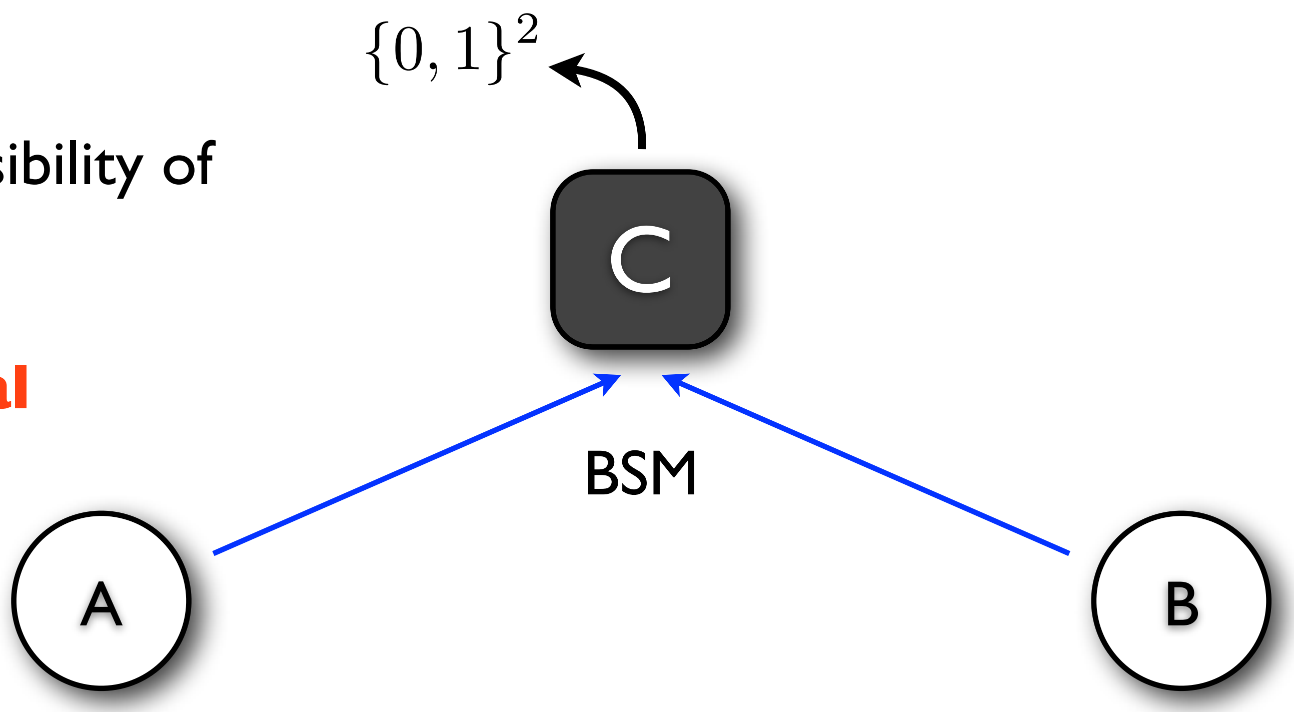
In this picture, one does not have the responsibility of the detectors.

But Alice and Bob are still using ideal devices.

Lo, Curty and Qi (2012) and Braunstein and Pirandola (2012)

Qn: It is too cumbersome to obtain a complete knowledge of all my local devices, I just want to use my devices, regardless of all those small discrepancies. Can I still generate secure keys with them?

Building a clean approach



In this picture, one does not have the responsibility of the detectors.

But Alice and Bob are still using ideal devices.

Lo, Curty and Qi (2012) and Braunstein and Pirandola (2012)

Qn: It is too cumbersome to obtain a complete knowledge of all my local devices, I just want to use my devices, regardless of all those small discrepancies. Can I still generate secure keys with them?

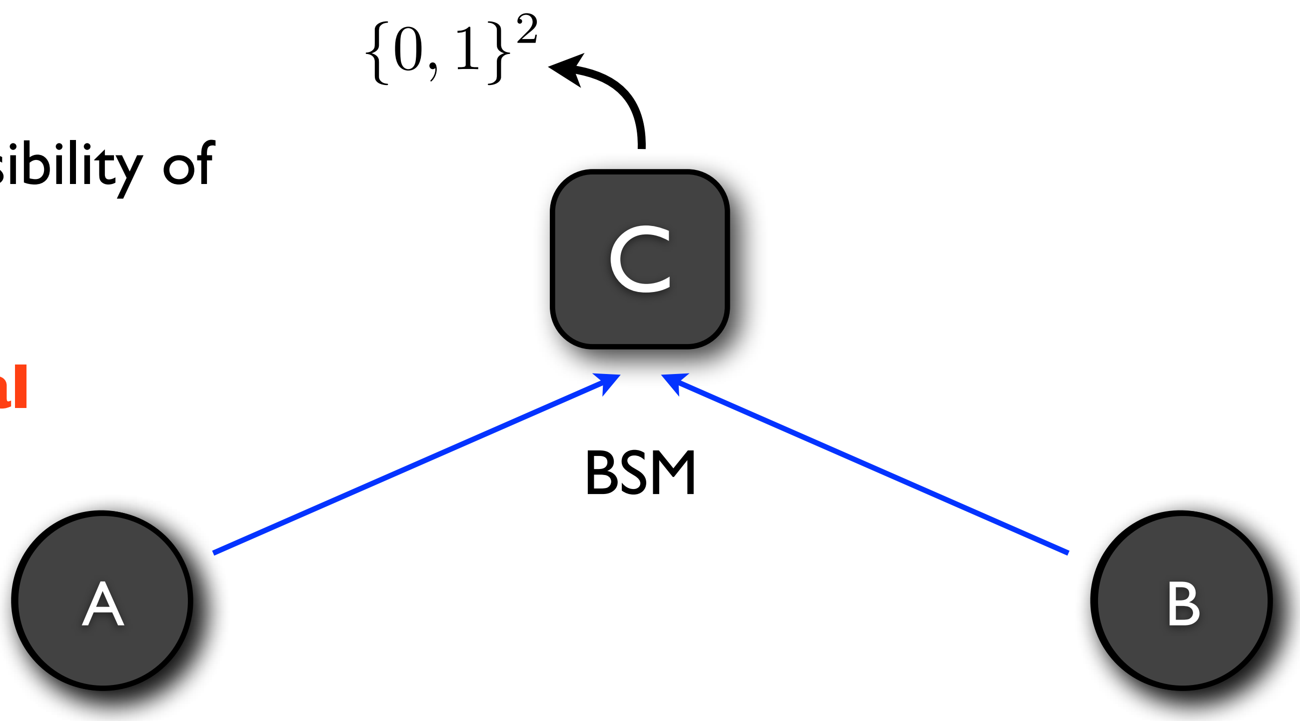
Ans: The first yes: output a key (of zero length) and you get an unconditionally secure key. The second yes...

Building a clean approach

In this picture, one does not have the responsibility of the detectors.

But Alice and Bob are still using ideal devices.

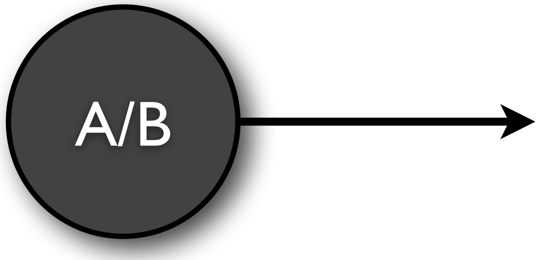
Lo, Curty and Qi (2012) and Braunstein and Pirandola (2012)



Qn: It is too cumbersome to obtain a complete knowledge of all my local devices, I just want to use my devices, regardless of all those small discrepancies. Can I still generate secure keys with them?

Ans: The first yes: output a key (of zero length) and you get an unconditionally secure key. The second yes...

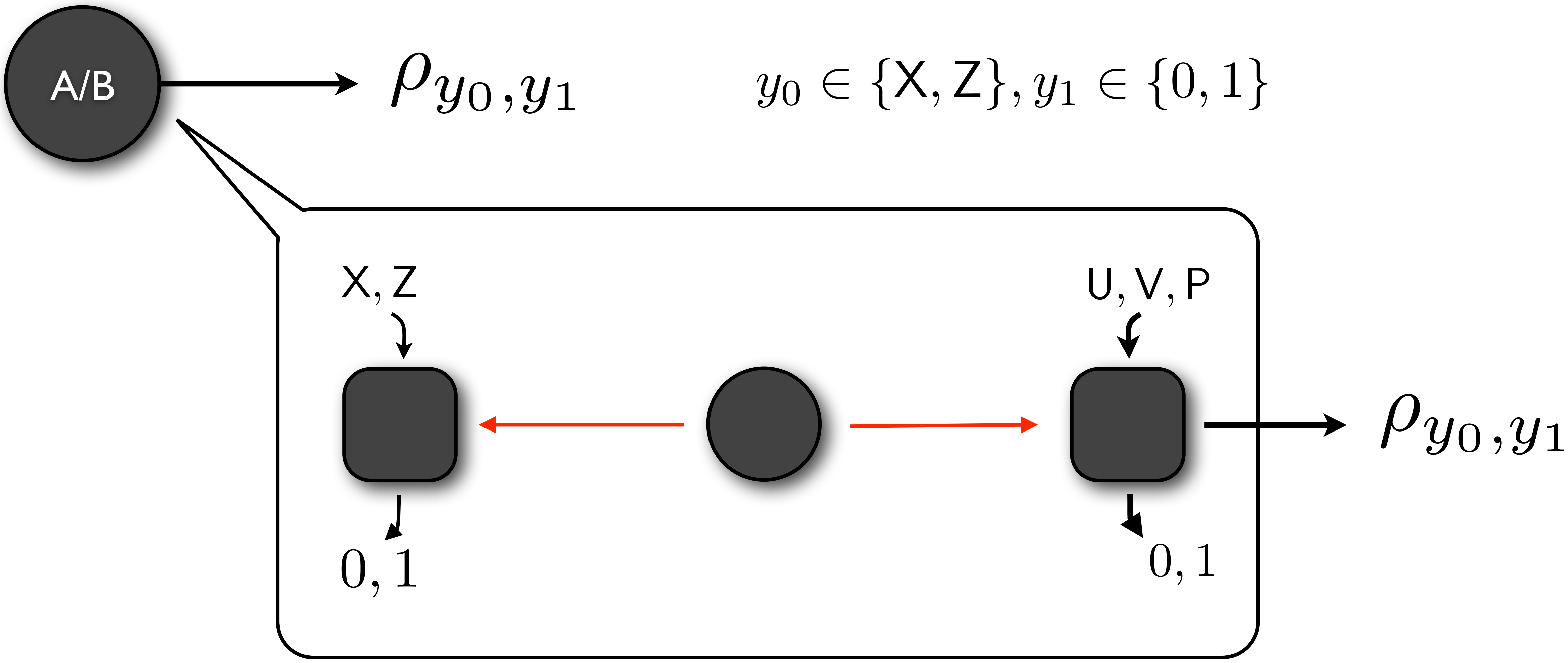
Building a clean approach



ρ_{y_0,y_1}

$y_0 \in \{\mathsf{X}, \mathsf{Z}\}, y_1 \in \{0, 1\}$

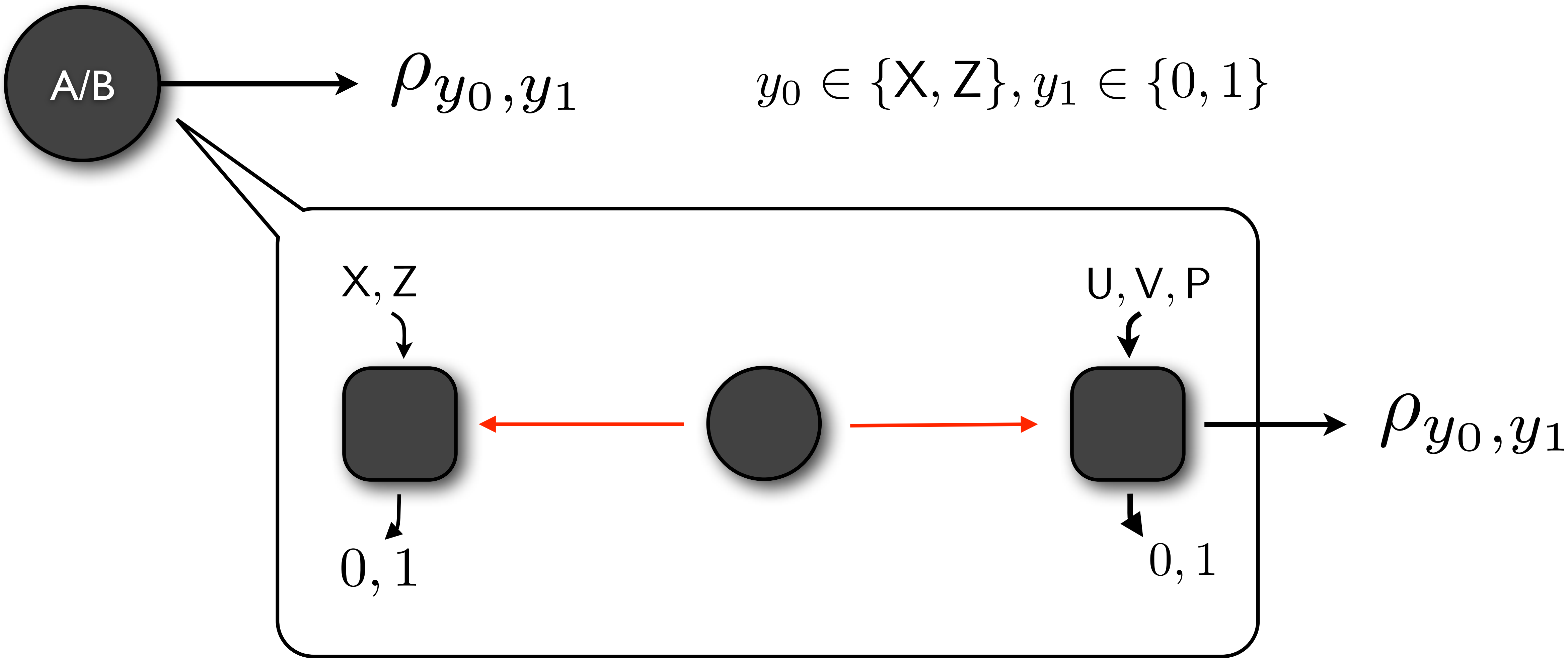
Building a clean approach



Tomamichel and Hanggi (2011)
and Lim *et al* (2012)

Key Idea: Run the CHSH test

Building a clean approach



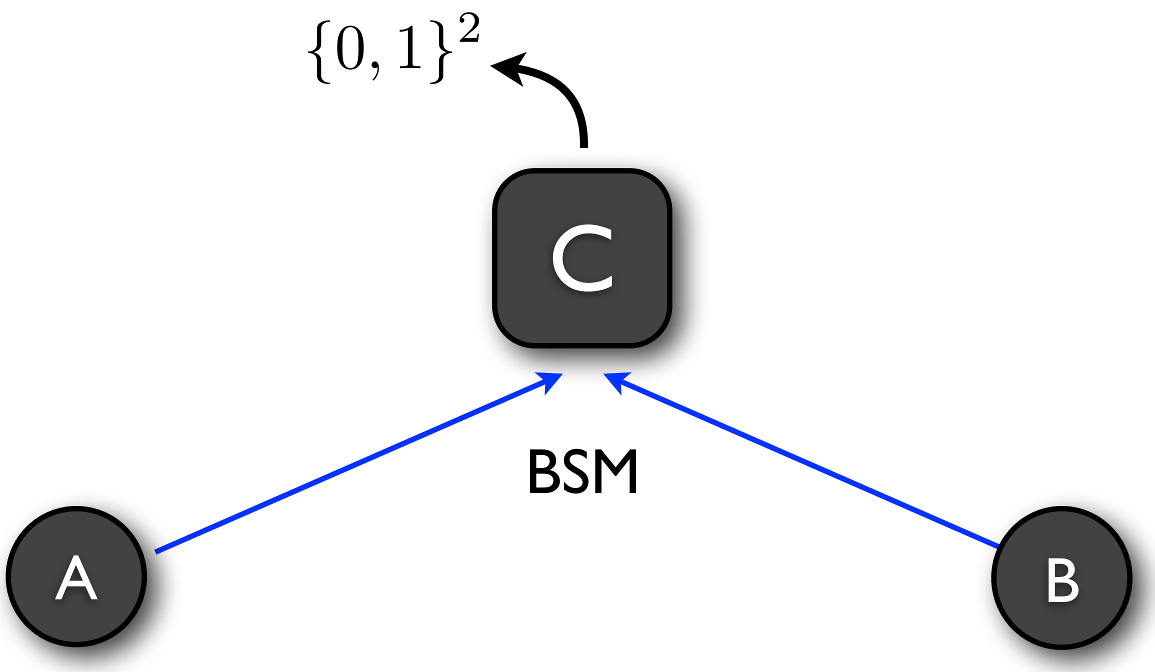
Tomamichel and Hanggi (2011)
and Lim *et al* (2012)

Key Idea: Run the CHSH test

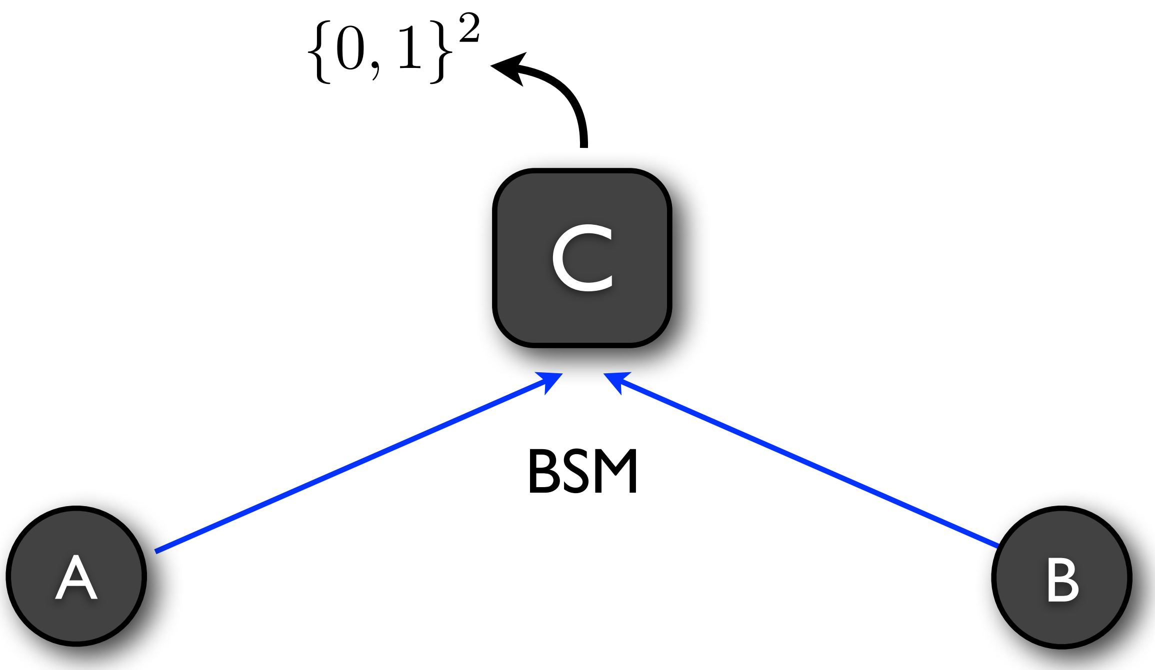
Certification of BB84 states (limiting case)

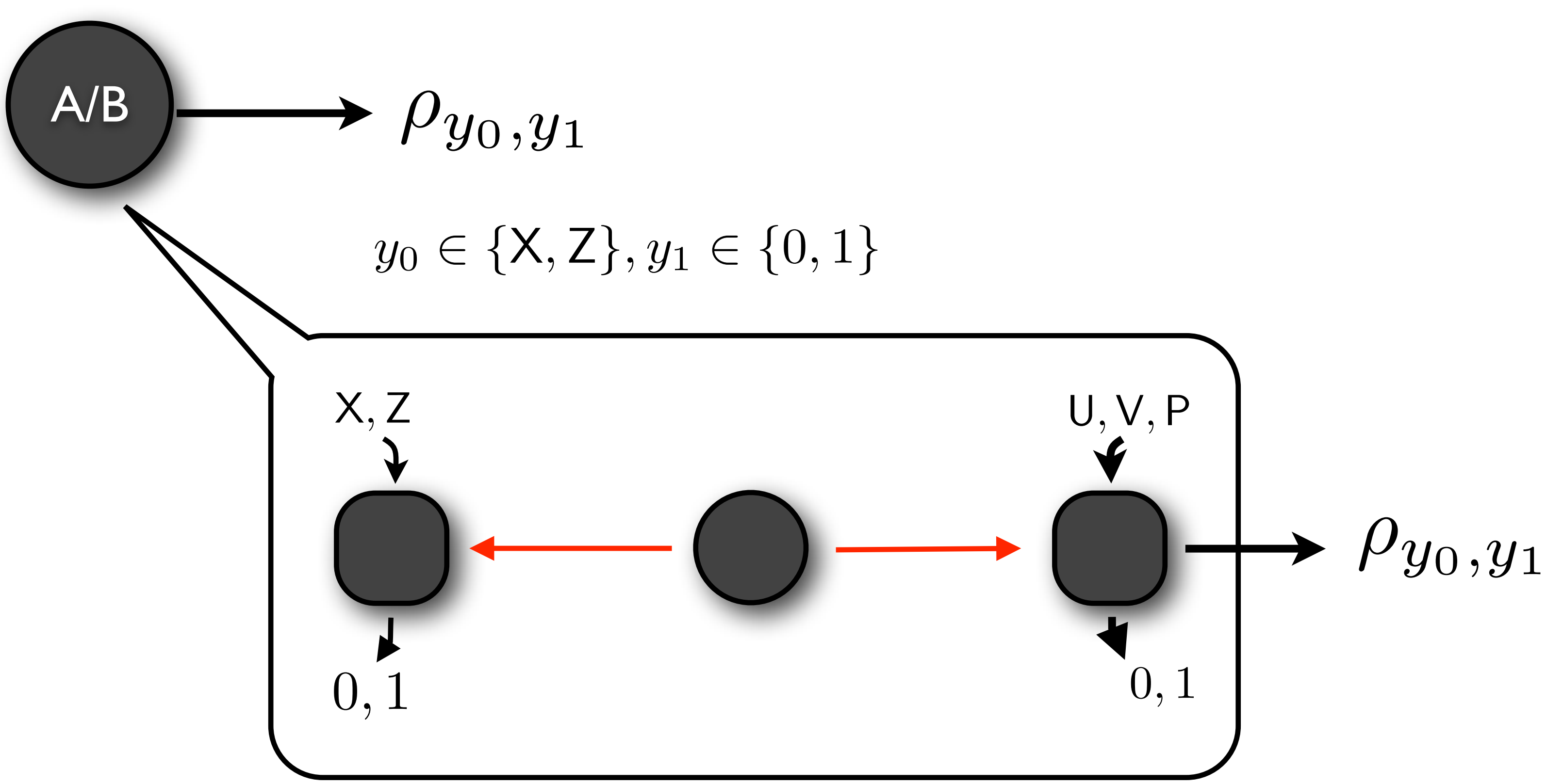
If the maximal violation of the CHSH test is observed, then the output states are the BB84 states.

Building a clean approach

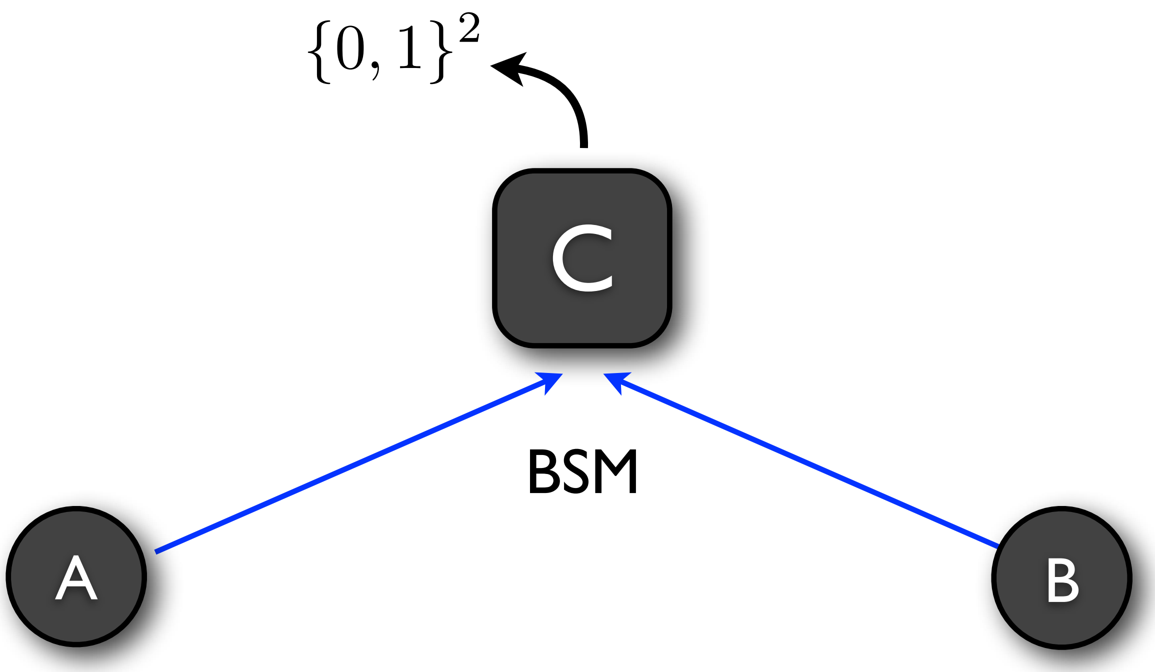


Building a clean approach

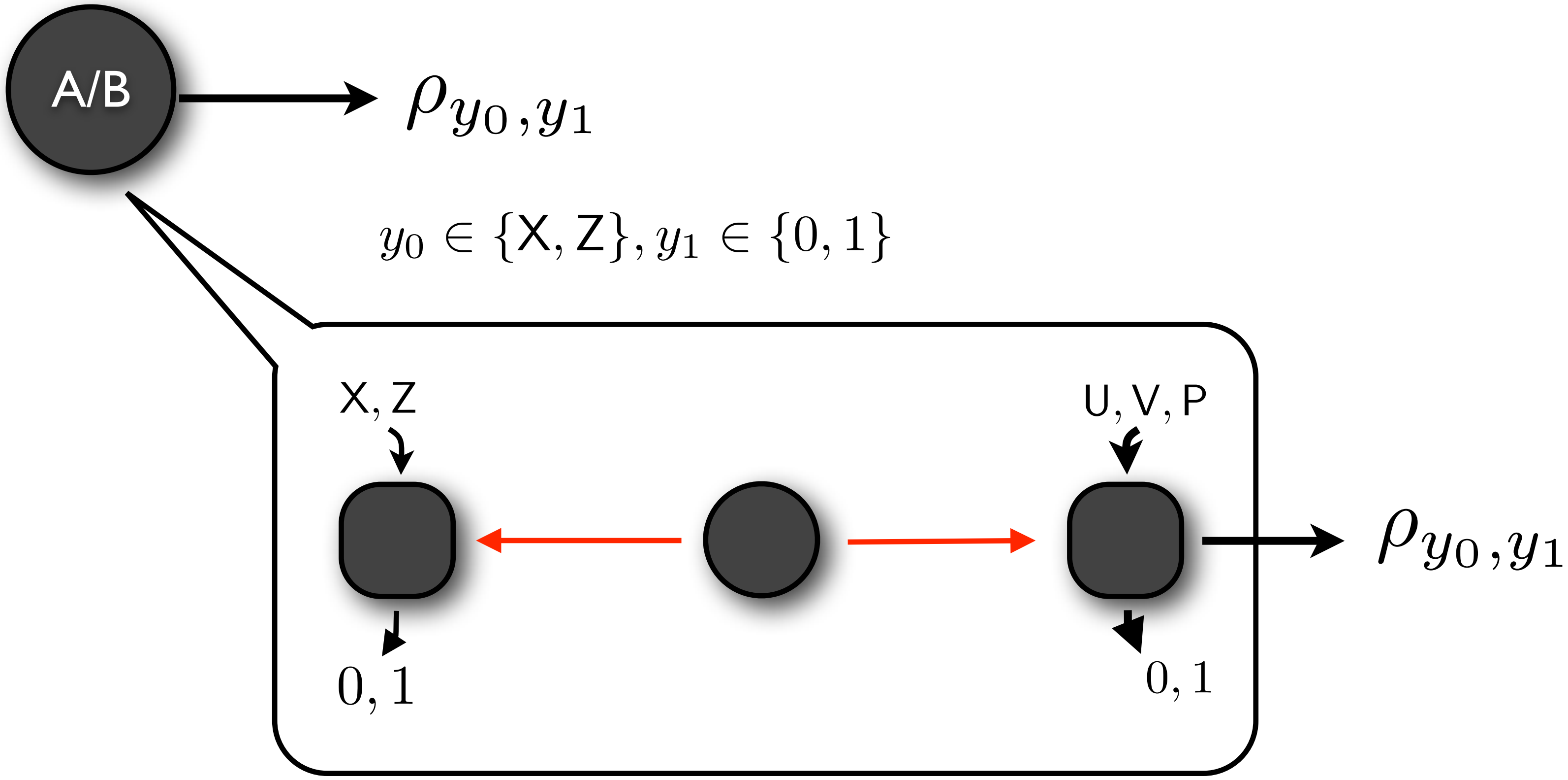




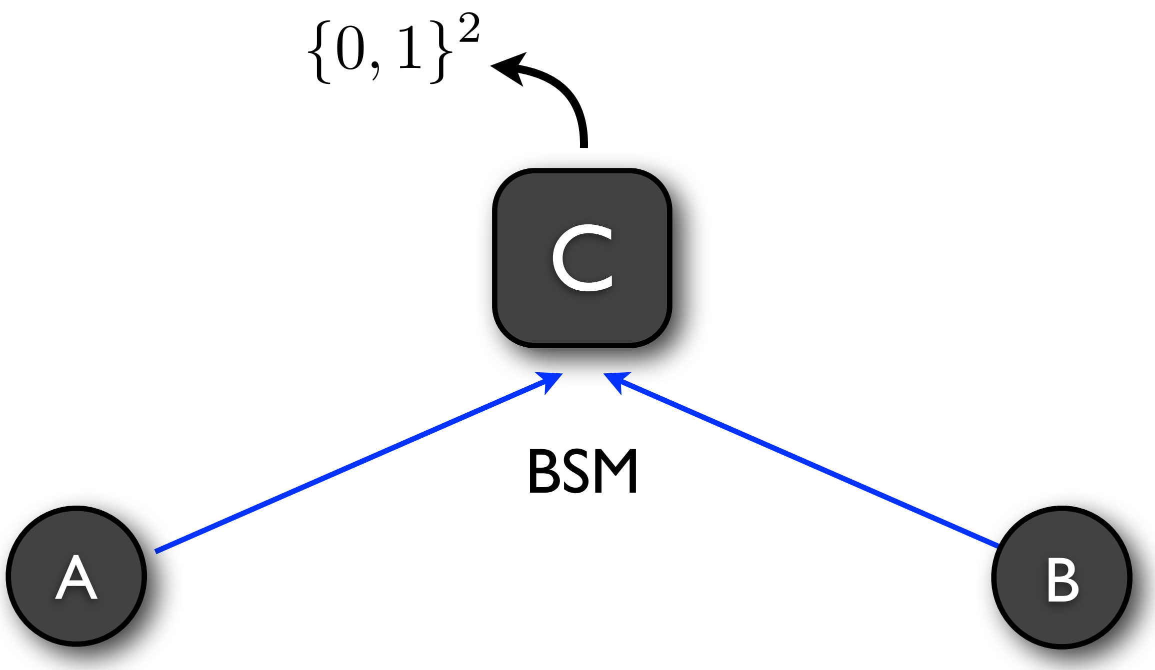
Building a clean approach



Advantages

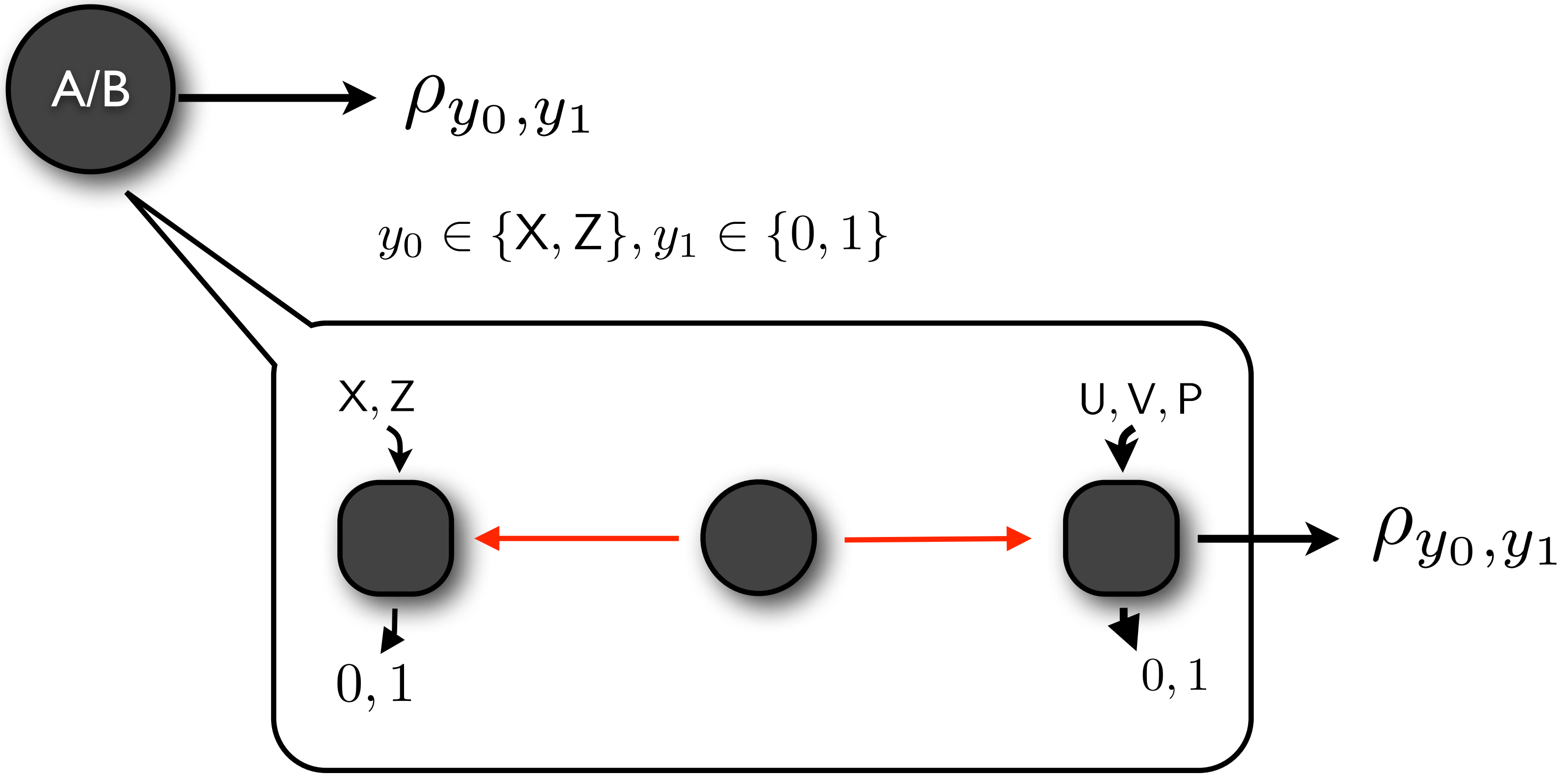


Building a clean approach

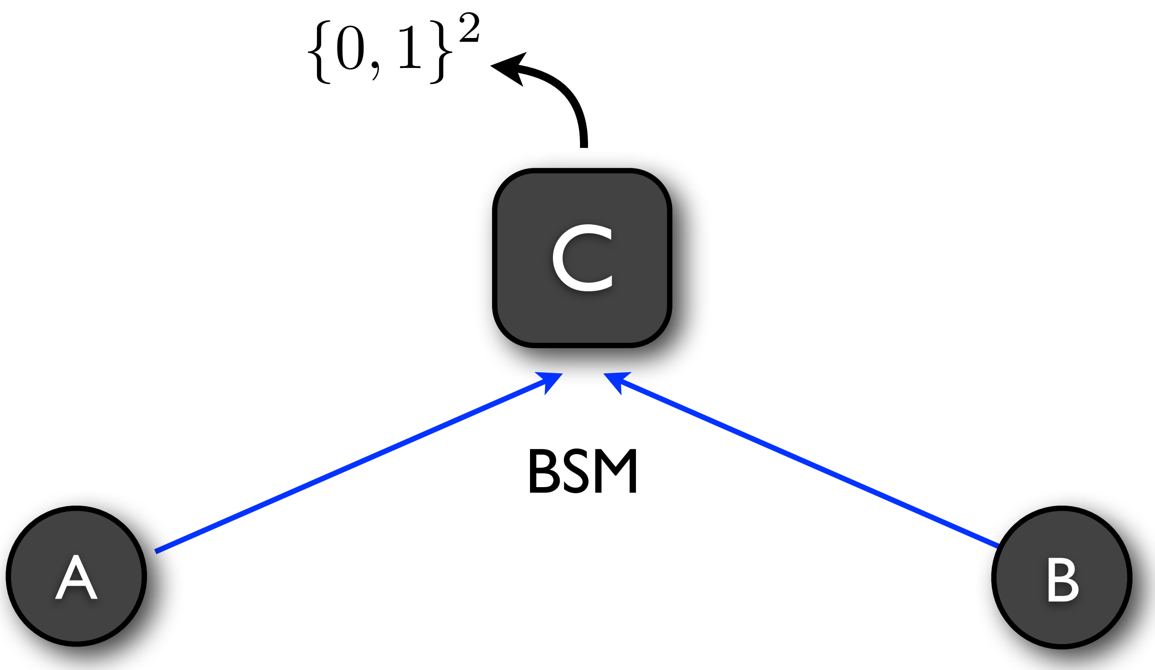


Advantages

- Trojan-Horse and Blinding attacks free.

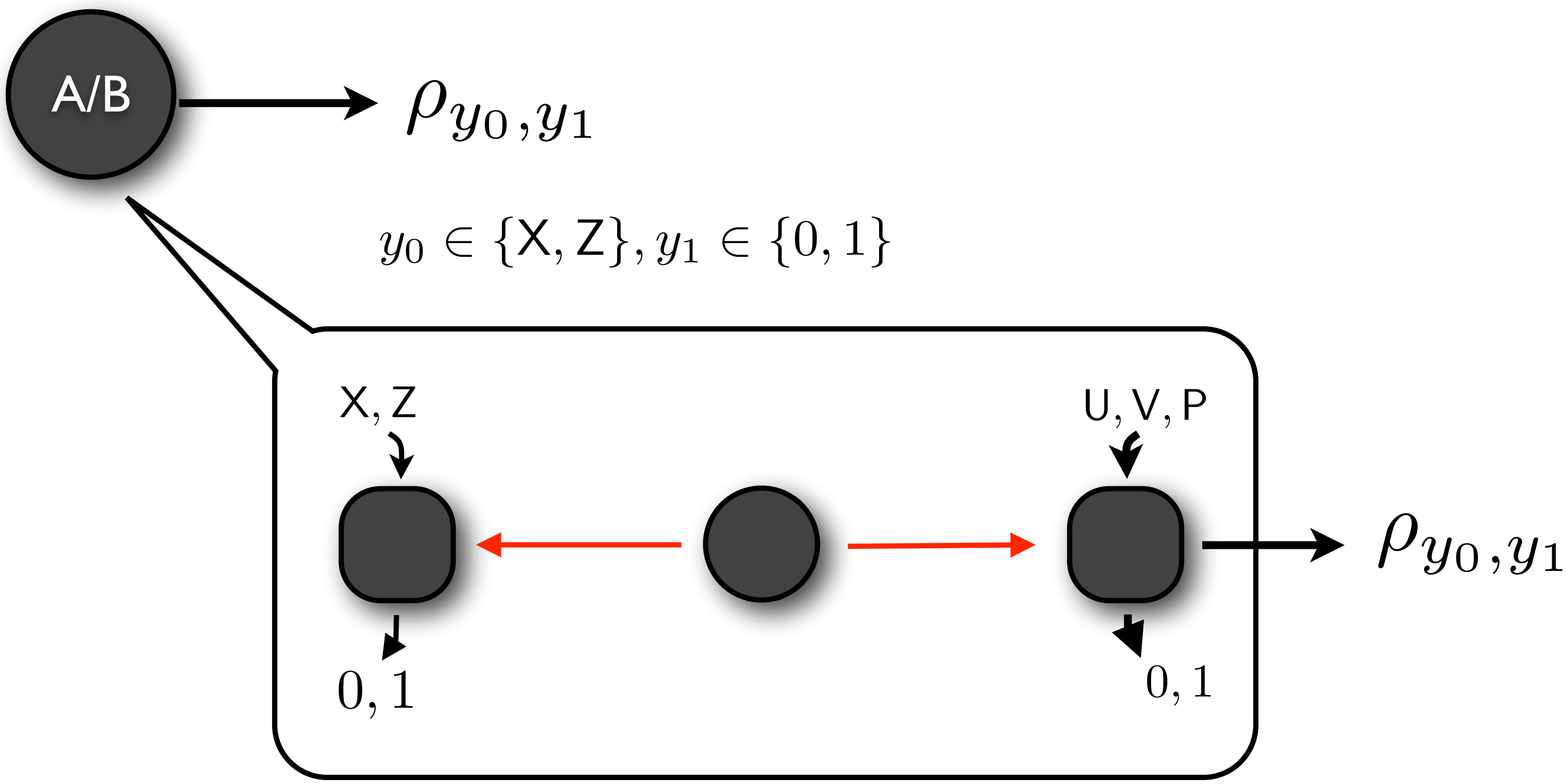


Building a clean approach

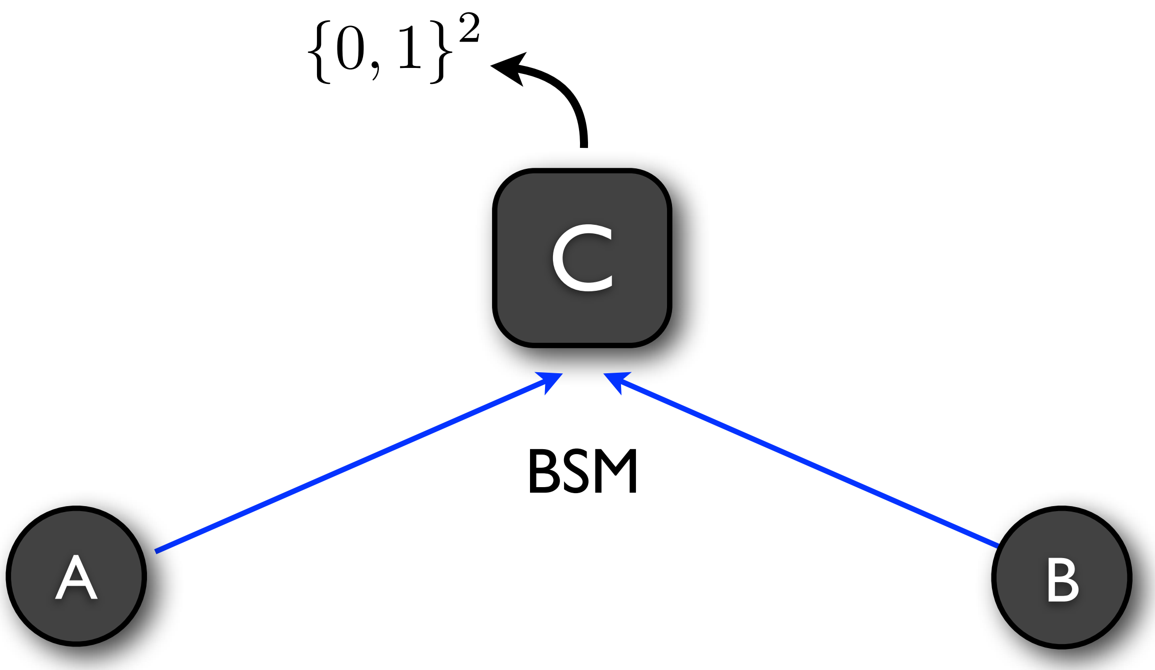


Advantages

- Trojan-Horse and Blinding attacks free.
- The devices only need to be characterized by one parameter, regardless of the number of discrepancies.

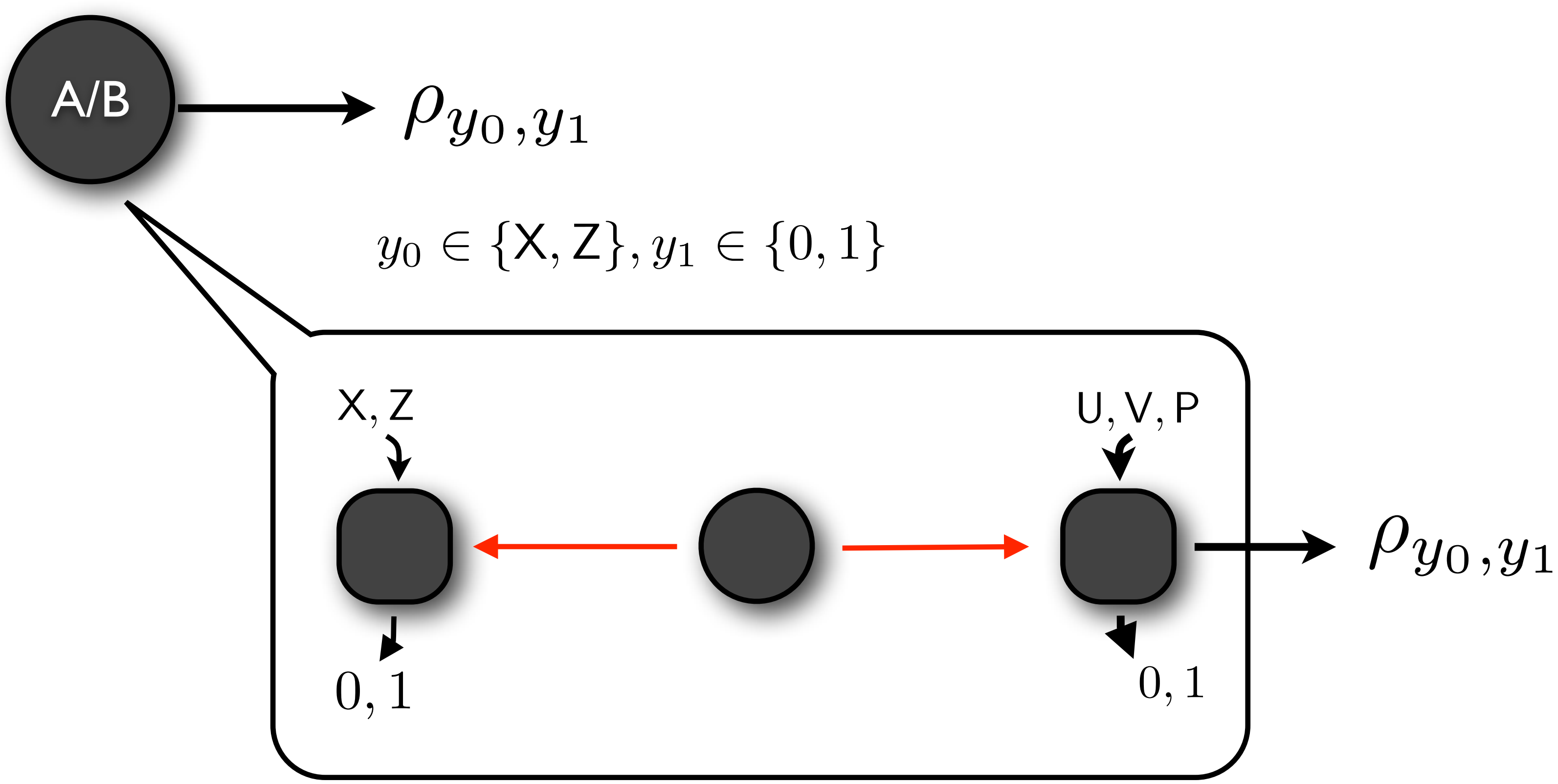


Building a clean approach

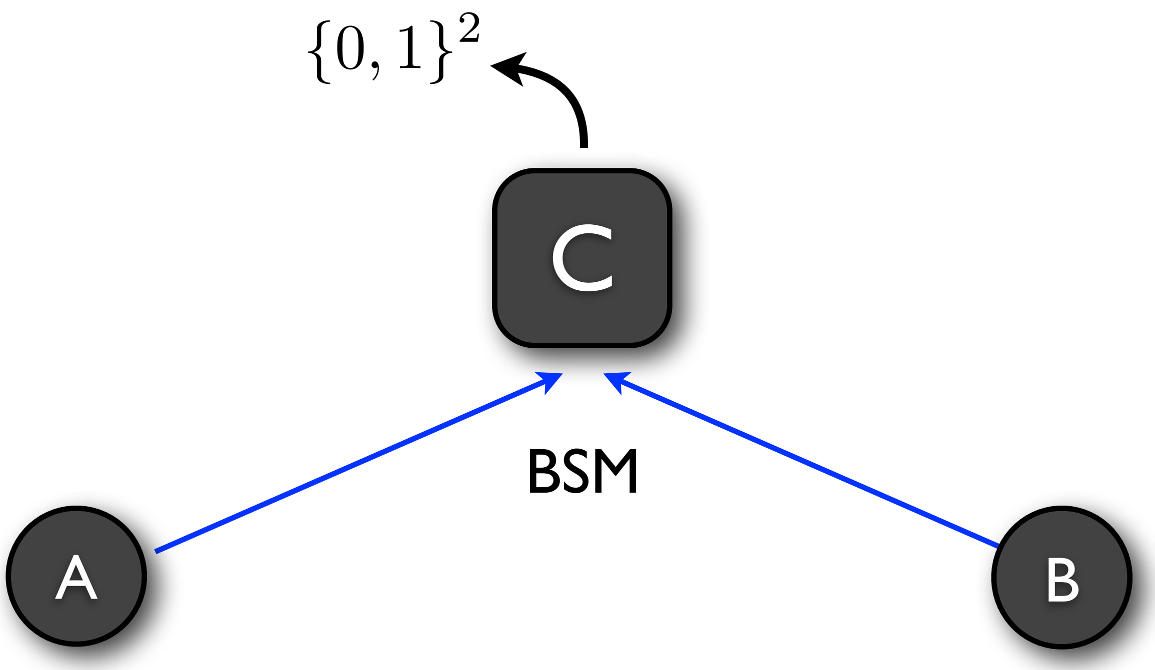


Advantages

- Trojan-Horse and Blinding attacks free.
- The devices only need to be characterized by one parameter, regardless of the number of discrepancies.
- The security proof is valid in the finite key size regime.



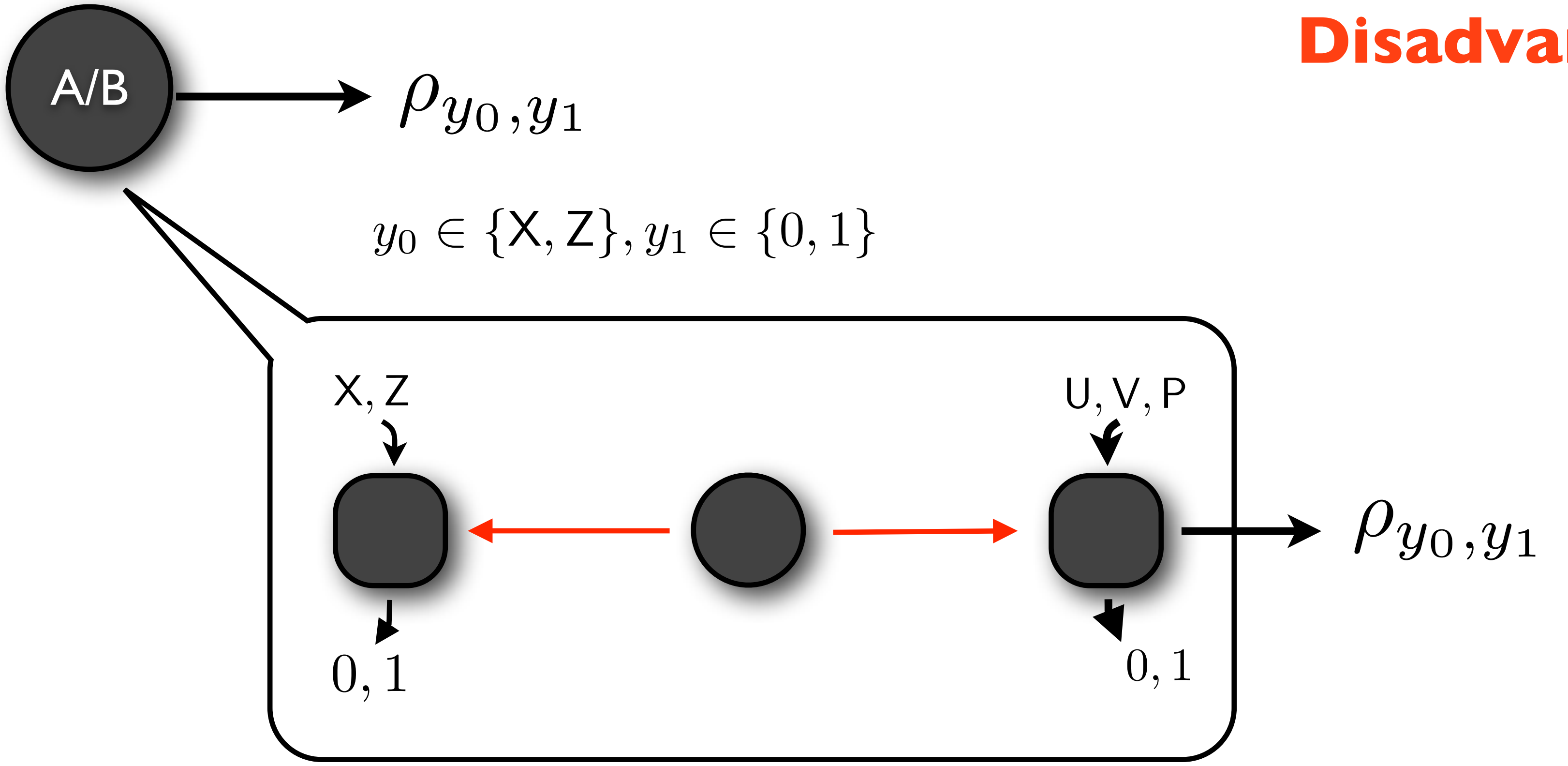
Building a clean approach



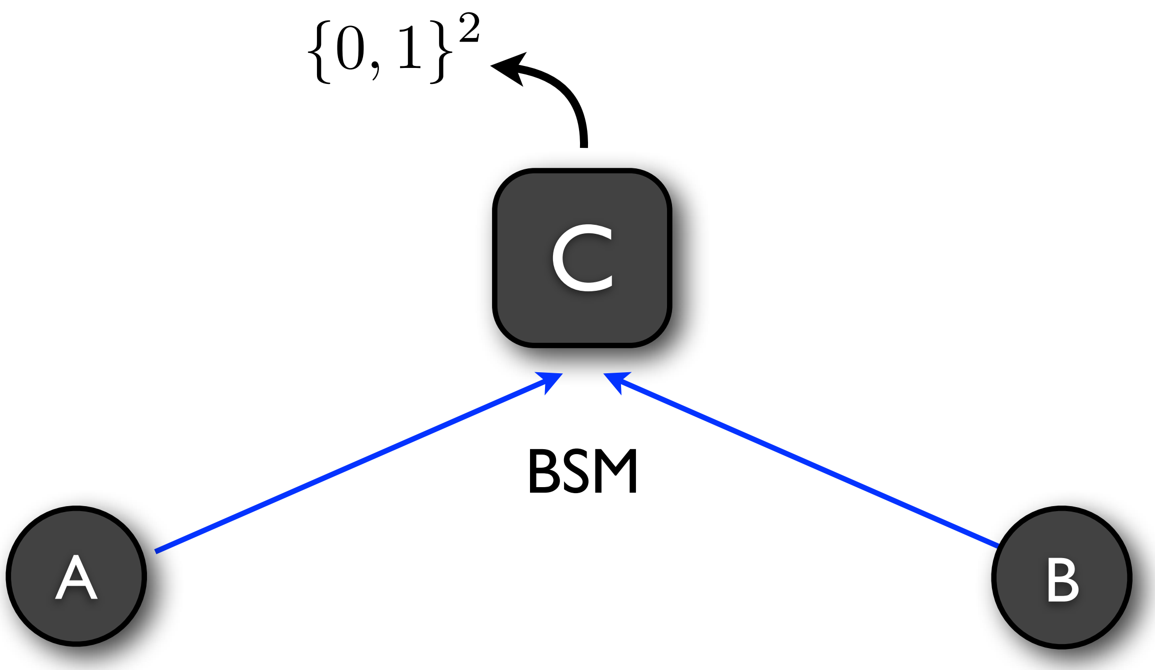
Advantages

- Trojan-Horse and Blinding attacks free.
- The devices only need to be characterized by one parameter, regardless of the number of discrepancies.
- The security proof is valid in the finite key size regime.

Disadvantages

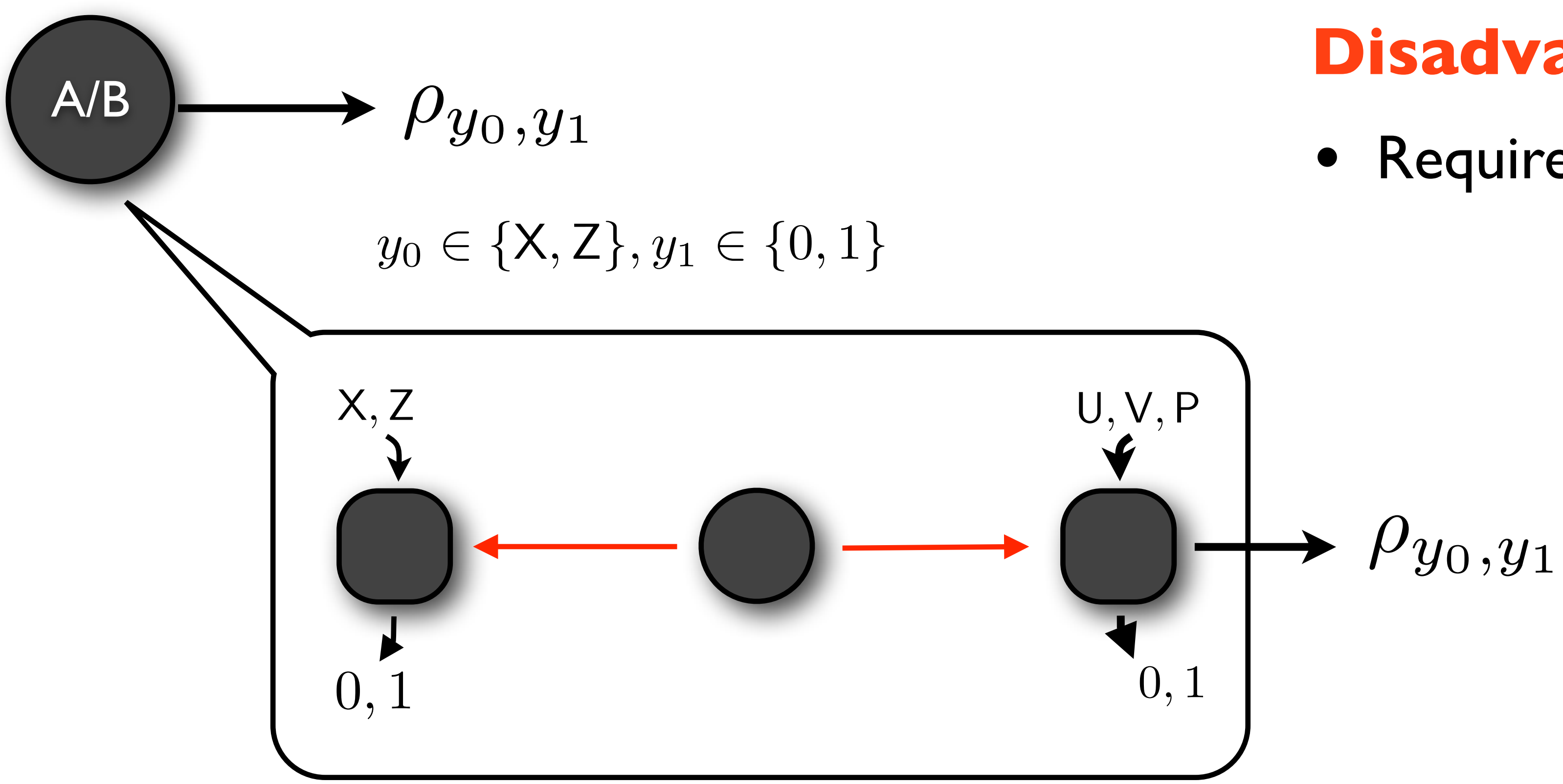


Building a clean approach



Advantages

- Trojan-Horse and Blinding attacks free.
- The devices only need to be characterized by one parameter, regardless of the number of discrepancies.
- The security proof is valid in the finite key size regime.



Disadvantages

- Requires local entanglement sources.

Secret key fraction

$$K_\infty = 1 - 2\mathrm{h}_2(e) - \log_2\left(1 + \frac{S}{4}\sqrt{8 - S^2}\right)$$

Secret key fraction

$$K_\infty = 1 - 2\mathrm{h}_2(e) - \log_2\left(1 + \frac{S}{4}\sqrt{8 - S^2}\right)$$

Secret key fraction of the BB84 protocol

Secret key fraction

$$K_\infty = 1 - 2\mathrm{h}_2(e) - \log_2\left(1 + \frac{S}{4}\sqrt{8 - S^2}\right)$$

Secret key fraction of the BB84 protocol

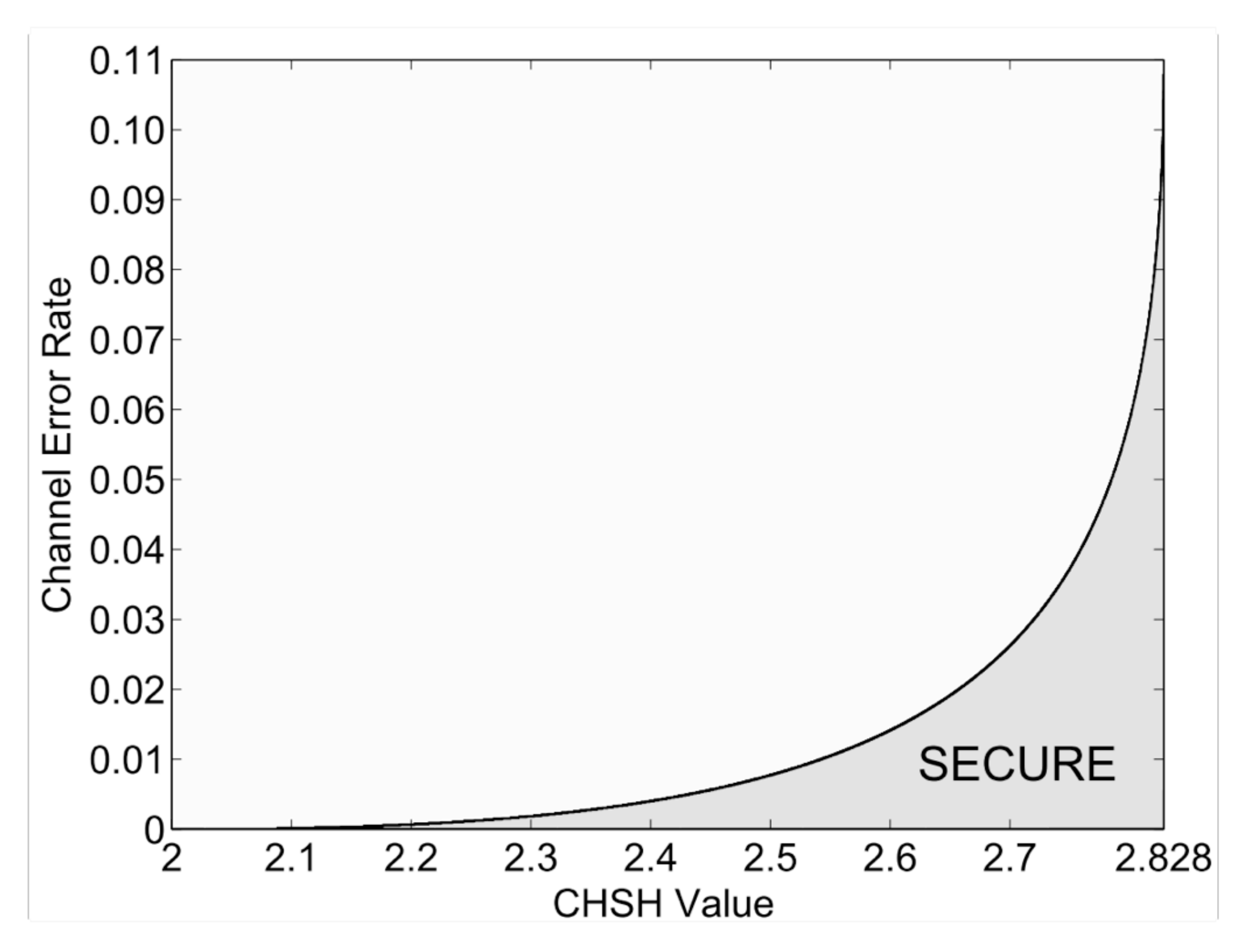
Correction due to the imperfect devices

Secret key fraction

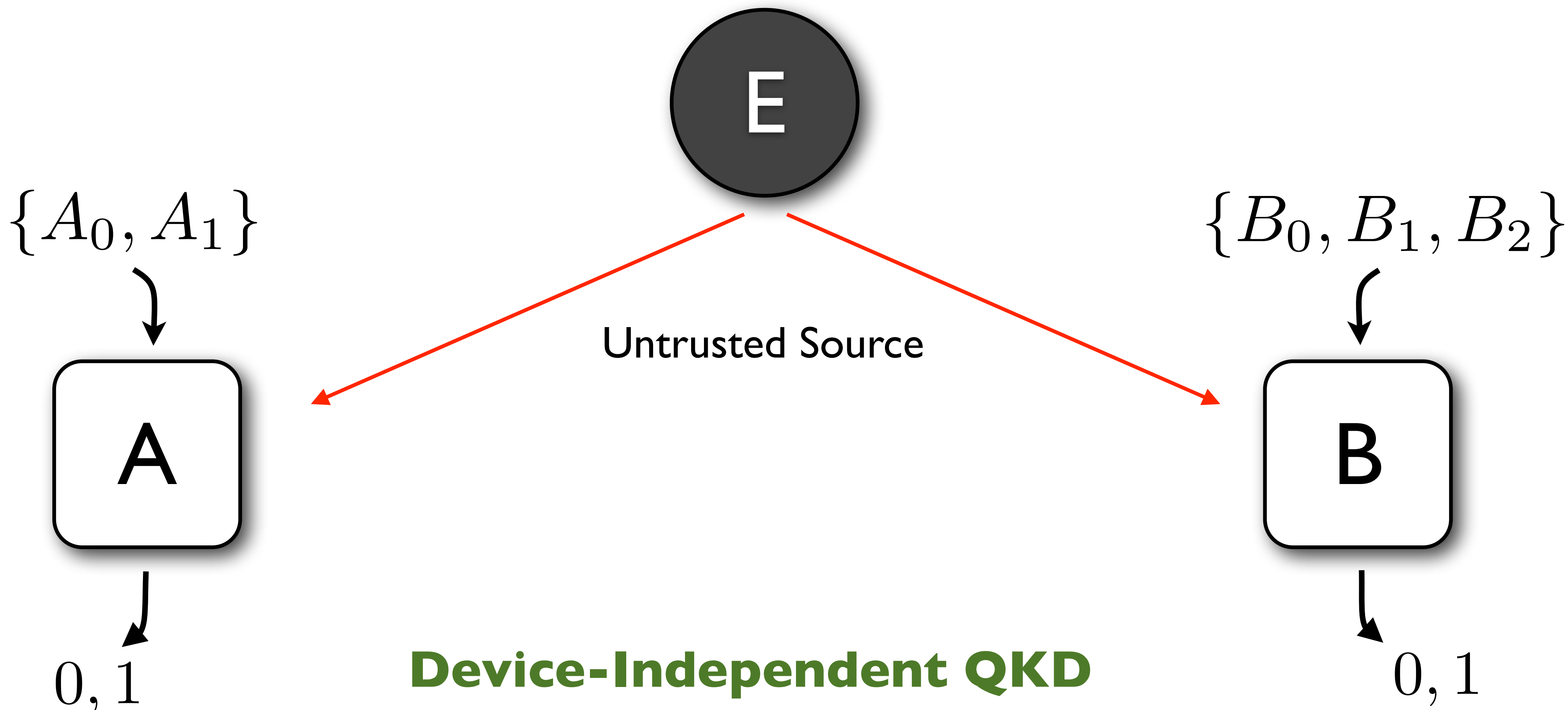
$$K_\infty = 1 - 2\mathrm{h}_2(e) - \log_2\left(1 + \frac{S}{4}\sqrt{8 - S^2}\right)$$

Secret key fraction of the BB84 protocol

Correction due to the imperfect devices



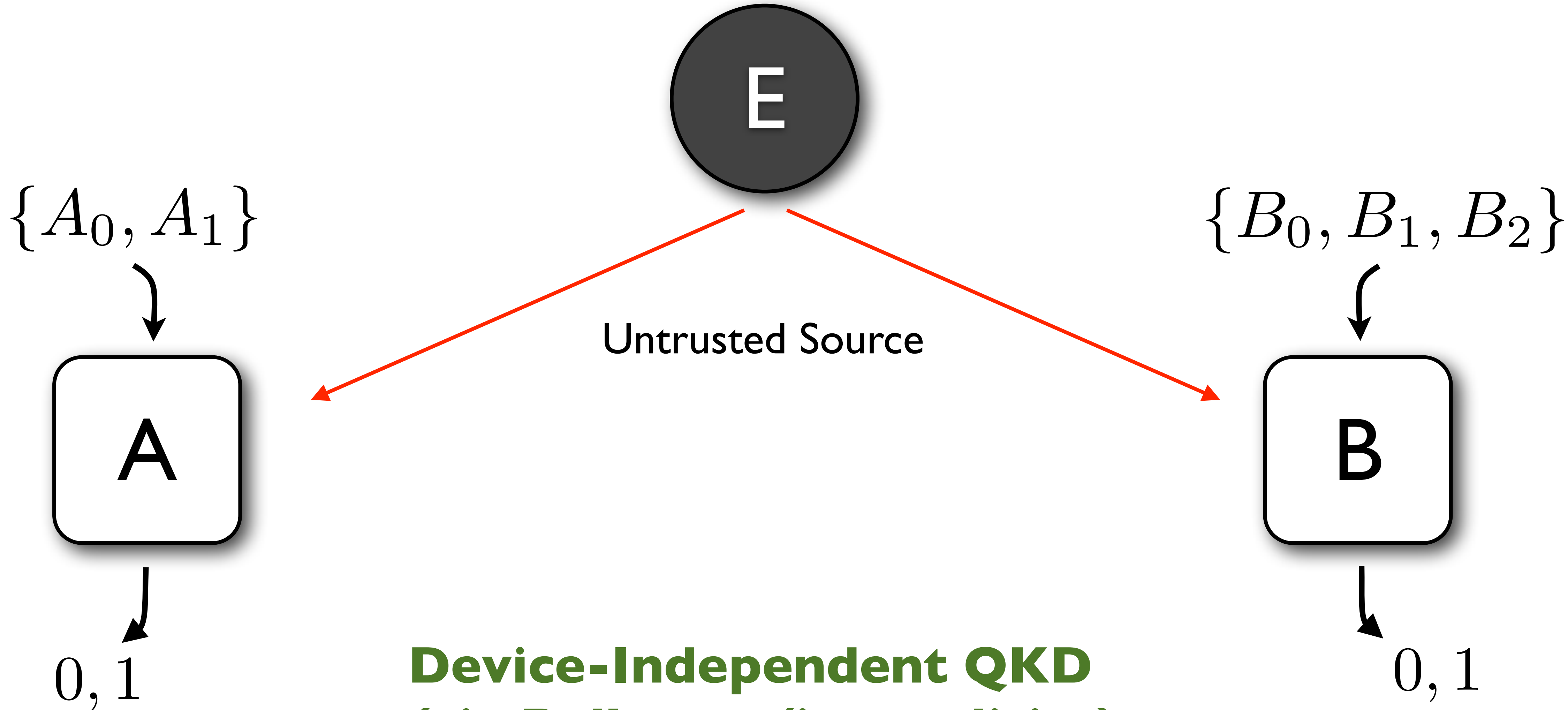
Related Work and Connections



Device-Independent QKD
(via Bell tests/inequalities)

Pironio et al (2009), Mckague (2009), Hanggi and Renner (2010), Masanes, Pironio and Acin (2011).

Related Work and Connections



Device-Independent QKD
(via Bell tests/inequalities)

Pironio et al (2009), Mckague (2009), Hanggi and Renner (2010), Masanes, Pironio and Acin (2011).

The Bell test is used to evaluate the quantum channel and devices!!

Related Work and Connections

Device-Independent QKD achieves the same advantage but is limited directly by the channel loss, i.e., detection loophole

Related Work and Connections

Device-Independent QKD achieves the same advantage but is limited directly by the channel loss, i.e., detection loophole

With **local Bell tests**, we do not have such a problem, in fact, we only need to consider local losses.

Related Work and Connections

Device-Independent QKD achieves the same advantage but is limited directly by the channel loss, i.e., detection loophole

↓

Can be rectified with Heralded Qubit Amplifier or Entanglement Swapping (See Gisin, Pironio, Sangouard (2010) and Curty and Moroder (2011)).

With **local Bell tests**, we do not have such a problem, in fact, we only need to consider local losses.

Related Work and Connections

Device-Independent QKD achieves the same advantage but is limited directly by the channel loss, i.e., detection loophole

↓

Can be rectified with Heralded Qubit Amplifier or Entanglement Swapping (See Gisin, Pironio, Sangouard (2010) and Curty and Moroder (2011)).

↓

The quantum channel - Bell Test
Imperfect devices - Bell Test

With **local Bell tests**, we do not have such a problem, in fact, we only need to consider local losses.

↓

The quantum channel - Error rate estimation
Imperfect devices - Bell Test

Related Work and Connections

Device-Independent QKD achieves the same advantage but is limited directly by the channel loss, i.e., detection loophole

↓

Can be rectified with Heralded Qubit Amplifier or Entanglement Swapping (See Gisin, Pironio, Sangouard (2010) and Curty and Moroder (2011)).

↓

The quantum channel - Bell Test
Imperfect devices - Bell Test

With **local Bell tests**, we do not have such a problem, in fact, we only need to consider local losses.

↓

The quantum channel - Error rate estimation
Imperfect devices - Bell Test

QKD with local Bell tests

Detection Loophole can be closed more readily.

Related Work and Connections

Device-Independent QKD achieves the same advantage but is limited directly by the channel loss, i.e., detection loophole

↓

Can be rectified with Heralded Qubit Amplifier or Entanglement Swapping (See Gisin, Pironio, Sangouard (2010) and Curty and Moroder (2011)).

↓

The quantum channel - Bell Test
Imperfect devices - Bell Test

With **local Bell tests**, we do not have such a problem, in fact, we only need to consider local losses.

↓

The quantum channel - Error rate estimation
Imperfect devices - Bell Test

QKD with local Bell tests

Detection Loophole can be closed more readily.

Refined error analysis.

Working Assumptions

1. Alice and Bob have access to trusted local sources of randomness.
2. Alice and Bob have access to an authenticated, but otherwise insecure classical channel.
3. No information leaves the laboratories unless the protocol allows it.
4. Alice and Bob have access to trusted classical operations
5. The devices do not have internal memories
6. The marginal states of Alice/Bob are independent whether Charlie's entangling measurement fails.

Working Assumptions

1. Alice and Bob have access to trusted local sources of randomness.
2. Alice and Bob have access to an authenticated, but otherwise insecure classical channel.
3. No information leaves the laboratories unless the protocol allows it.
4. Alice and Bob have access to trusted classical operations
5. The devices do not have internal memories
6. The marginal states of Alice/Bob are independent whether Charlie's entangling measurement fails.

Assumptions 1-4 are common assumptions

Working Assumptions

1. Alice and Bob have access to trusted local sources of randomness.
2. Alice and Bob have access to an authenticated, but otherwise insecure classical channel.
3. No information leaves the laboratories unless the protocol allows it.
4. Alice and Bob have access to trusted classical operations
5. The devices do not have internal memories
6. The marginal states of Alice/Bob are independent whether Charlie's entangling measurement fails.

Assumptions 1-4 are common assumptions

Current device-independent QKD uses assumptions 1-5

Working Assumptions

1. Alice and Bob have access to trusted local sources of randomness.
2. Alice and Bob have access to an authenticated, but otherwise insecure classical channel.
3. No information leaves the laboratories unless the protocol allows it.
4. Alice and Bob have access to trusted classical operations
5. The devices do not have internal memories
6. The marginal states of Alice/Bob are independent whether Charlie's entangling measurement fails.

Assumptions 1-4 are common assumptions

Current device-independent QKD uses assumptions 1-5

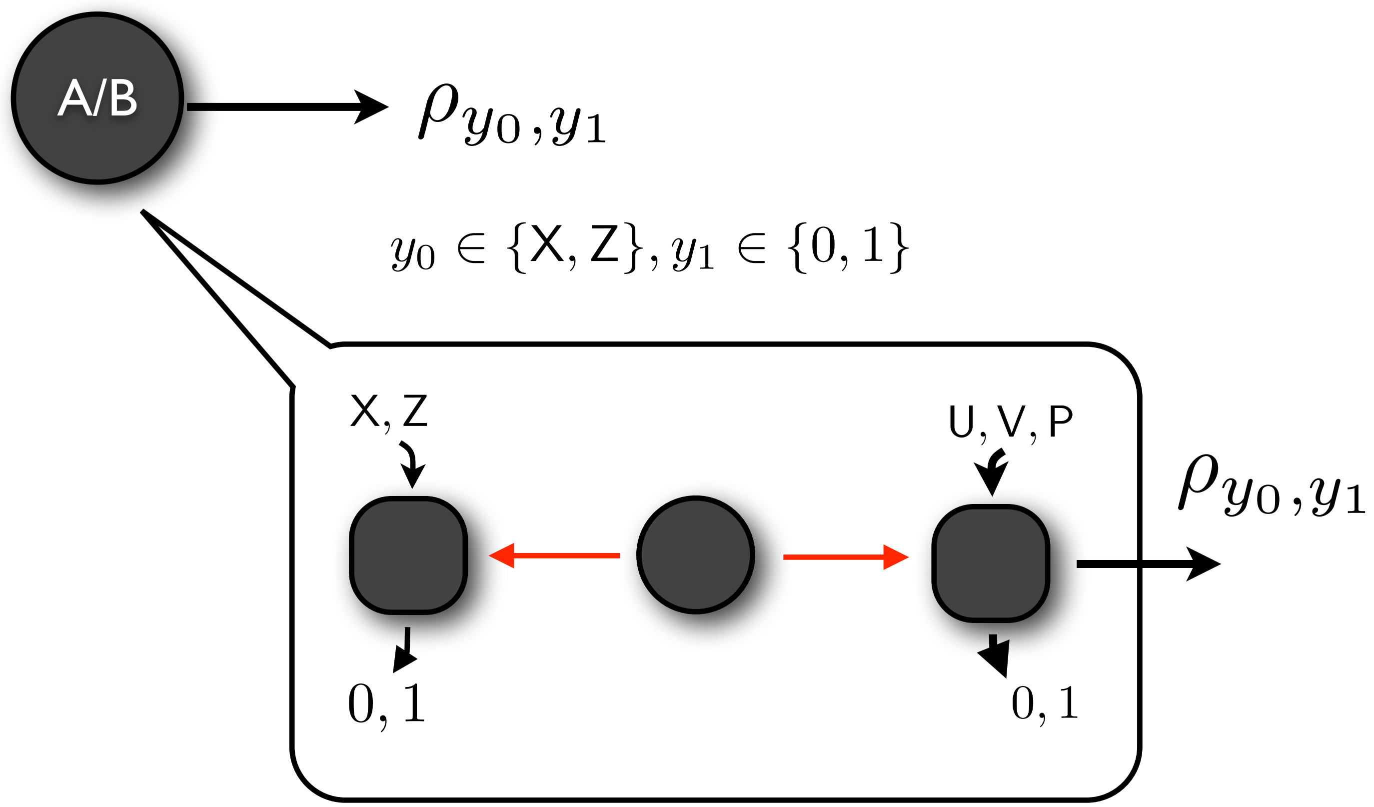
Why do we need assumption 6?

Additional working assumptions

- The marginal states of Alice/Bob are independent whether Charlie's entangling measurement fails.

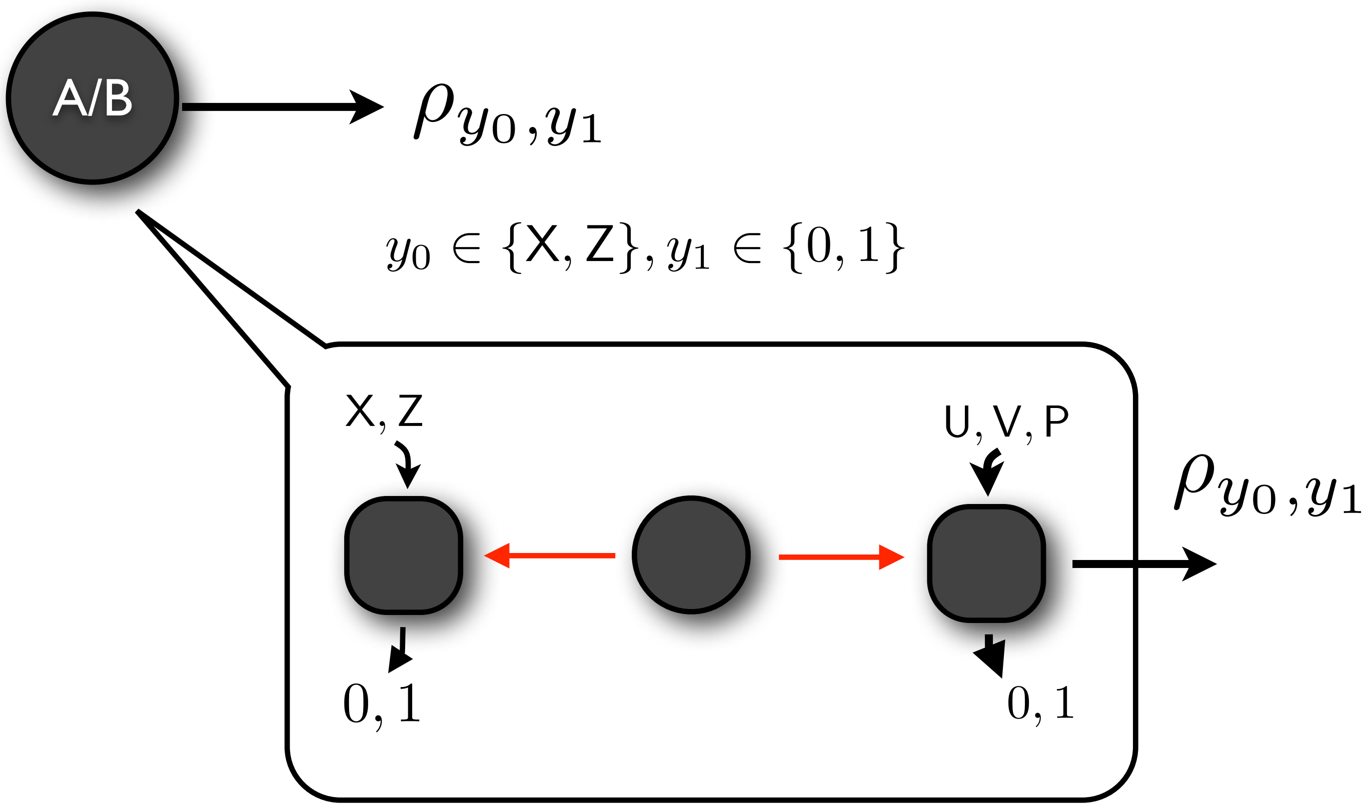
Additional working assumptions

- The marginal states of Alice/Bob are independent whether Charlie's entangling measurement fails.



Additional working assumptions

- The marginal states of Alice/Bob are independent whether Charlie's entangling measurement fails.

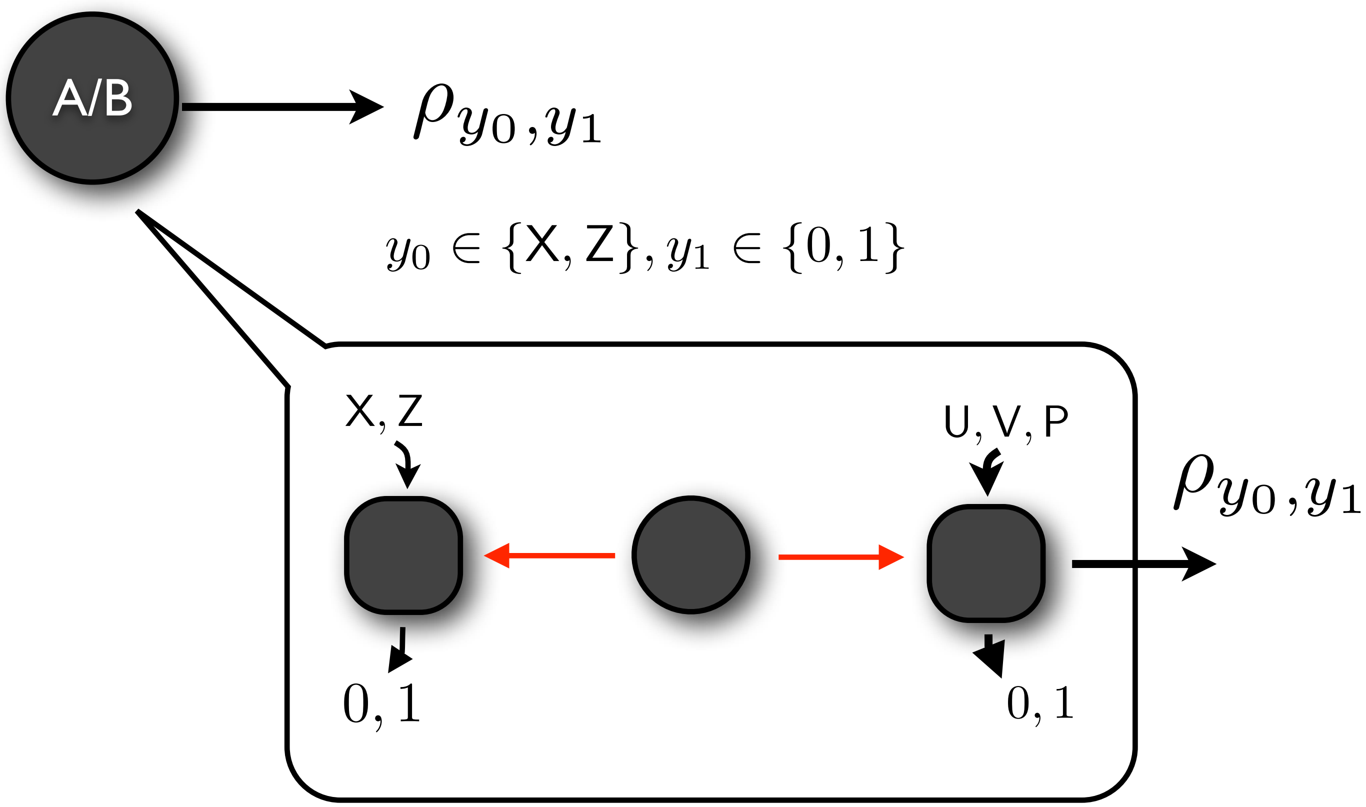


With the above assumption:

- The secret key fraction is independent of the distance between Alice and Bob.
- The protocol is secure as long as we see some Bell violation.

Additional working assumptions

- The marginal states of Alice/Bob are independent whether Charlie's entangling measurement fails.



With the above assumption:

- The secret key fraction is independent of the distance between Alice and Bob.
- The protocol is secure as long as we see some Bell violation.

However, if the Bell violation is maximal, then the above assumption can removed!!

Note: we also have the security bound for non-maximal Bell violation with the assumption removed.

Summary

Summary

At hand: A security proof that has the following features

- Applies to a very general class of devices.
- Only two parameters are required to bound the secrecy of the key.
- Performs well in the finite key size regime.

Summary

At hand: A security proof that has the following features

- Applies to a very general class of devices.
- Only two parameters are required to bound the secrecy of the key.
- Performs well in the finite key size regime.

Interesting points:

- Reaches the BB84 key rate (for qubits) in the limiting case.
- Local CHSH tests are independent of the distance between Alice and Bob (towards a loophole-free Bell test).

Summary

At hand: A security proof that has the following features

- Applies to a very general class of devices.
- Only two parameters are required to bound the secrecy of the key.
- Performs well in the finite key size regime.

Interesting points:

- Reaches the BB84 key rate (for qubits) in the limiting case.
- Local CHSH tests are independent of the distance between Alice and Bob (towards a loophole-free Bell test).

In other words..

It is "device-independent" and is secure against the most general attacks in the finite key size regime.

Relevant Work in QCRYPT2012

Talks

- Memory attacks on device-independent quantum cryptography
- A quantum key distribution system immune to detector attacks

Poster

- Alternative schemes for measurement device independent QKD
- Device independent QKD with Reused Devices
- Security Proof of two-way QKD protocols with partial device independence
- Semi-device Independent QKD based on BB84 and a CHSH type estimation
- The link between entropic uncertainty and non-locality

Relevant Work in QCRYPT2012

Talks

- Memory attacks on device-independent quantum cryptography
- A quantum key distribution system immune to detector attacks

Poster

- Alternative schemes for measurement device independent QKD
- Device independent QKD with Reused Devices
- Security Proof of two-way QKD protocols with partial device independence
- Semi-device Independent QKD based on BB84 and a CHSH type estimation
- The link between entropic uncertainty and non-locality

Supplementary Information

For more details, please refer to **arXiv:1208.0023**