Quantum Science and Technology

RECEIVED
12 January 2017

REVISED
12 July 2017

ACCEPTED FOR PUBLICATION
18 July 2017

PUBLISHED
14 August 2017

PAPER

Finite-key-size effect in a commercial plug-and-play QKD system

Poompong Chaiwongkhot[1,2], **Shihan Sajeed**[1,3], **Lars Lydersen**[4] **and Vadim Makarov**[2,3]

[1] Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1 Canada
[2] Department of Physics and Astronomy, University of Waterloo, Waterloo, ON, N2L 3G1 Canada
[3] Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, N2L 3G1 Canada
[4] Department of Electronics Systems, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway

E-mail: poompong.ch@gmail.com

Keywords: quantum key distribution, finite-key-size effect, plug-and-play system

Abstract

A security evaluation against the finite-key-size effect was performed for a commercial plug-and-play quantum key distribution (QKD) system. We demonstrate the ability of an eavesdropper to force the system to distill key from a smaller length of sifted-key. We also derive a key-rate equation that is specific for this system. This equation provides bounds above the upper bound of secure key under finite-key-size analysis. From this equation and our experimental data, we show that the keys that have been distilled from the smaller sifted-key size fall above our bound. Thus, their security is not covered by finite-key-size analysis. Experimentally, we could consistently force the system to generate the key outside of the bound. We also test manufacturer's software update. Although all the keys after the patch fall under our bound, their security cannot be guaranteed under this analysis. Our methodology can be used for security certification and standardization of QKD systems.

1. Introduction

Quantum key distribution (QKD) systems are expected to provide unconditionally secure keys between two parties [1–6]. To fulfill that expectation, every feature, imperfection, and loophole both in theory and practice has to be taken into account. One of these features is that, with limited resources and time, a QKD system can exchange only a finite length of raw key. The knowledge of an adversary about the key is estimated by the number of errors in it [7, 8]. Since the bound on the adversary's knowledge is estimated from a finite sample, the smaller the sample is, the less accurate the estimate becomes. Thus, the estimated knowledge might deviate from the actual value and, if it is underestimated, the security of the secret key might be compromised. Finite-key-size analysis [9–14] takes these statistical deviations into account and modifies the key-rate equation accordingly.

Many of the practical QKD systems used today were developed before the finite-key-size analysis in QKD protocols became available. Although some form of finite-key-size effect has been considered in the literature since the year 2000 [4], a rigorous proof was first published in 2005 and developed in the subsequent years [9–14]. While the finite-size analysis was not considered in the security assumptions of the early systems, the generated secret key may still be secure if the raw-key sample size is large enough to neglect the finite-size effects. However, if the sample size is smaller, the effects can no longer be neglected and an absence of the finite-key analysis may render the generated key insecure. This is the main focus of this work. We emphasize the significance of the finite-key-size effects in a practical QKD system. We also demonstrate the ability of an eavesdropper to amplify these effects by actively interfering with the transmission and forcing the system to generate secret key from a smaller sample size. In section 2, we experimentally demonstrate a simple attack that forces a commercial QKD system to use a smaller sample size. The key-rate equation for this specific system is derived in section 3. In section 4, we compare the finite-key security bounds with our experimental data. We test the system again after manufacturer's security update in section 5, and conclude in section 6.

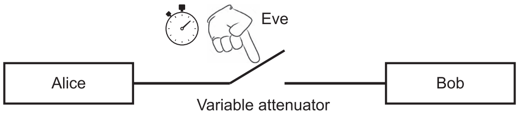

Figure 1. Scheme of experiment.

2. Experiment

The subject of this study is the security of a plug-and-play QKD system Clavis2 produced by ID Quantique [15, 16]. Although updated configurations for plug-and-play systems exist [17], we have not modified the system under test and all tests were performed in the same configuration, as provided by the manufacturer. The QKD protocol under study is Bennett–Brassard 1984 (BB84) protocol without decoy states [1, 7], as implemented in Clavis2. The security of this system implemented in the manufacturer's software is based on the security analysis in [18], which is an analysis against photon-number-splitting attack and cloning attack. The analysis in [18] neither considers the finite-key-size effects nor takes into account the lack of phase randomization in the system. It also assume that Eve cannot change detectors efficiency.

Under normal operation, the system exchanges the quantum signals until the memory buffer for the states sent by Alice is filled. This leads to the raw-key size being limited. This limit varies depending on the line loss (at higher loss fewer photons are received by Bob, and the key is smaller as our experimental data show below). Then, Alice and Bob perform post-processing: sifting, error correction, and privacy amplification [7, 15, 16]. One of the features of Clavis2 is that the system terminates the raw-key exchange process if Bob's photon detection efficiency drops below a certain threshold, and performs a recalibration procedure for the timing alignment of detector gates [16, 19]. This timing alignment greatly affects the photon detection efficiency, is sensitive to environmental fluctuations, and needs to be restored from time to time by performing this recalibration. However the system does not discard the raw key already accumulated in the buffer (as long as it has accumulated at least 80 kbit), and performs the post-processing from the available amount at the time of termination. Eve may take an advantage of this feature. Since the security proof of the system did not take into account the statistical deviation due to non-infinite key length, the deviation can be further amplified if the interruption for recalibration occurs early in the raw-key exchange session.

To demonstrate Eve's ability to force the system to distill from a short raw-key length, we first ran the system in a normal operation mode. The quantum channel between Alice and Bob consisted of a 2 m long optical fiber, and a variable attenuator (OZ Optics DD-100-11-1550) was added to simulate transmission line loss of 2, 3 and 4 dB (see figure 1). We ran multiple sessions of key distribution. In each session, during the raw-key exchange phase, we let the system exchange quantum signals for time τ, then abruptly increased the attenuation to $\approx$40 dB. This reduced the detection rate in Bob below the threshold and forced the system to terminate the key exchange. After that, the system performed post-processing of the already exchanged raw key and reported the secret-key length for that session. At the same time, we reset the variable attenuator to the original loss value. The system then recalibrated the timing alignment, and proceeded to the next raw-key exchange session. We varied τ between 10 and 280 s, so that the raw-key size after termination was between the system's minimum threshold of 80 kbit and the memory buffer limit of 1.6–4 Mbit in Bob (depending on the line loss), corresponding to the leftmost and rightmost experimental points in each plot in figure 2. We also allowed the system to complete some of the sessions naturally without Eve's intervention, which mostly resulted in the maximum key length but occasionally a shorter one. The plots show the variation of secret-key size as a function of the sifted-key size, for different transmission loss values. Note that the sifted-key size plotted is half the raw-key size. The amount of the raw key exchanged did not depend solely on τ. Some sessions experienced fluctuations in transmission loss and detection rate, which caused a lower key exchange rate but not below the termination threshold. Some sessions terminated before we induced the loss, when the detection efficiency dropped below the threshold as the result of naturally occurring timing drift, without Eve's help.

In our analysis, we consider the length of secret key as a function of the sifted-key length, rather than the session time duration. For each session that produced non-zero secret key, we recorded the length of the sifted key, the number of bits disclosed in the error correction, the error rate, and the length of the secret key reported by the system. The system under test did not include finite-key-size analysis in its post-processing. Rather, the post-processing step was programmed to subtract an arbitrarily chosen amount of the key in addition to the value given by the asymptotic security analysis [20]. This subtraction was done to account for any unknown effects that were not included in the system's security analysis. Prior to this study, the security of this arbitrary key subtraction has not been verified. We check this hypothesis below. Note that we consider only the case where

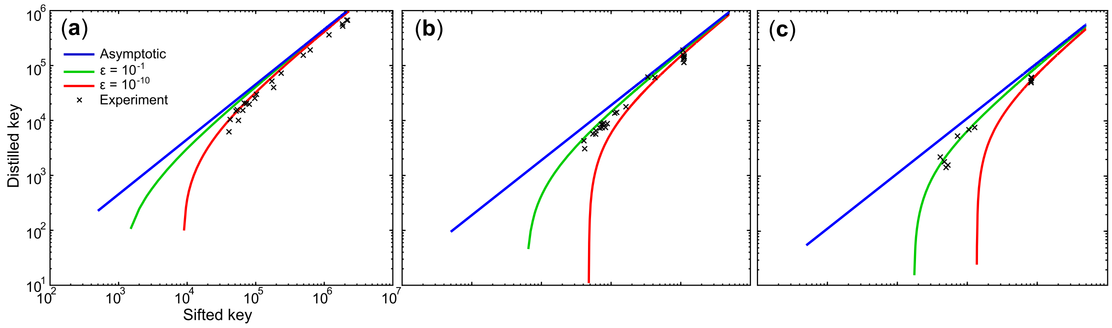

Figure 2. Secret-key size versus sifted-key size. Black × are experimental results with (a) 2 dB line loss and 2.5% error rate averaged over all sessions, (b) 3 dB line loss with 5.2% error rate, and (c) 4 dB line loss with 6.2% error rate. The experiment error rate in individual sessions deviated less than ±0.5% from the average. Blue (dark gray) curve is the infinite-key bound obtained from equation (6). Red (gray) curve is a finite-key-size bound with $\varepsilon = 10^{-10}$ using equation (5). Green (light gray) curve is the finite-key-size bound with $\varepsilon = 10^{-1}$. Secure-key bounds in each sub-figure were calculated separately according to the error rate and line loss of each experiment. Experimental points that lie above each line are considered insecure under those conditions used in each calculation. The detector's efficiency during the experiment was 0.08. The dark count rate was 2×10^{-5} counts per second for each detector.

Eve attempts to control the sifted-key-size before the post-processing. No other attack or flaw is considered in this study.

3. Derivation of key-rate equation

For finite-key-size effects, we need to formulate the key-rate equation for this specific system. To our knowledge, there is no finite-key-size analysis that covers all assumption in this system without hardware modification [21]. In this section, we use available derivation technique to find a secure key bound of the key generated by the system. We assume here that Eve does not interfere with the bright pulses sent from Bob to Alice, and assume that the phase of signal in different time slots is random. As a result, the key bound in this analysis would lie above the upper bound of secure key, which takes into account the lack of phase randomization [22]. Although we cannot conclude that the keys below our bound are secure, it can be used to justify that the secret keys that fall above this bound are not covered by the finite-key-size analysis. Thus, we need to assume the worst case that such keys are insecure.

Our analysis covers the process starting with the raw-key exchange step of plug-and-play system, where Alice attenuates the laser pulses from Bob and encodes each pulse in one of the four possible phase values: 0, $\pi/2$, π, and $3\pi/2$. Alice then sends the encoded signal back to Bob where he measures the signal in one of the two bases, and gets his raw key. They perform sifting and error correction afterwards. The system then performs privacy amplification process where the key is shortened with a universal-2 hash function to exclude Eve's information about the key. The key after this step is the secret key. Eve's information is estimated from quantum bit error rate found during the error correction and probability of having multi-photon pulses during raw key exchange. This process allows us to use a common procedure of secret-key analysis based on [9–11], which stated that, by using the universal-2 hash function as privacy amplification, a secret key K of secret key probability per bit l_K is ε-secure if the protocol is not aborted, and l_K satisfies the relation

$$\varepsilon_{\mathrm{PA}} < 2^{-\frac{1}{2}(H_{\min}(K|E')-l_K)}. \tag{1}$$

Here, $\varepsilon_{\mathrm{PA}}$ is the collision probability of hash function, which is the probability of two different input strings being projected into the same string of output. $H_{\min}(K|E')$ is smooth min-entropy of the system, which represents the probability of Eve guessing the key K correctly using an optimal strategy, given her information about the key before privacy amplification E'.

The goal of this derivation is to replace the smooth min-entropy with a function of measurable parameters from the system. Since the information leakage during error correction is independent of other processes prior to that, E' can be decomposed into Eve's knowledge before error correction E and information leakage during error correction process L. By inequality of smooth entropy [11], we have

$$H_{\min}(K|E') \geqslant H_{\min}(K|E'') - L - 7\sqrt{\frac{1}{n}\log_2\frac{2}{\tilde{\varepsilon}}}, \tag{2}$$

where $H_{\min}(K|E'')$ is the smooth min-entropy of the system before the error correction step. The last term is a statistical correction under finite-key-size regime, where $\tilde{\varepsilon}$ is the probability that Eve's information is underestimated when using smooth min-entropy [12]. The analysis in [12, 23] gave us the bound of $H_{\min}(K|E'')$

as a function of measurable parameters

$$H_{\min}(K|E'') \geqslant A\left(1 - h\left(\frac{\tilde{E}}{A}\right)\right), \tag{3}$$

where $h(x) = -x\log_2(x) - (1 - x)\log_2(1 - x)$ is the binary Shannon entropy, $\tilde{E} = E + \frac{1}{2}\sqrt{\{2\ln(1/\varepsilon_{\mathrm{PE}}) + 2\ln(n + 1)\}(1/n)}$ takes into account a chance that the error rate estimated from a sifted key of size n in the protocol might deviate from the actual value [12], $\varepsilon_{\mathrm{PE}}$ is the probability that such deviation occurs, and E is the observed error rate. The single photon detection probability $A = (p_{\mathrm{det}} - p_{\mathrm{multi}})/p_{\mathrm{det}}$ is a correction term for weak coherent laser used to exchange the raw key in the system [5], where p_{det} is the probability of detection and p_{multi} is the probability of a multi-photon pulse generated by Alice [16].

Now we consider information leakage during the error correction. In theory, the minimum portion of the key with error probability E that needs to be disclosed to correct all the errors is $h(E)$. Using this limit along with the finite-key-size analysis from [13], we have the upper bound of information leakage during error correction

$$L \leqslant \mathrm{leak}_{\mathrm{EC}}A + \log_2\frac{8}{\varepsilon_{\mathrm{EC}}}, \tag{4}$$

where $\mathrm{leak}_{\mathrm{EC}} = f_{\mathrm{EC}}h(E)$ is an estimated portion of the key disclosed during error correction. The factor $f_{\mathrm{EC}} = 1.2$ is a practical efficiency of the error correction protocol [8, 12]. In the system log of system under test, this value varied between 1.1 and 1.3. The last term takes account of a failure probability $\varepsilon_{\mathrm{EC}}$ that the error correction leaves non-zero number of errors [13]. This can occur, for example, owing to a non-zero probability of at least one parity check block containing an even number of error bits in every iteration of CASCADE error-correction code and the following parity check rounds in Clavis2 [16].

Since the experimental results are the secret key size as a function of the sifted key length n, we need a secure key bound $l = nl_K$. Substituting equations (2)–(4) into equation (1), taking the logarithm, then multiplying by n on both sides, we obtain

$$l \leqslant nA\left(1 - h\left(\frac{\tilde{E}}{A}\right)\right) - n\ \mathrm{leak}_{\mathrm{EC}} - 7n\sqrt{\frac{1}{n}\log_2\frac{2}{\tilde{\varepsilon}}} - 2\log_2\frac{1}{\varepsilon_{\mathrm{PA}}} - \log_2\frac{2}{\varepsilon_{\mathrm{EC}}}, \tag{5}$$

with security parameter $\varepsilon = \varepsilon_{\mathrm{PE}} + \tilde{\varepsilon} + \varepsilon_{\mathrm{PA}} + \varepsilon_{\mathrm{EC}}$ [11–14]. Since secret-key-rate analyses under collective and coherent attack on non-decoy state BB84 are equivalent [6, 24], the present analysis also covers coherent attack, which is the most general form of attacks on QKD system.

The asymptotic key-rate equation for this specific system can be derived in the same way, but without considering statistical deviation due to finite-size effects. The asymptotic key-rate is

$$l_\infty \leqslant nA\left(1 - h\left(\frac{E}{A}\right)\right) - n\ \mathrm{leak}_{\mathrm{EC}}. \tag{6}$$

4. Security verification

To verify the security of the secret key, we compare the experimental result with the bound of the secret key under the asymptotic assumption and finite-key-size analysis. For the asymptotic case, we use equation (6) as the secure key bound. For finite-key-size effect, we use a numerical optimization to find a combination of security parameters ($\varepsilon_{\mathrm{PE}}$, $\tilde{\varepsilon}$, $\varepsilon_{\mathrm{PA}}$, and $\varepsilon_{\mathrm{EC}}$) that maximizes the key length in equation (5). The observed error rate E is an average of the error rates reported by the system after each key distillation at a given transmission loss. The term A is calculated assuming the Poisson distribution with a mean photon number per pulse $\mu = 0.2$ sent by Alice. The value of μ varied between 0.2 and 0.4 in the experiment, however the lowest value gives the highest bound for the secret key rate. We thus obtain bounds of secure key length, plotted in figure 2. Above each curve lies the zone where the security of the key is not covered by finite-key-size analysis.

The experimental secret key sizes, denoted by black ×, always satisfy the security criteria for the asymptotic assumption. When the size of the input sifted key is large, the key-rate bounds with and without finite-size assumption lie very close to each other (see figure 2). This might put the experimentally distilled key size below the finite-key-size bound, i.e., on the safe side. However, when the sifted key size is reduced, the key-rate bounds with and without finite-key assumption diverge significantly. Higher loss results in higher divergence. A fraction of the experimental results falls outside the secure zone for the finite-key-size analysis with values of ε up to 10^{-1}. The latter value means there is a 10% chance that the information of the key generated under this condition might be leaked to Eve. In practice, the security parameter ε can be picked to be of the same order as the probability of major natural disasters such as a serious earthquake, nearby volcanic eruption or nuclear power plant meltdown [25]. If such disaster happened, it is most likely that the security of the key would not matter

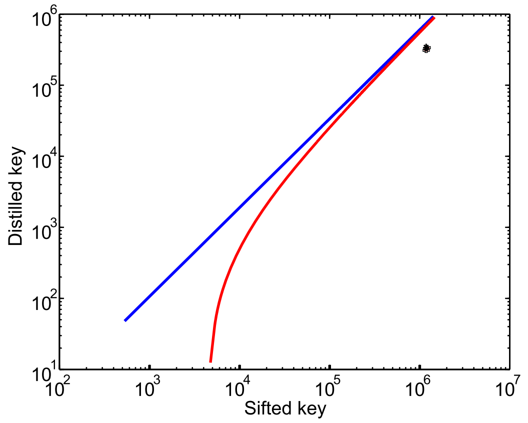

Figure 3. Experimental result with new software. The line loss was 3 dB and error rate was 1%. Blue (dark gray) curve is the asymptotic key bound given by equation (6). Red (gray) curve is the finite-key-size bound for $\varepsilon = 10^{-10}$ given by equation (5). A group of × presents results of 8 key distillations.

anymore. For example, the probability of a nuclear power plant meltdown is 10^{-4} per year, according to the Nuclear Regulatory Commission [26]. If our QKD machine generates two keys every minute or approximately 10^6 keys a year, one might pick $\varepsilon = 10^{-10}$ so that the probability that at least one key leaks to Eve is of the same order as such disasters [25]. However, our experiment shows that Eve can consistently induce a much higher risk probability of key leakage. She can do this by applying our channel interruption technique for BB84 protocol at channel loss values >2 dB (or line distances longer than about 12 km, given typical fiber loss value of 0.17 dB km^{-1}).

5. Testing manufacturer's patch

In the middle of our study in 2014, ID Quantique released a software update for Clavis2. After the update, the system accumulates the raw key over multiple key exchange sessions, and performs post-processing only when the sifted-key size reaches a threshold of about 2 Mbit.

We have repeated our experiment and recalculated our plot using the new parameters acquired from the updated system. The result shows that the secret key is within the secure bound of $\varepsilon = 10^{-10}$ (see figure 3). Regardless of our channel interruptions, we observed that the system has retained the raw key exchanged before termination of each raw-key exchange session, and accumulated it until the size reached about 2 Mbit before proceeding to the distillation. This behavior is clearly visible in the system log and confirmed by the manufacturer [20].

6. Conclusion

In this work, we have done a security evaluation of the finite-key-size effect for Clavis2 system that included derivation of the specific key-rate equation, developing a testing methodology, using it to test the system's security against finite-key-size effects, and testing the manufacturer's patch. Although rigorous security proofs with finite-key-size assumptions were abundant in the literature during the start of this work, they were not assembled together into a key-rate equation suitable for the system under test. Our work has assembled the components of the key-rate equation, verified the assumptions, and put them together into the form of equation (5). However, under our assumptions, the equation does not give the upper bound to evaluate the security of the secret key. Using our result, we can only verify that the keys that fall above the bound are not secure under finite-key-size analysis.

We have shown that by dynamically controlling the channel loss, Eve can force the system to distill key from a shorter sifted-key length to bring the finite-key-effects into play. Using our derived key-rate equation, equation (5), we have shown that key distilled from a sufficiently small length of sifted-key is not guaranteed to be secure, even with the manufacturer's added post-processing step of secret-key subtraction. We have also investigated the security update from ID Quantique, and found that all experimental results fall under the bound in this study. Unfortunately the security of the key against this attack cannot be concluded from this result. Our study only covers statistical evidence from the system against a theoretical bound. An explicit attack that exploits this effect is still open for future study.

Our investigation highlights the significance and importance of finite-key-size analysis in the implementations of QKD, especially in commercial systems. Our method of attack can be used as basis of a testing methodology for security certification. It should be incorporated in the standardization of QKD, which is the next step this technology field faces [27].

We responsibly disclosed to ID Quantique partial results of this investigation before the 2014 patch. Publication has been delayed in order to give the company enough time for patch deployment.

Acknowledgments

We thank the anonymous referee for the insightful and thorough criticism that led to the improvement of the theory in this study. We thank M Curty, N Lütkenhaus, R Renner, and J Skaar for discussions. We thank ID Quantique for cooperation, technical assistance, and providing us the QKD hardware. This work was supported by Industry Canada, NSERC (programs Discovery and CryptoWorks21), CFI and Ontario MRI. PC acknowledges support by Thai DPST scholarship.

Competing interests. The authors have a research collaboration on security analysis of QKD products with ID Quantique. No other competing interests are declared.

ORCID iDs

Poompong Chaiwongkhot https://orcid.org/0000-0002-2825-8287

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE International Conference on Computers, Systems, and Signal Processing (Bangalore, India)* (New York: IEEE Press) pp 175–9
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Lo H-K and Chau H F 1999 *Science* **283** 2050
[4] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[5] Lütkenhaus N 2000 *Phys. Rev.* A **61** 052304
[6] Renner R, Gisin N and Kraus B 2005 *Phys. Rev.* A **72** 012332
[7] Bennett C H, Bessette F, Salvail L, Brassard G and Smolin J 1992 *J. Cryptol.* **5** 3
[8] Brassard G and Salvail L 1994 *Lect. Notes Comp. Sci.* **765** 410
[9] Ben-Or M, Horodecki M, Leung D, Mayers D and Oppenheim J 2005 *Lect. Notes Comp. Sci.* **3378** 386
[10] Renner R and Koenig R 2005 *Lect. Notes Comp. Sci.* **3378** 407
[11] Renner R 2005 Security of quantum key distribution *PhD Thesis* ETH Zürich (https://doi.org/10.3929/ethz-a-005115027)
[12] Scarani V and Renner R 2008 *Phys. Rev. Lett.* **100** 200501
[13] Cai R Y Q and Scarani V 2009 *New J. Phys.* **11** 045024
[14] Tomamichel M, Lim C C W, Gisin N and Renner R 2012 *Nat. Commun.* **3** 634
[15] Stucki D, Gisin N, Guinnard O, Ribordy G and Zbinden H 2002 *New J. Phys.* **4** 41
[16] Clavis2 specification sheet, http://idquantique.com/images/stories/PDF/clavis2-quantum-key-distribution/clavis2-specs.pdf (visited: 4 July 2014)
[17] Zhao Y, Qi B, Lo H-K and Qian L 2010 *New J. Phys.* **12** 023024
[18] Niederberger A, Scarani V and Gisin N 2005 *Phys. Rev.* A **71** 042316
[19] Jain N, Wittmann C, Lydersen L, Wiechers C, Elser D, Marquardt C, Makarov V and Leuchs G 2011 *Phys. Rev. Lett.* **107** 110501
[20] I D Quantique 2014 private communication
[21] Zhao Y, Qi B and Lo H-K 2007 *Appl. Phys. Lett.* **90** 044106
[22] Lo H-K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[23] Tomamichel M and Renner R 2011 *Phys. Rev. Lett.* **106** 110506
[24] Kraus B, Gisin N and Renner R 2005 *Phys. Rev. Lett.* **95** 080501
[25] Renner R 2014 Private communication and lectures
[26] Office of Nuclear Regulatory Research, Regulatory analysis guidelines of the U.S. Nuclear Regulatory Commission NUREG/BR-0058, Rev. 4 (2004), http://nrc.gov/reading-rm/doc-collections/nuregs/brochures/br0058/br0058r4.pdf
[27] Länger T and Lenhart G 2009 *New J. Phys.* **11** 055051