PAPER • OPEN ACCESS

Quantum security and theory of decoherence

To cite this article: P Mironowicz 2022 *New J. Phys.* **24** 113054

IOP Publishing New J. Phys. 24 (2022) 113054 https://doi.org/10.1088/1367-2630/aca558

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
20 June 2022

REVISED
11 November 2022

ACCEPTED FOR PUBLICATION
23 November 2022

PUBLISHED
5 December 2022

PAPER

Quantum security and theory of decoherence

P Mironowicz

International Centre for Theory of Quantum Technologies, University of Gdańsk, Wita Stwosza 63, 80-308 Gdańsk, Poland
Department of Algorithms and System Modeling, Faculty of Electronics, Telecommunications and Informatics, Gdańsk University of Technology, Gabriela Narutowicza 11/12, 80-233 Gdańsk, Poland

E-mail: piotr.mironowicz@gmail.com

Keywords: quantum cryptography, quantum Darwinism, decoherence

Abstract

We sketch a relation between two crucial, yet independent, fields in quantum information research, *viz.* quantum decoherence and quantum cryptography. We investigate here how the standard cryptographic assumption of shielded laboratory, stating that data generated by a secure quantum device remain private unless explicitly published, is disturbed by the *einselection* mechanism of quantum Darwinism explaining the measurement process by interaction with the external environment. We illustrate the idea with a paradigmatic example of a quantum random number generator compromised by a quantum analog of the Van Eck phreaking. In particular, we derive a trade-off relation between the eavesdropper's guessing probability P_{guess} and the collective decoherence factor Γ of the simple form $P_{guess} + \Gamma \geqslant 1$.

Quantum cryptography [1, 2] is one of the most spectacular successes of quantum information theory. It provides new means of detection of eavesdropping by observing a disturbance of intercepted quantum states [3] not possible in classical cryptography, and even allows to certify security when using cryptographical systems from untrusted vendors [4]. Quantum devices can be used for such applications as secure key distribution [5] or generation of private random number [6] based on elementary physical phenomena.

Still, humans can deal only with classical data, and thus at some stage, any quantum cryptographic device has to generate classical output data. This process is known as quantum measurement [7]. Even though the measurement is one of the most basic processes in quantum mechanics, it remains to be one of the most mysterious phenomena since the very beginning of the theory [8–10]. This so-called measurement problem still lacks a definitive solution, with the decoherence theory being one of the most popular approaches [11].

The trailblazing works of Żurek [12, 13] elucidated the problem in which basis the quantum measurement is actually being performed, by the introduction of the concept of the *pointer basis*, *i.e.* the eigenbasis of observables commuting with the Hamiltonian determining the interaction of the measuring apparatus with the environment; the fact that the interaction with the environment is the factor that determines the measurement basis is called environment-induced superselection, or *einselection* [13, 14]. This result accentuated the role of the external world in the process of measurement and revealed that without this interaction, only the *premeasurement*, i.e. the correlation of the apparatus with the observed system, can occur.

The idea developed into the quantum Darwinism theory [15] explaining that information that is being successfully proliferated and distributed in many copies in multiple parts of the environment becomes classical. Such a framework directly relates classical outcomes of quantum devices with information leakage beyond the scope of the control. The process of information propagation can be viewed as *eavesdropping* of the information about the system being measured by the environment [16].

The role of the exterior world in the working of quantum devices seemingly contradicts the natural and necessary assumption, that the cryptographic devices are located inside a *shielded laboratory* protecting against the outflowing of the private data. Indeed, a crucial condition for the privacy of numbers, constituting e.g. a secure key, is that they remain secret unless intentionally revealed. This is particularly important for providing the information-theoretic level of security [17, 18].

On the other hand, quantum Darwinism [15] suggests that without this information propagation or leakage, the decoherence will not occur, leading, in principle to Wigner's friend paradox [19, 20]. To our knowledge, the problem of this prominent role of the environment has not been investigated in the context of cryptographical applications. The most related considerations concerned only the role of noise in cryptography [21, 22]. This paper aims to provide an example, of how the direct connection between the low-level description of the measurement process, and the high-level specification of application protocols can be done.

We emphasize the role of quantum Darwinism theory in the proposed cryptographical examination. This goes beyond the classical analysis of quantum cryptographical devices that would take into account only the bounds of the correlations between the eavesdropper and the device. The undertaken survey scrutinizes the information transfer not directly to the eavesdropper, but a more subtle and general scenario of leakage outside the safe room, and the imminence that this can be further exploited by the eavesdropper.

The information broadcast elucidated by quantum Darwinism, up to our knowledge, has not been investigated in the cryptographical context before this work. The community working on the decoherence theory, in particular with quantum Darwinism, has been widely investigating the fact that the information widespread is present and necessary for the quantum-to-classical transition, but it has never been examined whether this widespread has any relevance to cryptography. The leakage is inevitable and beyond any control by the very fact that a quantum-to-classical transition has taken place.

Since the topic of this paper is highly interdisciplinary, integrating results of decoherence theory and quantum Darwinism, with attacks characteristic to classical devices in the framework of quantum communication protocols with an application for secure randomness generation, we decided to provide a relatively expanded introduction with an overview of basic concepts of each of these fields. In particular, we propose a quantity investigated in cryptography, *viz.* the guessing probability, and the closely related min-entropy, as a new figure of merit of investigation of the quantum Darwinism theory, that was till now concerned mainly with the mutual information.

In section 1 we overview the decoherence theory, with particular attention to information imprinting in the environment as analyzed by quantum Darwinism. Then, in section 2.1 we describe a particular form of attacks on classical devices called *Van Eck phreaking* and efforts to protect against it called *emission security*. Next, in section 2.2 we overview a particularly relevant type of attack on quantum protocols called *intercept-and-resend* attacks. In section 2.3 we argue that the topic of providing privacy for random numbers has many important applications and point out that the aspect of their security analyzed in this work has till now been neglected. We describe the formalism and methodology used in our security analysis of randomness generation using quantum measurements in shielded laboratories in section 3, and in section 4 apply these methods to cases of incoherent attacks in section 4.1 and coherent attacks in section 4.2. We conclude and pose some new open problems in section 5.

1. Decoherence theory and quantum Darwinism

Decoherence is the process of losing the coherence between subsystems, where the *coherence* is a uniquely quantum type of correlation between separated objects, represented by off-diagonal terms of the density matrix. A perfectly isolated system remains coherent, whereas in open systems coherence is being gradually shared with the environment, ultimately leading to its decay. The notion of decoherence has first been used by Zeh in 1970 [23]. The review of the theory describing the decoherence process is given in [11, 24].

Suppose a quantum state is represented by a normalized positive semi-definite matrix $[\sigma_{i,j}]_{i,j}$. One often measures decoherence using the *collective decoherence factor* [25]:

$$\Gamma \equiv \sum_{i \neq j} \left| \sigma_{i,j} \right| . \tag{1}$$

Obviously, this quantity depends on the choice of the basis in which the quantum state representation is given, but for any practical application one considers the unique (up to permutations) classically meaningful basis of macroscopically observed quantities, *viz.* the pointer basis. For a decohered quantum state, we have $\Gamma \approx 0$.

The key element of decoherence is the following fact. Even though the evolution of every quantum system is given by unitary operators, and thus is reversible, when only one subsystem is considered and the rest is being ignored, or *traced out*, its evolution may not be unitary [26–28]. This allows for relieving the tension between the unitary character of quantum evolution and the irreversibility of quantum measurement. In particular, it can be shown that quantum randomness is a result of losing the coherence [29, 30]. The decoherence theory is used to model the collapse of the wave function, and

transition to a mixed state in the eigenbasis of some local observable, while the quantum superposition of the state of the global wave function of the Universe undergoes the unitary evolution.

Important progress in the theory of decoherence was a series of works by Żurek in 1980s [12, 13] explaining that the basis in which the wave function collapse occurs, *viz.* the mentioned above pointer basis, is determined by the interaction with the exterior of the measured system and the measuring apparatus, i.e. with the environment, in the process called einselection. We elaborate on this idea more in section 3, when we adopt the formalism of these works. This approach allowed Żurek to compute the rate at which a pure state evolves into a mixed state via an interaction with the environment in a thermal equilibrium [31].

Another crucial progress made by Żurek was giving an even more important role in the quantum measurements to the environment. In [32] it was shown that the environment not only plays the passive role of a reservoir selectively destroying the coherence but also the environment selectively proliferates some part of the information about the system in multiple copies. It revealed that the pointer states are the ones that are able to leave a redundant and thus detectable imprint on the environment. In consequence, many observers by probing different parts of the environment can gain consistent information about the pointer basis, and this consent is the distinctive property of classical information that, in opposition to the quantum information [33], can be cloned [34].

The work [34] elucidated the nature of the existence of multiple copies of classical information by the introduction of the notion of the *information plateau*, as defined below. The whole considered Universe in this framework of quantum Darwinism consists of the system S and the environment E. The environment E is divided in arbitrary way into multiple *subenvironments* $\{E_i\}_{i=1}^{N}$, in a sense $E = E_1 \otimes E_2 \otimes \cdots \otimes E_N$. A *fragment*, or macrofraction [25], is a grouping of several subenvironments, with notation $E_M = \bigotimes_{i\in M} E_i$ for $M \subseteq \{1, \cdots, N\}$. Each observer is assumed to capture a random fragment of the environment.

The maximum information that potentially can be accessed about the system S is its von Neumann entropy $H(S) = -\mathrm{Tr}\,[S\log(S)]$. Quantum Darwinism consider the information about S contained in a fragment E_M, i.e. the mutual information $\mathcal{I}_{S:E_M} = H(S) + H(E_M) - H(S, E_M)$. If this information satisfies $(1-\delta)H(S) = \mathcal{I}_{S:E_M}$ we say that δ is the *information deficit* of E_M. Define N_δ as the number of disjoint fragments E_M satisfying $\mathcal{I}_{S:E_M} \geqslant (1-\delta)H(S)$, and for $\delta \ll 1$ this number is closely related the so-called *redundancy* of the information, with large N_δ being an indicator that indeed the information, called classical information, is present in multiple copies in different fragments of the environment; see section 2 of [34] for a detailed discussion.

Note that the maximal value of $\mathcal{I}_{S:E_M}$ is $2H(S)$, not $H(S)$, as it stems from a well-known fact that for pure ρ_{SE} it holds that $H(\rho_{SE}) = 0$ and $H(\rho_S) = H(\rho_E)$.

The average mutual information $\bar{\mathcal{I}}_m$ is the result of averaging over all fragments of size m. It was observed [34] that for relatively small values of m it holds

$$\bar{\mathcal{I}}_m \approx H(S), \tag{2}$$

and that only for m close to N it holds that $\bar{\mathcal{I}}_m \approx 2H(S)$. The large region of values of m satisfying (2), that excludes only very small and very large m, is the information plateau; see [15] for a concise overview of the main properties of quantum Darwinism.

2. Classical and quantum cryptography overview

In this section, we provide a brief overview of selected topics and tasks from classical and quantum cryptography that are relevant to this work. In section 2.1 we describe a particular type of attack on classical devices with support of antennas, then in section 2.2 we discuss the intercept-and-resent type of attacks on quantum cryptography, being a quantum version of the classical man-in-the-middle attacks [35], and in section 2.3 we overview the problems of random number generation, classical and quantum, and its vital role for security.

2.1. Van Eck eavesdropping

All electronic devices necessarily radiate some electromagnetic signals that are correlated to their current state and working. If this radiation is not properly shielded, then an eavesdropper can collect with an antenna part of this signal and use it to regain some information regarding the devices. This kind of attack is sometimes called *electromagnetic analysis attack* [36].

National Security Agency provides so-called TEMPEST specifications referring to security against information leakage through unintentional radiation. The investigation covers both the ways to convey such attacks and protect against them; the latter is referred to as emission security (EMSEC), and covers not only electromagnetic radiations but also mechanical vibrations and sounds caused by the working of devices. We refer to [37, 38] for an overview.

Whereas this potentiality was obvious for most of the engineers and military, with the earliest mentions in the 19th Century [39], it was Van Eck [40] who first showed that such an attack is possible to be conducted using cheap equipment at a range of a hundred meters and that this way a substantial amount of information about real working devices can be obtained. In classical cryptography, this kind of attack with introducing additional side channels [41] gains a large interest and is considered a serious threat [42].

It has been shown that e.g. by monitoring power consumption signals one may breach smart-card security and vulnerability of the Data Encryption Standard (DES) [43–46] and Advanced Encryption Standard [47]. In [40, 48] eavesdropping risk from cathode-ray tube (CRT) monitors, and in [49] for LCDs, has been analyzed. The work [50] considers four types of emanation analysis attacks on wired and wireless keyboards, in [51] attacks using radiation of field programmable gate array are discussed, [52] consider similar attacks on RS-232 cables, [53] analyze an optical attack via LED indicators, [54] attacks on displays using reflections from other objects, [55] acoustic attacks on printers.

In [56] a way of software control over electromagnetic radiation has been proposed, both as a way to reduce the vulnerability to eavesdropping, and as a new possibility for a malevolent designer to increase its susceptibility. Also, hardware designers consider ways to prevent attacks based on radiation [36, 57]. Both power consumption and electromagnetic analysis attacks have simple and differential variants. One of the approaches is to employ a red-black architecture that separates carefully shielded plain-text data, called *red*, and encrypted information, called *black*, so that the shielding requirements may be lessened.

2.2. Intercept and resend attacks in quantum cryptography

The first cryptographical protocol with security arising from the use of quantum resources is the well-known BB84 protocol [3] for quantum key distribution (QKD), where one of the communicating parties, Alice, transmits to the other party, Bob, a qubit either in the computational basis $\mathcal{B}_0 \equiv \{|0\rangle, |1\rangle\}$, or in the Hadamard (conjugate) basis $\mathcal{B}_1 \equiv \{|+\rangle, |-\rangle\}$ with $|+\rangle \equiv (1/\sqrt{2})[|0\rangle + |1\rangle]$ and $|-\rangle \equiv (1/\sqrt{2})[|0\rangle - |1\rangle]$, and afterward Bob performs his measurement also in one of these bases. The procedure is repeated multiple times for subsequent quantum systems. Finally, both parties reveal part of their results, use them to evaluate the reliability of their communication, which covers potential eavesdropping, and eventually perform some post-processing for error correction and privacy amplification [58]. This is paradigmatic for further developed protocols, see [1] for an overview.

A possible attack on a wide class of protocols is for the eavesdropper, Eve, to *intercept* some of the transmitted states, perform some action on them, and in place pass (*resend*) some quantum states to Bob. The passed state can either be transformed [59, 60], or Eve can measure the intercepted state and prepare a new one [61], or use some implementation-dependent attacks [62–66].

The former approach uses the concept of nondemolition measurement [67]. The idea is the following [59]. We assume that Eve knows that the intercepted state will be one of the *non-orthogonal* states $\{|\psi_i\rangle\}_i$, each occurring with probability p_i. This assumption is justified by the construction of the cryptographic scheme. Without measurement Eve's uncertainty regarding the transmitted subsystem is the ordinary Shannon entropy $-\sum_i p_i \log p_i$. The most general unitary transformation U possible to be performed by Eve on an intercepted qubit is [60]

$$U|0\rangle|0\rangle = \sqrt{F}|0\rangle|a\rangle + \sqrt{1-F}|1\rangle|b\rangle, \tag{3a}$$

$$U|1\rangle|0\rangle = \sqrt{1-F}|0\rangle|c\rangle + \sqrt{F}|1\rangle|d\rangle, \tag{3b}$$

where $|a\rangle$, $|b\rangle$, $|c\rangle$, and $|d\rangle$ are states of Eve's subsystem after the interaction, and F is the fidelity of Bob's subsystem. In [59, 60] a trade-off between the gain of information by Eve, and the disturbance caused to Bob, was investigated.

2.3. Private randomness generation

Randomness is a crucial resource for multiple tasks in information and communications technology (ICT). Random numbers have many uses in such fields of application as cryptography and authentication, system modeling and simulation e.g. using Monte Carlo methods, or in gambling. Most random number generators (RNGs) are based on purely algebraic manipulations on an initial seed. Because the series of numbers produced in such a generator is created in a deterministic way, those RNGs are called pseudo-RNGs (PRNGs).

There are also RNGs based on some chaotic classical physical processes such as electrical or atmospheric noise or by estimating the entropy of hardware state [68]. In order to validate that the source of the numbers is reliable, some statistical tests can be used [69]. Still, these tests are not able to guarantee that the numbers were indeed *private*, that is, cannot be predicted by an eavesdropper.

To see why privacy and unpredictability of the sequences of numbers are important, let us note the following places, where random numbers are crucial in establishing a secure classical cryptographical protocol. Out of 64 bits used for the DES key, 56 are randomized (Federal Information Processing Standards, FIPS 46, 1977); ANSI X9.8-1:2003 standard for PIN and FIPS 181-1993 for automatic password generation extensively use random numbers; the standard ANSI—X9.82-1 provides general requirements for (pseudo) random numbers to be used in all cases where security has to be ensured; see [70–77] for an overview of attacks on classical computing systems based on weaknesses of used PRNGs.

Thus, it is natural to try to use a property of quantum mechanics to generate completely random sequences of numbers. There exist methods exploiting such quantum processes as nuclear decay [78–80], or photons hitting a translucent mirror, e.g. id Quantique RNG [81]. Intrinsic indeterminacy of measurement results of quantum mechanics in a simple way enables the generation of numbers that are guaranteed to be unpredictable by the laws of Nature.

The most trivial case is the quantum measurement of a state prepared in a basis different from the one used in the measurement. For instance, a qubit prepared in the computational basis $\mathcal{B}_0$, being thus either $|0\rangle$ or $|1\rangle$, when measured in the Hadamard basis $\mathcal{B}_1$ will result in outcomes $+$ and $-$ with equal probability 0.5, leading to perfectly random numbers, see the discussion in section 3 below.

A great effort has been put into ensuring that the numbers generated by a quantum device are indeed random, with most of the current attention paid to validation that the devices work in a way declared by the constructor, who is considered to be untrusted [82, 83].

Below in this paper, we consider a caveat omitted by all these analyses, as we show that even if the constructor is trustworthy, the very nature of the quantum measurement forces the information about the random number to be insecure and publicly accessible. Similarly, the fact that every electric device is necessarily sending some radiation was well known much earlier than the work of Van Eck in the 1980s, as discussed in section 2.1. Nonetheless, before his work, it was not considered a real danger. The Van Eck innovation was in showing that radiation can substantially be used for wiretapping. We show that the information propagation recognized earlier by the quantum Darwinism research to be ineluctable is also actually cryptographically sound.

3. Methods

We concentrate on an elementary operation of a qubit measurement, as a basic operation for the majority of quantum devices. We follow [12] and call the observed qubit a *system* (S), the measuring device an *apparatus* (A); the third subsystem an environment (E).

We model the premeasurement upon rank-1 projectors $\{P_0^{(S)}, P_1^{(S)}\}$, with $P_0^{(S)} + P_1^{(S)} = \mathbb{1}^{(S)}$ by a CNOT operation conditioned on them, i.e. $U^{(SA)} = P_0^{(S)} \otimes \mathbb{1}^{(A)} + P_1^{(S)} \otimes \sigma_x^{(A)}$, where superscripts in parenthesis denote the subsystem. The interaction of the apparatus with the environment is given by the unitary transformation:

$$U^{(AE)} = |0\rangle\langle 0|^{(A)} \otimes U_0^{(E)} + |1\rangle\langle 1|^{(A)} \otimes U_1^{(E)}, \tag{4}$$

leading to the decoherence in the computational basis $\mathcal{B}_0$ of (A).

To illustrate a simple scenario of quantum randomness generation we consider the measurement of the state $|+\rangle^{(S)} = 1/\sqrt{2}(|0\rangle^{(S)} + |1\rangle^{(S)})$ in the computational basis, with projectors $P_i^{(S)} = |i\rangle\langle i|^{(S)}$, $i = 0, 1$, and with subsystems (A) and (E) initially in 0th state leading to $\rho^{(SA)}(T) \equiv \mathrm{Tr}_E\left[|\phi\rangle\langle\phi|^{(SAE)}\right]$, where

$$|\phi\rangle^{(SAE)} \equiv U^{(AE)} U^{(SA)} |+\rangle^{(S)} \otimes |0\rangle^{(A)} \otimes |0\rangle^{(E)}, \tag{5}$$

and where T is the time after which all the interactions occur. We get that $\Gamma = \left|\langle 0|^{(E)} U_1^{(E)\dagger} U_0^{(E)} |0\rangle^{(E)}\right|$ is the collective decoherence factor, see (1), of the joint state $\rho^{(SA)}(T)$ equal to

$$\frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & \langle 0|^{(E)} U_1^{(E)\dagger} U_0^{(E)} |0\rangle^{(E)} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \langle 0|^{(E)} U_0^{(E)\dagger} U_1^{(E)} |0\rangle^{(E)} & 0 & 0 & 1 \end{bmatrix}, \tag{6}$$

and the full orthogonalization of measurement results occur [25]. For the measurement to betide we need also the full decoherence, i.e. $\Gamma \ll 1$.

The above model refers to the simplest quantum randomness generation, where the measured state $|+\rangle^{(S)}$ is prepared in a basis that is unbiased [84] to the basis $\{P_i^{(S)}\}$ in which the premeasurement is

performed, and the results are stored in the computational basis of the subsystem (A) that is initially preset to $|0\rangle^{(A)}$ to maximize its information capacity [85]. The interaction part $U^{(SA)}$ is designed by the user of the quantum device that calibrates the measuring device to measure in the selected basis, possibly taking into account the characteristics of his source of states; this part is also responsible for apparatus state orthogonalization.

The actual measurement is finalized by the interaction $U^{(AE)}$. $U^{(AE)}$ is partially engineered by the vendor of the measuring apparatus; the computational basis of (A) is actually the one that is being *displayed* to the user and the shape of $U^{(AE)}$ is determined by the device's *case*, like e.g. plastic housing of a USB stick, or metal frame of a rack-mounted multimeter together with the shielding of the laboratory, thus it also depends on the owner of the laboratory and should be considered as a part of the quantum device.

We consider a 4th subsystem, denoted (V) for Van Eck-type eavesdropper since our approach is a quantum analog of the Van Eck attack in classical cryptography, see section 2.1, where the electromagnetic radiation of classical devices is captured by antennas and used to intercept the private content.

In the attack, the eavesdropper intends to capture information regarding the measurement result stored in the apparatus. Since both the former and latter are classical data, we assume the result of wiretapping is stored in the computational basis. We consider a passive reception of the content of the environment, i.e. eavesdropper does not change it. This restricts his action to unitary operations conditioned on some projectors. Further in this text, we consider the particular case of the CNOT operation conditioned on a pair of orthogonal projectors $\{P_0^{(E)}, P_1^{(E)}\}$, with $P_0^{(E)} + P_1^{(E)} = \mathbb{1}^{(E)}$, i.e.

$$U^{(EV)} = P_0^{(E)} \otimes \mathbb{1}^{(V)} + P_1^{(E)} \otimes \sigma_x^{(V)}. \tag{7}$$

The eavesdropper's initial state is $|0\rangle^{(V)}$.

Direct calculations show the final state $|\psi\rangle^{(SAEV)}$ is

$$\begin{aligned}(P_0^{(E)} U_0^{(E)} |0000\rangle^{(SAEV)} + P_1^{(E)} U_0^{(E)} |0001\rangle^{(SAEV)} \\ + P_0^{(E)} U_1^{(E)} |1100\rangle^{(SAEV)} + P_1^{(E)} U_1^{(E)} |1101\rangle^{(SAEV)})/\sqrt{2},\end{aligned} \tag{8}$$

and thus the joint state of the user apparatus and the eavesdropper $\rho^{(AV)}(T) = \mathrm{Tr}_{SE}\left[|\psi\rangle\langle\psi|^{(SAEV)}\right]$ is a state diagonal in the computational basis with coefficients: $\langle 0|U_0^\dagger P_1\, U_0|0\rangle/2$, $\langle 0|U_0^\dagger P_0\, U_0|0\rangle/2$, $\langle 0|U_1^\dagger P_1\, U_1|0\rangle/2$, and $\langle 0|U_1^\dagger P_0\, U_1|0\rangle/2$, where we omitted the superscript (E).

The figure of cryptographical merit we consider here is the probability that the eavesdropper correctly guesses the measurement result of the apparatus [86–89], denoted $\mathrm{P}_{\mathrm{guess}}$. This happens when both two-dimensional subsystems (A) and (V) indicate the same binary value, thus it is given by:

$$\begin{aligned}\langle 00|^{(AV)} \rho^{(AV)}(T) |00\rangle^{(AV)} + \langle 11|^{(AV)} \rho^{(AV)}(T) |11\rangle^{(AV)} \\ = \frac{1}{2}\langle 0|^{(E)} (U_0^{(E)\dagger} P_0^{(E)} U_0^{(E)} + U_1^{(E)\dagger} P_1^{(E)} U_1^{(E)}) |0\rangle^{(E)}.\end{aligned} \tag{9}$$

The environment (E) mediates between subsystems (A) and (V) and can be of a much larger dimension.

From (9) we see, that the guessing probability depends both on the ability of the environment to gather information regarding the apparatus, modeled by $\{U_0^{(E)}, U_1^{(E)}\}$, and on the possibility of collecting the signal from the environment through the Van Eck-type antenna, modeled by $\{P_0^{(E)}, P_1^{(E)}\}$. The shielded laboratory assumption refers to the case with $U_0^{(E)} = U_1^{(E)} = \mathbb{1}^{(E)}$; then the value of (9) is 0.5, so no information leaks outside the laboratory, and simultaneously $\Gamma = 1$, thus the measurement does not occur. Note that the guessing probability in (14) is the probability that the eavesdropper's subsystem (V) indicates the same state as the apparatus (A), and since we consider binary measurement, both subsystems are two-dimensional.

The antenna determines the evolution $U^{(EV)}$ and is possessed by the wiretapper, and its capabilities are limited by his resources, reflecting his control over the information scattering. The rest of this paper aims to model the dependence of the guessing probability (9) on the power of the eavesdropper.

The scheme for information retrieval by an eavesdropper we propose here can be compared to the intercept-and-resend attack on QKD protocols discussed in section 2.2. Even though we deal with a single honest party, Alice, and there is no intentionally communicated second party, Bob, we still can view the protocol of a measurement process as a state preparation of the environment, that is formally close to the state submission to another party. From this point of view, the subsystem of the environment (E) plays a partially analogous role to the prepared and transmitted state; thus the first subsystem in (3) refers to (E) and the second subsystem to (V) using the notation of this section. Nonetheless, the differences between both schemes are fundamental, and should not be neglected. We summarize them as follows:

(a) The essence of the security assured in QKD protocols against intercept-and-resend attack stem from the fact that the eavesdropper does not know the correct measurement basis. Thus, in the average case, the eavesdropper necessarily introduces some disturbance to the transferred quantum systems. Security is achieved as this disturbance can be further utilized by the users of the quantum protocol to detect the fact of wiretapping. In the attack proposed in this paper, any disturbance pertains to the environment external to the cryptographic system and has not been investigated as a potential diagnostic of aggression.

(b) In QKD protocols, the prepared and transmitted quantum state is intended to be further measured after being received. After the measurement, the information can be copied perfectly and under control without any disturbance. In the introduced attack, the preparation of the state of the environment is unintentional, and the environment is beyond the control of the users of the QKD protocol. Nonetheless, the eavesdropper can perform a measurement on part of the environment, that, as shown in this work, can influence security.

(c) In the proposed scheme the preparation of the state accessible to the eavesdropper is not *intended* to transmit information to other parts of the world; what is more, any information transfer is a kind of *necessary evil* needed for the local process of the measurement to betide, and the violated shielded laboratory assumption would demand this information be nullified if it were possible. On contrary, in ordinary quantum cryptographic protocols, the transmitted subsystem intentionally contains information, in fact as much information as it could accommodate.

(d) In the proposed scheme the eavesdropper has much more control over the 'transferred' subsystem, *viz.* the environment after the measurement process containing information on the measurement result, that is intended to be kept secret. In QKD protocols the integrity of the transmitted states is checked at the stage when parties publish parts of their data and use it to evaluate some certificate of their security. This aspect has not been to date considered from the point of view of necessary information wide spreading during the measurement process, and thus in all currently existing protocols, Alice overlooked an eavesdropping antenna potentially standing very next to her laboratory.

In other words, there is no other way to use any quantum device and perform a quantum measurement than to make the measurement result publicly accessible to the environment outside the shielding. This is an intrinsic property of any possible quantum protocol, not only the simplified randomness generation in the considered example. If one uses a perfectly shielded laboratory, then she or he cannot perform a quantum measurement; if one performs a quantum measurement, then her or his laboratory cannot be perfectly shielded—if it can be shielded at all.

4. Results

In this section, we provide the results of applying the techniques of section 3 to two particular examples of the interaction of the measuring apparatus with the environment with the eavesdropper monitoring it with an antenna. In section 4.1 we provide an analytical study of a case with an environment consisting of multi two-level quantum system, and an eavesdropper accessing part of them in an incoherent way. In section 4.2 we present numerical results regarding a coherent attack on a part of a multi-level coherent environment.

4.1. Multi-qubit environment with incoherent eavesdropper

Now, let us use the above results to analyze a case of the environment consisting of N qubits. We follow the standard approach [16, 90] and model the $U^{(AE)}$ interaction as N independent imperfect CNOT defined as

$$U_{\oslash}(\theta) \equiv |0\rangle\langle 0|^{(A)} \otimes \mathbb{1}_2^{(\cdot)} + |1\rangle\langle 1|^{(A)} \otimes P_{\oslash}^{(\cdot)}, \tag{10}$$

with $P_{\oslash} \equiv \begin{pmatrix} \sin\theta & \cos\theta \\ \cos\theta & -\sin\theta \end{pmatrix}$, and θ fixed for the setup, i.e.

$$U_{\oslash}(\theta) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \sin\theta & \cos\theta \\ 0 & 0 & \cos\theta & -\sin\theta \end{bmatrix}. \tag{11}$$

Thus, we have $U_0^{(E)} = \mathbb{1}_{2^N}$ and $U_1^{(E)} = \bigotimes_{s=1}^{N} P_{\oslash}^{(s)}$, where (s) denotes sth environmental qubit.

From this, it follows that the collective decoherence factor $\Gamma = |\sin\theta|^N$, or, that for a specific value of Γ an interaction with at least $N \geqslant \frac{-\ln\Gamma}{-\ln|\sin\theta|}$ environmental qubits is required. The factor dependent on θ is an

engineering parameter, and Γ is a quantumness parameter, thus we may assume that the number $n \leqslant N$ of qubits accessible to the eavesdropper is $\frac{\mu(-\ln\Gamma)}{-\ln|\sin\theta|}$, for some function μ.

Let us consider the case when the eavesdropper is not able to perform a coherent measurement on multiple qubits and needs to perform the guess based on many separate single-qubit measurements. If he performs the Helstrom measurement [91], with one of the projectors given by $\begin{pmatrix} \cos^2(\theta/2) & -(\sin\theta)/2 \\ -(\sin\theta)/2 & \sin^2(\theta/2) \end{pmatrix}$, on a specific environmental qubit, the success probability of correct distinguishing its state is $p \equiv (1+|\cos\theta|)/2$.

Suppose that the guess is given as the majority of n single-qubit guesses, i.e. it succeeds when at least $n/2$ of these guesses is correct. Thus, the total success probability of the guess (9) is equal to $1 - F(n/2; n, p)$, where $F(\cdot; n, p)$ is the cumulative distribution function of the binomial distribution with n Bernoulli trials with success probability p. Now, we ask, for what range of Γ, θ, and μ do we have $\mathrm{P}_{\mathrm{guess}} \gg 1/2$?

It can be shown [92, 93] that for $p \in (0,1)$ and $a < p$ it holds $F(an; n, p) \leqslant \exp(-nD(a||p))$, where $D(a||p) \equiv a\ln\frac{a}{p} + (1-a)\ln\frac{1-a}{1-p}$ is the Kullback–Leibler divergence between Bernoulli random variables. Using the above formulae for n and p we directly get

$$D(1/2||(1+|\cos\theta|)/2) = -\ln|\sin\theta|, \tag{12}$$

and thus

$$\mathrm{P}_{\mathrm{guess}} \geqslant 1 - \exp(-\mu(-\ln\Gamma)), \tag{13}$$

and the lower bound does not depend on θ. From these considerations it follows that taking any μ satisfying $\lim_{x\to\infty}\mu(x) = \infty$ and $\lim_{x\to\infty}\frac{\mu(x)}{x} = 0$ we have that in the classical limit an arbitrarily small fraction of all environmental qubits is enough to provide the eavesdropper full access to cryptographic data.

The fact expressed in (13), that the larger part of the environment is being observed, the more information about the system is gathered, complies with the information plateau observation of the quantum Darwinism [15, 34, 94], see section 1. We would like at this point to briefly discuss the relation between these two facts.

One of the central outcomes of quantum Darwinism is the result, that the mutual information between a measured (or *observed*) subsystem and a small fraction of the surrounding environment, is close to the von Neumann entropy of the former, $H(S)$. In a sense, $H(S)$ sets the limit on the classical information that the environment (E) can acquire about (S). It can also be observed, that when almost all the environment (E) is considered, it contains also the almost full quantum information about (S), as noted in section 1. It can be shown that the potential of acquisition of the quantum information is significantly diminished when any initial mixedness, or *haziness*, is present in the environment [94].

On the other hand, the quantity being paramount to our analysis is the guessing probability, directly related to min-entropy H_∞ [88], *viz.* for a classical probability distribution we have $H_\infty = -\log_2 \mathrm{P}_{\mathrm{guess}}$. The conditional quantum min-entropy is a single-shot [95] version of the conditional quantum entropy, in a sense that the latter may be considered as a limit of the former when an infinite number of copies of the states are available, as stated by the quantum asymptotic equipartition property (QAEP) [96].

Thus, the approach to quantum Darwinism that we propose, employing the analysis of the guessing probability instead of the mutual information, supplies a related, but a new point of view on the concept of redundant imprinting of information in quantum Darwinism. Obviously, the larger the quantum mutual information the larger the classical guessing probability can be expected, and vice versa. However, a goal of quantum Darwinism, as a quantum-to-classical transition theory, is to elucidate the classical properties of quantum systems. Thus, a quantity that is classical in its nature, *viz.* the guessing probability, may be expected to provide new insight into the problem.

In quantum Darwinism, the fact that the classical information about (S) is present in the environment is expressed by the observation that multiple fragments of the environment (E) have large mutual information with (S). In contrast, in the view of QAEP, min-entropy and the guessing probability concern the situation when there exists at least one fragment of the environment with the classical information imprint. We leave a further investigation of the relation of these approaches to quantum Darwinism for future work.

We note that when the whole environment is accessible to the eavesdropper, even in an incoherent, semi-classical, manner, i.e. for $\mu(x) = x$, the relation (13) takes a simple trade-off form

$$\mathrm{P}_{\mathrm{guess}} + \Gamma \geqslant 1. \tag{14}$$

We see that the shielded laboratory assumption $\mathrm{P}_{\mathrm{guess}} \leqslant 1/2$ entails $\Gamma \geqslant 1/2$, *viz.* restricts the measurement to premeasurement. The trade-off (14) in particular states that the eavesdropper's ability to read out the information of the measurement limits the degree of decoherence.

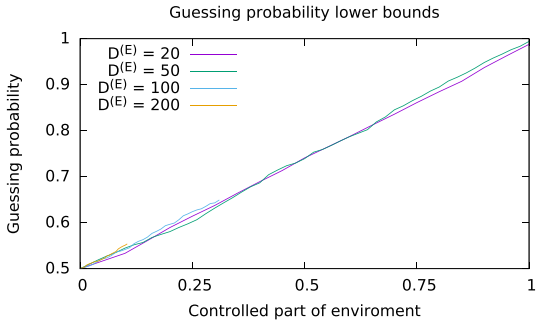

Figure 1. The dependence of the guessing probability of the indicator of the measuring apparatus by a Van Eck-type eavesdropper depending on the relative size of the part of the environment observed by the wiretapping antenna for different dimensions $D^{(E)}$ of the environment.

The above model is exceedingly simplistic, covering only a particular form of potential attacks of Van Eck's type, and may not be the most efficient one. Yet, this restricted and fairly simple and natural form of gathering information from the surroundings is enough to compromise the security of a device producing private numbers showing that the discussed sort of attack is a serious threat.

Let us summarize the assumptions we make in the derivation of the lower bound (13). We assume a particular form of the interaction $U^{(SA)}$ justified by the functioning of a measuring device. The decomposition of the measurement process into parts $U^{(SA)}$ and $U^{(AE)}$ is justified by its logical order in the measurement, i.e. first occurs the premeasurement, and then occurs the decoherence. Thus, stating that the measuring device interacts with the environment via some interaction $U^{(AE)}$ is not restrictive. Next, we perform the calculations using a particular form of $U^{(AE)}$ used in [16, 90]; we leave considerations with more general $U^{(AE)}$ as an important new engineering task of designing cryptographical devices in a way more secure against Van Eck's attacks. The considered form of the interaction $U^{(EV)}$ does not restrict the generality of our results, as it is sufficient for the trade-off relation to occur. We show that such interaction exists, possibly there exists another interaction $U^{(EV)}$ for which the trade-off relation is even stronger; we also leave this for a further study of the interplay between designing devices with more suitable $U^{(AE)}$ and attacks with more efficient $U^{(EV)}$.

To see the consequences of the above analysis, we start with the simplest case with one environmental qubit interacting via a perfect CNOT, *viz.* $N = 1$ and $\theta = 0$. We have the full decoherence with $\Gamma = 0$ but, if the only environmental qubit is intercepted by the eavesdropper, we also have $\mathrm{P}_{\mathrm{guess}} = 1$. For a toy model of decoherence with $N = 20$ and $\theta = \pi/4$ we have $\Gamma \approx 0.001$; then for 1, 3, and 5 intercepted environmental qubits $\mathrm{P}_{\mathrm{guess}}$ is 0.85, 0.94, and 0.98, respectively. For the more realistic case with $\Gamma \approx 10^{-40}$ [97] if the van Eck's antenna observes 1% or 5% of the environment, then $\mathrm{P}_{\mathrm{guess}}$ is 0.6 or 0.99, respectively.

4.2. Coherent eavesdropping from moderate-size environment

To investigate how the privacy of quantum random numbers from the above model is compromised by a coherent Van Eck-type antenna we performed also numerical simulations. Let $D^{(E)}$ denote the dimension of the environment, and $k \in \{2, \cdots, D^{(E)}\}$ be the number of degrees of freedom of the environment the antenna can faithfully distinguish; the ratio $k/D^{(E)}$ can be considered as the measure of how much of the environment is monitored, or controlled, by the eavesdropper.

In the numerical calculations we consider Haar distributed [98] $\{U_0^{(E)}, U_1^{(E)}\}$. To simulate the limitations of Van Eck's antenna we now consider $P_0^{(E)}$ of the following form. We decompose the space of the environment $\mathcal{H}^{(E)}$ into two parts: $\mathcal{H}^{(\hat{E})}$, and $\mathcal{H}^{(\tilde{E})}$, with dimensions k and $D^{(E)} - k$, respectively; so that $\mathcal{H}^{(E)} = \mathcal{H}^{(\hat{E})} \oplus \mathcal{H}^{(\tilde{E})}$, where $\oplus$ denotes the direct sum of spaces. We take $P_0^{(E)} = P^{(\hat{E})} \oplus \mathbb{1}^{(\tilde{E})}$, where $P^{(\hat{E})}$ is an arbitrary projector on $\mathcal{H}^{(\hat{E})}$ with the rank $\lfloor k/2 \rfloor$.

We executed the computation of (9) for $D^{(E)} = 20, 50, 100, 200$. To this end, for each instance, we parametrized the operator $P^{(\hat{E})}$ and performed a gradient search to maximize the value of the guessing probability. We averaged the results of several (15, 8, 11, and 4, respectively) instances with different $\{U_0^{(E)}, U_1^{(E)}\}$. The results are shown in figure 1.

It can be observed that the guessing probability is more or less proportional to the observed part of the environment. We note that even when the eavesdropper possesses full access to the environment's information, she or he still may not be able to achieve the value 1 of guessing probability since not all

information could have been propagated, especially when the value of $D^{(E)}$ is small. This relates to the situation with $\Gamma \gg 0$, so with no full measurement inside the laboratory.

5. Conclusions

Despite this work being embedded in the framework of einselection and quantum Darwinism, we do not consider here the usual scenario of information widespread in multiple copies of independent parts of the environment. We concentrate on the observation of a single observer, so, this cannot be understood as a model of *objectivity* [99] (or *inter-subjectivity* [25, 100]) as investigated in the recent works [16]. Yet, it is obvious, that after a measurement is performed, then knowing *what* has been measured (i.e. the basis), should imply the ability to copy and disseminate the result [33, 101].

We have seen that the shielded laboratory assumption prevents the occurrence of measurement; and that by relaxing this assumption, we open a way for attacks similar to the Van Eck phreaking. We note that although figure 1 shows cases with relatively small sizes of the environment compared to macroscopic objects, it suggests that the greater the dimension, the lower part of the laboratory's surroundings has to be under control for the significant potential for eavesdropping. Indeed, the relation (13) we derived for incoherent qubits phreaking clearly indicates that any sort of cryptographic protocol is prone to the discussed type of attacks.

We would like to stress that our topic is not the analysis of the case when the device that processes quantum information happens not to be perfectly shielded due to imperfections. We also do not consider the case when the eavesdropper is vetting any classical information encoded microscopically in the cryptographical equipment after potentially gaining access to it. On contrary, we show that for any quantum measuring-based device to function properly it is *necessary to drop* the perfect shielding assumption by the design, and adjust to the fact delivered from quantum Darwinism, that after the quantum-to-classical transition the uncontrolled information leakage is ineluctable.

In this preliminary study, we investigated only the simplest case where the quantum randomness is obtained from the measurement on a different basis than the prepared state. Although simple, this scenario is ubiquitous as an ingredient of more involved and complex quantum protocols.

This work intends to show that the quantitative investigation of the relation between two important, yet till now disjoint, areas of quantum information, *viz.* theory (quantum Darwinism) and application (quantum cryptography) of measurements are possible. Quantum cryptography is a wide field and is currently the only quantum information research area with serious commercial deployments [102, 103]. Our main premise is to change one of the essential parts of the paradigm of quantum cryptography that was based on neglecting, or abstracting from, the way the quantum measurement is performed in cryptographic devices. We also suggest that the guessing probability together with the related concept of min-entropy may be a relevant quantity to be investigated in quantum Darwinism in a way similar to the mutual information.

We expect the presented result will encourage researchers working on decoherence theory to contribute to the development of the design of cryptographic devices, similarly as they contribute to the area of quantum computation [104–106]. We consider it an interesting and vital problem, how such analysis can be extended to more complicated scenarios, and cover such problems as quantum communication [3] or QKD [107], not only in a device-dependent scenario, like in this work, but possibly in device-independent [108], or semi-device-independent [109] frameworks.

We close this work with the practical open question of whether it is possible to protect against the introduced type of attacks. We predict the general answer, with the eavesdropper with sufficient control over the environment, to be negative. Still, it is plausible that under some reasonable assumptions regarding the technology of the eavesdropper, one can engineer the shielding in such a way that the measurement does occur while the wiretapping task becomes burdensome. Another possible way of defense could potentially be to adopt the ordinary quantum cryptographical methods [3, 60] to somehow detect the action of a Van Eck-type eavesdropper on the environment.

Data availability statement

The work does not involve any data not included in the text. The MATLAB source codes used to prepare figure 1 are available upon request from the author. All data that support the findings of this study are included within the article (and any supplementary files).

Acknowledgment

The work is supported by the Foundation for Polish Science (IRAP project, ICTQT, Contract No. 2018/MAB/5, co-financed by EU within Smart Growth Operational Programme), NCBiR QUANTERA/2/2020 (www.quantera.eu), an ERA-Net cofund in Quantum Technologies, under the project eDICT, and NCN grant SHENG (Contract No. 2018/30/Q/ST2/00625). The numerical calculations we conducted using OCTAVE 6.1 [110], and packages QETLAB 0.9 [111] and Quantinf 0.5.1 [112].

Conflicts of Interest

The author declare no conflict of interest.

Ethical statement

The work is purely theoretical. No ethical issues were noted by the author.

ORCID iD

P Mironowicz https://orcid.org/0000-0003-4122-5372

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography *Rev. Mod. Phys.* **74** 145
[2] Portmann C and Renner R 2022 Security in quantum cryptography *Rev. Mod. Phys.* **94** 025008
[3] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India)* (arXiv:2003.06557) pp 175–9
[4] Vazirani U and Vidick T 2014 Fully device-independent quantum key distribution *Phys. Rev. Lett.* **113** 140501
[5] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 The security of practical quantum key distribution *Rev. Mod. Phys.* **81** 1301
[6] Herrero-Collantes M and Garcia-Escartin J C 2017 Quantum random number generators *Rev. Mod. Phys.* **89** 015004
[7] Herrero-Collantes M and Garcia-Escartin J C 1995 *Quantum Measurement* (Cambridge: Cambridge University Press)
[8] Schroedinger E 1935 Die gegenwärtige situation in der quantenmechanik *Naturwissenschaften* **23** 823–8
[9] Wigner E P 1963 The problem of measurement *Am. J. Phys.* **31** 6–15
[10] Leggett A J 2005 The quantum measurement problem *Science* **307** 871–2
[11] Schlosshauer M A 2007 *Decoherence: and the Quantum-to-Classical Transition* (Heidelberg: Springer)
[12] Żurek W H 1981 Pointer basis of quantum apparatus: into what mixture does the wave packet collapse? *Phys. Rev.* D **24** 1516
[13] Żurek W H 1982 Environment-induced superselection rules *Phys. Rev.* D **26** 1862
[14] Żurek W H 2003 Decoherence, einselection and the quantum origins of the classical *Rev. Mod. Phys.* **75** 715
[15] Żurek W H 2009 Quantum Darwinism *Nat. Phys.* **5** 181–8
[16] Touil A, Yan B, Girolami D, Deffner S and Żurek W H 2022 Eavesdropping on the decohering environment: quantum Darwinism, amplification and the origin of objective classical reality *Phys. Rev. Lett.* **128** 010401
[17] Shannon C E 1949 Communication theory of secrecy systems *Bell Syst. Tech. J.* **28** 656–715
[18] Diffie W and Hellman M 1976 New directions in cryptography *IEEE Trans. Inf. Theory* **22** 644–54
[19] Wigner E P 1961 Remarks on the Mind-Body Question *The Scientist Speculates* ed I J Good (Portsmouth, NH: Heineman)
[20] Deutsch D 1985 Quantum theory as a universal physical theory *Int. J. Theor. Phys.* **24** 1–41
[21] Brandt H E 1999 Qubit devices and the issue of quantum decoherence *Prog. Quantum Electron.* **22** 257–370
[22] Sharma V, Shrikant U, Srikanth R and Banerjee S 2018 Decoherence can help quantum cryptographic security *Quantum Inf. Process.* **17** 1–16
[23] Zeh H D 1970 On the interpretation of measurement in quantum theory *Found. Phys.* **1** 69–76
[24] Schlosshauer M 2005 Decoherence, the measurement problem and interpretations of quantum mechanics *Rev. Mod. Phys.* **76** 1267
[25] Mironowicz P, Korbicz J K and Horodecki P 2017 Monitoring of the process of system information broadcasting in time *Phys. Rev. Lett.* **118** 150501
[26] Breuer H P and Petruccione F 2002 *The Theory of Open Quantum Systems* (Oxford: Oxford University Press)
[27] Gorini V, Kossakowski A and Sudarshan E C G 1976 Completely positive dynamical semigroups of N-level systems *J. Math. Phys.* **17** 821–5
[28] Lindblad G 1976 On the generators of quantum dynamical semigroups *Commun. Math. Phys.* **48** 119–30
[29] Yuan X, Zhou H, Cao Z and Ma X 2015 Intrinsic randomness as a measure of quantum coherence *Phys. Rev.* A **92** 022124
[30] Yuan X, Zhao Q, Girolami D and Ma X 2019 Quantum coherence and intrinsic randomness *Adv. Quantum Technol.* **2** 1900053
[31] Zurek W H, Habib S and Paz J P 1993 Coherent states via decoherence *Phys. Rev. Lett.* **70** 1187
[32] Ollivier H, Poulin D and Żurek W H 2004 Objective properties from subjective quantum states: environment as a witness *Phys. Rev. Lett.* **93** 220401
[33] Wootters W K and Żurek W H 1982 A single quantum cannot be cloned *Nature* **299** 802–3
[34] Blume-Kohout R and Żurek W H 2006 Quantum Darwinism: entanglement, branches and the emergent classicality of redundantly stored quantum information *Phys. Rev.* A **73** 062310

[35] Bhushan B, Sahoo G and Rai A K 2017 Man-in-the-middle attack in wireless and computer networking - a review *2017 3rd Int. Conf. on Advances in Computing, Communication and Automation (ICACCAFall)* (IEEE) pp 1–6
[36] Kocher P, Lee R, McGraw G and Raghunathan A 2004 Security as a new dimension in embedded system design *Proc. 41st Annual Design Automation Conf.* pp 753–60
[37] Kuhn M G 2005 Security limits for compromising emanations *International Workshop on Cryptographic Hardware and Embedded Systems* (Berlin: Springer) pp 265–79
[38] Lavaud C, Gerzaguet R, Gautier M, Berder O, Nogues E and Molton S 2021 Whispering devices: a survey on how side-channels lead to compromised information *J. Hardware Syst. Secur.* **5** 143–68
[39] (Available at: https://cryptome.org/tempest-old.htm)
[40] Van Eck W 1985 Electromagnetic radiation from video display units: an eavesdropping risk? *Comput. Secur.* **4** 269–86
[41] Kelsey J, Schneier B, Wagner D and Hall C 1998 Side channel cryptanalysis of product ciphers *European Symp. on Research in Computer Security* (Berlin: Springer) pp 97–110
[42] US Air Force 1998 *Air Force Systems Security Memorandum 7011-Emission Security Countermeasures Review*
[43] Messerges T S, Dabbish E A and Sloan R H 1999 Investigations of power analysis attacks on smartcards *Smartcard* **99** 151–61
[44] Gandolfi K, Mourtel C and Olivier F 2001 Electromagnetic analysis: concrete results *International Workshop on Cryptographic Hardware and Embedded Systems* (Berlin: Springer) pp 251–61
[45] Quisquater J J and Samyde D 2001 Electromagnetic analysis (ema): measures and counter-measures for smart cards *Int. Conf. on Research in Smart Cards* (Berlin: Springer) pp 200–10
[46] Messerges T S, Dabbish E A and Sloan R H 2002 Examining smart-card security under the threat of power analysis attacks *IEEE Trans. Comput.* **51** 541–52
[47] Messerges T S 2000 Securing the AES Finalists Against Power Analysis Attacks *International Workshop on Fast Software Encryption* (Berlin: Springer) pp 150–64
[48] Kuhn M G 2002 Compromising emanations: eavesdropping risks of computer displays *Doctoral Dissertation* University of Cambridge
[49] Kuhn M G 2004 Electromagnetic eavesdropping risks of flat-panel displays *International Workshop on Privacy Enhancing Technologies* (Berlin: Springer) pp 88–107
[50] Vuagnoux M and Pasini S 2009 Compromising electromagnetic emanations of wired and wireless keyboards *USENIX Security Symp.* vol 1
[51] De Mulder E, Örs S B, Preneel B and Verbauwhede I 2007 Differential power and electromagnetic attacks on a FPGA implementation of elliptic curve cryptosystems *Comput. Electr. Eng.* **33** 367–82
[52] Smulders P 1990 The threat of information theft by reception of electromagnetic radiation from RS-232 cables *Comput. Secur.* **9** 53–58
[53] Loughry J and Umphress D A 2002 Information leakage from optical emanations *ACM Trans. Inf. Syst. Secur. (TISSEC)* **5** 262–89
[54] Backes M, Dürmuth M and Unruh D 2008 Compromising reflections-or-how to read LCD monitors around the corner *2008 IEEE Symp. on Security and Privacy* (IEEE) pp 158–69
[55] Backes M, Dürmuth M, Gerling S, Pinkal M and Sporleder C 2010 Acoustic side-channel attacks on printers *19th USENIX Security Symp., USENIX Security* vol 10
[56] Kuhn M G and Anderson R J 1998 Soft tempest: hidden data transmission using electromagnetic emanations *Int. Workshop on Information Hiding* (Berlin: Springer) pp 124–42
[57] Wang Y and Jing X 2005 Intrinsically conducting polymers for electromagnetic interference shielding *Polym. Adv. Technol.* **16** 344–51
[58] Bennett C H, Brassard G and Robert J M 1988 Privacy amplification by public discussion *SIAM J. Comput.* **17** 210–29
[59] Fuchs C A and Peres A 1996 Quantum-state disturbance versus information gain: uncertainty relations for quantum information *Phys. Rev.* A **53** 2038
[60] Bruß D 1998 Optimal eavesdropping in quantum cryptography with six states *Phys. Rev. Lett.* **81** 3018
[61] Bennett C H, Bessette F, Brassard G, Salvail L and Smolin J 1992 Experimental quantum cryptography *J. Cryptol.* **5** 3–28
[62] Dušek M, Jahma M and Lütkenhaus N 2000 Unambiguous state discrimination in quantum cryptography with weak coherent states *Phys. Rev.* A **62** 022306
[63] Curty M and Lütkenhaus N 2005 Intercept-resend attacks in the Bennett-Brassard 1984 quantum-key-distribution protocol with weak coherent pulses *Phys. Rev.* A **71** 062301
[64] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 Hacking commercial quantum cryptography systems by tailored bright illumination *Nat. Photon.* **4** 686–9
[65] Gerhardt I, Liu Q, Lamas-Linares A, Skaar J, Kurtsiefer C and Makarov V 2011 Full-field implementation of a perfect eavesdropper on a quantum cryptography system *Nat. Commun.* **2** 1–6
[66] Chaturvedi A, Ray M, Veynar R and Pawłowski M 2018 On the security of semi-device-independent QKD protocols *Quantum Inf. Process.* **17** 1–20
[67] Unruh W G 1978 Analysis of quantum-nondemolition measurement *Phys. Rev.* D **18** 1764
[68] Kim J S, Patel M, Hassan H, Orosa L and Mutlu O 2019 D-RaNGe: using commodity DRAM devices to generate true random numbers with low latency and high throughput *2019 IEEE Int. Symp. on High Performance Computer Architecture (HPCA)* (IEEE) pp 582–95
[69] Bassham L, Rukhin A, Soto J, Nechvatal J, Smid M, Leigh S, Levenson M, Vangel M, Heckert N and Banks D 2010 *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* (Gaithersburg, MD: Special Publication (NIST SP), National Institute of Standards and Technology)
[70] Dorrendorf L, Gutterman Z and Pinkas B 2007 Cryptanalysis of the windows random number generator *Proc. 14th ACM Conf. on Computer and Communications Security* pp 476–85
[71] Naor M and Segev G 2009 Public-key cryptosystems resilient to key leakage *Annual Int. Cryptology Conf.* (*Berlin: Springer*) pp 18–35
[72] Bellare M, Brakerski Z, Naor M, Ristenpart T, Segev G, Shacham H and Yilek S 2009 Hedged public-key encryption: how to protect against bad randomness *Int. Conf. on the Theory and Application of Cryptology and Information Security* (Berlin: Springer) pp 232–49
[73] Schindler W 2009 Random number generators for cryptographic applications *Cryptographic Engineering* (Boston, MA: Springer) pp 5–23

[74] Krawczyk H 2010 Cryptographic extraction and key derivation: the HKDF scheme *Annual Cryptology Conf.* (*Berlin: Springer*) pp 631–48
[75] Ristenpart T and Yilek S 2010 When good randomness goes bad: virtual machine reset vulnerabilities and hedging deployed cryptography *Proc. Network and Distributed Security Symp. (NDSS)* (San Diego, CA: The Internet Society) pp 1–18
[76] Marton K, Suciu A and Ignat I 2010 Randomness in digital cryptography: a survey *Rom. J. Inf. Sci. Technol.* **13** 219–40
[77] Heninger N, Durumeric Z, Wustrow E and Halderman J A 2012 Mining your Ps and Qs: detection of widespread weak keys in network devices *21st USENIX Security Symp. (USENIX Security 12)* pp 205–20
[78] Rohe M 2003 *Randy-A True-Random Generator Based On Radioactive Decay* (Saarbrücken: Fortgeschrittenenpraktikum, Security and Cryptography Research Group Saarland University)
[79] Park K H, Park S M, Choi B G, Kim J B and Son K J 2020 High rate true random number generator using beta radiation *AIP Conf. Proc.* vol 2295 (AIP Publishing LLC) p 020020
[80] Park K, Park S, Choi B G, Kang T, Kim J, Kim Y H and Jin H Z 2020 A lightweight true random number generator using beta radiation for IoT applications *Electron. Telecommun. Res. Inst. J.* **42** 951–64
[81] (Available at: www.idquantique.com)
[82] Pironio S *et al* 2010 Random numbers certified by Bell's theorem *Nature* **464** 1021–4
[83] Liu Y *et al* 2018 Device-independent quantum random-number generation *Nature* **562** 548–51
[84] Bengtsson I 2007 Three ways to look at mutually unbiased bases *AIP Conf. Proc.* vol 889 (American Institute of Physics) pp 40–51
[85] Zwolak M, Quan H T and Żurek W H 2009 Quantum Darwinism in a mixed environment *Phys. Rev. Lett.* **103** 110402
[86] Chor B and Goldreich O 1988 Unbiased bits from sources of weak randomness and probabilistic communication complexity *SIAM J. Comput.* **17** 230–61
[87] Impagliazzo R, Levin L A and Luby M 1989 Pseudo-random generation from one-way functions *Proc. 21st Annual ACM Symp. on Theory of Computing* pp 12–24
[88] Konig R, Renner R and Schaffner C 2009 The operational meaning of min-and max-entropy *IEEE Trans. Inf. Theory* **55** 4337–47
[89] Issa I and Wagner A B 2017 Measuring secrecy by the probability of a successful guess *IEEE Trans. Inf. Theory* **63** 3783–803
[90] Mironowicz P, Horodecki P and Horodecki R 2022 Non-Perfect propagation of information to a noisy environment with self-evolution *Entropy* **24** 467
[91] Helstrom C W 1969 Quantum detection and estimation theory *J. Stat. Phys.* **1** 231–52
[92] Bernstein S N 1964 *Collected Works* vol 4 (Moscow: USSR Academy of Sciences)
[93] Ferrante G C 2021 Bounds on binomial tails with applications *IEEE Trans. Inf. Theory* **67** 8273–9
[94] Zwolak M, Quan H T and Żurek W H 2010 Redundant imprinting of information in nonideal environments: Objective reality via a noisy channel *Phys. Rev.* A **81** 062110
[95] Berta M 2009 Single-shot quantum state merging (arXiv:0912.4495) (https://doi.org/10.48550/arXiv.0912.4495)
[96] Tomamichel M, Colbeck R and Renner R 2009 A fully quantum asymptotic equipartition property *IEEE Trans. Inf. Theory* **55** 5840–7
[97] Żurek W H 1986 Reduction of the wavepacket: how long does it take? *Frontiers of Nonequilibrium Statistical Physics* (Boston, MA: Springer) pp 145–9
[98] Haar A 1933 Der Massbegriff in der theorie der kontinuierlichen gruppen *Ann. Math.* **34** 147–69
[99] Korbicz J K 2021 Roads to objectivity: quantum Darwinism, spectrum broadcast structures and strong quantum Darwinism - a review *Quantum* **5** 571
[100] Ajdukiewicz K and Giedymin J 1978 *The Scientific World-Perspective and Other Essays, 1931-1963* (Dordrecht: Reidel) pp 155–64
[101] Żurek W H 2000 Schrödinger's sheep *Nature* **404** 130–1
[102] Shenoy-Hejamadi A, Pathak A and Radhakrishna S 2018 Quantum cryptography: key distribution and beyond *Quanta* **6** 1–47
[103] Pljonkin A and Singh P K 2018 The review of the commercial quantum key distribution system *2018 50th Int. Conf. on Parallel, Distributed and Grid Computing (PDGC)* (IEEE) pp 795–9
[104] Chuang I L, Laflamme R, Shor P W and Żurek W H 1995 Quantum computers, factoring and decoherence *Science* **270** 1633–5
[105] Bacon D M 2001 *Decoherence, Control and Symmetry in Quantum Computers* (Berkeley, CA: University of California Press)
[106] Gardas B, Dziarmaga J, Żurek W H and Zwolak M 2018 Defects in quantum computers *Sci. Rep.* **8** 1–10
[107] Renner R 2008 Security of quantum key distribution *Int. J. Quantum Inf.* **6** 1–127
[108] Mayers D and Yao A 1998 Quantum cryptography with imperfect apparatus *Proc. 39th Annual Symp. on Foundations of Computer Science (Cat. No. 98CB36280)* (IEEE) pp 503–9
[109] Pawłowski M and Brunner N 2011 Semi-device-independent security of one-way quantum key distribution *Phys. Rev.* A **84** 010302(R)
[110] Eaton J W, Bateman D, Hauberg S and Wehbring R 2020 GNU Octave version 6.1.0 manual: a high-level interactive language for numerical computations (available at: www.gnu.org/software/octave/doc/v6.1.0/) (Accessed 11 November 2022)
[111] Johnston N 2016 QETLAB: A MATLAB toolbox for quantum entanglement, version 0.9 (available at: http://qetlab.com) (Accessed 11 November 2022)
[112] Toby C 2013 Quantinf Matlab Package, version 0.5.1 (available at: www.dr-qubit.org/matlab.html) (Accessed 11 November 2022)