A semi-device-independent framework based on natural physical assumptions and its application to random number generation

T. Van Himbeeck, E. Woodhead, N. Cerf, R. García-Patrón, S. Pironio

arXiv:1612.06828

AQIS 2017 – 4-8 September 2017
There exist vulnerabilities in quantum cryptography, successfully exploited by quantum hackers. These attacks exploit a mismatch between the theoretical model used to prove security and the actual implementation.
Device-independent quantum cryptography

This approach can be used to certify the security of RNG and QKD protocols, or even the performance of quantum computers.
Usual, “device-dependent” quantum cryptography

Based on a detailed characterization of the devices

Semi-device-independent quantum cryptography

Based on a few assumptions. Devices are partly untrusted.

E.g.:
• Measurement-device-independence
• One-sided quantum cryptography
• Source-independent QRNG
• Qubit assumption
• Source & measurement independence
• ...

Advantage: higher rate, easier to implement than fully device-independent protocols

Fully “device-independent” quantum cryptography

Based on minimal assumptions. Devices can be untrusted.
Semi-device-independent protocols based on an energy constraint

Devices viewed as black boxes…

... except for a single assumption:
\( \rho_x \) are optical signals close to the vacuum:
\[ \langle 0 | \rho_x | 0 \rangle \geq \omega \]

This assumption is sufficient to guarantee that devices behave in a genuinely quantum way.
In particular, it allows for secure RNG protocols.
Hopefully, it can also be used for QKD.

Region not allowed by quantum theory if prepared states satisfy the energy constraint
Device-independent quantum cryptography

This approach can be used to certify the security of RNG and QKD protocols, or even the performance of quantum computers.
Semi-device-independent protocols based on an energy constraint

\[ \rho \] are optical signals close to the vacuum:
\[ \langle 0 | \rho_x | 0 \rangle \geq \omega \]

This assumption is sufficient to guarantee that devices behave in a genuinely quantum way.
In particular, it allows for secure RNG protocols.
Hopefully, it can also be used for QKD.
Usual, “device-dependent” quantum cryptography

Based on a detailed characterization of the devices

Semi-device-independent quantum cryptography

Based on a few assumptions. Devices are partly untrusted.

E.g.:
- Measurement-device-independence
- One-sided quantum cryptography
- Qubit assumption
- Source & measurement independence
- ...
- Energy constraint

Fully “device-independent” quantum cryptography

Based on minimal assumptions. Devices can be untrusted.
Outline

• Why semi-device-independent quantum cryptography?

• Motivation for our energy constraint assumption

• Results
Outline

• Why semi-device-independent quantum cryptography?

• Motivation for our energy constraint assumption

• Results
Even full DI requires non-trivial assumptions

Usual, "device-dependent" quantum cryptography

Semi-device-independent quantum cryptography

• Laser power is limited

Fully "device-independent" quantum cryptography

• Electronics and classical computers are trusted
• No information leakage
• GPS are accurate
• ...

• Lasers are limited
we extracted 256 bits, certified to be uniform to within 0.001.

in [18], which is titled “XOR 3” and consists of a total of 182,161,215 trials, acquired in 30 min of running the experiment, improving on the approximately one month duration of data.
Don’t waste time developing cars: in the future planes will be easy to build, common, and affordable.
DI RNG implementations

Monroe experiment

Kwiat experiment / NIST analysis

Aggregate Pulses

1 \( p\)-value = 0.0025
3 \( p\)-value = \(2.4 \times 10^{-6}\)
5 \( p\)-value = \(5.8 \times 10^{-9}\)
7 \( p\)-value = \(2.0 \times 10^{-7}\)

we extracted 256 bits, certified to be uniform to within 0.001.

in [18], which is titled “XOR 3” and consists of a total of 182,161,215 trials, acquired in 30 min of running the experiment, improving on the approximately one month duration of data
Semi-DI protocols based on a qubit assumption
Semi-DI protocols based on a qubit assumption
Mismatch between model used for security proof and implementation!

Qubit assumption is an idealization.
→ Shows that it is important to choose well the assumptions.
\[ \alpha |0\rangle + \beta |1\rangle + \gamma |2\rangle + \ldots \]

Click with prob \(1 - \alpha^2\)
No-click with prob \(\alpha^2\)
Outline

• Why semi-device-independent quantum cryptography?

• Motivation for our energy constraint assumption

• Results
Semi-device-independent protocols based on an energy constraint

Assumption: $\langle 0 | \rho_x | 0 \rangle \geq \omega_x$
Semi-device-independent protocols based on an energy constraint

Assumption: no-communication

\[ \langle 0 | \rho_x | 0 \rangle = 1 \]
Semi-device-independent protocols based on an energy constraint

Assumption: $\langle 0 | \rho_x | 0 \rangle \geq \omega_x$

- Natural relaxation of the no-communication assumption of full DI protocols
Semi-device-independent protocols based on an energy constraint

- Natural relaxation of the no-communication assumption of full DI protocols
- The appropriate space to describe quantum optics experiments is the Fock space of several quantum optical modes. In this context, it is natural to bound the average number of photons.
- This is an assumption anyway made in many quantum optics experiments in which attenuated laser sources are used.

Assumption: $\langle 0|\rho_x|0 \rangle \geq \omega_x$
Semi-device-independent protocols based on an energy constraint

Assumption: $\langle 0 | \rho_x | 0 \rangle \geq \omega_x$

- Natural relaxation of the no-communication assumption of full DI protocols
- The appropriate space to describe quantum optics experiments is the Fock space of several quantum optical modes. In this context, it is natural to bound the average number of photons.
- This is an assumption anyway made in many quantum optics experiments in which attenuated laser sources are used.
- It is directly related to simple characteristics of the device components (laser power, attenuator) and robust to device imperfections.
Semi-device-independent protocols based on an energy constraint

- Natural relaxation of the no-communication assumption of full DI protocols
- The appropriate space to describe quantum optics experiments is the Fock space of several quantum optical modes. In this context, it is natural to bound the average number of photons.
- This is an assumption anyway made in many quantum optics experiments in which attenuated laser sources are used.
- It is directly related to simple characteristics of the device components (laser power, attenuator) and robust to device imperfections.
Semi-device-independent protocols based on an energy constraint

Assumption: \( \langle 0 | \rho_x | 0 \rangle \geq \omega_x \)

- Natural relaxation of the no-communication assumption of full DI protocols
- The appropriate space to describe quantum optics experiments is the Fock space of several quantum optical modes. In this context, it is natural to bound the average number of photons.
- This is an assumption anyway made in many quantum optics experiments in which attenuated laser sources are used.
- It is directly related to simple characteristics of the device components (laser power, attenuator) and robust to device imperfections.
- It could be directly monitored (calibrated power meter) or enforced (optical fuse).
Outline

• Why semi-device-independent quantum cryptography?

• Motivation for our energy constraint assumption

• Results
No-communication assumption

Violation of Bell inequalities

\[ Q > C \]

Qubit assumption

Violation of “dimension witnesses”

\[ Q > C \]

Energy constraint assumption

\[ Q > C \] ??
Input-output statistics

\[ P(b|x) = Tr[\rho_x M_b] \quad \text{or} \quad P(b|x) = \sum_\lambda p_\lambda Tr[\rho_x^\lambda M_b^\lambda] \]

Equivalent to knowledge of the bias of \( b \) given \( x \):

\[ E_x = P(b = 1|x) - P(b = -1|x) \]

\[ E_x = Tr[\rho_x M] \quad \text{or} \quad E_x = \sum_\lambda p_\lambda Tr[\rho_x^\lambda M^\lambda] \]

Output of devices is non-trivial if \( b \) is correlated to \( x \)

Amount of correlations can be measured by quantity

\[ E_- = (E_1 - E_2) / 2 \]

Probability to guess correctly \( x \) given \( b \) is

\[ \frac{1}{2} + \frac{|E_-|}{2} \]

- \( b \) does not depend on \( x \): \( E_- = 0 \)
- \( b \) fully correlated to \( x \): \( |E_-| = 1 \)
Input-output statistics

\[ P(b|x) = \text{Tr}[\rho_x M_b] \quad \text{or} \quad P(b|x) = \sum_{\lambda} p_\lambda \text{Tr}[\rho_{x,\lambda} M_{b,\lambda}] \]

Equivalent to knowledge of the bias of \( b \) given \( x \):

\[ E_x = P(b = 1|x) - P(b = -1|x) \]
\[ E_x = \text{Tr}[\rho_x M] \quad \text{or} \quad E_x = \sum_{\lambda} p_\lambda \text{Tr}[\rho_{x,\lambda} M_{\lambda}] \]

Output of devices is non-trivial if \( b \) is correlated to \( x \)

Amount of correlations can be measured by quantity

\[ E_- = (E_1 - E_2)/2 \]

Probability to guess correctly \( x \) given \( b \) is

\[ \frac{1}{2} + \frac{|E_-|}{2} \]

- \( b \) does not depend on \( x \): \( E_- = 0 \)
- \( b \) fully correlated to \( x \): \( |E_-| = 1 \)

Assumption

Energy constraint:

\[ \langle 0| \sum_{\lambda} p_\lambda \rho_{x,\lambda} |0 \rangle \geq w_x \]
Input-output statistics

\[ P(b|x) = \text{Tr}[\rho_x M_b] \quad \text{or} \quad P(b|x) = \sum_\lambda p_\lambda \text{Tr}[\rho_x^{\lambda} M_b^{\lambda}] \]

Equivalent to knowledge of the bias of \( b \) given \( x \):
\[ E_x = P(b = 1|x) - P(b = -1|x) \]
\[ E_x = \text{Tr}[\rho_x M] \quad \text{or} \quad E_x = \sum_\lambda p_\lambda \text{Tr}[\rho_x^{\lambda} M^{\lambda}] \]

Output of devices is non-trivial if \( b \) is correlated to \( x \)
Amount of correlations can be measured by quantity
\[ E_- = (E_1 - E_2)/2 \]
Probability to guess correctly \( x \) given \( b \) is
\[ \frac{1}{2} + \frac{|E_-|}{2} \]

- \( b \) does not depend on \( x \): \( E_- = 0 \)
- \( b \) fully correlated to \( x \): \( |E_-| = 1 \)

Assumption

Energy constraint:
\[ \langle 0| \sum_\lambda p_\lambda \rho_\lambda^x |0 \rangle \geq w_x \]

or
\[ \sum_\lambda p_\lambda \text{Tr}[H \rho_\lambda^x] \leq 1 - w_x \]
Maximal value for $E_-$ given $w_1 = w_2 = w$?

- $w = 1 \rightarrow E_- = (E_1 - E_2)/2 = 0$
- $w = 1/2 \rightarrow |\rho_{1,2}⟩ = (|0⟩ ± |1⟩)/\sqrt{2}$
  \[ \rightarrow E_- = (E_1 - E_2)/2 = 1 \]
- $\frac{1}{2} \leq w \leq 1$ arbitrary
  \[ |\rho_1⟩ = \sqrt{w}|0⟩ + \sqrt{1 - w}|ϕ_1⟩ \]
  \[ |\rho_2⟩ = \sqrt{w}|0⟩ + \sqrt{1 - w}|ϕ_2⟩ \]

Scalar product minimal if $|ϕ_1⟩ = -|ϕ_2⟩ = |1⟩$

\[ \Rightarrow |ρ_{1,2}⟩ = \sqrt{w}|0⟩ ± \sqrt{1 - w}|1⟩ \]

Best distinguishing measurement: $M = σ_x$

$\rightarrow$ We find the inequality $E_- = \frac{E_1 - E_2}{2} \leq 2\sqrt{w(1 - w)}$
According to quantum strategies: \( E_- = \frac{E_1 - E_2}{2} \leq 2\sqrt{w(1 - w)} = Q_{\text{max}} \)

Maximal value for “classical” strategies?

How to define “classical” strategies?
One possibility:

“classical” strategies = “deterministic” strategies (or convex combinations thereof)

\[ E_x = \sum_{\lambda} p_{\lambda} E_x^{\lambda} \text{ with } E_x^{\lambda} = \pm 1 \]

Let’s be more conservative and compare \( Q_{\text{max}} \) to strategies where only \( E_1 \) is deterministic

\[ E_1 = \sum_{\lambda} p_{\lambda} E_1^{\lambda} \text{ with } E_1^{\lambda} = \pm 1, \text{ no constraint on } E_2 \]

\( \rightarrow \text{If } Q_{\text{max}} > D_{\text{max}} \rightarrow \) the output of \( x = 1 \) is random (even to adversary with arbitrary knowledge of the devices)
\[ E_1 = \langle \rho_1 | M | \rho_1 \rangle = 1 \implies M = 2|\rho_1 \rangle \langle \rho_1 | - I \]

\[ \Rightarrow E_2 = \langle \rho_2 | M | \rho_2 \rangle = 2|\rho_2 \rangle \langle \rho_1 |^2 - 1 \]

\[ \Rightarrow E_- = \frac{E_1 - E_2}{2} = 2 - 2 |\langle \rho_2 | \rho_1 \rangle|^2 \]

Minimal value of \(|\langle \rho_2 | \rho_1 \rangle|^2\) given \(w\)

\[ \Rightarrow E_- \leq 4w(1 - w) = D_{\text{max}} \]
\( x = 1, 2 \)

\[ b = \pm 1 \]

- \( E_- = \frac{E_1 - E_2}{2} \)

- If \( E_1 \) is deterministic, we have the “Bell inequality”
  \[ E_- \leq 4w(1 - w) = D_{\text{max}} \]

- According to a general quantum strategy
  \[ E_- \leq 2\sqrt{w(1 - w)} = Q_{\text{max}} = \sqrt{D_{\text{max}}} > D_{\text{max}} \]

Assumption

Energy constraint:

\[ \langle 0| \sum_\lambda p_\lambda \rho_x^2 |0 \rangle \geq w_x \]
More generally, it is possible to characterize completely the set of allowed values \((E_1, E_2)\) for given energy bounds \((w_1, w_2)\).

One nice way to do it:

\[
\begin{align*}
x &= 1, 2 \\
y &= M \\
b &= \pm 1
\end{align*}
\]

\[
\begin{align*}
E_x &= \text{Tr}[\rho_x M] \\
w_x &= \text{Tr}[\rho_x V]
\end{align*}
\]

Given this characterization, one can also put rigorous bounds on the output entropy given \((E_1, E_2)\) straightforward to build a RNG protocol where amount of randomness produced is evaluated assuming only the energy bound, but no other assumption on the devices.
How to produce “non-deterministic” correlations in the lab?

A practical implementation with gaussian states and homodyne measurements:

Source prepares:

Measurement:
Homodyne measurement of $X$ quadrature with $b = \text{sign}(X)$
A simpler implementation with a slightly stronger assumption

\[ x \in \{1, 2\} \]

\[ b \in \{0, 1\} \]

Average energy constraint:

\[ \langle 0 | \sum_{\lambda} p_{\lambda} \rho_{x}^{\lambda} | 0 \rangle \geq w_{x} \]

Peak energy constraint

\[ \langle 0 | \rho_{x}^{\lambda 4} | 0 \rangle \geq w_{x} \text{ for all } \lambda \]
Summary

• We propose to use a bound on the energy of optical signals as a unique assumption on which to prove the security of prepare-and-measure quantum cryptography protocol (with no other assumptions on the devices)

• We have shown that there is a gap between what can be achieved with very simple quantum implementations and deterministic strategies. This is equivalent to the violation of Bell inequalities in full DI protocols.

• These results immediately imply the existence of RNG protocols where the amount of randomness produced can be certified without making any assumptions about the devices except the energy assumption.
Open question

• Is the energy assumption sufficient to prove the security of a QKD protocol?

• We implicitly assumed that the preparation and measurement device did not share prior entanglement. Can this be relaxed?

• One extra motivation for the energy assumption is that it is in principle compatible with CV protocols for which no DI or semi-DI implementations have been introduced. Can we analyze the security of a genuinely CV protocol in a DI setting using the energy assumption?