IEEE TRANSACTIONS ON
INFORMATION FORENSICS AND SECURITY

IEEE Xplore® Digital Library
http://ieeexplore.ieee.org/Xplore

Secure Storage Capacity under Rate Constraints — Continuity and Super Activation

Sebastian Baur, *Student Member, IEEE*, Holger Boche, *Fellow, IEEE*, Rafael F. Schaefer, *Senior Member, IEEE* and H. Vincent Poor, *Fellow, IEEE*

***Abstract*—The source model for secret key generation with one way public communication refers to a setting in which a secret key should be agreed upon at two terminals. At both terminals correlated components of a common source are available. Additionally, a message can be sent from one terminal to the other via a public channel. In this work a related scenario is considered where instead of secret key generation, the goal is to securely store data in a public database. The database allows for error-free storing of the data, but is constrained in its size which imposes a rate constraint on the storing. The corresponding capacity for secure storage is known and it has been shown that the capacity-achieving strategy satisfies the strong secrecy criterion. Then the case when the storage in the public database is subject to errors is considered and the corresponding capacity is characterized. Additionally, the continuity properties of the two capacity functions are analyzed. These capacity functions are continuous as opposed to the discontinuous secret key capacity with rate constraint. It is shown that for secure storage the phenomenon of super activation can occur. Finally, it is discussed how the results in this paper differ from previous results on super activation.**

I. Introduction

Lately, considerable effort has been devoted to deriving information theoretic results that can be applied in communication scenarios where low delay is an essential requirement [1]. For many of these applications, the communication task should be performed securely due to the presence of eavesdroppers. Examples for such applications in the context of the Tactile Internet are discussed in [2]. The authors of [2] also discuss the infrastructure requirements needed in order to realize these applications. The Tactile Internet is considered a promising forthcoming innovation and motivated considerable fundamental research. Currently the Tactile Internet is in the process of standardization and the corresponding results can contribute fundamentally to the fifth generation mobile network 5G and systems beyond, especially 6G [3]. As discussed in [2], information theoretic security can contribute significantly to realize communication systems that combine low latency and security. For an overview of recent results in information theoretic security, see for example [4], [5] and [6].

A well known model in information theoretic security is the source model for secret key (SK) generation with one way public communication. It was first considered in [7] and [8]. In this model we consider two legitimate users who should agree upon a common SK. For this purpose, each of the legitimate users has access to an output of a discrete memoryless multiple source (DMMS) with two components. Additionally, a message can be sent from one legitimate user to the other over a noiseless public channel. An eavesdropper who can overhear the public communication should be kept ignorant of the SK.

This model of secret key generation further serves as the basis for an information theoretic treatment of authentication when an additional privacy leakage constraint on the source observations is imposed [4], [9], [10].

In this work we consider a related model which is a source model for secure data storage. (In [9] and [11] this model is called the chosen-secret model.) Here we consider two legitimate users and each of them has access to an output of a DMMS. The first legitimate user can store a message on a public database which can be read by the second legitimate user. There is an eavesdropper, who can also access the public database. The data that should be stored in the database are encoded in the message. The eavesdropper is interested in the data. So the legitimate users use the outputs of the DMMS to encode and decode the data such that the eavesdropper is kept ignorant of the data.

In the context of the Tactile Internet a possible application that can be modeled in such a way is secure storage in so called Mobile-Edge Clouds. As described in [2] storage in Mobile-Edge Clouds means that latency critical server requests are processed by servers that are close to the user. As information theoretic security enables security in combination with low delay it makes sense to realize secure storage in Mobile-Edge Clouds as described in this work. Thus the model for secure storage can provide insights for the future network topology of cellular operators [2], [3].

Due to practical limitations, it is reasonable to assume that the public database is storage constrained which imposes a rate

Sebastian Baur is with the Lehrstuhl für Theoretische Informationstechnik, Technische Universität München, 80290 Munich, Germany (email: s.j.baur@tum.de).

Holger Boche is with the Lehrstuhl für Theoretische Informationstechnik, Technische Universität München, 80290 Munich, Germany, and the Munich Center for Quantum Science and Technology (MCQST), Schellingstr. 4, 80799 Munich, Germany (email: boche@tum.de).

Rafael F. Schaefer is with the Information Theory and Applications Chair, Technische Universität Berlin, 10587 Berlin, Germany (email: rafael.schaefer@tu-berlin.de).

H. Vincent Poor is with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA (e-mail: poor@princeton.edu).

This work of H. Boche was supported in part by the German Federal Ministry of Education and Research (BMBF) within the national initiative for "Molecular Communication (MAMOKO)" under Grant 16KIS0914 and in part by the Gottfried Wilhelm Leibniz Prize of the German Research Foundation (DFG) under Grant BO 1734/20-1. This work of R. F. Schaefer and S. Baur was supported by the German Federal Ministry of Education and Research (BMBF) within the national initiative for "Post Shannon Communication (NewCom)" under Grants 16KIS1004 and 16KIS1003K. This work of H. V. Poor was supported by the U.S. National Science Foundation under Grants CCF-0939370 and CCF-1513915.

Digital Object Identifier: 10.1109/TIFS.2019.2929945

constraint on the public message to be stored in the database. Further, the database is assumed to be perfect in the sense that the storing itself is error-free. The corresponding capacity of secure storage has been derived in [11] and it is of interest to further study the capacity function and its properties in detail.

To this end, we show in this paper that the capacity function is continuous so that small variations of the system parameters result in small changes of the capacity only. This shows the robustness of the capacity function making it a desirable behavior. Comparing this with the corresponding secret key generation problem reveals fundamental differences between both problems. While the capacity of secured storage under rate constraints is a continuous function, the capacity of secret key generation under rate constraints is a discontinuous function [12], [13].

The continuity result is of practical importance as it implies that the capacity, describing the best possible performance of protocols for the model under consideration, is not sensitive to small variations of the model. Continuity of the capacity function also is a necessary requirement for being computable on any digital computer (Turing machine).

Our model becomes even more realistic when we consider storage on hardware that is not perfect, i.e., subject to errors. Accordingly we generalize the model in the sense that we replace the perfect public database by an imperfect, i.e. erroneous, public database. We use a discrete memoryless channel (DMC) to model the imperfectness. (Similarly, in [14] a generalized model for SK generation with one way public communication with a noisy DMC is analyzed.) Using the results derived for secure storage with a perfect database, we define protocols for the new model and characterize the corresponding storage capacity. Then we argue that this capacity function is continuous too.

Finally we prove that the phenomenon of super activation [15] can occur in this setting. This means that two parallel pairs of resources, i.e., two pairs of a source and a DMC, where each pair of resources has a zero storage capacity, together can have a storage capacity greater than zero if they are used jointly.

A related problem has already been considered in 1956 by Shannon. As described for example in [16], Shannon conjectured in [17] that the zero error capacity is additive, like the capacity of a DMC with maximum or average error criterion, see also [18]. This was later disproved by Haemers [19] and Alon [20]. The zero error capacity is super additive. This means there are examples where the zero error capacity of jointly used parallel channels is greater than the sum of the zero error capacities of the individual channels. The strongest form of super additivity is the phenomenon of super activation.

The capacity function for secure storage without a rate constraint on the public message is additive. It is surprising that introducing a rate constraint on the public communication can result in the capacity function to become super additive.

This behavior is also interesting in the following sense. To the best of our knowledge, there are no comparable results (in classical information theory) known where super activation occurs for continuous capacity functions. Today the only examples known in classical information theory where super activation can occur have a discontinuous capacity function. An example is the arbitrarily varying wiretap channel [21], [16]. It has been conjectured that the property of super activation in classical information theory is linked to the discontinuity of the corresponding capacity function. In this work we show that this is not the case and super activation can occur for continuous capacities as well.

Our result also shows that super activation is possible for an i.i.d. problem in classical information theory. In literature, all models of classical information theory where super activation occurs comprise non i.i.d. random vectors (like the arbitrarily varying wiretap channel).

These results provide insightful approaches to the solution of problems in system design concerned with medium access control in communication scenarios where we want to allocate resources efficiently. This means that our results show how resources such as the outputs of a DMMS or a public database should be used in an efficient way. They imply that in some cases joint processing of the available resources permit large gains in terms of performance compared to separate processing. This has far-reaching implications on the system design.

Our contribution is the following. We show that the capacity function for secure data storage is continuous in the case of a perfect database. Additionally we characterize the capacity for secure data storage with an imperfect database. To the best of our knowledge, this has not been considered for the storage problem yet; it has been considered for the problem of SK generation for an even more general setting in [14]. We show that this capacity function is continuous too. We also provide the description of an example where super activation occurs for secure data storage. As an interesting byproduct we discuss how our results differ to the literature on super activation. So our work also contributes to the fundamental understanding of classical and quantum communication.

This work is organized as follows. In Section II we introduce the models for SK generation and secure storage. We also give characterizations of the corresponding capacities. We prove that the capacity function of secure storage is continuous in Section III. In Section IV we consider the model for secure storage with an imperfect database. We characterize the corresponding capacity and also show that this capacity function is continuous. We give an example of secure storage where super activation occurs in Section V.

Notation. We use standard notation, comparable to the notation introduced in [22]. In contrast to [22], for random variables X and Y we denote the mutual information by $I(X;Y)$. We denote the set of all distributions on $\mathcal{X}$ by $\mathcal{P}(\mathcal{X})$ and define the set of all channels from $\mathcal{X}$ to $\mathcal{Y}$

$$\mathcal{P}(\mathcal{Y}|\mathcal{X}) = \{(P_{Y|X}(\cdot|x))_{x\in\mathcal{X}} \colon P_{Y|X}(\cdot|x) \in \mathcal{P}(\mathcal{Y}) \quad \forall x \in \mathcal{X}\}.$$

Let $P, Q \in \mathcal{P}(\mathcal{X})$. We define the total variation distance between P and Q such that

$$\|P - Q\|_{TV} = \sum_{x\in\mathcal{X}} |P(x) - Q(x)|.$$

For $P \in \mathcal{P}(\mathcal{X})$, $Q \in \mathcal{P}(\mathcal{Y})$, $W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ and $V \in \mathcal{P}(\bar{\mathcal{Y}}|\bar{\mathcal{X}})$ we define $P \otimes Q \in \mathcal{P}(\mathcal{X}\times\mathcal{Y})$ by $(P\otimes Q)(x,y) = P(x)Q(y)$ for all $(x,y) \in \mathcal{X}\times\mathcal{Y}$. For $n \in \mathbb{N}$ we define $P^{\otimes n} \in \mathcal{P}(\mathcal{X}^n)$ by

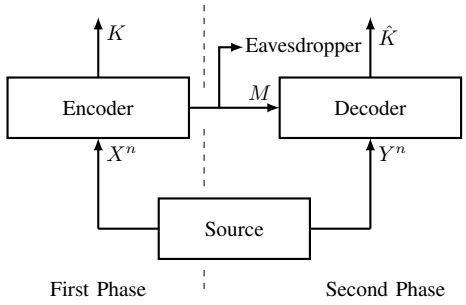

Fig. 1. Standard SK generation process with one way public communication as in [7], [8].

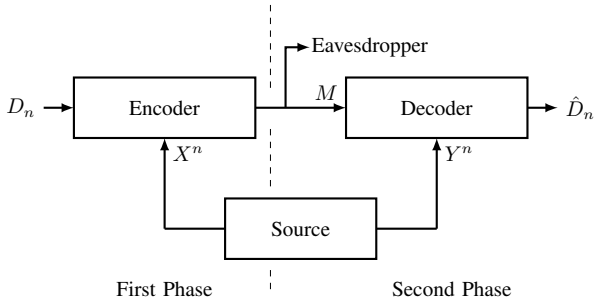

Fig. 2. Standard secure storage process as in [9].

$P^{\otimes n}(x^n) = \prod_{i=1}^n P(x_i)$ for all $x^n \in \mathcal{X}^n$. We define $W \otimes V \in \mathcal{P}(\mathcal{Y} \times \bar{\mathcal{Y}} | \mathcal{X} \times \bar{\mathcal{X}})$ by $(W \otimes V)(y, \bar{y}|x, \bar{x}) = W(y|x)V(\bar{y}|\bar{x})$ for all $(x, \bar{x}, y, \bar{y}) \in \mathcal{X} \times \bar{\mathcal{X}} \times \mathcal{Y} \times \bar{\mathcal{Y}}$.

II. Secret Key Generation and Secure Storage

A. Secret Key Generation

At first we consider SK generation with one way public communication from a source with two components. The standard scenario for SK generation with one way public communication considered in [7], [8] is depicted in Figure 1.

The process consists of two phases. In the first phase, the first legitimate user reads X^n from the source. Then the first legitimate user generates the SK K and the helper message M from X^n using an encoder. The first legitimate user then sends M to the second legitimate user. In the second phase, the second legitimate user has access to M and reads Y^n from the source. The second legitimate user then uses a decoder to reconstruct the SK from M and Y^n and thus generates $\hat{K}$. The eavesdropper interested in K also has access to M.

We now properly define the information theoretic model for the standard process of SK generation with one way public communication [7], [8].

Definition 1. Let $n \in \mathbb{N}$. The *source model* consists of the random variables (RVs) X and Y with $P_{XY} \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$, an encoder $f \colon \mathcal{X}^n \to \mathcal{K} \times \mathcal{M}$ and a decoder $g \colon \mathcal{Y}^n \times \mathcal{M} \to \hat{\mathcal{K}}$. Consider the RV $X^n Y^n$ with $P_{X^n Y^n} = P_{XY}^{\otimes n}$. The RVs K and M are generated from X^n using f and the RV $\hat{K}$ is generated from Y^n and M using g. We call (f, g) a *SK generation protocol*.

We now discuss properties of intuitively good SK generation protocols. We want to use the available resources as efficiently as possible. This means we want to generate the largest possible SK from the source output. This means we are interested in the largest possible SK generation rate. The SK should be reconstructed correctly with high probability. As the eavesdropper has access to the helper message, we want the average information required to specify the SK when the helper message is known to be as large as possible. From an information theoretic point of view this is equivalent to requiring that the SK be uniformly distributed and independent of the helper message. We also want to control the rate of the helper message, i.e., the size of the helper message per symbol read from the source.

This suggests the following definition of achievability for the source model.

Definition 2. Let $L \geq 0$. We call the rate $R \geq 0$ an *achievable SK rate with rate constraint* L for the source model if for all $\delta > 0$ there is an $n_0 = n_0(\delta)$ such that for all $n \geq n_0$ there is an SK generation protocol such that

$$\Pr(K = \hat{K}) \geq 1 - \delta \tag{1}$$
$$H(K) \geq \log |\mathcal{K}| - \delta \tag{2}$$
$$I(M; K) \leq \delta \tag{3}$$
$$\tfrac{1}{n} \log |\mathcal{K}| \geq R - \delta$$
$$\tfrac{1}{n} \log |\mathcal{M}| \leq L + \delta.$$

We call the supremum of all achievable SK rates with rate constraint L the SK capacity $C_{SK}(P_{XY}, L)$.

From [22] we know the following characterization of $C_{SK}(P_{XY}, L)$ for $L \geq 0$, $P_{XY} \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$.

Theorem 1 ([22] Theorem 17.21)**.** It holds that

$$C_{SK}(P_{XY}, L) = \max_U I(U; Y)$$

with RVs UXY such that $U - X - Y$ and $I(U; X|Y) \leq L$.

Remark 1. For the maximization in Theorem 1 it is sufficient to consider alphabets $\mathcal{U}$ with $|\mathcal{U}| \leq |\mathcal{X}| + 1$. (See for example [22, Theorem 17.21].)

Remark 2. The results in [13], where the continuity properties of C_{SK} are examined, are based on the characterization of C_{SK} and its dependence on P_{XY} and L. In particular in [13] it is shown that for all $|\mathcal{Y}| \geq 2$ and $|\mathcal{X}| \geq 2$ the function C_{SK} that depends on $P_{XY} \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$ and $L \geq 0$ is discontinuous. We provide a more detailed discussion on this proof of discontinuity in Remark 6.

B. Secure Storage

We also consider secure storage using a source with two components. This scenario is depicted in Figure 2.

The process consists of two phases. In the first phase, the first legitimate user reads X^n from the source and gets the data to be stored D_n. Then the first legitimate user generates the helper message M from X^n and D_n using an encoder. Finally the first legitimate user stores M in a public database. In the second phase, the second legitimate user reads M from the public database and Y^n from the source. The second legitimate

user then uses a decoder to reconstruct D_n from the stored M and Y^n and thus generates $\hat{D}_n$. The eavesdropper interested in D_n can read M from the public database too.

We now define an information theoretic model for the secure storage process. It is very similar to the chosen-secret model in [9], cf. [23].

Definition 3. Let $n \in \mathbb{N}$. The *storage model* consists of the RVs X, Y and D_n with $P_{XY} \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$ and $P_{D_n} \in \mathcal{P}(\mathcal{D}_n)$, the encoder $\phi\colon \mathcal{X}^n \times \mathcal{D}_n \to \mathcal{M}$ and the decoder $\psi\colon \mathcal{Y}^n \times \mathcal{M} \to \hat{\mathcal{D}}_n$. Consider the RV X^nY^n with $P_{X^nY^n} = P_{XY}^{\otimes n}$ and independent of D_n. The RV M is generated from X^n and D_n using ϕ. The RV $\hat{D}_n$ is generated from Y^n and M using ψ. We use the term *storage protocol* for (ϕ, ψ). Additionally it holds that for all $\delta > 0$ there is an $n_0 = n_0(\delta)$ such that for all $n \geq n_0$

$$\tfrac{1}{n} D(P_{D_n} \| U_{\mathcal{D}_n}) < \delta, \tag{4}$$

where $U_{\mathcal{D}_n}$ denotes the uniform distribution on $\mathcal{D}_n$.

Remark 3. In the storage model we consider $P_{D_n} \in \mathcal{P}(\mathcal{D}_n)$ such that (4) is satisfied. This is justified because a good compression protocol ensures the data to be approximately uniformly distributed, cf. [24].

We now discuss properties of intuitively good storage protocols. Again we want to use the source output as efficiently as possible. This means we want to store the largest possible message using the available source output. So we are interested in determining the largest possible storage rate. Additionally, D_n should be reconstructed correctly with high probability. As the eavesdropper has access to the stored helper message, we want the average information required to specify D_n to be as large as possible when the helper message is known. From an information theoretic point of view this is equivalent to requiring D_n be independent of the helper message. We also want to control the rate of the helper message (as for SK generation protocols).

This suggests the following definition of achievability for the storage model.

Definition 4. Let $L \geq 0$. We call the rate $R \geq 0$ an *achievable secure storage rate with rate contraint* L for the storage model if for all $\delta > 0$ there is an $n_0 = n_0(\delta)$ such that for all $n \geq n_0$ there is a storage protocol such that

$$\begin{aligned} &\Pr(D_n = \hat{D}_n) \geq 1 - \delta \\ &I(M; D_n) \leq \delta \\ &\tfrac{1}{n} \log |\mathcal{D}_n| \geq R - \delta \\ &\tfrac{1}{n} \log |\mathcal{M}| \leq L + \delta. \end{aligned}$$

We call the supremum of all achievable secure storage rates with rate constraint L the secure storage capacity $C_S(P_{XY}, L)$.

From [11] we know the characterization of $C_S(P_{XY}, L)$ for $L \geq 0$, $P_{XY} \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$.

Theorem 2 ([11])**.** It holds that

$$C_S(P_{XY}, L) = \max_U I(U; Y)$$

with RVs UXY such that $U - X - Y$ and $I(U; X) \leq L$.

Remark 4. In the remainder of this work C_S plays a central role. Thus we give a proof of Theorem 2 in the Appendix. This is motivated by the fact that we want to provide more details of the proof compared to [11] as we refer to the proof in Section IV when proving the capacity result for secure storage with an imperfect database.

Comparing Theorem 1 and Theorem 2 we notice that C_{SK} and C_S seem to have a similar structure but we will see that both functions have different continuity properties. In particular we have

$$\lim_{L \to \infty} C_S(P_{XY}, L) = \lim_{L \to \infty} C_{SK}(P_{XY}, L) = I(X; Y).$$

We define

$$C_S(P_{XY}, \infty) = \lim_{L \to \infty} C_S(P_{XY}, L)$$

and

$$C_{SK}(P_{XY}, \infty) = \lim_{L \to \infty} C_{SK}(P_{XY}, L).$$

Of course $C_{SK}(P_{XY}, \infty)$ (and equivalently $C_S(P_{XY}, \infty)$) is continuous as a function of P_{XY}. But this is not true for $C_{SK}(P_{XY}, L)$ as a function of (P_{XY}, L). In [13] it is shown that $C_{SK}(P_{XY}, L)$ is discontinuous. However, in Section III we show that $C_S(P_{XY}, L)$ is continuous on $\mathcal{P}(\mathcal{X} \times \mathcal{Y}) \times \mathbb{R}_{\geq 0}$. So from a practical point of view $C_S(P_{XY}, L)$ has the desirable property of being robust to small variations of the system parameters, as described before, while $C_{SK}(P_{XY}, L)$ does not have this property.

Remark 5. For the maximization in Theorem 2 it is sufficient to consider alphabets $\mathcal{U}$ with $|\mathcal{U}| \leq |\mathcal{X}| + 1$. (See for example [22].)

III. Continuity of the Secure Storage Capacity

As mentioned before, continuity of the function that describes the performance of a system is important in practice. If the function is continuous, the system performance is not sensitive to small variations of the system parameters. This is relevant because the system parameters can only be determined with a limited precision (for example due to imperfect channel measurements).

We now want to show that the secure storage capacity C_S is a continuous function. For this purpose we define a distance and continuity as follows.

Consider the tuples $(P_1, L_1), (P_2, L_2) \in \mathcal{P}(\mathcal{X} \times \mathcal{Y}) \times \mathbb{R}_{\geq 0}$. We define the distance between these tuples as

$$d((P_1, L_1), (P_2, L_2)) = \|P_1 - P_2\|_{TV} + |L_1 - L_2|.$$

Definition 5. $C_S\colon \mathcal{P}(\mathcal{X} \times \mathcal{Y}) \times \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is said to be *continuous* in $(P, L) \in \mathcal{P}(\mathcal{X} \times \mathcal{Y}) \times \mathbb{R}_{\geq 0}$ if for each sequence $(P_n, L_n)_{n \in \mathbb{N}}$, $(P_n, L_n) \in \mathcal{P}(\mathcal{X} \times \mathcal{Y}) \times \mathbb{R}_{\geq 0}$ for all $n \in \mathbb{N}$, with

$$\lim_{n \to \infty} d((P, L), (P_n, L_n)) = 0$$

we have

$$\lim_{n \to \infty} C_S(P_n, L_n) = C_S(P, L).$$

Remark 6. In contrast to C_S, the SK capacity C_{SK} is discontinuous. In [12], [13] it is shown that there are sequences

$(P_n)_{n\in\mathbb{N}}$, $P_n \in \mathcal{P}(\mathcal{X}\times\mathcal{Y})$ and $(L_n)_{n\in\mathbb{N}}$, $L_n \in \mathbb{R}_{\geq 0}$ and $\hat{P} \in \mathcal{P}(\mathcal{X}\times\mathcal{Y}), \hat{L} \in \mathbb{R}_{\geq 0}$ such that

$$\lim_{n\to\infty} d((P_n, L_n), (\hat{P}, \hat{L})) = 0$$

but

$$\limsup_{n\to\infty} C_{SK}(P_n, L_n) \neq C_{SK}(\hat{P}, \hat{L}),$$

i.e. C_{SK} is discontinuous.

In [13] SK generation is related to common randomness (CR) generation from a correlated source P_{XY} without public communication. CR generation is very similar to SK generation inasmuch as in both settings, two legitimate users observe correlated sequences X^n and Y^n respectively. They generate $K = K(X^n)$ and $\hat{K} = \hat{K}(Y^n)$ from X^n and Y^n respectively using randomized functions. We define achievability for CR generation similarly to achievability for SK generation without public communication. The difference to SK generation is that we omit the secrecy requirement (3) in Definition 2. We define the CR generation capacity $C_{CR}(P_{XY})$ accordingly. It is clear that $C_{CR}(P_{XY}) \geq C_{SK}(P_{XY}, 0)$. (As without public communication the secrecy requirement is met trivially we even have $C_{CR}(P_{XY}) = C_{SK}(P_{XY}, 0)$.)

Now we consider the case $|\mathcal{X}| = |\mathcal{Y}| = 2$. (The general case follows as described in [13].) According to [25] it holds for $n \geq 2$ that $C_{CR}(P_n) = 0$ (and thus $C_{SK}(P_n, 0) = 0$) for

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

Furthermore we have $C_{CR}(P_*) = C_{SK}(P_*, 0) = 1$ where

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

It also holds that

$$\lim_{n\to\infty} \|P_n - P_*\|_{TV} = 0.$$

This is used in [13] to prove the discontinuity of $C_{SK}(P, L)$ as a function of $(P, L) \in \mathcal{P}(\mathcal{X}\times\mathcal{Y}) \times \mathbb{R}_{\geq 0}$.

We now show that this behaviour can not occur for C_S, i.e. C_S is indeed continuous.

Theorem 3. $C_S \colon \mathcal{P}(\mathcal{X}\times\mathcal{Y}) \times \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is continuous on its domain.

Proof: For the proof we show that $\{C_S(P_{XY}, L)\}_{P_{XY}\in\mathcal{P}(\mathcal{X}\times\mathcal{Y})}$ is equicontinuous in L and for all $L \in \mathbb{R}_{\geq 0}$ we show that $C_S(P_{XY}, L)$ is continuous in P_{XY}. Then we combine both results to get the continuity in (P_{XY}, L). We start with the proof that $\{C_S(P_{XY}, L)\}_{P_{XY}\in\mathcal{P}(\mathcal{X}\times\mathcal{Y})}$ is equicontinuous in L.

Let $P_{XY} \in \mathcal{P}(\mathcal{X}\times\mathcal{Y})$ and $L_1, L_2 \geq 0$ with $|L_1 - L_2| \leq \epsilon$, $\epsilon > 0$. We divide the proof in two parts. At first we consider the case $L_1 > 0$. Then we consider the case $L_1 = 0$.

So first assume $L_1 \geq L_2 > 0$. Consider the RVs U_1, U_2 such that $U_1 - X - Y$, $U_2 - X - Y$,

$$C_S(P_{XY}, L_1) = I(U_1; Y)$$
$$C_S(P_{XY}, L_2) = I(U_2; Y)$$

and

$$I(U_1; X) \leq L_1$$
$$I(U_2; X) \leq L_2.$$

It is clear that

$$I(U_1; Y) \geq I(U_2; Y). \tag{5}$$

Consider the RV U_0 such that $U_0 - X - Y$ and $I(U_0; X) = 0$ (i.e. the RVs U_0 and X are independent). Let $1 \geq \lambda > 0$ and define the RV $\bar{U}$ with $\bar{U} - X - Y$ and

$$P_{\bar{U}|X} = \lambda P_{U_1|X} + (1-\lambda) P_{U_0|X}.$$

We have

$$\begin{aligned}
&\max_{x\in\mathcal{X}} \|P_{U_1|X}(\cdot|x) - P_{\bar{U}|X}(\cdot|x)\|_{TV} \\
&= \max_{x\in\mathcal{X}} \|P_{U_1|X}(\cdot|x) - \lambda P_{U_1|X}(\cdot|x) - (1-\lambda) P_{U_0|X}(\cdot|x)\|_{TV} \\
&= (1-\lambda) \max_{x\in\mathcal{X}} \|P_{U_1|X}(\cdot|x) - P_{U_0|X}(\cdot|x)\|_{TV} \\
&\leq (1-\lambda) 2 =: \theta.
\end{aligned} \tag{6}$$

As $I(U; X)$ is convex in $P_{U|X}$ (for a RV U) we get

$$\begin{aligned}
I(\bar{U}; X) &\leq \lambda I(U_1; X) + (1-\lambda) I(U_0; X) \\
&= \lambda I(U_1; X).
\end{aligned} \tag{7}$$

From (7) we get

$$I(\bar{U}; X) \leq \lambda L_1 = L_2$$

for $\lambda = \frac{L_2}{L_1}$. Thus, for this choice of λ it is clear that $\bar{U}$ is an element of the feasible set of the optimization problem that determines $C_S(P_{XY}, L_2)$. So

$$I(\bar{U}; Y) \leq I(U_2; Y) \leq I(U_1; Y)$$

where for the last inequality we use (5). We get from (6)

$$\begin{aligned}
&\|P_{\bar{U}XY} - P_{U_1XY}\|_{TV} \\
&= \sum_{u,x,y} |P_{\bar{U}XY}(u,x,y) - P_{U_1XY}(u,x,y)| \\
&\leq \sum_{x,y} P_{XY}(x,y) \max_{x\in\mathcal{X}} \|P_{U_1|X}(\cdot|x) - P_{\bar{U}|X}(\cdot|x)\|_{TV} \leq \theta.
\end{aligned}$$

Thus we can also upper bound the variational distance of the corresponding marginals by θ using the triangle inequality. We have

$$\begin{aligned}
I(\bar{U}; Y) &= H(Y) - (H(\bar{U}Y) - H(\bar{U})) \\
&\geq H(Y) - H(U_1Y) - \theta \log \tfrac{|\mathcal{Y}||\mathcal{U}|}{\theta} + H(U_1) - \theta \log \tfrac{|\mathcal{U}|}{\theta},
\end{aligned}$$

cf. [22, Lemma 2.7]. (As we use [22, Lemma 2.7] we need $\theta \leq \frac{1}{2}$ which is equivalent to $\lambda \geq \frac{3}{4}$. This requirement is met for ϵ small enough.) So

$$I(\bar{U}; Y) \geq I(U_1; Y) - \theta \log \tfrac{|\mathcal{Y}|(|\mathcal{X}|+1)^2}{\theta^2}.$$

Note that the second term does not depend on P_{XY}. So we now know

$$\begin{aligned}
&C_S(P_{XY}, L_1) - \theta \log \tfrac{|\mathcal{Y}|(|\mathcal{X}|+1)^2}{\theta^2} \\
&\leq C_S(P_{XY}, L_2) \leq C_S(P_{XY}, L_1)
\end{aligned}$$

which implies

$$|C_S(P_{XY}, L_1) - C_S(P_{XY}, L_2)| \leq \theta \log \tfrac{|\mathcal{Y}|(|\mathcal{X}|+1)^2}{\theta^2}.$$

Equivalently we get for $L_2 \geq L_1 > 0$ that

$$\begin{aligned} &C_S(P_{XY}, L_2) - \theta \log \tfrac{|\mathcal{Y}|(|\mathcal{X}|+1)^2}{\theta^2} \\ &\leq C_S(P_{XY}, L_1) \leq C_S(P_{XY}, L_2) \end{aligned}$$

which implies

$$|C_S(P_{XY}, L_1) - C_S(P_{XY}, L_2)| \leq \theta \log \tfrac{|\mathcal{Y}|(|\mathcal{X}|+1)^2}{\theta^2}.$$

So the family $\{C_S(P_{XY}, \cdot)\}_{P_{XY} \in \mathcal{P}(\mathcal{X}\times\mathcal{Y})}$ is equicontinuous on $\mathbb{R}_{>0}$.

For the second part of the proof we consider the case $L = 0$. In order to prove equicontinuity for the point $L = 0$ consider $C_S(P_{XY}, \epsilon)$, $\epsilon > 0$. As for a RV U with $U - X - Y$

$$I(U;Y) \leq I(U;X)$$

we have $C_S(P_{XY}, \epsilon) \leq \epsilon$ and $C_S(P_{XY}, 0) = 0$ and thus equicontinuity also for $L = 0$.

Now we prove that $C_S(P_{XY}, L)$ is continuous in P_{XY}.

At first we fix $L = 0$. As $C_S(P_{XY}, 0) = 0$ for all $P_{XY} \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$ it holds that $C_S(\cdot, 0)$ is continuous on $\mathcal{P}(\mathcal{X} \times \mathcal{Y})$.

Now consider $L > 0$. Let $P_{X_1Y_1}, P_{X_2Y_2} \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$ such that $\|P_{X_1Y_1} - P_{X_2Y_2}\|_{TV} \leq \epsilon$, $\epsilon > 0$. Consider RVs U_1, U_2 such that

$$\begin{aligned} U_1 - X_1 - Y_1, \\ U_2 - X_2 - Y_2, \end{aligned}$$

$$\begin{aligned} C_{SK}(P_{X_1Y_1}, L) = I(U_1;Y_1), \\ C_{SK}(P_{X_2Y_2}, L) = I(U_2;Y_2) \end{aligned}$$

and

$$I(U_1;X_1) \leq L, \qquad I(U_2;X_2) \leq L.$$

We have

$$\begin{aligned} &\sum_{u,x,y} |P_{U_2|X_2}(u|x)P_{X_2Y_2}(x,y) - P_{U_2|X_2}(u|x)P_{X_1Y_1}(x,y)| \\ &= \sum_{u,x,y} P_{U_2|X_2}(u|x)|P_{X_2Y_2}(x,y) - P_{X_1Y_1}(x,y)| \\ &\leq (\sum_{u} \max_x P_{U_2|X_2}(u|x))\epsilon \leq |\mathcal{U}|\epsilon. \end{aligned}$$

Define RVs $U_3X_3Y_3$ such that

$$P_{U_3X_3Y_3}(u,x,y) = P_{U_2|X_2}(u|x)P_{X_1Y_1}(x,y)$$

for all $(u,x,y) \in \mathcal{U} \times \mathcal{X} \times \mathcal{Y}$. We have

$$\begin{aligned} &I(U_3;X_3) = H(U_3) + H(X_3) - H(U_3X_3) \\ &= H(U_3) - H(U_3X_3) + H(X_1) \\ &\leq H(U_2) + |\mathcal{U}|\epsilon \log \tfrac{1}{\epsilon} \\ &- H(U_2X_2) + |\mathcal{U}|\epsilon \log \tfrac{|\mathcal{X}|}{\epsilon} \\ &+ H(X_2) + \epsilon \log \tfrac{|\mathcal{X}|}{\epsilon} \\ &= I(U_2;X_2) + \big(|\mathcal{U}|\epsilon \log \tfrac{|\mathcal{X}|}{\epsilon^2} + \epsilon \log \tfrac{|\mathcal{X}|}{\epsilon}\big). \end{aligned}$$

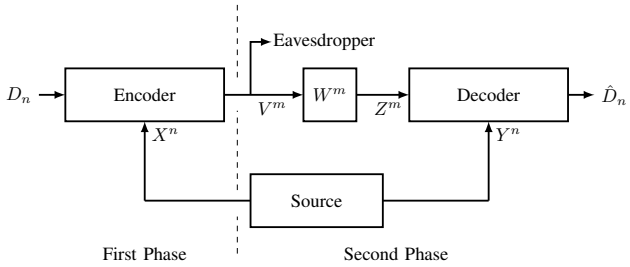

Fig. 3. Secure storage process with imperfect database.

Here we use [22, Lemma 2.7]. With $\delta = \big(|\mathcal{U}|\epsilon \log \frac{|\mathcal{X}|}{\epsilon^2} + \epsilon \log \frac{|\mathcal{X}|}{\epsilon}\big)$ we thus have

$$I(U_3;X_3) \leq \delta + L.$$

This implies

$$\begin{aligned} &I(U_3;Y_3) \leq C_S(P_{X_1Y_1}, L + \delta) \\ &\leq C_S(P_{X_1Y_1}, L) + \xi = I(U_1;Y_1) + \xi \end{aligned}$$

for a $\xi > 0$ arbitrarily small for δ small enough (which follows from the continuity of C_S in L). Now consider

$$\begin{aligned} &I(U_3;Y_3) = H(U_3) + H(Y_3) - H(U_3Y_3) \\ &\geq I(U_2;Y_2) - \big(|\mathcal{U}|\epsilon \log \tfrac{|\mathcal{Y}|}{\epsilon^2} + \epsilon \log \tfrac{|\mathcal{Y}|}{\epsilon}\big) \end{aligned}$$

which follows again from [22, Lemma 2.7] and we define $\bar{\xi} = \big(|\mathcal{U}|\epsilon \log \frac{|\mathcal{Y}|}{\epsilon^2} + \epsilon \log \frac{|\mathcal{Y}|}{\epsilon}\big)$. So

$$I(U_1;Y_1) \geq I(U_3;Y_3) - \xi \geq I(U_2;Y_2) - \xi - \bar{\xi}$$

which means

$$C_S(P_{X_1Y_1}, L) \geq C_S(P_{X_2Y_2}, L) - \xi - \bar{\xi}.$$

Using similar steps we can show

$$C_S(P_{X_2Y_2}, L) \geq C_S(P_{X_1Y_1}, L) - \xi - \bar{\xi}.$$

Now we put the two results together. Consider a sequence $(P_{XY,n}, L_n)_{n\in\mathbb{N}}$ that converges to (P^*_{XY}, L^*) with respect to d. Now we have

$$\begin{aligned} &|C_S(P_{XY,n}, L_n) - C_S(P^*_{XY}, L^*)| \\ &\leq |C_S(P_{XY,n}, L_n) - C_S(P_{XY,n}, L^*)| \\ &+ |C_S(P_{XY,n}, L^*) - C_S(P^*_{XY}, L^*)|. \end{aligned}$$

The second summand is arbitrarily small for n large enough which follows from the continuity in P_{XY} of $C_S(P_{XY}, L^*)$. The first summand also gets arbitrarily small which follows from the equicontinuity in L. ∎

IV. Secure Storage on Imperfect Database

Finally we consider the process for secure storage depicted in Figure 3, where we replace the perfect database by an imperfect one. Thus we have a more realistic model which takes into account the imperfectness of the hardware used for storage.

As before the process consists of two phases. In the first phase, the first legitimate user reads X^n from the source and gets the message to be stored D_n. Then the first legitimate

user generates the helper message V^m from X^n and D_n using an encoder and stores it in the public database. In the second phase the second legitimate user reads Z^m from the database and Y^n from the source. The second legitimate user then uses a decoder to reconstruct D_n from Z^m and Y^n and thus generates $\hat{D}_n$. The eavesdropper interested in D_n reads V^m from the public database.

Remark 7. We consider the worst case scenario in the sense that the eavesdropper knows V^m and not a distorted version of it.

We now define an information theoretic model for this secure storage process.

Definition 6. Let $n, m \in \mathbb{N}$. The *imperfect storage model* consists of $W \in \mathcal{P}(\mathcal{Z}|\mathcal{V})$, the RVs XY with $P_{XY} \in \mathcal{P}(\mathcal{X}\times\mathcal{Y})$, the RV D_n with $P_{D_n} \in \mathcal{P}(\mathcal{D}_n)$, the encoder $\phi\colon \mathcal{X}^n \times \mathcal{D}_n \to \mathcal{V}^m$ and the decoder $\psi\colon \mathcal{Y}^n \times \mathcal{Z}^m \to \hat{\mathcal{D}}_n$. Consider the RV X^nY^n with $P_{X^nY^n} = P_{XY}^{\otimes n}$ and independent of D_n. The RV V^m is generated from X^n and D_n using ϕ. The RV Z^m is the output of the memoryless channel W^m with channel input V^m. The RV $\hat{D}_n$ is generated from Y^n and Z^m using ψ. We use the term *imperfect storage protocol* for (ϕ, ψ). Additionally, it holds that for all $\delta > 0$ there is an $n_0 = n_0(\delta)$ such that for all $n \geq n_0$

$$\tfrac{1}{n} D(P_{D_n} \| U_{\mathcal{D}_n}) < \delta,$$

where $U_{\mathcal{D}_n}$ denotes the uniform distribution on $\mathcal{D}_n$.

Remark 8. We model the imperfect database (that consists of m storage cells) by the DMC W^m.

We now discuss properties of intuitively good imperfect storage protocols. We are interested in the largest possible storage rate. Additionally, D_n should be reconstructed correctly with high probability. As the eavesdropper has access to V^m, we want the average information required to specify D_n when the V^m is known to be as large as possible. From an information theoretic point of view this is equivalent to requiring that D_n be independent of V^m.

We assume that the DMC is used $\eta > 0$ times for each symbol read from the source, i.e. $m = \lceil \eta n \rceil$.

This suggests the following definitions of achievability for the imperfect storage model.

Definition 7. Let $\eta > 0$. We call the rate $R \geq 0$ an *achievable secure storage rate* for the imperfect storage model if for all $\delta > 0$ there is an $n_0 = n_0(\delta)$ such that for all $n \geq n_0$ there is an imperfect storage protocol with $m = \lceil \eta n \rceil$ such that

$$\begin{aligned} &\Pr(D_n = \hat{D}_n) \geq 1 - \delta \\ &I(V^m; D_n) \leq \delta \\ &\tfrac{1}{n} \log |\mathcal{D}_n| \geq R - \delta. \end{aligned}$$

We call the supremum of all achievable secure storage rates the imperfect secure storage capacity $C_S^\eta(P_{XY}, W)$.

We now want to characterize $C_S^\eta(P_{XY}, W)$ as follows.

Theorem 4. It holds that

$$C_S^\eta(P_{XY}, W) = \max_U I(U;Y)$$

with RVs UXY such that $U - X - Y$ and $I(U;X) \leq \eta \max_{P_V \in \mathcal{P}(\mathcal{V})} I(P_V; W)$.

Remark 9. This means that $C_S^\eta(P_{XY}, W) = C_S(P_{XY}, \eta C(W))$, where $C(W)$ is the Shannon capacity of W.

Proof: According to Theorem 2, given $\delta > 0$ we can find a $n_0(\delta)$ such that for all $n \geq n_0$ there is a storage protocol with rate constraint (ϕ, ψ) such that

$$\tfrac{1}{n} \log |\mathcal{M}_n| = \eta C(W) - \epsilon$$

for $\delta > \epsilon > 0$ and

$$\tfrac{1}{n} \log |\mathcal{D}_n| = \max_{\substack{U\colon U-X-Y \\ I(U;X) \leq \eta C(W) - \delta}} I(U;Y).$$

For n_0 large enough there also is a channel code (f, g), $f\colon \mathcal{M}_n \to \mathcal{V}^m$ and $g\colon \mathcal{Z}^m \to \mathcal{M}_n$, (to account for the imperfect storage medium) such that

$$W^m(g^{-1}(\bar{m}) | f(\bar{m})) \geq 1 - \epsilon$$

for all $\bar{m} \in \mathcal{M}_n$ as

$$\begin{aligned} &\tfrac{1}{m} \log |\mathcal{M}_n| = \tfrac{n}{m} \tfrac{1}{n} \log |\mathcal{M}_n| \\ &= \tfrac{n}{\lceil \eta n \rceil} (\eta C(W) - \epsilon) \leq C(W) - \tfrac{\epsilon}{\eta}. \end{aligned}$$

We define the imperfect storage protocol (ϕ_n, ψ_n) for all $(x^n, y^n, d_n, z^m) \in \mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{D}_n \times \mathcal{Z}^m$ as

$$\begin{aligned} \phi_n(x^n, d_n) &= f(\phi(x^n, d_n)) \\ \psi_n(y^n, z^m) &= \psi(y^n, g(z^m)). \end{aligned}$$

Using this protocol we have $I(V^m; D_n) \leq I(M_n; D_n) \leq \delta$ and $\Pr(D_n \neq \hat{D}_n) \leq 2\delta$. We also have

$$\tfrac{1}{n} \log |\mathcal{D}_n| \geq \max_{\substack{U\colon U-X-Y \\ I(U;X) \leq \eta C(W)}} I(U;Y) - \bar{\delta}(\delta).$$

This follows from the continuity of $C_S(P_{XY}, L)$ in L.

For the converse consider

$$\begin{aligned} &\log |\mathcal{D}_n| \\ &\leq \sum_{i=1}^n I(D_n Z^m X^{i-1}; Y_i) + F + D(P_{D_n} \| U_{\mathcal{D}_n}) + \delta, \end{aligned} \quad (8)$$

which is derived as in the converse proof of Theorem 2, with M replaced by Z^m, see (11). Now consider RVs VZ with $P_{VZ} \in \mathcal{P}(\mathcal{V} \times \mathcal{Z})$ such that $I(V;Z) = \max_{P_V \in \mathcal{P}(\mathcal{V})} I(P_V, W)$. We have

$$I(D_n X^n; Z^m) \leq I(V^m; Z^m) \leq m I(V;Z)$$

from the data processing inequality and the fact that the noisy channel is a DMC. (To see this consider $P_{V^m Z^m}$ which implies $Z_i - V_i - V_1^{i-1} V_{i+1}^m Z_1^{i-1} Z_{i+1}^m$ for all i. So

$$I(V^m; Z^m) \leq \sum_{i=1}^m H(Z_i) - H(Z_i | V^m Z^{i-1}) = \sum_{i=1}^m I(V_i; Z_i)$$

which implies the bound above.) Now consider (for $i \in \{1, \cdots, n\}$)

$$\begin{aligned} &I(Z^m; X_i | D_n X^{i-1}) \\ &= H(X_i | D_n X^{i-1}) - H(X_i | Z^m D_n X^{i-1}) \\ &= H(X_i) - H(X_i | Z^m D_n X^{i-1}) \\ &= I(Z^m D_n X^{i-1}; X_i). \end{aligned}$$

Using this equality we get

$$\begin{aligned} mI(V;Z) &\geq I(D_n X^n; Z^m) \\ &= I(D_n; Z^m) + I(X^n; Z^m | D_n) \\ &= I(D_n; Z^m) + \sum_{i=1}^{n} I(Z^m; X_i | D_n X^{i-1}) \\ &= I(D_n; Z^m) + \sum_{i=1}^{n} I(D_n Z^m X^{i-1}; X_i) \\ &\geq \sum_{i=1}^{n} I(D_n Z^m X^{i-1}; X_i), \end{aligned} \tag{9}$$

where the last expression equals (10) with M replaced by Z^m. From (8) and (9) and using the same steps as in the converse proof of Theorem 2 we get for all $\epsilon > 0$ that there is a RV U with $U - X - Y$ and

$$mI(V;Z) \geq nI(U;X), \qquad \tfrac{1}{n} \log |\mathcal{D}_n| \leq I(U;Y) + \epsilon.$$

So

$$\lceil n\eta \rceil I(V;Z) \geq nI(U;X),$$

which implies

$$(\eta + \tfrac{1}{n}) I(V;Z) \geq I(U;X)$$

for all n. This implies $\eta I(V;Z) \geq I(U;X)$. This concludes the converse proof. ∎

Remark 10. For the maximization in Theorem 4 it suffices to consider alphabets $\mathcal{U}$ with $|\mathcal{U}| \leq |\mathcal{X}| + 1$.

As before we now show the continuity of C_S^η. Consider the tuples $(P_1, W_1), (P_2, W_2) \in \mathcal{P}(\mathcal{X} \times \mathcal{Y}) \times \mathcal{P}(\mathcal{Z}|\mathcal{V})$. We define the distance between these tuples as

$$\begin{aligned} &d_W((P_1, W_1), (P_2, W_2)) \\ &= \|P_1 - P_2\|_{TV} + \max_{v \in \mathcal{V}} \|W_1(\cdot|v) - W_2(\cdot|v)\|_{TV}. \end{aligned}$$

Definition 8. $C_S^\eta \colon \mathcal{P}(\mathcal{X} \times \mathcal{Y}) \times \mathcal{P}(\mathcal{Z}|\mathcal{V}) \to \mathbb{R}_{\geq 0}$ is said to be continuous in $(P, W) \in \mathcal{P}(\mathcal{X} \times \mathcal{Y}) \times \mathcal{P}(\mathcal{Z}|\mathcal{V})$ if for each sequence $(P_n, W_n)_{n \in \mathbb{N}}$, $(P_n, W_n) \in \mathcal{P}(\mathcal{X} \times \mathcal{Y}) \times \mathcal{P}(\mathcal{Z}|\mathcal{V})$ for all $n \in \mathbb{N}$, with

$$\lim_{n \to \infty} d_W((P, W), (P_n, W_n)) = 0$$

we have

$$\lim_{n \to \infty} C_S^\eta(P_n, W_n) = C_S^\eta(P, W).$$

Theorem 5. $C_S^\eta \colon \mathcal{P}(\mathcal{X} \times \mathcal{Y}) \times \mathcal{P}(\mathcal{Z}|\mathcal{V}) \to \mathbb{R}_{\geq 0}$ is continuous on its domain.

Proof: We know that $C_S^\eta(P, W) = C_S(P, \eta C(W))$, cf. Remark 9. So $C_S^\eta(P, W)$ is a composition $f_1 \circ f_2^\eta$ of two functions f_1 and f_2^η, namely $f_1 \colon \mathcal{P}(\mathcal{X} \times \mathcal{Y}) \times \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$, $f_1(P, L) = C_S(P, L)$ and $f_2^\eta \colon \mathcal{P}(\mathcal{X} \times \mathcal{Y}) \times \mathcal{P}(\mathcal{Z}|\mathcal{V}) \to \mathcal{P}(\mathcal{X} \times \mathcal{Y}) \times \mathbb{R}_{\geq 0}$, $f_2^\eta(P, W) = (P, \eta C(W))$.

From Theorem 3 we know that f_1 is continuous. We also know that the Shannon capacity $C(W)$ is continuous, cf. for example [22, p. 211]. So f_2^η is continuous too. As the composition of continuous functions is continuous, the desired result follows. ∎

V. Super Activation

As discussed before, the phenomenon of super activation is of practical interest. For example in the context of medium access control and resource allocation, super activation can be used profitable. As super activation means that parallel resources which are useless when used separately become useful when used jointly, joint processing can lead to significant better performance compared to separate processing.

In order to show that super activation occurs for a specific scenario, we have to show that there exists an example of parallel resources where the joint processing of the resouces yields a capacity larger than zero, but where the capacities of each individual resource are zero. We now consider super activation in the context of the secure storage setting. Consider the parallel resources corresponding to $P_{XY}^1, P_{XY}^2 \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$ and $W_1, W_2 \in \mathcal{P}(\mathcal{Z}|\mathcal{V})$ respectively, i.e. $P_{X_1Y_1} \otimes P_{X_2Y_2}$ and $W_1 \otimes W_2$. In this context we mean by super activation that we can choose $P_{X_1Y_1}$, $P_{X_2Y_2}$, W_1 and W_2 such that $C_S^\eta(P_{X_1Y_1}, W_1) = 0$, $C_S^\eta(P_{X_2Y_2}, W_2) = 0$ but $C_S^\eta(P_{X_1Y_1} \otimes P_{X_2Y_2}, W_1 \otimes W_2) > 0$.

Remark 11. It is not a restriction that we assume that the statistics of the independent resources are defined on the same alphabets. If the alphabets are different, we can simply take the union of the alphabets as the new alphabet.

Theorem 6. The phenomenon of super activation occurs for C_S^η for all $\eta > 0$.

Remark 12. As the secure storage capacity without a rate constraint on the helper message is $C_S(P_{XY}, \infty) = I(X;Y)$, we have for RVs $X_1X_2Y_1Y_2$ with $P_{X_1Y_1X_2Y_2} = P_{X_1Y_1} \otimes P_{X_2Y_2}$, $P_{X_1Y_1}, P_{X_2Y_2} \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$ that

$$\begin{aligned} I(X_1X_2; Y_1Y_2) &= H(X_1X_2) + H(Y_1Y_2) - H(X_1X_2Y_1Y_2) \\ &= H(X_1) + H(X_2) + H(Y_1) + H(Y_2) \\ &\qquad - H(X_1Y_1) - H(X_2Y_2) \\ &= I(X_1;Y_1) + I(X_2;Y_2) \end{aligned}$$

and thus

$$C_S(P_{X_1Y_1} \otimes P_{X_2Y_2}, \infty) = C_S(P_{X_1Y_1}, \infty) + C_S(P_{X_2Y_2}, \infty),$$

i.e. we have additivity in the case of no rate constraint. Comparing this to Theorem 6 we conclude that restricting resources, as is done here for the rate of the helper message, can have a great impact on the capacity and its behaviour as a function of the system parameters.

Proof: Consider $P_{X_1Y_1}, P_{X_2Y_2} \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$ and $W_1, W_2 \in \mathcal{P}(\mathcal{Z}|\mathcal{V})$. Assume $\mathcal{X} = \mathcal{Y}$, $P_{X_2Y_2}$ is a product distribution and $P_{X_1Y_1}(x, y) = \frac{1}{|\mathcal{X}|}$ for $x = y$. Additionally,

assume that $\max_{P_V \in \mathcal{P}(\mathcal{V})} I(P_V, W_1) = C(W_1) = 0$ but $\max_{P_V \in \mathcal{P}(\mathcal{V})} I(P_V, W_2) = C(W_2) > 0$.

We have

$$C_S^{\eta}(P_{X_1Y_1}, W_1) = \max_U I(U;Y_1) \overset{a)}{=} \max_U I(U;X_1)$$

where the maximization is over all RVs U such that $I(U;X_1) \leq \eta C(W_1)$ and $U - X_1 - Y_1$ and $a)$ follows from our assumption on $P_{X_1Y_1}$. From our assumption on W_1 the rightmost term equals $\max_U I(U;X_1)$, where the maximization is over all RVs U such that $I(U;X_1) = 0$ and $U - X_1 - Y_1$, which equals 0.

We also have

$$C_S^{\eta}(P_{X_2Y_2}, W_2) = \max_U I(U;Y_2)$$

where the maximization is over all RVs U such that $I(U;X_2) \leq \eta C(W_2)$ and $U - X_2 - Y_2$. This expression can be upper bounded by $I(X_2;Y_2)$ which follows from $U - X_2 - Y_2$. From our assumption on $P_{X_2Y_2}$ this equals 0.

We know that $C(W_1 \otimes W_2) = C(W_1) + C(W_2)$ (see for example [22, Exercise 6.14]).

We thus have $C(W_1 \otimes W_2) = C(W_2) > 0$ due to our assumptions on W_1 and W_2.

Now consider

$$C_S^{\eta}(P_{X_1Y_1} \otimes P_{X_2Y_2}, W_1 \otimes W_2) = \max_{U_1,U_2} I(U_1U_2; Y_1Y_2)$$

where the maximization is over all RVs U_1, U_2 such that $I(U_1U_2; X_1X_2) \leq \eta C(W_1 \otimes W_2) = \eta C(W_2)$ and $U_1U_2 - X_1X_2 - Y_1Y_2$. This expression can be lower bounded by $\max_{U_1,U_2} I(U_1U_2;Y_1Y_2)$ where the maximization is over all RVs U_1, U_2 such that $I(U_1U_2;X_1X_2) \leq \eta C(W_2)$ and

$$\begin{aligned} &P_{U_1U_2X_1X_2Y_1Y_2}(u_1,u_2,x_1,x_2,y_1,y_2) \\ &\quad = P_{XY}^1(x_1,y_1)P_{XY}^2(x_2,y_2)P_{U_1|X_1}(u_1|x_1)P_{U_2|X_2}(u_2|x_2) \end{aligned}$$

for all $(u_1,u_2,x_1,x_2,y_1,y_2) \in \mathcal{U}^2 \times \mathcal{X}^2 \times \mathcal{Y}^2$. For these $P_{U_1U_2X_1X_2Y_1Y_2}$ we see, using the chain rule, that

$$\begin{aligned} I(U_1U_2;Y_1Y_2) &= I(U_1;Y_1) + I(U_2;Y_2) \\ I(U_1U_2;X_1X_2) &= I(U_1;X_1) + I(U_2;X_2). \end{aligned}$$

So we have

$$\begin{aligned} &C_S^{\eta}(P_{X_1Y_1} \otimes P_{X_2Y_2}, W_1 \otimes W_2) \\ &\qquad \geq \max_{U_1,U_2} I(U_1;Y_1) + I(U_2;Y_2) \end{aligned}$$

where the maximization is over all RVs U_1, U_2 such that $I(U_1;X_1) + I(U_2;X_2) \leq \eta C(W_2)$ and

$$\begin{aligned} &P_{U_1U_2X_1X_2Y_1Y_2}(u_1,u_2,x_1,x_2,y_1,y_2) \\ &\quad = P_{XY}^1(x_1,y_1)P_{XY}^2(x_2,y_2)P_{U_1|X_1}(u_1|x_1)P_{U_2|X_2}(u_2|x_2) \end{aligned}$$

for all $(u_1,u_2,x_1,x_2,y_1,y_2) \in \mathcal{U}^2 \times \mathcal{X}^2 \times \mathcal{Y}^2$. From our assumptions on $P_{X_1Y_1}$, $P_{X_2Y_2}$ and $U_2 - X_2 - Y_2$ this lower bound equals $\max_{U_1} I(U_1;X_1)$ where the maximization is over all RVs U_1 such that $I(U_1;X_1) \leq \eta C(W_2)$. As $C(W_2) > 0$ this expression is greater than 0. ∎

Super activation for channels has been shown for quantum channels for the first time in [26], [27] for different scenarios. Here the channel is modelled as an i.i.d. quantum channel. This behaviour of i.i.d. quantum channels has long been conjectured in quantum physics and both works contribute fundamentally to quantum physics and resulted in many follow up works as discussed in great detail by Renato Renner in his plenary talk at the international congress of mathematical physics, ICMP 2012, and Charles Bennett at the international symposium on information theory, ISIT 2019.

In quantum physics it has been assumed that super activation is a special property of quantum systems and that for classical communication this behaviour can not appear. This perception is disproved in [28] for the first time. Here, it is shown that for wiretap channels with an active attacker, i.e., a jammer, super activation occurs for the secrecy capacity. Of course this result is of interest for physical layer security where the influence of jammers on secure communication is a significant field of study. But in general the active attacker can not be modelled using an i.i.d. model. In this respect we know from [28] that super activation is indeed possible in classical information theory, but these models are non-i.i.d. models.

In this work, we present the first classical communication scenario where super activation can be shown for i.i.d. models. Thus, the assumption on super activation being a special feature of quantum information theory can even be disproved with a classical i.i.d. model.

There is another interesting observation for the communication scenario considered in this work. The occurance of super activation for secure communication over wiretap channels with a jammer is strongly connected to the discontinuity of the secrecy capacity, which results from the possible jamming attacks. In contrast, the capacity for transmission of quantum information over i.i.d. quantum channels allows for super activation (as discussed above) but is a continuous function of the quantum channel parameters. The results of this work show that for classical i.i.d. communication scenarios super activation can occur together with a continuous capacity function. This means we have the same properties for a classical communication scenario as for the quantum channel considered in [26], [27]. In this respect, there is no principle difference between quantum i.i.d. communication scenarios and classical i.i.d. communication scenarios.

VI. Acknowledgement

H. Boche would like to thank Charles Bennett for his valuable remarks concerning super activation and quantum information theory at ISIT 2019.

Appendix
Proof of Theorem 2

For the achievability part we choose the RV U. From Theorem 1 we know that for all $n \geq n_0(\delta)$ there is a SK generation protocol (f_n, g_n), $f_n \colon \mathcal{X}^n \to \mathcal{K}_n \times \mathcal{M}_n$ and $g_n \colon \mathcal{Y}^n \times \mathcal{M}_n \to \mathcal{K}_n$, with

$$\begin{aligned} \tfrac{1}{n} \log |\mathcal{K}_n| &= I(U;Y) - \delta \\ \tfrac{1}{n} \log |\mathcal{M}_n| &= I(U;X|Y) + \delta \end{aligned}$$

for $\delta > 0$ and (1), (2) and (3) hold (where the DMMS is the DMMS from the storage model). Define the following storage

protocol (ϕ_n, ψ_n), $\phi_n \colon \mathcal{X}^n \times \mathcal{D}_n \to \mathcal{M}_n^{com}$, where $\mathcal{M}_n^{com} = \mathcal{M}_n \times \mathcal{D}_n$, and $\psi_n \colon \mathcal{Y}^n \times \mathcal{M}_n^{com} \to \mathcal{D}_n$, for $\mathcal{D}_n = \mathcal{K}_n$.

$$\begin{aligned}&\phi_n(x^n, d_n) = \Big(p_2\big(f_n(x^n)\big), p_1\big(f_n(x^n)\big) \oplus d_n\Big)\\ &\psi_n(y^n, m_n^{com})\\ &\quad = p_2\big(m_n^{com}\big) \oplus \bigg(- g_n\Big(y^n, p_1\big(m_n^{com}\big)\Big)\bigg)\end{aligned}$$

for all $(x^n, y^n, d_n, m_n^{com}) \in \mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{D}_n \times \mathcal{M}_n^{com}$, where we define the commutative group $(\mathcal{D}_n, \oplus)$, cf. [22, Proposition 17.1] and write $p_i(m_n^{com})$, $i \in \{1, 2\}$ for the ith component of m_n^{com}. This means the encoder ϕ_n works as follows. We generate a SK and a corresponding helper message using f_n and encrypt the data to be stored on the database with this SK. We store the helper message for SK generation together with the encrypted data on the database. For the decoder ψ_n we reconstruct the SK using g_n and use it to decrypt the data. We now analyse this storage protocol. For the error probability we get

$$\begin{aligned}&\Pr(D_n = \hat{D}_n)\\ &\quad = \Pr\Big(p_1\big(f_n(X^n)\big) = g_n\Big(Y^n, p_2\big(f_n(X^n)\big)\Big)\Big) \geq 1 - \delta.\end{aligned}$$

We also have

$$\tfrac{1}{n} \log |\mathcal{D}_n| = \tfrac{1}{n} \log |\mathcal{K}_n| = I(U;Y) - \delta.$$

For the secrecy requirement we get

$$\begin{aligned}&I(M_n, D_n \oplus K; D_n)\\ &\qquad = I(D_n \oplus K; D_n) + I(M_n; D_n | D_n \oplus K_n).\end{aligned}$$

It holds that

$$H(D_n \oplus K_n | D_n) = \sum_{d_n \in \mathcal{D}_n} P_{D_n}(d_n) H(d_n \oplus K_n).$$

As $f_{d_n} \colon \mathcal{K}_n \to \mathcal{K}_n$, $f_{d_n}(k_n) = d_n \oplus k_n$ for all $k_n \in \mathcal{K}_n$, is bijective for all $d_n \in \mathcal{D}_n$ we have $H(d_n \oplus K_n) = H(K_n)$ for all $d_n \in \mathcal{D}_n$. So

$$H(D_n \oplus K_n | D_n) = H(K_n) \geq \log |\mathcal{K}_n| - \delta.$$

As $H(D_n \oplus K_n) \leq \log |\mathcal{K}_n|$ we have

$$I(D_n \oplus K_n; D_n) = H(D_n \oplus K_n) - H(D_n \oplus K_n | D_n) \leq \delta.$$

Now consider

$$\begin{aligned}&I(M_n; D_n | D_n \oplus K_n)\\ &\qquad = H(M_n | D_n \oplus K_n) - H(M_n | D_n \oplus K_n, D_n).\end{aligned}$$

We have

$$\begin{aligned}&H(M_n | D_n \oplus K_n, D_n)\\ &\qquad = H(M_n | D_n \oplus K_n, D_n, -D_n \oplus D_n \oplus K_n)\\ &\qquad = H(M_n | D_n K_n) = H(M_n | K_n)\end{aligned}$$

where for the last step we use that D_n is independent of $M_n K_n$. So

$$\begin{aligned}&I(M_n; D_n | D_n \oplus K_n)\\ &\qquad \leq H(M_n) - H(M_n | K_n) = I(M_n; K_n) \leq \delta.\end{aligned}$$

Therefore we have

$$I(M_n, D_n \oplus K; D_n) \leq 2\delta.$$

For the rate of the helper message we get

$$\begin{aligned}\tfrac{1}{n} \log |\mathcal{M}_n^{com}| &= \tfrac{1}{n} \log |\mathcal{M}_n| + \tfrac{1}{n} \log |\mathcal{K}_n|\\ &= I(U; X|Y) + I(U;Y) = I(U;X).\end{aligned}$$

So the storage protocol (ϕ_n, ψ_n) satisfies

$$\tfrac{1}{n} \log |\mathcal{D}_n| \geq I(U;Y) - \delta, \quad \tfrac{1}{n} \log |\mathcal{M}_n^{com}| \leq I(U;X) + \delta$$

and $\Pr(D_n = \hat{D}_n) \geq 1 - \delta$ and $I(M_n^{com}; D_n) \leq \delta$ for $\delta > 0$ and n large enough for all $P_{U|X} \in \mathcal{P}(\mathcal{U}|\mathcal{X})$. So given a $L \geq 0$, when we want

$$\tfrac{1}{n} \log |\mathcal{M}_n^{com}| \leq L + \delta,$$

we can choose all U such that $I(U;X) \leq L$ which concludes the achievability proof.

For the converse, consider

$$\begin{aligned}\log |\mathcal{M}| &\geq H(M)\\ &= I(MD_n; X^n) - H(D_n|M) + H(MD_n|X^n)\\ &= I(MD_n; X^n) - H(D_n|M)\\ &+ H(D_n|X^n) + H(M|D_n X^n)\\ &= I(MD_n; X^n) + I(D_n; M) \geq I(MD_n; X^n)\\ &= \sum_{i=1}^n I(MD_n; X_i | X^{i-1}) = \sum_{i=1}^n I(MD_n X^{i-1}; X_i)\end{aligned} \tag{10}$$

and

$$\begin{aligned}\log |\mathcal{D}_n| &= H(D_n) + D(P_{D_n} \| U_{\mathcal{D}_n})\\ &= I(D_n; \hat{D}_n) + H(D_n|\hat{D}_n) + D(P_{D_n} \| U_{\mathcal{D}_n})\\ &\leq I(D_n; MY^n) + F + D(P_{D_n} \| U_{\mathcal{D}_n})\\ &\leq I(D_n; M) + I(D_n M; Y^n) + F + D(P_{D_n} \| U_{\mathcal{D}_n})\\ &\leq \sum_{i=1}^n I(D_n M; Y_i | Y^{i-1}) + F + D(P_{D_n} \| U_{\mathcal{D}_n}) + \delta\\ &= \sum_{i=1}^n I(D_n M Y^{i-1}; Y_i) + F + D(P_{D_n} \| U_{\mathcal{D}_n}) + \delta,\end{aligned}$$

where we use Fano's inequality, the data processing inequality and the strong secrecy requirement that the storage protocol satisfies. (From Fano's inequality $F = \delta \log(|\mathcal{D}_n| - 1) + h(\delta)$, where h is the binary entropy.) As $M - X^n D_n - Y^n$ we have $M - X^{i-1} D_n X_i Y_i - Y^{i-1}$ which implies $Y_i - M X^{i-1} D_n - Y^{i-1}$. So

$$\begin{aligned}I(D_n M Y^{i-1}; Y_i) &\leq I(D_n M Y^{i-1} X^{i-1}; Y_i)\\ &= I(D_n M X^{i-1}; Y_i)\end{aligned}$$

and thus

$$\log |\mathcal{D}_n| \leq \sum_{i=1}^n I(D_n M X^{i-1}; Y_i) + F + D(P_{D_n} \| U_{\mathcal{D}_n}) + \delta. \tag{11}$$

We now define $U_i = D_n M X^{i-1}$. Consider the RV J that is uniformly distributed on $\mathcal{J} = \{1, \cdots, n\}$ and independent

of $X^nY^nD_n$. We have $M - D_nX^n - Y^n$ which implies $D_nMX^{i-1} - X_i - Y_i$ for all $i \in \{1, \cdots, n\}$. So we have $U_i - X_i - Y_i$. We also have

$$\begin{aligned}\sum_{i=1}^{n} I(U_i;Y_i) &= n\sum_{i=1}^{n} \tfrac{1}{n} I(U_i;Y_i) \\ &= n\sum_{i=1}^{n} P_J(i) I(U_i;Y_i) = nI(U_J;Y_J|J) \\ &= n(H(Y_J|J) - H(Y_J|U_JJ)) \\ &\overset{a)}{=} nI(Y_J;U_JJ) = nI(\bar{Y};\bar{U})\end{aligned}$$

and equivalently

$$\sum_{i=1}^{n} I(U_i;X_i) = nI(\bar{X};\bar{U})$$

where we define $\bar{Y} = Y_J$, $\bar{X} = X_J$ and $\bar{U} = U_JJ$. For $a)$ we use the fact that

$$P_{X_JJ}(x,i) = \tfrac{1}{n} P_{X_i}(x) = P_X(x)\tfrac{1}{n}$$

and thus

$$P_{X_J}(x) = \sum_{i=1}^{n} P_{X_JJ}(x,i) = P_X(x).$$

So

$$H(X_J|J) = \sum_{i=1}^{n} \tfrac{1}{n} H(X_i) = H(P_X) = H(X_J)$$

(and equivalently $H(Y_J|J) = H(Y_J)$). We also have

$$\begin{aligned}P_{\bar{X}\bar{Y}}(x,y) &= P_{X_JY_J}(x,y) \\ &= \sum_{i=1}^{n} P_{X_JY_JJ}(x,y,i) = \sum_{i=1}^{n} P_{X_iY_i}(x,y)\tfrac{1}{n} \\ &= \sum_{i=1}^{n} P_{XY}(x,y)\tfrac{1}{n} = P_{XY}(x,y)\end{aligned}$$

and $\bar{U} - \bar{X} - \bar{Y}$ as

$$\begin{aligned}P_{\bar{U}\bar{X}\bar{Y}}((j,u_j),x,y) &= P_{JU_jX_jY_j}((j,u_j),x,y) \\ &= P_J(j) P_{U_jX_jY_j}(u_j,x,y) \\ &= P_J(j) P_{U_j|X_j}(u_j,x) P_{X_jY_j}(x,y) \\ &= P_{JU_j|X_j}((j,u_j)|x) P_{XY}(x,y) \\ &= P_{\bar{U}|\bar{X}}((j,u_j)|x) P_{\bar{X}\bar{Y}}(x,y).\end{aligned}$$

So if we choose n large enough and δ small enough, for every $\epsilon > 0$ there is RV U with $U - X - Y$ and

$$\tfrac{1}{n}\log|\mathcal{D}_n| \le I(U;Y) + \epsilon \quad L + \epsilon \ge \tfrac{1}{n}\log|\mathcal{M}| \ge I(U;X).$$

This completes the converse proof.

REFERENCES

[1] Y. Polyanskiy, H. V. Poor, and S. Verdú, "Channel coding rate in the finite blocklength regime," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, May 2010.

[2] G. Fettweis *et al.*, "The Tactile Internet," *ITU-T Technology Watch Report*, 2014.

[3] "IEEE Communications Society Tactile Internet Emerging Technical Subcommittee," http://ti.committees.comsoc.org/standardisation/, Accessed 15 Oct. 2018.

[4] Y. Liang, H. V. Poor, and S. Shamai (Shitz), *Information Theoretic Security*. Now Publishers, Inc., 2009, vol. 5, no. 4–5.

[5] M. Bloch and J. Barros, *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.

[6] R. F. Schaefer, H. Boche, A. Khisti, and H. V. Poor, *Information Theoretic Security and Privacy of Information Systems*. Cambridge University Press, 2017.

[7] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography–part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

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

[9] T. Ignatenko and F. M. J. Willems, *Biometric Security from an Information-Theoretical Perspective*. Now Publishers, Inc., 2012, vol. 7, no. 2–3.

[10] L. Lai, S.-W. Ho, and H. V. Poor, "Privacy–security trade-offs in biometric security systems—part I: Single use case," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 122–139, Mar. 2011.

[11] O. Günlü, *Key Agreement with Physical Unclonable Functions and Biometric Identifiers*. Dissertation, Inst. Comm. Eng., TUM, 2019.

[12] H. Boche, R. F. Schaefer, and H. V. Poor, "On the computability of the secret key capacity under rate constraints," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Proc.*, Brighton, United Kingdom, May 2019.

[13] H. Boche, R. F. Schaefer, S. Baur, and H. V. Poor, "On the algorithmic computability of the secret key and authentication capacity under channel, storage, and privacy leakage constraints," *IEEE Trans. Signal Process.*, accepted for publication.

[14] G. Bassi, P. Piantanida, and S. Shamai (Shitz), "Secret key generation over noisy channels with common randomness," in *Proc. IEEE Int. Symp. Inf. Theory*, Barcelona, Spain, Jul. 2016, pp. 510–514.

[15] R. F. Schaefer, H. Boche, and H. V. Poor, "Secure communication under channel uncertainty and adversarial attacks," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1796–1813, Oct. 2015.

[16] H. Boche, R. F. Schaefer, and H. V. Poor, "Analytical properties of shannon's capacity of arbitrarily varying channels under list decoding: Super-additivity and discontinuity behavior," *Probl. Inf. Transmission*, vol. 54, no. 3, pp. 199–228, Jul. 2018.

[17] C. E. Shannon, "The zero error capacity of a noisy channel," *IRE Trans. Inf. Theory*, vol. 2, no. 3, pp. 8–19, Sep. 1956.

[18] L. Lovász, "On the shannon capacity of a graph," *IEEE Trans. Inf. Theory*, vol. 25, no. 1, pp. 1–7, Jan. 1979.

[19] W. Haemers, "On some problems of lovász concerning the shannon capacity of a graph," *IEEE Trans. Inf. Theory*, vol. 25, no. 2, pp. 231–232, Jan. 1979.

[20] N. Alon, "The shannon capacity of a union," *Combinatorica*, vol. 18, no. 3, pp. 301–310, Mar. 1998.

[21] J. Nötzel, M. Wiese, and H. Boche, "The arbitrarily varying wiretap channel—secret randomness, stability, and super-activation," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3504–3531, Jun. 2016.

[22] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge University Press, 2011.

[23] S. Baur and H. Boche, "Robust authentication and data storage with perfect secrecy," in *Proc. IEEE Int. Conf. Computer Communications Workshops*, Atlanta, GA, USA, May 2017, pp. 553–558.

[24] ——, "Storage of General Data Sources on a Public Database with Security and Privacy Constraints," in *Proc. IEEE Conf. Communications Network Sec.*, Las Vegas, NV, USA, Oct. 2017, pp. 555–559.

[25] H. S. Witsenhausen, "On sequences of pairs of dependent random variables," *SIAM Journal on Applied Mathematics*, vol. 28, no. 1, pp. 100–113, 1975.

[26] G. Smith and J. Yard, "Quantum communication with zero-capacity channels," *Science*, vol. 321, no. 5897, pp. 1812–1815, 2008.

[27] G. Smith, J. A. Smolin, and J. Yard, "Quantum communication with gaussian channels of zero quantum capacity," *Nature Photonics*, vol. 5, no. 10, p. 624, 2011.

[28] H. Boche and R. F. Schaefer, "Capacity results and super-activation for wiretap channels with active wiretappers," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 9, pp. 1482–1496, 2013.

Sebastian Baur received the B.S. and M.S. degree in electrical engineering from the Technische Universität München in 2013 and 2016, respectively. He is currently pursuing a Dr.-Ing. degree in electrical engineering at the Institute of Theoretical Information Technology at the Technische Universität München.

Holger Boche (M'04–SM'07–F'11) received the Dipl.-Ing. and Dr.-Ing. degrees in electrical engineering from the Technische Universität Dresden, Dresden, Germany, in 1990 and 1994, respectively. He graduated in mathematics from the Technische Universität Dresden in1992. From 1994 to 1997, he did Postgraduate studies in mathematics at the Friedrich-Schiller-Universität Jena, Jena, Germany. He received his Dr. rer. nat. degree in pure mathematics from the Technische Universität Berlin, Berlin, Germany, in 1998. In 1997, he joined the Heinrich-Hertz-Institut (HHI) für Nachrichtentechnik Berlin, Berlin, Germany. Starting in 2002, he was a Full Professor for mobile communication networks with the Institute for Communications Systems, Technische Universität Berlin. In 2003, he became Director of the Fraunhofer German-Sino Lab for Mobile Communications, Berlin, Germany, and in 2004 he became the Director of the Fraunhofer Institute for Telecommunications (HHI), Berlin, Germany. Since October 2010 he has been with the Institute of Theoretical Information Technology and Full Professor at the Technische Universität München, Munich, Germany. Since 2014 he has been a member and honorary fellow of the TUM Institute for Advanced Study, Munich, Germany. Since May 2018, he has been one of two directors of the national center for Quantum Engineering (ZQE) at the Technical University of Munich. Since November 2018 he has been a member of the Munich Center for Quantum Science and Technology (MCQST), which is funded by the German Research Foundation (DFG - Deutsche Forschungsgemeinschaft) under Germany's Excellence Strategy EXC-2111-390814868. He was a Visiting Professor with the ETH Zurich, Zurich, Switzerland, during the 2004 and 2006 Winter terms, and with KTH Stockholm, Stockholm, Sweden, during the 2005 Summer term. Prof. Boche is a Member of IEEE Signal Processing Society SPCOM and SPTM Technical Committee. He was elected a Member of the German Academy of Sciences (Leopoldina) in 2008 and of the Berlin Brandenburg Academy of Sciences and Humanities in 2009. He received the Research Award "Technische Kommunikation" from the Alcatel SEL Foundation in October 2003, the "Innovation Award" from the Vodafone Foundation in June 2006, and the Gottfried Wilhelm Leibniz Prize from the Deutsche Forschungsgemeinschaft (German Research Foundation) in 2008. He was co-recipient of the 2006 IEEE Signal Processing Society Best Paper Award and recipient of the 2007 IEEE Signal Processing Society Best Paper Award. He was the General Chair of the Symposium on Information Theoretic Approaches to Security and Privacy at IEEE GlobalSIP 2016. Among his publications is the recent book *Information Theoretic Security and Privacy of Information Systems* (Cambridge University Press).

Rafael F. Schaefer (S'08–M'12–SM'17) received the Dipl.-Ing. degree in electrical engineering and computer science from the Technische Universität Berlin, Germany, in 2007, and the Dr.-Ing. degree in electrical engineering from the Technische Universität München, Germany, in 2012. From 2013 to 2015, he was a Post-Doctoral Research Fellow with Princeton University. Since 2015, he has been an Assistant Professor with the Technische Universität Berlin. Among his publications is the recent book *Information Theoretic Security and Privacy of Information Systems* (Cambridge University Press, 2017). He was a recipient of the VDE Johann-Philipp-Reis Prize in 2013. He received the best paper award of the German Information Technology Society (ITG-Preis) in 2016. He was one of the exemplary reviewers of the IEEE COMMUNICATION LETTERS in 2013. He is currently an Associate Editor of the IEEE TRANSACTIONS OF COMMUNICATIONS and a Member of the IEEE Information Forensics and Security Technical Committee.

H. Vincent Poor (S'72, M'77, SM'82, F'87) received the Ph.D. degree in EECS from Princeton University in 1977. From 1977 until 1990, he was on the faculty of the University of Illinois at Urbana-Champaign. Since 1990 he has been on the faculty at Princeton, where he is currently the Michael Henry Strater University Professor of Electrical Engineering. During 2006 to 2016, he served as Dean of Princeton's School of Engineering and Applied Science. He has also held visiting appointments at several other universities, including most recently at Berkeley and Cambridge. His research interests are in the areas of information theory and signal processing, and their applications in wireless networks, energy systems and related fields. Among his publications in these areas is the recent book *Multiple Access Techniques for 5G Wireless Networks and Beyond* (Springer, 2019).

Dr. Poor is a member of the National Academy of Engineering and the National Academy of Sciences, and is a foreign member of the Chinese Academy of Sciences, the Royal Society, and other national and international academies. Recent recognition of his work includes the 2019 ASEE Benjamin Garver Lamme Award, and a D.Eng. *honoris causa* from the University of Waterloo, also awarded in 2019.