ON THE COMPUTABILITY OF THE SECRET KEY CAPACITY UNDER RATE CONSTRAINTS

Holger Boche[*], *Rafael F. Schaefer*[†], *and H. Vincent Poor*[‡]

[*]Theoretische Informationstechnik
Technische Universität München
München, Germany
boche@tum.de

[†]Information Theory and Applications
Technische Universität Berlin
Berlin, Germany
rafael.schaefer@tu-berlin.de

[‡]Dept. Electrical Engineering
Princeton University
Princeton, USA
poor@princeton.edu

ABSTRACT

Secret key generation refers to the problem of generating a common secret key without revealing any information about it to an eavesdropper. All users observe correlated components of a common source and can further use a rate-limited public channel for discussion which is open to eavesdroppers. This paper studies the Turing computability of the secret key capacity with a single rate-limited public forward transmission. Turing computability provides fundamental performance limits for today's digital computers. It is shown that the secret key capacity under rate constraints is not Turing computable, and consequently there is no algorithm that can simulate or compute the secret key capacity, even if there are no limitations on computational complexity and computing power. On the other hand, if there are no rate constraints on the forward transmission, the secret key capacity is Turing computable. This shows that restricting the communication rate over the public channel transforms a Turing computable problem into a non-computable problem. To the best of our knowledge, this is the first time that such a phenomenon has been observed.

Index Terms— Secret key generation, secret key capacity, rate constraint, Turing computability.

1. INTRODUCTION

Secret keys shared by transmitter and receiver can be used for encryption to keep eavesdroppers ignorant and thus enable a subsequent secure communication. Accordingly, it is an important task to generate secret keys at distant locations in such a way that possible eavesdroppers obtain no information about them.

Current approaches at higher layers are usually based on cryptographic principles. These have a wide variety of uses and rely on the assumption of insufficient computational capabilities of non-legitimate receivers. Due to increasing computational power, improved algorithms, and recent advances in number theory, these techniques are becoming less and less secure. Here we consider a *physical layer* or *information theoretic approach to security* [1–4]. This approach is not only relevant for the task of secret key generation [5, 6], but also for secure communication [7] and authentication [8]. Accordingly, this approach has been identified to be a promising candidate to meet the strict requirements on reliability, robustness, and latency of future communication systems such as the Tactile Internet, cf. for example [9] for a detailed discussion. It further plays a major role in the concept of physical layer service integration [10].

The generation of secret keys is done by using observations of a common source. This was first studied by Ahlswede and Csiszár [5] and Maurer [6]. To this end, two users Alice and Bob observe correlated components of a source and further use a noiseless channel for additional discussion. Information sent over the noiseless channel is public and therefore known to possible eavesdroppers. Thus, the task is to use the public channel in such a way that both users can generate a common secret key using their source observations and, at the same time, keeping eavesdroppers ignorant of it. Secret key generation is further studied in [8, 11–13]. Particularly in [5, 6] the communication over the public channel is not rate-limited, i.e., an arbitrary amount of information can be exchanged in order to enable the secret key generation.

This work particularly addresses the need for secrecy requirements and for the spectrally efficient use of resources. Such requirements are usually first identified and proposed by national agencies for security and subsequently reviewed and verified by governmental agencies. The overall process is very complex and imposes significant challenges. Particularly, the ever increasing number of new and evolving (communication) systems makes it practically impossible to effectively *verify* the afore imposed requirements. Even worse, to date, it is not clear how to decide and prove whether or not a certain system satisfies the requirements.

The verification task, i.e., the effective validation of whether or not a secret key generation system meets its performance requirements, has drawn surprisingly little attention. To address this issue, we use the concept of a *Turing machine* [14–16]. This is a mathematical model of an abstract machine that manipulates symbols on a strip of tape according to certain given rules. It can simulate any given algorithm and therewith provides a simple but very powerful model of computation. Turing machines have no limitations on computational complexity, unlimited computing capacity and storage, and execute programs completely error-free. Accordingly they provide fundamental performance limits for today's digital computers and they are the ideal concept to decide whether such a verification task is effectively possible at all. With the latter we mean that we are interested in understanding whether or not this task can in principle be solved algorithmically (without putting any constraints on the computational complexity of such algorithms).

In this work, we study secret key generation with a single rate-limited forward transmission. Obviously, the public forward trans-

The work of H. Boche and R. F. Schaefer was supported by the Gottfried Wilhelm Leibniz program of the German Research Foundation (DFG) under Grant BO 1734/20-1. H. Boche's research on molecular communication was supported by the German Ministry of Education and Research (BMBF) within the national initiative for molecular communication under Grant 16KIS0914. The work of H. V. Poor was supported by the U.S. National Science Foundation under Grants CCF-093970, CCF-1513915, and CNS-1702808. The research direction of Turing computability for communication systems was initiated by the German Research Foundation (DFG) under Grants BO 1734/24-3 and BO 1734/25-1.

978-1-5386-4658-8/18/$31.00 ©2019 IEEE

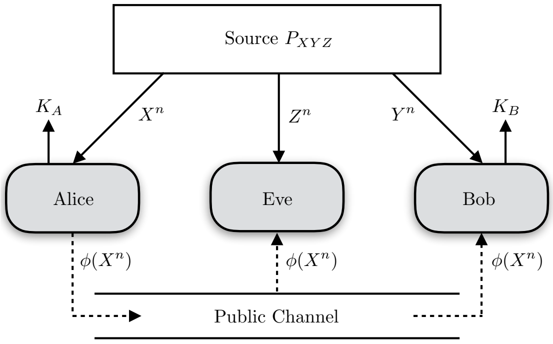

Fig. 1. Secret key generation with a single forward transmission. Eve observes an own observation Z^n of the source as well as the helper message $\phi(X^n)$.

mission is an important resource which needs to be effectively exploited in the secret key generation process. We show that when the public communication is not rate-limited, the corresponding secret key (SK) capacity displays a simple algorithmic structure in the sense that it is Turing computable. On the other hand, we show that when the forward transmission is rate-limited, the corresponding SK capacity becomes non-computable displaying a much more complicated algorithmic structure. This shows that imposing a rate constraint on the public forward transmission transforms a Turing computable problem into a non-computable problem. Accordingly, there is a strict phase transition between both regimes and, to the best of our knowledge, this is the first time that such a phenomenon has been observed.

In practical systems, the public communication will always be rate-limited. Furthermore, it will usually take place over noisy communication channels which has been studied in [17]. This is particularly relevant for new communication scenarios such as molecular communication, for which security-related questions are relevant as well. In [18] an overview of molecular communication and its future applications is given. There, a secret key shared between transmitter and receiver can be used for private or secret synchronization.[1]

2. SECRET KEY GENERATION

Here, we introduce the model of secret key generation as shown in Fig. 1. It consists of two legitimate users Alice and Bob, who want to generate a secret key keeping the eavesdropper Eve ignorant of it.

Let $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ be finite alphabets. Alice, Bob, and Eve have access to a common random source which is characterized by its joint distribution $P_{XYZ} \in \mathcal{P}(\mathcal{X} \times \mathcal{Y} \times \mathcal{Z})$. Alice observes the source outputs $X^n = (X_1, ..., X_n) \in \mathcal{X}^n$, Bob observes $Y^n = (Y_1, ..., Y_n) \in \mathcal{Y}^n$, while Eve observes $Z^n = (Z_1, ..., Z_n) \in \mathcal{Z}^n$. Additionally, a rate-limited public channel is available for further communication and discussion.

After having received their source observations, Alice and Bob can use the public channel to exchange helper data to agree on the same secret key. Everything that is sent over this channel is available to Eve as well. Permissible secret key generation protocols over the public channel can be quite general including multiple iterations of forward and backward transmissions as well as randomized strategies, cf. for example [5]. In this paper, we consider the case of a single forward transmission only so that the secret key generation protocol reduces to the following steps:

- After having received the observations X^n and Y^n at Alice and Bob, Alice transmits a helper message $\phi(X^n)$ over the public channel to Bob.
- Both Alice and Bob compute the secret key as
$$K_A = K_A(X^n) \quad \text{and} \quad K_B(Y^n, \phi(X^n)) \tag{1}$$
with $K_A, K_B \in \mathcal{K}$ and $\mathcal{K}$ is the set of all possible keys.

A successful secret key generation protocol has to satisfy certain conditions as specified in the following definition.

Definition 1. *A number R_{SK} is said to be an* achievable SK rate *if for any $\epsilon > 0$ and sufficiently large n there is a permissible protocol with rate constraint R such that K_A and K_B, cf.* (1)*, satisfy*

$$\mathbb{P}\{K_A \neq K_B\} < \epsilon \tag{2a}$$
$$I(\phi(X^n), Z^n; K_A) < \epsilon \tag{2b}$$
$$\tfrac{1}{n} H(K_A) > R_{SK} - \epsilon \tag{2c}$$
$$\tfrac{1}{n} \log |\mathcal{K}| < \tfrac{1}{n} H(K_A) + \epsilon \tag{2d}$$
$$\tfrac{1}{n} \log \|\phi\| < R + \epsilon. \tag{2e}$$

The forward SK capacity $C_{SK}(R, P_{XYZ})$ is the largest achievable SK rate. If there is no rate constraint, then condition (2e) *is inactive and the forward SK capacity is denoted by $C_{SK}(P_{XYZ})$.*

Here, condition (2a) ensures that both Alice and Bob have generated the same key. Condition (2b) ensures that this key is secret, i.e., Eve who has access to the public transmission $\phi(X^n)$ and its own observation Z^n learns nothing about the secret key. Condition (2d) finally states that the secret key is nearly uniformly distributed.

Remark 1. *As the task of Alice and Bob is to generate a common key, this scenario is often referred to as* generated secret key. *There is variation of this scenario in which a certain secret key is given to Alice and the task is to generate the same key at Bob. As the secret key is chosen before the actual secret key generation process, this is often called* chosen secret key. *It perfectly applies to the application of secure data storage in which confidential information needs to be securely stored in a public database, cf. for example [19].*

Now we can state the forward SK capacity with rate constraint.

Theorem 1 ([11], [20])**.** *The forward SK capacity $C_{SK}(R, P_{XYZ})$ for the source P_{XYZ} with rate constraint $R \in \mathbb{R}^+$ is*

$$C_{SK}(R, P_{XYZ}) = \max_{U,V} \big[I(V;Y|U) - I(V;Z|U) \big]$$

such that

$$U - V - X - (Y, Z) \quad \text{and} \quad I(V; X|Y) \leq R.$$

Moreover, it is may be assumed that $V = (U, V')$ where the cardinalities of the alphabets of both U and V' are at most $|\mathcal{X}| + 1$, cf. also [21, Theorem 17.21].

If Eve has no access to the source and does not observe an own correlated version, the forward SK capacity simplifies as follows.

[1] *Notation:* Discrete random variables are denoted by capital letters and their realizations and ranges by lower case and script letters, respectively; $\mathbb{N}$, $\mathbb{R}$, and $\mathbb{R}_c$ are the sets of non-negative integers, real numbers, and computable real numbers; $\mathcal{P}(\mathcal{X})$ denotes the set of all probability distributions on $\mathcal{X}$; $\|P - Q\| = \sum_{a \in \mathcal{A}} |P(a) - Q(a)|$ is the total variation distance between $P \in \mathcal{P}(\mathcal{A})$ and $Q \in \mathcal{P}(\mathcal{A})$.

Corollary 1. *The forward SK capacity $C_{SK}(R, P_{XY})$ for the source P_{XY} with rate constraint $R \in \mathbb{R}^+$ is*

$$C_{SK}(R, P_{XY}) = \max_{V} I(V;Y)$$

such that

$$V - X - Y \quad and \quad I(V;X|Y) \leq R.$$

For $R \to \infty$, the rate constraint becomes inactive and the corresponding forward SK capacity is given as follows.

Corollary 2 ([5]). *The forward SK capacity $C_{SK}(P_{XYZ})$ for the source P_{XYZ} is*

$$C_{SK}(P_{XYZ}) = \max_{U,V} \left[I(V;Y|U) - I(V;Z|U) \right]$$

such that $U - V - X - (Y,Z)$ form a Markov chain. Moreover, it is may be assumed that $V = (U, V')$ where the cardinalities of the alphabets of both U and V' are at most $|\mathcal{X}| + 1$, cf. also [21, Theorem 17.21].

We see that the SK capacity C_{SK} is a function of the rate constraint R and the underlying source P_{XYZ}. In the following we study whether or not the SK capacity is Turing computable, i.e., whether or not there exists an algorithm (or Turing machine) that can compute the function C_{SK}.

3. COMPUTABILITY FRAMEWORK

Here, we formally introduce the computability framework for which we need some basic definitions and concepts briefly reviewed in the following. The concept of computability and computable real numbers was first introduced by Turing in [14] and [15].

A sequence of rational numbers $\{r_n\}_{n\in\mathbb{N}}$ is called a *computable sequence* if there exist recursive functions $a, b, s : \mathbb{N} \to \mathbb{N}$ with $b(n) \neq 0$ for all $n \in \mathbb{N}$ and

$$r_n = (-1)^{s(n)} \frac{a(n)}{b(n)}, \qquad n \in \mathbb{N},$$

cf. [22, Def. 2.1 and 2.2] for a detailed treatment. A real number x is said to be *computable* if there exists a computable sequence of rational numbers $\{r_n\}_{n\in\mathbb{N}}$ such that

$$|x - r_n| < 2^{-n}$$

for all $n \in \mathbb{N}$. We denote the set of computable real numbers by $\mathbb{R}_c$. Based on this, we define the set of computable probability distributions $\mathcal{P}_c(\mathcal{X})$ as the set of all probability distributions $P \in \mathcal{P}(\mathcal{X})$ such that $P(x) \in \mathbb{R}_c$, $x \in \mathcal{X}$. This is important since a Turing machine can only work with computable real numbers.

Definition 2. *A function $f : \mathbb{R}_c \to \mathbb{R}_c$ is called* Borel computable *if there is an algorithm that transforms each given computable sequence of a computable real x into a corresponding representation for $f(x)$.*

We note that Turing's definition of computability conforms to the definition of Borel computability above. There are weaker forms of computability known as *Markov computability* and *Banach-Mazur computability*, of which the latter one is the weakest form of computability. In particular, Borel or Markov computability implies Banach-Mazur computability, but not vice versa. For an overview of the logical relations between different notions of computability we again refer to [23] and the introductory textbook [16].

We further need the concepts of a recursive set and a recursively enumerable set as for example defined in [22].

Definition 3. *A set $\mathcal{A} \subset \mathbb{N}$ is called* recursive *if there exists a computable function f such that $f(x) = 1$ if $x \in \mathcal{A}$ and $f(x) = 0$ if $x \notin \mathcal{A}$.*

Definition 4. *A set $\mathcal{A} \subset \mathbb{N}$ is* recursively enumerable *if there exists a recursive function whose domain is exactly $\mathcal{A}$.*

We have the following properties, cf. for example [22]

- $\mathcal{A}$ is recursive is equivalent to $\mathcal{A}$ is recursive enumerable and $\mathcal{A}^c$ is recursively enumerable.
- There exist recursively enumerable sets $\mathcal{A} \subset \mathbb{N}$ that are not recursive, i.e., $\mathcal{A}^c$ is not recursively enumerable. This means there are no computable, i.e., recursive, functions $f : \mathbb{N} \to \mathcal{A}^c$ with $[f(\mathbb{N})] = \mathcal{A}^c$.

Now we are in the position to introduce the concept of a Turing machine. Turing machines account for all those problems and tasks that are algorithmically solvable on a classical (i.e., non-quantum) machine. They are further equivalent to the von Neumann-architecture without hardware limitations and the theory of recursive functions, cf. also [24–27].

The task of a Turing machine $\mathfrak{T}$ is to verify the efficiency and security of a given secret key generation protocol as introduced in the previous section. To this end, let k specify the efficiency of the secret key generation protocol where $1/k$ is the maximum gap of the SK rate R_{SK} to the forward SK capacity C_{SK}. The Turing machine should output a "*yes*" if and only if the secret key generation protocol satisfies the performance requirements, cf. (2), and

$$C_{\text{SK}} - R_{\text{SK}} < \frac{1}{k}.$$

In particular, for verification of the latter condition, it is necessary that the forward SK capacity C_{SK} itself is Turing computable. This question is studied in detail in the next section.

4. NON-COMPUTABILITY

In this section, we study the Turing computability of the forward SK capacity C_{SK}. First, we study the case without rate constraints as stated in Corollary 2. The following result shows that the forward SK capacity is indeed Turing computable as expected.

Theorem 2. *The forward SK capacity $C_{SK}(P_{XYZ})$ is Turing computable.*

Sketch of Proof. Since $x \log_2 x$, $x \in [0,1]$, is a Borel computable function, the functions $I(V;Y|U)$ and $I(V;Z|U)$ for $P_{UVXYZ} \in \mathcal{P}_c(\mathcal{U} \times \mathcal{V} \times \mathcal{X} \times \mathcal{Y} \times \mathcal{Z})$ are computable as well. Then, the capacity function $C_{\text{SK}}(P_{XYZ}) = \max_{U,V}[I(V;Y|U) - I(V;Z|U)]$ is a computable function since it is the maximum of a difference of computable functions. We refer to [16] for a detailed introduction and discussion of these concepts and properties that are used here.

The next result shows that C_{SK} becomes non-computable when the forward transmission is rate limited.

Theorem 3. *For all $|\mathcal{X}| \geq 2$, $|\mathcal{Y}| \geq 2$, and $|\mathcal{Z}| \geq 2$, the forward SK capacity $C_{SK}(R, P_{XYZ})$ is not Banach-Mazur computable and therewith also not Turing computable.*

Before proving the result, we want to outline the important steps of the proof. For $R \to \infty$, i.e., the rate constraint of the forward transmission is inactive, the forward SK capacity becomes

$$C_{\text{SK}}(P_{XYZ}) = \max_{U,V} \left[I(V;Z|U) - I(V;Z|U) \right]$$

and this expression is Turing computable on the set of computable joint distributions $\mathcal{P}_c(\mathcal{U} \times \mathcal{V} \times \mathcal{X} \times \mathcal{Y} \times \mathcal{Z})$, cf. Theorem 2. We see also that the rate constraint R will play a crucial role for the non-computability of C_{SK}.

Instead of proving Theorem 3 directly, we argue further that it is sufficient to prove the non-computability for the special case, in which Eve does not receive its own observation Z^n, cf. also Corollary 1. This is contained in the general case by considering the structure of the source $P_{XYZ}(x, y, z) = P_{XY}(x, y)P_Z(z)$, $P_{XY} \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$, and $P_Z \in \mathcal{P}(\mathcal{Z})$. In the following we show that $C_{\text{SK}}(P_{XY})$ is already not Banach-Mazur computable, which then immediately implies that the general case as stated in Theorem 3 is also not Banach-Mazur computable.

Theorem 4. *For all $|\mathcal{X}| \geq 2$ and $|\mathcal{Y}| \geq 2$, the forward SK capacity $C_{SK}(R, P_{XY})$ is not Banach-Mazur computable and therewith also not Turing computable.*

Sketch of Proof. We prove the result for $|\mathcal{X}| = |\mathcal{Y}| = 2$. It can easily be extended to the general case of $|\mathcal{X}| \geq 2$ and $|\mathcal{Y}| \geq 2$. The details are omitted due to space constraints.

First, we consider the source

$$P_*(x, y) = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \tag{3}$$

and see that for this source, both Alice and Bob observe random variables X and Y that have the same value with probability one, i.e., $\mathbb{P}\{X = Y\} = 1$. This easily allows Alice and Bob to agree on the same secret key error-free, i.e., $\mathbb{P}\{K_A = K_B\} = 1$. Further no public communication is needed at all so that no information about the key is leaked to Eve. It follows that the forward SK capacity is $C_{\text{SK}}(R, P_*) = 1$, cf. also [28].

Next, we consider another source

$$P_n(x, y) = \begin{pmatrix} \frac{1}{2} - \frac{1}{2^n} & \frac{1}{2^n} \\ \frac{1}{2^n} & \frac{1}{2} - \frac{1}{2^n} \end{pmatrix}, \quad n \geq 2. \tag{4}$$

From (3) and (4) we get $\|P_n - P_*\| = \frac{4}{2^n}$ so that $\lim_{n\to\infty} \|P_n - P_*\| = 0$. Assume that $C_{\text{SK}}(R, P_n)$ is for $R \geq 0$, $R \in \mathbb{R}_c$ and $P_n \in \mathcal{P}_c(\mathcal{X} \times \mathcal{Y})$ Banach-Mazur computable. This implies that every computable sequence $\{(R_n, P_n)\}_{n\in\mathbb{N}}$ is mapped into a computable sequence $\{C_{\text{SK}}(R_n, P_n)\}_{n\in\mathbb{N}}$, i.e., this sequence must be a computable sequence of computable real numbers.

Let $P_n \in \mathcal{P}_c(\mathcal{X} \times \mathcal{Y})$, $n \geq 2$. We set $R_n = 0$ for all $n \in \mathbb{N}$, but keep the sequence $\{P_n\}_{n\in\mathbb{N}}$ as it is. By using results of [28] one can show that $\lim_{R\to 0} C_{\text{SK}}(R, P_n) = 0$ for all $n \in \mathbb{N}$. Accordingly, we have $C_{\text{SK}}(0, P_n) = 0$ for all $n \in \mathbb{N}$. From the beginning we further have $C_{\text{SK}}(0, P_*) = 1$.

Let $\mathcal{A} \subset \mathbb{N}$ be an arbitrary recursively enumerable set such that $\mathcal{A}$ is not recursive, i.e., $\mathcal{A}^c$ is not a recursively enumerable set. With the definition of recursively enumerable sets, cf. Definition 4, we can construct a total function g, i.e., domain$(g) = \mathbb{N}$, such that $[g(\mathbb{N})] = \mathcal{A}$ and g is recursive and therewith a computable function. Furthermore, without loss of generality, we can require that $g : \mathbb{N} \to \mathcal{A}$ is a one-to-one mapping from $\mathbb{N}$ to $\mathcal{A}$.

To show that the forward SK capacity is not Banach-Mazur computable, we will extend a construction of Pour-El, cf. Case I on page 336 in [29]. For every $(n, m) \in \mathbb{N} \times \mathbb{N}$ we define the computable function $q : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ as

$$q(n, m) = \begin{cases} 2^{m+2} & n \notin \{g(0), ..., g(2^{m+2})\} \\ r & n \in \{g(0), ..., g(2^{m+2})\} \text{ and } g(r) = n. \end{cases}$$

Note that r above is unique. Since $\mathcal{A}$ is recursively enumerable, the function q is recursive and therewith computable.

Next, we consider the double sequence $\{P_{q(n,m)}\}_{n\in\mathbb{N},m\in\mathbb{N}}$ of sources. Note that this is only a suitable variation of the sequence $\{P_n\}_{n\in\mathbb{N}}$ which is effectively computable since q is recursive function. The idea is to show that for all $n \in \mathbb{N}$ the double sequence $\{P_{q(n,m)}\}_{n\in\mathbb{N},m\in\mathbb{N}}$ effectively converges to a sequences of sources $\{P_n\}_{n\in\mathbb{N}}$. Then the sequence $\{P_n\}_{n\in\mathbb{N}}$ is a computable sequence as well. For this purpose we have construct a suitable function φ_n for each $n \in \mathbb{N}$, for which we then show that $\{P_{q(n,m)}\}_{m\in\mathbb{N}}$ converges effectively to P_*.

For $n \in \mathcal{A}$ let m_0 be the smallest index such that $n \in \{g(0), ..., g(2^{m_0+2})\}$ is satisfied. Now, for all $m \geq m_0$ we have $q(n, m) = r$, i.e., we have

$$P_{q(n,m)} = P_*. \tag{5}$$

If we define $\varphi_n(k) = m_0$, i.e., $\varphi_n(k)$ is constant for $n \in \mathcal{A}$, we have for the corresponding source $\|P_{q(n,m)} - P_r\| = 0 < \frac{1}{2^k}$ for all $m \geq m_0$, i.e., we have computable convergence for $n \in \mathcal{A}$.

For $n \in \mathcal{A}^c$ we can construct a similar construction to obtain a computable sequence $\{\hat{P}_n\}_{n\in\mathbb{N}}$ of computable probability distributions with

$$\hat{P}_n = \begin{cases} P_* & \text{if } n \in \mathcal{A}^c \\ P_r & \text{if } n \in \mathcal{A} \text{ and } g(r) = n. \end{cases}$$

This implies that the sequence $\{C_{\text{SK}}(0, \hat{P}_n)\}_{n\in\mathbb{N}}$ is a computable sequence. It holds that

$$C_{\text{SK}}(0, \hat{P}_n) = 0 \ \Leftrightarrow \ n \in \mathcal{A} \quad \text{and} \quad C_{\text{SK}}(0, \hat{P}_n) = 1 \ \Leftrightarrow \ n \in \mathcal{A}^c.$$

Since C_{SK} is assumed to be Banach-Mazur computable, the set $\mathcal{A}^c$ must be recursively enumerable so that the set $\mathcal{A}$ is recursive which is a contradiction to the initial assumption that $\mathcal{A}$ is recursively enumerable but not recursive. This implies that the assumption that there exists a Turing machine that can solve this task is wrong. This outlines the crucial steps. For the complete proof we refer to [17].

Remark 2. *Note that the proof ideas and techniques of Theorem 4 do not carry over to the secure storage problem in Remark 1. There, we observe a completely different behavior: the capacity function is continuous and further allows for super activation, cf. [19].*

Remark 3. *The problem of identification over correlation-assisted channels is of further interest to molecular communication. The question of computability of the corresponding identification capacity has been studied in [30].*

5. RELATION TO PRIOR WORK

Secret key generation has been studied under various aspects, cf. for example [5, 6, 8, 11–13]. However, secret key generation from a computability or algorithmic point of view has not been studied yet. To the best of our knowledge, the only works which study a similar scenario are the following: In [31] the computability of the capacity function of the wiretap channel under adversarial attacks is studied and in [30] that of the identification capacity of the correlation-assisted channel is studied. For molecular communication, secret key generation with rate-limited public discussion has not been studied at all [18].

6. REFERENCES

[1] Yingbin Liang, H. Vincent. Poor, and Shlomo Shamai (Shitz), "Information Theoretic Security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4-5, pp. 355–580, 2009.

[2] Matthieu Bloch and João Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, Cambridge University Press, 2011.

[3] Rafael F. Schaefer, Holger Boche, Ashish Khisti, and H. Vincent Poor, Eds., *Information Theoretic Security and Privacy of Information Systems*, Cambridge University Press, Cambridge, UK, 2017.

[4] H. Vincent Poor and Rafael F. Schaefer, "Wireless physical layer security," *Proc. Natl. Acad. Sci. U.S.A.*, vol. 114, no. 1, pp. 19–26, Jan. 2017.

[5] Rudolf Ahlswede and Imre Csiszár, "Common randomness in information theory and cryptography—Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, July 1993.

[6] Ueli M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[7] Aaron D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.

[8] Lifeng Lai, Yingbin Liang, and H. Vincent Poor, "A unified framework for key agreement over wireless fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 480–490, Apr. 2012.

[9] G. Fettweis, H. Boche, T. Wiegand, *et al.*, "The Tactile Internet," Tech. Rep., ITU-T Tech. Watch Rep., Aug. 2014.

[10] Rafael F. Schaefer and Holger Boche, "Physical layer service integration in wireless networks — Signal processing challenges," *IEEE Signal Process. Mag.*, vol. 31, no. 3, pp. 147–156, May 2014.

[11] Imre Csiszár and Prakash Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 344–366, Mar. 2000.

[12] Imre Csiszár and Prakash Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, Dec. 2004.

[13] Ashish Khisti, Suhas N. Diggavi, and Gregory W. Wornell, "Secret-key generation using correlated sources and channels," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 652–670, Feb. 2012.

[14] Alan M. Turing, "On computable numbers, with an application to the Entscheidungsproblem," *Proc. London Math. Soc.*, vol. 2, no. 42, pp. 230–265, 1936.

[15] Alan M. Turing, "On computable numbers, with an application to the Entscheidungsproblem. A correction," *Proc. London Math. Soc.*, vol. 2, no. 43, pp. 544–546, 1937.

[16] Klaus Weihrauch, *Computable Analysis - An Introduction*, Springer-Verlag, Berlin Heidelberg, 2000.

[17] Holger Boche, Rafael F. Schaefer, Sebastian Baur, and H. Vincent Poor, "On the algorithmic computability of the secret key and authentication capacity under channel, storage, and privacy leakage constraints," submitted.

[18] Werner Haselmayr, Andreas Springer, Georg Fischer, Christoph Alexiou, Holger Boche, Peter A. Hoeher, Falko Dressler, and Robert Schober, "Integration of molecular communications into future generation wireless networks," in *6G Wireless Summit*, Levi, Finland, Mar. 2019.

[19] Sebastian Baur, Holger Boche, Rafael F. Schaefer, and H. Vincent Poor, "Secure storage capacity under rate constraints — Continuity and super activation," 2019, submitted.

[20] Germán Bassi, Pablo Piantanida, and Shlomo Shamai (Shitz), "Secret key generation over noisy channels with common randomness," in *Proc. IEEE Int. Symp. Inf. Theory*, Barcelona, Spain, July 2016, pp. 510–514.

[21] Imre Csiszár and János Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, Cambridge University Press, Cambridge, UK, 2 edition, 2011.

[22] Robert I. Soare, *Recursively Enumerable Sets and Degrees*, Springer-Verlag Berlin Heidelberg, Berlin, Heidelberg, 1987.

[23] Jeremy Avigad and Vasco Brattka, "Computability and analysis: The legacy of Alan Turing," in *Turing's Legacy: Developments from Turing's Ideas in Logic*, Rod Downey, Ed. Cambridge University Press, Cambridge, UK, 2014.

[24] Kurt Gödel, "Die Vollständigkeit der Axiome des logischen Funktionenkalküls," *Monatshefte für Mathematik*, vol. 37, no. 1, pp. 349–360, 1930.

[25] Kurt Gödel, "On undecidable propositions of formal mathematical systems," *Notes by Stephen C. Kleene and Barkely Rosser on Lectures at the Institute for Advanced Study, Princeton, NJ*, 1934.

[26] Stephen C. Kleene, *Introduction to Metamathematics*, Wolters-Noordhoffv, Van Nostrand, New York, 1952.

[27] Marvin Minsky, "Recursive unsolvability of Post's problem of 'tag' and other topics in theory of Turing machines," *Ann. Math.*, vol. 74, no. 3, pp. 437–455, 1961.

[28] Hans S. Witsenhausen, "On sequences of pairs of dependent random variables," *SIAM J. Appl. Math.*, vol. 28, no. 1, pp. 100–113, Jan. 1975.

[29] Marian Boykan Pour-El, "A comparison of five "computable" operators," *Math. Logic Quart.*, vol. 6, no. 15-22, pp. 325–340, 1960.

[30] Holger Boche, Rafael F. Schaefer, and H. Vincent Poor, "Identification capacity of correlation-assisted discrete memoryless channels: Analytical properties and representations," submitted.

[31] Holger Boche, Rafael F. Schaefer, and H. Vincent Poor, "Performance evaluation of secure communication systems on Turing machines," in *Proc. 10th IEEE Int. Workshop Inf. Forensics Security*, Hong Kong, Dec. 2018, pp. 1–7.