Masaryk University, Faculty of Informatics

Randomness in (Quantum) Information Processing

Habilitation thesis

(Collection of Papers)

Jan Bouda

Brno, 2015

Contents

Abstract

Theoretical computer science has proven itself as a basic building stone of all applications related to computation or communication devices. With the rise of quantum information processing, one big problem of theoretical computer science becomes more and more apparent. All contemporary theoretical computer science models are based on classical physics, and do not achieve full generality in the real world, where the quantum mechanics represents the current state of our knowledge. Quantum information processing aims to reestablish the theoretical computer science by replacing insufficiently general classical models with quantum ones, and by showing that particular classical models are sufficient. Second, not less important, goal is to build theoretical foundations of quantum information processing, on which quantum computation and communication devices can be based.

This thesis concentrates on one particular part of author′s research, on the role of randomness in (quantum) information processing. It deals mainly with production of high quality (almost uniform) randomness from a real world random number generators, possibilities of using low quality (weak) randomness in cryptographic applications, and with (efficient) usage of high quality randomness in cryptographic primitives.

The thesis has the form of a collection of articles accompanied by a commentary. The collection contains eight journal papers with impact factor, one journal paper indexed in Scopus, two ISI proceedings papers, and two proceedings papers from international conferences. One paper was written solely by the author of the thesis. In case of all other papers, the contribution is at least proportional to the number of co-authors. The author contributed to these papers in various ways: by suggesting the topic, by bringing the ideas of solution, by discussing and improving solutions, and by writing down significant parts of texts.

Abstrakt

Teoretická informatika prokázala svůj význam jako základní stavební kámen všech aplikací týkajících se výpočetních či komunikačních zařízení. Postupný vývoj kvantového zpracování informace odhalil základní nedostatek současné teoretické informatiky. Všechny současné modely využívané teoretickou informatikou jsou založeny na klasické fyzice. V důsledku toho nejsou dostatečně obecné, aby popisovaly všechny výpočetní situace nastávající v reálném světě, který dle současného poznání funguje na principech fyziky kvantové. Úkolem kvantového zpracování informace je zavedení nových výsledků založených na kvantových modelech, případně důkaz, že v některých specifických případech jsou existující klasické modely dostatečné. Druhým, neméně důležitým, úkolem je vybudovat teoretické základy kvantového zpracování informace, které umožní návrh kvantových výpočetních a komunikačních zařízení.

Tato práce se zabývá jednou konkrétní částí autorova výzkumu, rolí náhodnosti v klasickém a kvantovém zpracování informace. Soustředí se především na generování vysoce kvalitní (téměř uniformní) náhodnosti z praktických náhodných generátorů, na využitelnost slabé náhodnosti v kryptografických aplikacích, a na (efektivní) využívání vysoce kvalitní náhodnosti v kryptografických primitivech.

Tato práce je koncipována jako soubor uveřejněných vědeckých prací doplněných komentářem. Sestává z osmi článků uveřejněných v impaktovaných časopisech, jednoho článku v časopise indexovaném v databázi Scopus, dvou článků ve sbornících indexovaných v ISI a dvou článků ve sbornících mezinárodních konferencí. Jeden článek byl napsán pouze autorem této práce. V případě všech článků autor přispěl k jejich obsahu podílem alespoň odpovídajícím počtu spoluatorů. Autor k těmto výsledkům přispěl různými způsoby: návrhem problému, řešením problému, diskusí a vylepšením existujících řešení, i vlastním psaním článku.

Chapter 1

Introduction

1.1 Motivation

Quantum information processing is based on a surprisingly simple observation: Classical computers were designed in the time when quantum theory only started to emerge, and theoretical computer science was growing from the existing computer architecture. Even the most prominent theoretical models of computation (Turing machines, logical circuits, programming languages) were introduced and well established before quantum theory could evolve and be experimentally verified.

Along the evolution of computer design, and namely theoretical computer science, one major flaw was present. Computing, communication and information models were respecting the design of existing computers, and even the most general approaches did not go beyond the laws of classical physics. Nowadays it is already well established that the classical description of the world is insufficient, and while the quantum description might not be the definite answer, it is certainly more accurate. As a consequence, computer science based on classical physics sometimes gives incorrect results, and one has to be very careful whether and when he can use the simplified models based on classical physics.

The recent discoveries of quantum information processing demonstrated that model of computation and communication that uses laws of quantum physics has different communication complexity classes and even information quantities, with the difference in time complexity and space complexity classes conjectured. Remarkably, even Shannon's information theory – designed to be independent of the information carrier – is not sufficiently general to describe quantum information processing, and there are results based on Shannon's information theory [31] that are not valid in the real world. As a consequence, one of the main challenges of theoretical computer science is to determine areas where classical computational models can continue to be used, and areas where quantum based models must be introduced in order

to guarantee real-world validity of the results.

Considering this, quantum information processing offers two benefits. It utilizes laws and phenomena of quantum physics for information processing. This offers more efficient, robust and/or secure solutions for a vast number of information processing problems, spanning cryptography and computational complexity theory through to communication complexity and the theory of information.

The second, and equally important, reason to study quantum information processing is that it is a generalization of classical information processing. It addresses all problems of information processing, but the main difference lies in the model of information, communication and computation. The quantum model is (strictly) more general and respects our present knowledge of the nature in a more exact way than the classical information processing does. This allows us to derive computer science results that are valid with respect to our current knowledge of physics.

Randomness is an omnipresent quantity in the field of information processing and technology, it is used in virtually every area of computer science. The most famous applications of randomness include randomized algorithms, i.e. algorithms that make random choices during the computation, distributed computation protocols, and last, but not least, cryptography. It is especially cryptography, that is virtually built on top of randomness. Privately shared randomness, known as the key in cryptography, is the concept that has allowed essentially all contemporary cryptographic achievements.

This thesis adopts a practical approach to randomness. The goal is not to argue what is the right definition of randomness, but rather to see it as a resource to be used in computer science. For such a resource we raise three criteria:

1. It must be possible to obtain and use this resource in practice. We want random number generators to exist.

2. We must be able to verify that we are possessing a true random number generator.

3. Such a resource has to be useful. We need applications, where using random bits satisfying our definition makes improvement over solutions not using randomness.

It is especially the 3rd criterion that favors strongly the definition of randomness based on likelihood and probability theory over the approaches based on compressibility and shortest possible description of a (random) bit string.

The typical form randomness takes in computer science applications is a string of uniformly distributed independents bits (fair coin flips). Such a resource has proven itself to be tremendously useful, but it also carries the

burden of real world random number generators, that are typically unable to produce such a bit string. It is this observation that motivates the study of weak randomness, i.e. randomness that comes in the form of non uniform correlated bits.

1.2 Focus of the Thesis

The main focus of this thesis are applications of randomness in classical and quantum information processing, especially in cryptography. The accent is on production of high-quality randomness (randomness extraction), efficient usage of randomness (design of applications consuming as little randomness as possible), and role of weak randomness in applications - in what applications and to what extent it makes a difference over perfect randomness. The span of the thesis can be divided into three areas.

Randomness in Encryption and Unitary k-designs

This area includes papers analyzing encryption of quantum information from various security, application and key-efficiency aspects [4, 5, 8, 16]. We concentrated mainly on minimal entropy of key necessary for various sets of plaintexts. We also introduced a number of concepts, namely the known-ciphertext attack (see Section 3.1), that does not exist in classical encryption, and the relation between encryption and secret sharing of quantum and classical information. In a related setting, we show that there in order to encrypt k copies of a pure state ciphertext, one can use a unitary k-design [11]. Encryption of mixed states in this scenario is not possible.

In addition to this, we studied the role of randomness in unitary k-designs, namely the minimum amount of randomness necessary to implement (approximate) 2-design, and non-malleable encryption in general [2, 6]. We show the equivalence of non-malleable encryption to the unitary 2-design and give a new proof of a previous known lower bound on size of a 2-design, that can be generalized for approximate 2-designs.

Weak Randomness in Cryptographic Applications

Here we obtained one positive and one negative (from the quantum information processing point of view) result. On one hand we designed encryption system [14] with classical plaintext and key, and with a quantum ciphertext, that breaks the McInnes-Pinkas bound, thus showing the quantum technique is better than any possible classical encryption system. On the other hand we have shown that BB84 QKD protocol is highly vulnerable to weak randomness [7].

Randomness Extraction

Here we propose an efficiency improvement of the classical Hadamard extractor [15], that is a basic building stone of many state-of-the-art randomness extractor including the celebrated Bourgain extractor [17]. Second result in this areas is a design of a device independent randomness extractor [13, 12] that can extract randomness with an arbitrarily small bias from arbitrarily weak min-entropy source, quite surprisingly using only a single source of randomness. This is impossible in the world of classical physics.

Chapter 2

State of the Art

In this chapter we describe the state of the art of the research areas addressed in this collection of papers. The main aim is to explain each particular area in more detail and describe the state of the art at the time when the research of JB in the area has started.

2.1 Weak randomness

Uniform randomness was proven to be a very useful resource, with the main applications including design of algorithms, cryptography and communication (complexity). Algorithms using randomness can be faster and easier to design (and analyze) in comparison to their deterministic counterparts. Security proofs of many cryptographic protocols are based on the fact that communicating parties have access to (shared) independent and unbiased bits.

Unfortunately, so far scientists and engineers have been unsuccessful in building a device that produces unbiased bits out of the first principle. Even in situations where the physical background of the device allows to produce perfect randomness (e. g. based on measurement of quantum states), the practical implementation may lead to a significant bias [29].

Another problem resulting in the same theoretical model of weak source is partial adversary′s knowledge about random number generator output. Assuming the adversary is able to learn some information about the randomness, cryptographic systems should be examined against the random bit strings distributed according to the probability distribution conditioned by the adversarys knowledge[1]. This distribution differs from the original (possibly uniform) distribution obtained from the source, thus turning even perfect source into a weak one. In example, learning parity of an n-bit string

[1]This applies to the classical adversary, the case of quantum side-knowledge is a bit different.

results in the uniform distribution on 2^{n-1} bit strings with the fixed parity in contrast to the original uniform distribution on all 2^n bit strings.

There are two basic approaches to deal with the aforementioned problems. The first one is to study possible usage of weak random sources in particular problems and applications. A bit surprisingly, for quite a few problems it is possible to design solutions that work sufficiently well even with weak random sources of a reasonably high quality. Examples of these are randomized algorithms [49] or message authentication. On the other hand, in other applications even a slightest weakness in randomness makes the who task impossible. In example, McInnes and Pinkas [40] have shown that symmetrical encryption is unattainable, if parties have only access to shared weak source of randomness (although only negligibly weak). Although better results are obtained if information is encrypted into a quantum state [14], general cryptographic techniques cannot be considered secure without uniform randomness.

The second approach tries to fix problems where no solution exists even for high-quality weak random sources. The central idea is to design efficient procedures to post-process the output of weak sources to obtain (almost) unbiased uncorrelated bits, usually at the cost that such a post-processing, or extraction, produces shorter output (when compared to input).

To introduce the main results it is necessary to define what we understand under the term weak source. The most prominent model describes weak sources in terms of their min-entropy $H_{\min}$. A random variable X defined over bit strings of length l is an (l, b)-source if for every $x \in \{0,1\}^l$ it holds $\Pr[X = x] \leq 2^{-b}$, that is $H_{\min}(X) = b$. This model was introduced by Chor and Goldreich [22]. Unfortunately, they also proved that a single source of this type is not sufficient to extract unbiased bits., i.e. there is no such postprocessing for a single source.

The first possible approach is to extract randomness from one weak source with aid of small uniformly random string, so called seed. Recent constructions and motivation is provided in [42, 50] and the state of the art constructions are contained in [34, 39]. More practical line of research considers extracting randomness from several independent weak sources. The most prominent results are published in [17, 28, 47, 48]. However there still are many improvement to be done, among them decreasing the necessary amount of entropy in the source [17] and decreasing the bias achieved by the extractor.

The problems arising when one is forced to use weak source of randomness (no source of uniform randomness is available) are well established and extensively studied in classical information processing. It turned out that some information processing tasks can be realized with (reasonably bounded) weak source of randomness, but many other cannot be implemented using even a slightly biased source. At the time JB and collaborators started their research, there was no such analysis for quantum information

processing tasks. This is quite surprising, since classical randomness plays a vital role in quantum information processing as well.

The reason for this lack of results seems to be the wide belief that randomness is essentially an ever present and free resource in QIP. This is, however, far from being true when requiring (almost) uniform randomness and even dedicated measurement-based quantum random number generators (QRNG) require postprocessing via randomness extractor [29]. Even worse, the relatively limited weakness of random bits in some implementations of QRNG can be turned into a complex problem when an adversary attacks such a system. He has a wide range of tools to use, starting with the change of the temperature of the device (or surrounding environment) affecting the wavelength of the lasers (and subsequently biasing the beam splitter), and ending by elaborate changes of voltage of the electricity input.

2.2 Encryption of quantum information

The goal of the encryption of quantum information is to transform quantum plaintext into a quantum ciphertext. This operation is analogous to the classical case, the encrypting transformation is selected according to a (secret) classical key. The standard practical restriction imposed is that the dimensions of plaintext and ciphertext are the same, what implies that encrypting transformations are unitary. This is known as the private quantum channel (PQC) originally introduced in [1]. A typical example of PQC is the quantum one-time pad proposed independently by [18]. Here the encryption operations are the Pauli operators $\mathbb{1}, \sigma_x, \sigma_y, \sigma_z$. It encrypts a single quantum bit using two classical bits of key (what is also proven to be optimal) and can encrypt multi-qubit states when applied qubit-wise with an independently chosen key.

While it seems to be impossible to reuse the key to encrypt multiple quantum systems in a straightforward way, it is possible to detect possible eavesdropping [44] in the spirit of the QKD protocols. Another possibility to decrease the key costs is to use an approximate encryption [36, 3], i.e. encryption where a small amount of information about the plaintext is leaked. Such a scheme can be implemented using only a half amount of the key as compared to exact encryption, i.e. to encrypt a d-level quantum system one needs a key of the length $d + o(d)$. Important observation is that the decrease in key length in approximate encryption comes with an extra cost. The approximate encryption schemes using $d + o(d)$ bits of key do not guarantee encryption of the whole system when applied on each subsystem independently. This is a big disadvantage in contrast to exact encryption.

It is possible to encrypt quantum ciphertext using a quantum key (i.e. randomness is replaced by entanglement) [38], this approach is, however, much less practical and motivated more by curiosity than application.

2.3 Unitary k-designs

Random unitary transformations (drawn from the Haar measure - the natural "uniform" distribution on the unitary transformations) have statistical properties that are very useful for applications in quantum information [26]. Unfortunately, the Haar-random transformation is very unlikely to be efficiently implementable by a quantum circuit and, for this reason, cannot be used in an efficient protocol for quantum communication (or other applications such as quantum state tomography [43]).

To deal with these problems, one has to consider sets of unitaries that are efficiently implementable but behave "as randomly as needed" (in some precise sense). In many applications it is easy to see that the Haar-random unitary solves the problem, but, in fact, it is not necessary to make the random choice over the whole unitary group. In example, while Haar-random unitary channel fully randomizes any (single qubit) state, it is sufficient to choose randomly only one out of 4 Pauli operators [1], much like in the case of quantum teleportation. This special case, known as unitary 1-design (see below), is the encryption of quantum information introduced in the previous section.

Such "pseudorandom unitaries", known as *unitary designs*, are a probability distribution over a finite set (subgroup) of unitary operators approximating properties of Haar-random unitary operators [32, 35].

The pair $(\{U_i\}_{i\in I}, (p_i)_{i\in I}), p_i \geq 0, \sum_{i\in I} p_i = 1$, is a **unitary** k**–design** iff for all $\rho \in \mathcal{B}\left(\mathcal{H}^{\otimes k}\right)$

$$\sum_{i\in I} p_i U_i^{\otimes k} \rho U_i^{\dagger\otimes k} = \int_U U^{\otimes k} \rho U^{\dagger\otimes k} dU,$$

where the integral is taken over the unitary group distributed according to the Haar measure.

Direct applications of unitary k-designs include quantum algorithms [27], quantum circuits [20], (non-malleable) encryption [1, 2] and many others [20].

Unlike the 1-designs, where size-optimal constructions are known, in the case of the 2-design we have to settle down for lower bounds on the size of the design, and constructions not attaining these bounds. For k-designs with $k \geq 3$ we have only a marginal knowledge regarding their optimal size, constructions or even applications.

2.4 Device-independence and randomness extraction

The idea of device independence comes from complexity and fragility of quantum devices. In case you buy a contemporary commercial quantum de-

vice, e.g. a random number generator or a pair of quantum key distribution devices, you are provided with a very expensive (literally) black box. Your means to verify the actual content of the quantum device are, due to the complexity and fragility of quantum technologies, essentially the same as verifying functionality of a theoretical black box device. You can supply it with pre-selected inputs and verify whether the outputs are consistent with the inputs and the specification of the device.

Contemporary and near future quantum devices are (will be) used almost exclusively for high-sensitivity applications (cryptographic and security applications, professional gambling, ...), where possible breach can yield a significant profit. Highly sophisticated attacks and device modifications must be expected.

Current quantum devices are highly expensive and require a highly non-trivial expertise and equipment to be assembled. This combination makes it a nice target for fraud companies producing low-cost devices not meeting the declared specifications.

Both these problems are addressed by the device-independent approach. The main idea is to design the device in such a way, that when supplying it with the right input, the device either performs its function according to the specification, or malfunctioning can be easily detected from the input-output combinations.

The concept of device independence was originally introduced in the context of QKD [53]. In this thesis, however, we will concentrate rather on the randomness expansion and extraction applications.

Classically the task of transforming a single weak source, characterized either as a Santha-Vazirani source [49], or a min-entropy (block) source [22] into a fully random bit is known to be impossible [49, 51]. However, with the non-classical resources the task becomes possible. More precisely, weak random source can be used to choose measurements for a Bell test in order to certify that observed correlations cannot be explained by local theories and thus must necessarily contain intrinsic randomness.

In their seminal paper Colbeck and Renner [24] showed that amplification of Santha-Vazirani sources is possible for a certain range of parameter ε and thus opened a line of research devoted to SV amplification. Subsequent works provided protocols that are able to amplify SV-sources for any $\varepsilon < \frac{1}{2}$ in various settings [30, 41, 33, 46]. This line of research culminated in the work of Brandão et. al. [19], who showed how to amplify such source of randomness with the use of only eight non-communicating devices. Their work was quickly followed by that of Coudron and Yuan [25], who showed how to use 20 non-communicating devices to obtain arbitrarily many bits from a Santha-Vazirani source.

On the other hand, extraction from min–entropy sources is relatively unexplored. There is a sequence of works exploring the validity of Bell tests if the measurements are chosen according to a min–entropy source

[37, 52] and MP$^{\times 2}$ [45] provided a protocol which uses 3-party GHZ-paradox to amplify sources with min-entropy rate $R > \frac{1}{4}\log_2(10)$ against quantum adversaries. Recently an extensive work on this topic was made public on pre-print archive [23].

Chapter 3

Thesis Contribution

3.1 Randomness in Encryption and Unitary k-designs

The relatively recent rise to prominence of pseudorandomness may have created an impression that randomness is a resource that is essentially for free. As we already explained at many places, true randomness is a valuable resource and should be used as efficiently as possible. Especially private randomness shared by two or more parties is a highly valuable resource, since to achieve it we have to employ some form of key distribution protocol.

The quest for efficient usage of randomness started essentially with its introduction to the computer science. In this collection we address the notion of (efficient) usage of randomness in the context of encryption of quantum information, and, more general, unitary k-designs.

In the early papers [4, 5, 9] on encryption of quantum information we studied security properties of encryption and its relation to other cryptographic primitives. We pointed out the problem of the known ciphertext attack for quantum information. Unlike classical encryption, there is a key difference between holding a single copy of ciphertext, and knowing complete description of the ciphertext state. In the quantum case, in some cases only two copies of the ciphertext state are sufficient to break the encryption scheme with large probability. To start with, this means that you cannot resend the same plaintext encrypted using the same key, unlike the classical case. In the classical case this would be even the preferred way of resending the plaintext due to known plaintext type attacks. It also appears naturally in physical devices in the case of a multi-photon pulse [11], and thus it is a very realistic scenario. We also discussed possible analogues of the known plaintext attack (again the single/multiple copy, or complete description), and randomizing correlations of a quantum system with another quantum system. Note that the known ciphertext attack is in some sense dual to the classical concept of the chosen ciphertext attack.

In the area of applications we proposed conversion of a wide class of cryp-

tosystems for classical information into systems for quantum information. The idea is to encrypt the quantum state, and and apply the cryptosystem for classical information on the classical key. Namely we proposed this for secret sharing, oblivious transfer and (qu)bit commitment.

The efficiency of encryption was extensively studied, and we managed to show that given a particular (encryption) channel, the entropy of its unitary decomposition is lower bounded by the von Neumann entropy of the average output state, as well as by the entropy exchange with the environment [16]. We used this to show that optimal entropy is always attained by decomposition into orthogonal unitaries (e.g. Pauli operators for qubit). We have characterized all possible single-qubit channels (including the optimal key entropy), to understand the difference between encryption of classical and quantum bit. Finally we discussed implementation of approximate private quantum channels.

Unitary k-designs are a generalization of encryption of quantum information, which itself is a 1-design.

The first problem we studied is the k photon pulse, which is equivalent to the aforementioned known-ciphertext attack. Here the adversary may receive k copies of the ciphertext. We managed to prove [11] that such a device is secure, if instead of plain 1-design we encrypt using k-design. This, however, randomizes only pure states, and encrypting mixed states is impossible in this scenario. As a consequence, encryption of subsystems of an entangled state leaves the global state insecure (recall the approximate encryption).

In paper [2] we raised an additional demand on encryption system. In addition to the fact that the plaintext should remain secret from the adversary, we also demand that the adversary cannot modify the plaintext in a predictable way. We show that maximum what we can achieve is that the adversary can introduce white noise into the plaintext, and can control the intensity of such a noise. Such an encryption scheme is equivalent to unitary 2-design. In the same paper we show a new proof of the previously known lower bound $(d^2-1)^2+1$ on the number of unitaries in a 2 design. We use this proof to show that there are always approximate 2-designs with $O(\epsilon^{-2}d^4 \log d)$ elements.

In [6] we adopted a different approach. Rather than concentrating on unitary k-designs we studied more general class of random unitary channels (k-design is a special random unitary channel). Instead of studying the worst-case scenario, we studied average (over all input states) properties of random unitary channels, namely quality of encryption and non-malleability.

3.2 Weak Randomness in Cryptographic Applications

While in the classical case the threat of weak randomness is well known and extensively documented, in quantum information processing there is still almost nothing known. We have started addressing this problem by our studies of encryption and QKD.

When analyzing the standard BB84 QKD protocol we realized [7], that the common practice to reduce the number of check measurements to roughly logarithm of the total number of qubits transmitted opens a possibility to attack the protocol using weak randomness. We concentrated on the randomness used to select the check positions. Quite surprisingly, an arbitrarily small amount of weakness in the randomness is sufficient to kill the protocol. Namely, with the number of BB84 rounds going to infinity, it is possible to attack the protocol using a randomness source with an arbitrarily high min-entropy rate, i.e. $\lim_{n\to\infty} \frac{k}{n} = n$ for n bit source and min-entropy k dependent on n.

A second result is the design [14] of an encryption system that encodes classical plaintext using a classical key into a quantum system. The classical McInees-Pinkas paper [40] shows that no classical encryption system remains secure when the key is selected from a weakly random source. In particular, for min-entropy loss 2 bits the plaintext can be always determined with certainty (regardless of the cryptosystem design). The McInees-Pinkas result gives a lower bound on probability that the input is revealed by the adversary. This probability is a function of the min-entropy loss. In contrast, our encryption system achieves probability of revealing the plaintext that breaks the McInnes-Pinkas bound for all values of min-entropy loss, except it coincides with the bound for the case of the loss of 1 bit and the trivial case of no loss (perfect randomness).

3.3 Randomness Extraction

Paper [15] proposes a single-bit classical randomness extractor based on the Hadamard matrix. This extractor is an important building block for many state-of-the-art randomness extractors. We proposed a strong extractor with two independent l bit input distributions with respective min entropies $x, y, x + y > l$. For $x, y \leq l - 1$, our extractor produces one bit which is by the factor of $\sqrt{2}$ closer to the uniform distribution, when compared to the Hadamard extractor. What is more, this distance drops to zero if at least one of the min entropies raises to l. This is in sharp contrast to the Hadamard extractor which fails to produce even a single unbiased bit, even if one of the input distributions is uniform. We also extend our construction to produce k bits of output with a bias that is by the factor of $\sqrt{3}/2$ smaller

than that of the corresponding Hadamard-based extractor and retains the ability to produce unbiased bits if one of the input distributions is uniform. The strongness property of the extractor is maintained in both cases, however, in the multi-bit strong extractor scenario the bias is increased by the factor of $\sqrt{3}/2$.

In papers [13, 12] we propose and analyze a highly interesting device-independent randomness extractor. We show how to extract a random bit with an arbitrarily low bias from a single arbitrarily weak min-entropy source. The only additional resource is a device with no guarantee of its internal structure. To do this we use a number of Mermin devices of a similar design, each composed of 3 isolated boxes. The key idea is to calculate the output of a class of hash functions applied on the weakly random input and use the output of every hash function as an input of each respective device. This is performed in a number of rounds. Simplifying a bit, the family of hash functions is constructed in the way that for an arbitrarily weak random source there is at least one device in each round that is tested with sufficiently strong random input. The number of devices used scales polynomially in the length of the random sequence n. Our protocol is robust, it can tolerate devices that malfunction with a probability dropping polynomially in n at the cost of a minor increase of the number of devices used.

Paper [10] is a study of practical applications of the theory of weak randomness. The goal was to propose a method how to generate high-quality randomness for cryptographical purposes in mobile devices (with an accent on cell phones). The first step was to identify the potential source of randomness that is available in a vast majority of existing mobile devices. Here mainly microphone and CCD chip of the camera were considered. Subsequent analysis excluded microphone due to its low bit rate, and because being relatively easier to influence. Camera CCD was able to produce much higher rate of random bits. Randomness was due to the thermal noise in the CCD - the same effect that makes digital cameras fail in the night. The phone generating random numbers was expected to have its lens covered (e.g. by finger) to simulate operation of the CCD in darkness. Even such a conditions do not guarantee fixed output distribution, hence we did extensive testing on how the distribution differs in different cell phones and with varying conditions, the most influential being the ambient temperature. Subsequently we performed analysis of matching theoretical results, chosen and implemented suitable randomness extractor. Using the Carter-Wegman [21] universal$_2$ families of function we were able to obtain bit rate 36 bits per second for bits of distance at most 2^{-64} from the uniform distribution in the trace distance. The bit rate is limited only to allow statistical testing at a reasonable level of confidence.

Chapter 4

Papers in Collection

4.1 Impacted Journal Papers

[**2**] Andris Ambainis, Jan Bouda, and Andreas Winter. Nonmalleable encryption of quantum information. *J. Math. Phys.*, 50:042106, 2009.

- Author's contribution: 60%
- Bringing the topic, substantial part of ideas and writing

[**4**] Jan Bouda and Vladimír Bužek. Encryption of quantum information. *Int. J. Found. Comput. Sci.*, 14(5):741–756, 2003.

- Author's contribution: 80%
- Bringing the topic, substantial part of ideas and writing
- This paper is listed only as a Scopus indexed publication in the list of publications. However, to the author's best knowledge it was part of the ISI impacted journals at the time of publication.

[**5**] Jan Bouda and Vladimír Bužek. Security of the private quantum channel. *Journal of Modern Optics*, 50:1071–1077, 2003.

- Author's contribution: 80%
- Bringing the topic, substantial part of ideas and writing

[**6**] Jan Bouda, Matyas Koniorczyk, and Andreas Varga. Random unitary qubit channels: entropy relations, private quantum channels and nonmalleability. *The European Physical Journal D*, 53(3):365–372, 2009.

- Author's contribution: 50%
- Bringing the topic, substantial part of ideas and writing

[**7**] Jan Bouda, Matej Pivoluska, Martin Plesch, and Colin Wilmott. Weak randomness seriously limits the security of quantum key distribution. *PRA*, 86(6):062308, December 2012.

- Author's contribution: 30%
- Bringing the topic, participated on ideas and writing

[13] Jan Bouda, Marcin Pawlowski, Matej Pivoluska, and Martin Plesch. Device-independent randomness extraction from an arbitrarily weak min-entropy source. *Phys. Rev. A*, 90, 2014.

- Author's contribution: 60%
- substantial part of ideas and writing

[14] Jan Bouda, Matej Pivoluska, and Martin Plesch. Encryption with weakly random keys using quantum ciphertext. *Quantum Information and Computing*, 12:395–403, 2012.

- Author's contribution: 60%
- Bringing the topic, substantial part of ideas, substantial part of the writing

[15] Jan Bouda, Matej Pivoluska, and Martin Plesch. Improving the Hadamard extractor. *Theor. Comput. Sci.*, 459:69–76, November 2012.

- Author's contribution: 20%
- Participation on ideas and writing

[16] Jan Bouda and Mario Ziman. Optimality of private quantum channels. *Journal of Physics A*, 40:5415–5426, 2007.

- Author's contribution: 50%
- Participation on all phases of the paper

4.2 Proceedings Papers

[9] Jan Bouda. Exact and approximate encryption of quantum information. *NATO Security through Science Series, D: Information and Communication Security*, 17:218–233, 2008.

- Author's contribution: 100%

[10] Jan Bouda, Jan Krhovjak, Vashek Matyas, and Petr Svenda. Towards true random number generation in mobile environments. In Audun Josang, Torleiv Maseng, and SveinJohan Knapskog, editors, *Identity and Privacy in the Internet Age*, volume 5838 of *Lecture Notes in Computer Science*, pages 179–189. Springer Berlin Heidelberg, 2009.

- Author's contribution: 60%
- Substantial part of ideas and writing

[11] Jan Bouda, Jaroslaw Adam Miszczak, and Mario Ziman. Private quantum channels, multi-photon pulses and unitary k-designs. In *AQIS*, 2009.

- Author's contribution: 40%
- substantial part of ideas and writing

[12] Jan Bouda, Marcin Pawlowski, Matej Pivoluska, and Martin Plesch. Device-independent randomness extraction for arbitrarily weak min-entropy source. In *SPIE Conference on Emerging Technologies in Security and Defence; Quantum-Physics-based Information Security*, 2014.

- Author's contribution: 60%
- substantial part of ideas and writing

Bibliography

[1] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf. Private quantum channels. In *FOCS 2000*, pages 547–553, 2000. quant-ph/0003101.

[2] Andris Ambainis, Jan Bouda, and Andreas Winter. Nonmalleable encryption of quantum information. *J. Math. Phys.*, 50:042106, 2009.

[3] Andris Ambainis and Adam Smith. Small pseudo-random families of matrices: derandomizing approximative quantum encryption. In *RANDOM*, pages 249–260, 2004. quant-ph/0404075.

[4] J. Bouda and V. Bužek. Encryption of quantum information. *Int. J. Found. Comput. Sci.*, 14(5):741–756, 2003.

[5] J. Bouda and V. Bužek. Security of the private quantum channel. *Journal of Modern Optics*, 50:1071–1077, 2003.

[6] J. Bouda, M. Koniorczyk, and A. Varga. Random unitary qubit channels: entropy relations,private quantum channels and non-malleability. *The European Physical Journal D*, 53(3):365–372, 2009.

[7] J. Bouda, M. Pivoluska, M. Plesch, and C. Wilmott. Weak randomness seriously limits the security of quantum key distribution. *PRA*, 86(6):062308, December 2012.

[8] J. Bouda and M. Ziman. Limits and restrictions of private quantum channel. quant-ph/0506107, submitted to QI&C, 2005.

[9] Jan Bouda. Exact and approximate encryption of quantum information. *NATO Security through Science Series, D: Information and Communication Security*, 17:218–233, 2008.

[10] Jan Bouda, Jan Krhovjak, Vashek Matyas, and Petr Svenda. Towards true random number generation in mobile environments. In Audun Josang, Torleiv Maseng, and SveinJohan Knapskog, editors, *Identity and Privacy in the Internet Age*, volume 5838 of *Lecture Notes in Computer Science*, pages 179–189. Springer Berlin Heidelberg, 2009.

[11] Jan Bouda, Jaroslaw Adam Miszczak, and Mario Ziman. Private quantum channels, multi-photon pulses and unitary k-designs. In *AQIS*, 2009.

[12] Jan Bouda, Marcin Pawlowski, Matej Pivoluska, and Martin Plesch. Device-independent randomness extraction for arbitrarily weak min-entropy source. In *SPIE Conference on Emerging Technologies in Security and Defence; Quantum-Physics-based Information Security*, 2014.

[13] Jan Bouda, Marcin Pawlowski, Matej Pivoluska, and Martin Plesch. Device-independent randomness extraction from an arbitrarily weak min-entropy source. *Phys. Rev. A*, 90, 2014.

[14] Jan Bouda, Matej Pivoluska, and Martin Plesch. Encryption with weakly random keys using quantum ciphertext. *Quantum Information and Computing*, 12:395–403, 2012.

[15] Jan Bouda, Matej Pivoluska, and Martin Plesch. Improving the hadamard extractor. *Theor. Comput. Sci.*, 459:69–76, November 2012.

[16] Jan Bouda and Mario Ziman. Optimality of private quantum channels. *Journal of Physics A*, 40:5415–5426, 2007.

[17] Jean Bourgain. More on the sum-product phenomenon in prime fields and its applications. *International Journal of Number Theory*, 1:1–32, 2005.

[18] P. O. Boykin and V. Roychowdhury. Optimal encryption of quantum bits. quant-ph/0003059, 2000.

[19] F. G. S. L. Brandão, R. Ramanathan, A. Grudka, K. Horodecki, M. Horodecki, and P. Horodecki. Robust Device-Independent Randomness Amplification with Few Devices. October 2013.

[20] F.G.S.L. Brandao, A.W. Harrow, and M. Horodecki. Local random circuits are approximate polynomial-designs. arXiv:1208.0692, 2012.

[21] J. L. Carter and M. N. Wegman. Universal hash functions. *Journal of Computer and System Sciences*, 18:143–144, 1979.

[22] Benny Chor and Oded Goldreich. Unbiased bits from sources of weak randomness and probabilistic communication complexity. *SIAM Journal on Computing*, 17(2):230–261, 1988.

[23] K.-M. Chung, Y. Shi, and X. Wu. Physical Randomness Extractors. 2014.

[24] R. Colbeck and R. Renner. Free randomness can be amplified. *Nature Physics*, 8:450–454, June 2012.

[25] M. Coudron and H. Yuen. Infinite Randomness Expansion and Amplification with a Constant Number of Devices. October 2013.

[26] Ch. Dankert, R. Cleve, J. Emerson, and E. Livine. Exact and approximate unitary 2-designs: Constructions and applications. quant-ph/0606161, 2006.

[27] Christoph Dankert. Efficient simulation of random quantum states and operators. Master's thesis, University of Waterloo, 2005. quant-ph/0512217.

[28] Y Dodis, A Elbaz, R Oliveira, and R Raz. Improved randomness extraction from two independent sources. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, volume 3122, pages 334–344. Springer Berlin / Heidelberg, 2004.

[29] Daniela Frauchiger, Renato Renner, and Matthias Troyer. True randomness from realistic quantum devices. arXiv:1311.4547 [quant-ph], 2013.

[30] R. Gallego, L. Masanes, G. de la Torre, C. Dhara, L. Aolita, and A. Acín. Full randomness from arbitrarily deterministic events. *Nature Communications*, 4, October 2013.

[31] D. Gavinsky, J. Kempe, I. Kerenidis, R. Raz, and R. de Wolf. Exponential separation for one-way quantum communication complexity, with applications to cryptography. *SIAM J. Comput*, 38(5):16951708, 2008.

[32] D. Gross, K. Audenaert, and J. Eisert. Evenly distributed unitaries: On the structure of unitary designs. *J. Math. Phys.*, 48:052104, 2007. quant-ph/0611002.

[33] A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, M. Pawłowski, and R. Ramanathan. Free randomness amplification using bipartite chain correlations. 2013.

[34] Venkatesan Guruswami, Christopher Umans, and Salil Vadhan. Unbalanced expanders and randomness extractors from parvaresh–vardy codes. *J. ACM*, 56(4):20:1–20:34, July 2009.

[35] Aram W. Harrow and Richard A. Low. Efficient quantum tensor product expanders and k-designs. *Proceedings of RANDOM, LNCS*, 5687:548–561, 2009.

[36] P. Hayden, D. W. Leung, P. W. Shor, and A. Winter. Randomizing quantum states: Constructions and applications. *Commun. Math. Phys.*, 250:371–391, 2004. quant-ph/0307104.

[37] Dax Enshan Koh, Michael J. W. Hall, Setiawan, James E. Pope, Chiara Marletto, Alastair Kay, Valerio Scarani, and Artur Ekert. Effects of reduced measurement independence on bell-based randomness expansion. *Phys. Rev. Lett.*, 109:160404, Oct 2012.

[38] D. W. Leung. Quantum vernam cipher. *Quantum Information and Computation*, 2(1):14–34, 2002. quant-ph/0012077.

[39] Chi-Jen Lu, Omer Reingold, Salil Vadhan, and Avi Wigderson. Extractors: Optimal up to constant factors. In *STOC 2003*, pages 602–611, 2003.

[40] J. L. McInnes and B. Pinkas. On the impossibility of private key cryptography with weakly random keys. In *Crypto'90*, pages 421–435, 1991. LNCS 537.

[41] P. Mironowicz and M. Pawlowski. Amplification of arbitrarily weak randomness. 2013.

[42] Naom Nisan and Amnon Ta-Shma. Extracting randomness: a survey and new constructions. *J. Comput. Syst. Sci.*, 58:148–173, February 1999.

[43] Matthias Ohliger, Vincent Nesme, and Jens Eisert. Efficient and feasible state tomography of quantum many-body systems. arXiv:1204.5735, 2012.

[44] J. Oppenheim and M. Horodecki. How to reuse a one–time pad and other notes on authentication and protection of quantum information. quant-ph/0306161, 2003.

[45] M. Plesch and M. Pivoluska. Single Min-Entropy Random Sources can be Amplified. May 2013.

[46] R. Ramanathan, F. G. S. L. Brandao, A. Grudka, K. Horodecki, M. Horodecki, and P. Horodecki. Robust Device Independent Randomness Amplification. 2013.

[47] Anup Rao. Extractors for a constant number of polynomially small min-entropy independent sources. In *Proceedings of the thirty-eighth annual ACM symposium on Theory of computing*, STOC '06, pages 497–506, New York, NY, USA, 2006. ACM.

[48] Ran Raz. Extractors with weak random seeds. In *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*, STOC '05, pages 11–20, New York, NY, USA, 2005. ACM.

[49] Miklos Santha and Umesh V. Vazirani. Generating quasi-random sequences from slightly-random sources. In *Proceedings of the 17th ACM Symposium on the Theory of Computing*, pages 366–378, 1985.

[50] Ronen Shaltiel. Recent developments in explicit constructions of extractors. *Bulletin of the EATCS*, 77:67–95, 2002.

[51] Ronen Shaltiel. An introduction to randomness extractors. In *Automata, Languages and Programming*, volume 6756 of *Lecture Notes in Computer Science*, pages 21–41. 2011.

[52] Le Phuc Thinh, Lana Sheridan, and Valerio Scarani. Bell tests with min-entropy sources. *Phys. Rev. A*, 87:062121, Jun 2013.

[53] Umesh Vazirani and Thomas Vidick. Fully device independent quantum key distribution. *Phys. Rev. Lett.*, 113:140501, 2014. arXiv:1210.1810 [quant-ph].

This is the public version of the habilitation thesis. It does not contain papers that are part of the collection, only the summary part. Including the papers would violate legal rights of journal publishers. These papers, however, are listed inside the summary part and can be easily downloaded from web pages of the respective publishers.