Secure Estimation and Zero-Error Secrecy Capacity

Moritz Wiese, *Member, IEEE*, Tobias J. Oechtering, *Senior Member, IEEE*,
Karl Henrik Johansson, *Fellow, IEEE*, Panagiotis Papadimitratos, *Member, IEEE*,
Henrik Sandberg, *Member, IEEE*, and Mikael Skoglund, *Senior Member, IEEE*

***Abstract*—We study the problem of securely estimating the states of an unstable dynamical system subject to nonstochastic disturbances. The estimator obtains all its information through an *uncertain channel*, which is subject to nonstochastic disturbances as well, and an eavesdropper obtains a disturbed version of the channel inputs through a second uncertain channel. An encoder observes and block encodes the states in such a way that, upon sending the generated codeword, the estimator's error is bounded and a security criterion is satisfied, thereby ensuring that the eavesdropper obtains as little state information as possible. Two security criteria are considered and discussed with the help of a numerical example. A sufficient condition on the *uncertain wiretap channel*, i.e., the pair formed by the uncertain channel from the encoder to the estimator and the uncertain channel from the encoder to the eavesdropper is derived, which ensures that a bounded estimation error and security are achieved. This condition is also shown to be necessary for a subclass of uncertain wiretap channels. To formulate the condition, the zero-error secrecy capacity of uncertain wiretap channels is introduced, i.e., the maximal rate at which data can be transmitted from the encoder to the estimator in such a way that the eavesdropper is unable to reconstruct the transmitted data. Finally, the zero-error secrecy capacity of uncertain wiretap channels is studied.**

***Index Terms*—Secure state estimation, uncertain wiretap channel, zero-error secrecy capacity.**

Manuscript received July 14, 2017; revised December 21, 2017; accepted April 13, 2018. Date of publication June 21, 2018; date of current version February 26, 2019. This work was supported in part by ACCESS Linnaeus Centre, and in part by the Swedish Research Council (VR) project CLONES under Grant E0628201. This paper was presented in part at the 2016 IEEE International Symposium on Information Theory in Barcelona, Spain, and at the 55th IEEE Conference on Decision and Control in Las Vegas, NV, USA. Recommended by Associate Editor W. X. Zheng. *(Corresponding author: Moritz Wiese.)*

M. Wiese was with the Department for Communication Theory, KTH Royal Institute of Technology, Stockholm SE-10044 Sweden. He is now with the Lehrstuhl für Theoretische Informationstechnik, Technische Universität München, Munich 80333, Germany (e-mail: wiese@tum.de).

T. J. Oechtering and M. Skoglund are with the Department for Information Science and Engineering, KTH Royal Institute of Technology, Stockholm SE-10044, Sweden (e-mail: oech@kth.se; skoglund@s3.kth.se).

K. H. Johansson and H. Sandberg are with the Department for Automatic Control, KTH Royal Institute of Technology, Stockholm SE-10044, Sweden (e-mail: kallej@kth.se; hsan@kth.se).

P. Papadimitratos is with the Networked Systems Security Group, KTH Royal Institute of Technology, Stockholm SE-10044, Sweden (e-mail: papadim@kth.se).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TAC.2018.2849620

I. Introduction

With the increasing deployment and growing importance of cyberphysical systems, the question of their security has recently become a focus of research activity in control theory [1]. One central vulnerability of networked control or estimation is the communication channel from the system, which is to be controlled/estimated by the controller/estimator, and possibly the feedback channel. A possible attack on the channels is to actively interfere with transmitted information, with the goal of degrading the control or estimation performance. However, if the state of a system is estimated remotely, e.g., in order to decide on the next control action at a remote controller, another possible attack is eavesdropping. An adversary might have the chance to overhear the transmitted information, to make its own state estimate, and thus obtain sensitive information. For example, if the system processes health information, leakage of its state might breach privacy. If the system is a production line, knowledge of its state could be valuable information for competitors or for criminals. This paper addresses the question of how to protect the transmitted information from such attackers.

We consider an unstable scalar, discrete-time, time-invariant linear system subject to nonstochastic disturbances, where both the initial state and the disturbances are arbitrary elements of a bounded interval. An *estimator* has the goal of estimating the system states in such a way that the supremum over time of the absolute differences between the true state and its estimate is bounded uniformly over all possible system state trajectories. We call this *reliability*. The estimator does not have a direct access to the system states. Instead, an *encoder* observes the system state and is linked to the estimator through an *uncertain channel*, where every input is disturbed in a nonstochastic manner, and the input and output alphabets are possibly finite. The encoder transforms blocks of state observations into codewords using an *encoding function*, while the estimator applies a *decoding function* for estimating the system states from the channel outputs. Together, the encoding and decoding functions form a *transmission scheme*.

Through another, different, uncertain channel, an adversary called the *eavesdropper* obtains a disturbed version of the encoder's channel input, and hence information about the system state. In addition to reliability, our goal is to make the information transmission from the encoder to the estimator secure in such a way that the eavesdropper obtains as little information as possible about the system state, in a sense to be defined. The main question of this paper is regarding conditions under which there exists a transmission scheme such that reliability and security are achieved simultaneously (see Fig. 1).

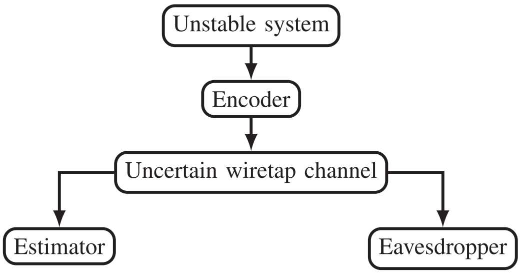

Fig. 1. Unstable system has to be estimated remotely. It obtains the state information through an uncertain wiretap channel. The outputs obtained by an eavesdropper at the other channel output need to satisfy an operational security criterion.

Contributions: We introduce the *uncertain wiretap channel*, defined as the pair consisting of the uncertain channel from the encoder to the estimator and the uncertain channel from the encoder to the eavesdropper. We also define the *zero-error secrecy capacity* of the uncertain wiretap channel, which describes the maximal block-encoding data rate, such that not only the estimator can decode the transmitted message, but also at the same time the eavesdropper always has at least two messages, of which the one that was actually transmitted cannot be distinguished. We show that it either equals zero or the zero-error capacity of the uncertain channel between the encoder and the estimator. The latter capacity was introduced by Shannon [2]. By definition, it is the maximal rate at which, using block-encoding, data can be transmitted from the encoder to the estimator through the uncertain channel in such a way that every possible channel output is generated by a unique message. A criterion to distinguish the cases of zero and positive zero-error secrecy capacity can be given in a special case. For the study of the zero-error secrecy capacity of uncertain wiretap channels, we introduce a hypergraph structure on the input alphabet in addition to the graph structure, which is applied in the study of the zero-error capacity of uncertain channels and which also goes back to Shannon's original paper [2].

With these information-theoretic tools, we address the main question formulated earlier. We define two security criteria for a secure estimation. The first, called *d-security*, is that there is no possibility for the eavesdropper to process the data it receives in order to obtain a bounded estimation error. The other security criterion is *v-security*, which requires that the volume of the set of system states at a given time that are possible according to the eavesdropper's information should tend to infinity. We identify a sufficient condition that says that reliability and both d- and v-security are achievable if the zero-error secrecy capacity of the uncertain wiretap channel is strictly larger than the logarithm of the coefficient of the unstable system. In the construction of reliable and d- or v-secure transmission schemes, we separate quantization/estimation from channel coding. We also give bounds on the speed of growth of the eavesdropper's estimation error and of the volume of the set of states at a given time that are possible according to the eavesdropper's information. A necessary condition for the simultaneous achievability of reliability and d- and v-security can be given for a subclass of uncertain wiretap channels.

Related work: Good overviews over the area of estimation and control under information constraints can be found in the introduction of [3] and in [4]. Matveev and Savkin [3] proved that if the system and channel disturbances are stochastic and the estimator's goal is to obtain an almost surely bounded estimation error, the crucial property of the channel is its Shannon zero-error capacity. This led Nair [5] to introduce a nonstochastic information theory for studying the zero-error capacity of uncertain channels and to consider the problem of estimation and control of linear unstable systems, where the information between the sensor and estimator has to be transmitted over an uncertain channel.

There exists a large body of work on information-theoretically secure communication (see [6] and [7]). Stochastic wiretap channels were introduced by Wyner [8]. Security in the context of estimation and control has so far mostly meant security against active adversaries, e.g., as in [9]–[13]. To our knowledge, only Li *et al.* [14] and Tsiamis *et al.* [15] have combined estimation and security against a passive adversary for an unstable system so far. Li *et al.* [14] consider general stochastic disturbances in the system and a stochastic wiretap channel with Gaussian noise and use a nonoperational security criterion based on entropy, whose implications are not immediately clear. Tsiamis *et al.* [15] consider a linear system with Gaussian disturbances and Gaussian observation noise, whereas the stochastic wiretap channel randomly and independently deletes input symbols. As a security criterion, Tsiamis *et al.* [15] require that the eavesdropper's estimation error tends to infinity.

Uncertain channels were introduced by Nair [5] but were previously considered implicitly in the study of the zero-error capacity of channels with stochastic disturbances, as introduced by Shannon [2]. The calculation of the zero-error capacity is known to be a difficult problem, which nowadays is mainly treated in graph theory [16].

Notations: The cardinality of a finite set $\mathcal{A}$ is denoted by $\sharp\,\mathcal{A}$. If $\sharp\,\mathcal{A} = 1$, we call $\mathcal{A}$ a *singleton*. An interval $\mathcal{I}$ will also be written $\mathcal{I} = [\mathcal{I}_{\min}, \mathcal{I}_{\max}]$. We define the length of $\mathcal{I}$ by $|\mathcal{I}|$. For two subsets $\mathcal{A}$ and $\mathcal{B}$ of the real numbers and a scalar λ, we set $\lambda\mathcal{A} + \mathcal{B} := \{\lambda a + b : a \in \mathcal{A}, b \in \mathcal{B}\}$. A sequence $(a(t))_{t=t_0}^{t_1}$ is denoted by $a(t_0 : t_1)$, where t_1 is allowed to equal ∞.

Outline: In Section II, uncertain wiretap channels are introduced and the main results concerning their zero-error secrecy capacity are stated. The problem of secure estimation is formulated and the corresponding results are presented in Section III. In Section IV, the quantizers applied in this paper are introduced and analyzed. This analysis is used in Section V for the proof of the results on secure estimation. Section VI discusses d- and v-security, including a numerical example. After the conclusion in Section VII, Appendix A contains the proofs from Section II and some additional discussion, and Appendix B provides the proofs from Section IV.

II. Uncertain Channels and Uncertain Wiretap Channels

Before we can present the model for secure estimation, we need to introduce the model for data communication between the encoder and receiving parties. This model is the uncertain wiretap channel. Since it is new and some results concerning uncertain wiretap channels are relevant for secure estimation, we devote the complete section to this topic. Our model for secure estimation will be defined in Section III.

1) Uncertain channels: Let $\mathcal{U}$ and $\mathcal{V}$ be arbitrary nonempty sets. An *uncertain channel from* $\mathcal{U}$ *to* $\mathcal{V}$ is a mapping $\mathbf{U} : \mathcal{U} \to 2_*^{\mathcal{V}} := 2^{\mathcal{V}} \setminus \{\varnothing\}$. For any $u \in \mathcal{U}$, the set $\mathbf{U}(u)$ is the family of all possible output values of the channel given the input u. When transmitting u, the output of $\mathbf{U}$ will be exactly one element of $\mathbf{U}(u)$. Here, $\mathbf{U}(u) \neq \varnothing$ for all u means that every input generates an output. Note that every mapping $\varphi : \mathcal{U} \to \mathcal{V}$ can be regarded as an uncertain channel $\Phi : \mathcal{U} \to 2^{\mathcal{V}}_*$ with singletons as outputs, i.e., $\Phi(u) = \{\varphi(u)\}$. Henceforth, we will not make any notational difference between a mapping and the corresponding uncertain channel.

Remark 1: Note that there are no probabilistic weights on the elements of $\mathbf{U}(u)$. Thus, $\mathbf{U}$ models a channel with nonstochastic noise, where $\mathbf{U}(u)$ describes the effect of the noise if the input is u.

We call the set $\operatorname{ran}(\mathbf{U}) := \cup_{u\in\mathcal{U}}\mathbf{U}(u)$ the *range of* $\mathbf{U}$. Given two uncertain channels $\mathbf{U}_1 : \mathcal{U} \to 2^{\mathcal{V}}_*$ and $\mathbf{U}_2 : \mathcal{V} \to 2^{\mathcal{W}}_*$, then first applying $\mathbf{U}_1$ and then $\mathbf{U}_2$ leads to a new uncertain channel $\mathbf{U}_2 \circ \mathbf{U}_1 : \mathcal{U} \to 2^{\mathcal{W}}_*$ called the *composition of* $\mathbf{U}_1$ *and* $\mathbf{U}_2$. Formally, for any $u \in \mathcal{U}$, we have

$$(\mathbf{U}_2 \circ \mathbf{U}_1)(u) := \mathbf{U}_2(\mathbf{U}_1(u)) := \bigcup_{v\in\mathbf{U}_1(u)} \mathbf{U}_2(v).$$

Every uncertain channel $\mathbf{U}$ defines a *reverse channel* $\mathbf{U}^{-1} : \operatorname{ran}(\mathbf{U}) \to 2^{\mathcal{U}}_*$ by

$$\mathbf{U}^{-1}(v) = \{u \in \mathcal{U} : v \in \mathbf{U}(u)\}.$$

Obviously, $\mathbf{U}^{-1}$ again is an uncertain channel.

Remark 2: We call $\mathbf{U}^{-1}$ the reverse instead of the inverse because usually $\sharp\,\mathbf{U}^{-1}(\mathbf{U}(u)) > 1$. We have $\mathbf{U}^{-1}(\mathbf{U}(u)) = \{u\}$ for all $u \in \mathcal{U}$ if and only if every output $v \in \operatorname{ran}(\mathbf{U})$ is generated by exactly one input u. If this is the case, we call $\mathbf{U}$ *injective*. If the uncertain channel $\mathbf{U}$ is injective, then $\mathbf{U}^{-1}$ is an ordinary mapping, in the sense that $\mathbf{U}^{-1}(v)$ is a singleton.

Given uncertain channels $\mathbf{U}_i : \mathcal{U}_i \to 2^{\mathcal{V}_i}_*$ $(1 \le i \le n)$, their *product* is the channel

$$\mathbf{U}_1 \times \cdots \times \mathbf{U}_n : \mathcal{U}_1 \times \cdots \times \mathcal{U}_n \longrightarrow 2^{\mathcal{V}_1}_* \times \cdots \times 2^{\mathcal{V}_n}_*$$

$$(\mathbf{U}_1 \times \cdots \times \mathbf{U}_n)(u(1{:}n)) = \mathbf{U}_1(u_1) \times \cdots \times \mathbf{U}_n(u_n).$$

If $\mathbf{U}_1 = \cdots = \mathbf{U}_n =: \mathbf{U}$, we write $\mathbf{U}_1 \times \cdots \times \mathbf{U}_n =: \mathbf{U}^n$. The reverse of $\mathbf{U}_1 \times \cdots \times \mathbf{U}_n$ is given by $\mathbf{U}_1^{-1} \times \cdots \times \mathbf{U}_n^{-1}$. We write $\mathbf{U}^{-n}$ for the reverse of $\mathbf{U}^n$.

2) Zero-error codes: An M*-code* on an alphabet $\mathcal{A}$ is a collection $\{\mathbf{F}(m) : 0 \le m \le M-1\}$ of nonempty and mutually disjoint subsets of $\mathcal{A}$. This is equivalent to an uncertain channel $\mathbf{F} : \{0,\dots,M-1\} \to 2^{\mathcal{A}}_*$ with disjoint output sets; thus, we will often denote such a code just by $\mathbf{F}$. The elements of $\operatorname{ran}(\mathbf{F})$ are called *codewords*. If $\sharp\,\mathbf{F}(m) = 1$ for all $0 \le m \le M-1$, then we call $\mathbf{F}$ a *singleton code*. Zero-error codes, which are not singleton codes, are introduced here for the first time.

Let $\mathbf{T} : \mathcal{A} \to 2^{\mathcal{B}}_*$ be an uncertain channel over which data are to be transmitted. A nonstochastic M-code $\mathbf{F}$ on $\mathcal{A}$ is called a *zero-error* M*-code for* $\mathbf{T}$ if for any $m, m' \in \{0,\dots,M-1\}$ with $m \ne m'$

$$\mathbf{T}(\mathbf{F}(m)) \cap \mathbf{T}(\mathbf{F}(m')) = \varnothing. \tag{1}$$

Thus, every possible channel output $y \in \operatorname{ran}(\mathbf{T}\circ\mathbf{F})$ can be associated with a unique message m. In other words, the channel $\mathbf{T}\circ\mathbf{F}$ is injective, or equivalently, $\mathbf{F}^{-1}\circ\mathbf{T}^{-1}$ is an ordinary mapping associating with each output y the message $\mathbf{F}^{-1}(\mathbf{T}^{-1}(y))$ by which it was generated (cf. Remark 2) [see Fig. 2(a) for an illustration].

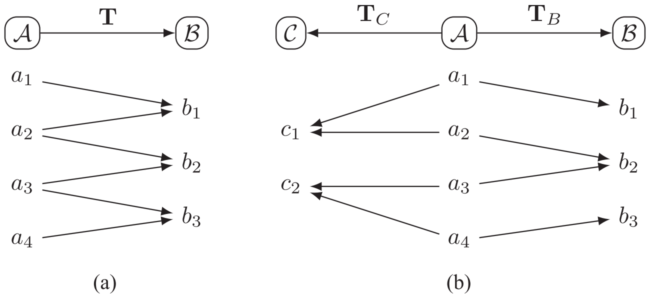

Fig. 2. (a) Uncertain channel $\mathbf{T}$. If one sets $\mathbf{F}(0) = \{a_1\}, \mathbf{F}(1) = \{a_3\}$, then $\mathbf{F}$ is a zero-error 2-code for $\mathbf{T}$. (b) Uncertain wiretap channel $(\mathbf{T}_B, \mathbf{T}_C)$. The uncertain channel $\mathbf{F} : \{0,1,2\} \to 2^{\mathcal{A}}_*$ defined by $\mathbf{F}(0) = \{a_1\}, \mathbf{F}(1) = \{a_2, a_3\}, \mathbf{F}(2) = \{a_4\}$ is a zero-error wiretap 3-code for $(\mathbf{T}_B, \mathbf{T}_C)$.

3) Uncertain wiretap channels and zero-error wiretap codes: Given an additional finite alphabet $\mathcal{C}$, an *uncertain wiretap channel* is a pair of uncertain channels $(\mathbf{T}_B : \mathcal{A} \to 2^{\mathcal{B}}_*, \mathbf{T}_C : \mathcal{A} \to 2^{\mathcal{C}}_*)$. The interpretation is that the outputs of channel $\mathbf{T}_B$ are received by an intended receiver, whereas the outputs of $\mathbf{T}_C$ are obtained by an eavesdropper, who should not be able to learn the data transmitted over $\mathbf{T}_B$.

An M-code $\mathbf{F}$ is called a *zero-error wiretap* M*-code for* $(\mathbf{T}_B, \mathbf{T}_C)$ if it is a zero-error M-code for $\mathbf{T}_B$, and additionally

$$\sharp\,\mathbf{F}^{-1}(\mathbf{T}_C^{-1}(c)) \ge 2 \tag{2}$$

for every $c \in \operatorname{ran}(\mathbf{T}_C \circ \mathbf{F})$. Thus, every output $c \in \operatorname{ran}(\mathbf{T}_C \circ \mathbf{F})$ can be generated by at least two messages. Due to the lack of further information, such as stochastic weights on the messages conditional on the output, the eavesdropper is unable to distinguish these messages [see Fig. 2(b) for an example].

4) Zero-error capacity and zero-error secrecy capacity: Given an uncertain channel $\mathbf{T} : \mathcal{A} \to 2^{\mathcal{B}}_*$, an M-code $\mathbf{F}$ on $\mathcal{A}^n$ is called a *zero-error* (n, M)*-code for* $\mathbf{T}$ if it is a zero-error M-code for $\mathbf{T}^n$. We call n the *blocklength* of $\mathbf{F}$. We set $N_{\mathbf{T}}(n)$ to be the maximal M such that there exists a zero-error (M, n)-code for $\mathbf{T}$ and define the *zero-error capacity of* $\mathbf{T}$ by

$$C_0(\mathbf{T}) := \sup_n \frac{\log N_{\mathbf{T}}(n)}{n}. \tag{3}$$

Due to the superadditivity of the sequence $\log N_{\mathbf{T}}(0{:}\infty)$ and Fekete's lemma [17], see also [18, Lemma 11.2], the supremum on the right-hand side of (3) can be replaced with a $\lim_{n\to\infty}$. Thus, $C_0(\mathbf{T})$ is the asymptotically largest exponential rate at which the number of messages, which can be transmitted through $\mathbf{T}$, free of error, grows in the blocklength.

Given an uncertain wiretap channel $(\mathbf{T}_B, \mathbf{T}_C)$, a zero-error (n, M)-code $\mathbf{F}$ for $\mathbf{T}_B$ is called a *zero-error wiretap* (n, M)*-code for* $(\mathbf{T}_B, \mathbf{T}_C)$ if it is a zero-error wiretap M-code for $(\mathbf{T}_B^n, \mathbf{T}_C^n)$. We define $N_{(\mathbf{T}_B,\mathbf{T}_C)}(n)$ to be the maximal M such that there exists a zero-error wiretap (M, n)-code for $(\mathbf{T}_B, \mathbf{T}_C)$. If no zero-error wiretap (n, M)-code exists, we set $N_{(\mathbf{T}_B,\mathbf{T}_C)}(n) = 1$. The *zero-error secrecy capacity of* $(\mathbf{T}_B, \mathbf{T}_C)$ is defined as follows:

$$C_0(\mathbf{T}_B, \mathbf{T}_C) := \sup_n \frac{\log N_{(\mathbf{T}_B,\mathbf{T}_C)}(n)}{n}. \tag{4}$$

Again, by superadditivity and Fekete's lemma [17], [18], the supremum in (4) can be replaced with a limit. Obviously, $C_0(\mathbf{T}_B, \mathbf{T}_C) \le C_0(\mathbf{T}_B)$.

5) Capacity results: The zero-error capacity of general uncertain channels is unknown, only a few special cases have been solved so far [16]. However, it is possible to relate the zero-error secrecy capacity of an uncertain wiretap channel $(\mathbf{T}_B, \mathbf{T}_C)$ to the zero-error capacity of $\mathbf{T}_B$ in a surprisingly simple way.

Theorem 1: The zero-error secrecy capacity of an uncertain wiretap channel $(\mathbf{T}_B, \mathbf{T}_C)$ either equals 0 or $C_0(\mathbf{T}_B)$.

The proof of this result can be found in Appendix A. The simple observation behind the proof is that the possibility of sending one bit securely over $(\mathbf{T}_B, \mathbf{T}_C)$ as a prefix to an arbitrary zero-error code $\mathbf{F}$ for $\mathbf{T}_B$ generates a zero-error wiretap code for $(\mathbf{T}_B, \mathbf{T}_C)$, whose rate is approximately the same as that of $\mathbf{F}$.

A necessary and sufficient criterion for the zero-error secrecy capacity to be positive is missing in Theorem 1. We can give one when $\mathbf{T}_B$ is injective and the input alphabet is finite.

Theorem 2: Let $(\mathbf{T}_B, \mathbf{T}_C)$ be an uncertain wiretap channel with finite input alphabet $\mathcal{A}$ such that $\mathbf{T}_B$ is injective. Then, $C_0(\mathbf{T}_B, \mathbf{T}_C) = 0$ if and only if $N_{(\mathbf{T}_B, \mathbf{T}_C)}(1) = 1$. If $C_0(\mathbf{T}_B, \mathbf{T}_C) > 0$, then $C_0(\mathbf{T}_B, \mathbf{T}_C) = \log(\sharp\, \mathcal{A})$.

The proof can be found in Appendix A. Theorem 2 gives a characterization of the positivity of the zero-error secrecy capacity if $\mathbf{T}_B$ is injective, which only involves $(\mathbf{T}_B, \mathbf{T}_C)$ at blocklength 1. Its proof also contains a simple procedure for finding $N_{(\mathbf{T}_B, \mathbf{T}_C)}(1)$. If $\mathbf{T}_B$ is not injective, finding $N_{(\mathbf{T}_B, \mathbf{T}_C)}(1)$ is harder but can be done by brute-force search for reasonably sized alphabets. More importantly, if $\mathbf{T}_B$ is not injective, it is possible that $N_{(\mathbf{T}_B, \mathbf{T}_C)}(1) = 1$ and $C_0(\mathbf{T}_B, \mathbf{T}_C) > 0$, see Example 3 in Appendix A. For general uncertain wiretap channels, one can use the procedure from the proof of Theorem 2 to reduce a zero-error code for $\mathbf{T}_B$ to a zero-error wiretap code. However, the code thus generated might have rate 0 although $C_0(\mathbf{T}_B, \mathbf{T}_C) > 0$. The question when $C_0(\mathbf{T}_B, \mathbf{T}_C) > 0$ for general uncertain wiretap channels seems to be a hard problem and has to be left open for now. Further discussion of zero-error secrecy capacity is included in Appendix A.

6) Degree of eavesdropper ignorance: In order to measure the achieved degree of security in greater detail, we introduce the number of messages that can generate a given eavesdropper output as an additional parameter. We call a zero-error wiretap (n, M)-code a zero-error wiretap (n, M, γ)-code if for every $c(1\!:\!n) \in \operatorname{ran}(\mathbf{T}_C^n \circ \mathbf{F})$

$$\sharp\, \mathbf{F}^{-1}(\mathbf{T}_C^{-n}(c(1\!:\!n))) \geq \gamma. \tag{5}$$

Clearly, $M \geq \gamma \geq 2$. This parameter can be interpreted as a measure of the minimal eavesdropper's confusion about the transmitted message guaranteed by the (n, M, γ)-code. It will be important in the analysis of one of the security criteria we apply for secure estimation.

III. Secure Estimation Over Uncertain Channels

A. Model

Let $\mathcal{I}_0$ be a closed real interval, and let $\Omega \geq 0$ and $\lambda > 1$ be real numbers such that $|\mathcal{I}_0| + \Omega > 0$. We then consider the real-valued time-invariant unstable linear system

$$x(t+1) = \lambda x(t) + w(t) \tag{6a}$$

$$x(0) \in \mathcal{I}_0. \tag{6b}$$

The initial state $x(0)$ can assume any value in $\mathcal{I}_0$ and is not known before its observation. The noise sequence $w(0:\infty)$ can be any sequence in $[-\Omega/2, \Omega/2]^\infty$. We call $x(t)$ the *system state at time* t. The system states are directly observable. Due to $|\mathcal{I}_0| + \Omega > 0$, the system suffers from nontrivial disturbances in the initial state or in the evolution. The set of possible system trajectories $x(0:t)$ until time t is denoted by $\mathcal{X}_{0:t}$.

Assume that an entity called the *encoder* is located at the system output and at time t, it records the corresponding system state $x(t)$. At every system time step, it has the possibility of using an uncertain wiretap channel $(\mathbf{T}_B : \mathcal{A} \to 2^{\mathcal{B}}_*, \mathbf{T}_C : \mathcal{A} \to 2^{\mathcal{C}}_*)$ exactly once, i.e., the system (6) and the channel are synchronous. At the output of $\mathbf{T}_B$, an estimator has the task of obtaining reliable estimates of the system states. An eavesdropper has access to the outputs of $\mathbf{T}_C$, which should satisfy a security criterion.

At time t, the encoder only knows $x(0\!:\!t)$ and the system dynamics (6), i.e., it has no acausal knowledge of future states. The estimator and the eavesdropper know the system dynamics (6), but the only information they have about the actual system states is what they receive from the encoder through $\mathbf{T}_B$ and $\mathbf{T}_C$, respectively. The eavesdropper also knows the transmission protocol applied by the encoder and the estimator.

The encoder also has knowledge of the complete uncertain wiretap channel, in particular the characteristics of the uncertain channel to the eavesdropper. This knowledge can be justified by assuming that the eavesdropper is part of the communication network without access rights for the system state, e.g., an "honest but curious" node in the home network. Uncertain wiretap channels can also be regarded as models of stochastic wiretap channels where the transition probabilities are unknown. In the other direction, there exist information-theoretic techniques for wiretap channels that do not require precise knowledge about the channel to the eavesdropper, but the case with eavesdropper channel knowledge serves as a building block and as a benchmark [19], [20].

The allowed protocols are defined in the following.

Definition 1: A *transmission scheme* consists of a positive integer n called the *blocklength* of the transmission scheme together with a sequence of pairs $(f_k, \varphi_k)_{k=0}^\infty$. Setting $\tau_k := kn + 1$ and $t_k := (k+1)n$, for every $k \geq 0$, we have the following:

1) the kth *encoding function* $f_k : \mathcal{X}_{0:\tau_k - 1} \to 2^{\mathcal{A}^n}_*$ is an uncertain channel;
2) the first *decoding function* $\varphi_1 : \mathcal{B}^n \to \mathbb{R}$ is an ordinary mapping;
3) for $k \geq 2$, the kth *decoding function* $\varphi_k : \mathcal{B}^{t_k} \to \mathbb{R}^n$ is an ordinary mapping.

The concept is illustrated in Fig. 3. The encoding function f_k takes the system path $x(0\!:\!\tau_k - 1)$ until time $\tau_k - 1$ as input and maps this into a codeword of length n. The blocks of new observations also have length n, except for the first one of length 1. Thus, the initial state gets a special treatment, but this is a technical detail the reason of which will become clear in the proof of Theorem 3. We allow f_k to be an uncertain channel for two reasons. One is that we do not have to distinguish between open- and closed quantizing sets—if a path or state is on the boundary, we make an uncertain decision. The more important reason is that uncertain encoding has to be allowed in order for uncertain wiretap channels to achieve capacity (see Example 2 in Appendix A).

The decoder φ_k takes the first t_k outputs of $\mathbf{T}_B$ and calculates an estimate of the states $x(\tau_{k-1}), \ldots, x(\tau_k - 1)$ (where we set $\tau_{-1} = 0$), which have not been estimated before. When we define the performance criterion for a transmission scheme,

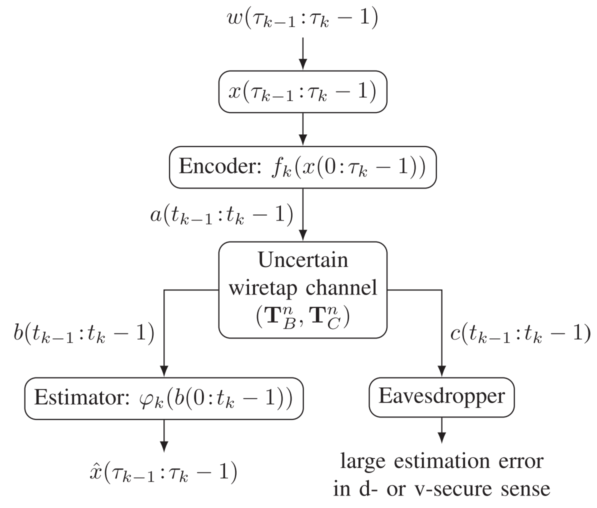
$w(\tau_{k-1}:\tau_k-1)$
$x(\tau_{k-1}:\tau_k-1)$
Encoder: $f_k(x(0:\tau_k-1))$
$a(t_{k-1}:t_k-1)$
Uncertain wiretap channel $(\mathbf{T}_B^n,\mathbf{T}_C^n)$
$b(t_{k-1}:t_k-1)$
$c(t_{k-1}:t_k-1)$
Estimator: $\varphi_k(b(0:t_k-1))$
Eavesdropper
$\hat{x}(\tau_{k-1}:\tau_k-1)$
large estimation error in d- or v-secure sense

Fig. 3. kth step of a transmission scheme $(f_k,\varphi_k)_{k=0}^{\infty}$ with blocklength n.

it will be seen that we do not lose generality by not allowing φ_k to be an uncertain channel.

Next, we come to the definition of reliability and security of a transmission scheme $(f_k,\varphi_k)_{k=0}^{\infty}$. Every such transmission scheme induces the (uncertain) channels

$$f_{0:k} := f_0\times\cdots\times f_k,\qquad \varphi_{0:k} := \varphi_0\times\cdots\times\varphi_k.$$

Observe that, given a sequence $\hat{x}(0:\tau_k-1)$ of system estimates, i.e., of outputs of $\varphi_{0:k}$, we can write the set of system states that can generate this output sequence as $(f_{0:k}^{-1}\circ\mathbf{T}_B^{-t_k}\circ\varphi_{0:k}^{-1})(\hat{x}(0:\tau_k-1))$.

Let T be a positive integer or ∞. The ∞-norm of a real sequence $y(0:T)$ is given by

$$\|y(0:T)\|_\infty := \begin{cases}\max_{0\le t\le T}|y(t)|, & \text{if } T<\infty\\ \sup_{0\le t<\infty}|y(t)|, & \text{if } T=\infty.\end{cases}$$

For a set $\mathcal{E}\subset\mathbb{R}^{T+1}$, where T is a positive integer or infinity, we define its diameter as

$$\mathrm{diam}_{T+1}(\mathcal{E})$$
$$:= \sup\{\|y(0:T)-y'(0:T)\|_\infty : y(0:T),y'(0:T)\in\mathcal{E}\}.$$

Definition 2: The transmission scheme $(f_k,\varphi_k)_{k=0}^{\infty}$ is called *reliable* if the estimation error is bounded uniformly in the estimates, i.e., if there exists a constant $\kappa>0$ such that for every possible[1] $\hat{x}(0:\infty)\in\mathrm{ran}(\varphi_{0:\infty}\circ\mathbf{T}_B^{\infty}\circ f_{0:\infty})$, we have

$$\sup_k \mathrm{diam}_{\tau_k}\left((f_{0:k}^{-1}\circ\mathbf{T}_B^{-t_k}\circ\varphi_{0:k}^{-1})(\hat{x}(0:\tau_k-1))\right)\le\kappa. \qquad (7)$$

Remark 3: One would not gain anything by allowing the decoding functions φ_k to be uncertain channels since this generalization could only increase the left-hand side of (7).

A transmission scheme only defines a decoder at the output of the estimator's channel $\mathbf{T}_B$, but every system path $x(0:\infty)$ also generates a sequence $c(0:\infty)\in\mathbf{T}_C^{\infty}(f_{0:\infty}(x(0:\infty)))$ of outputs obtained by the eavesdropper. The two security criteria, we define next, require the state information to be secure, no matter how the eavesdropper further processes its channel output sequence. The first criterion just ensures that the eavesdropper's estimation error grows unbounded with time.

Definition 3: The transmission scheme $(f_k,\varphi_k)_{k=0}^{\infty}$ is called *d-secure* if there exists a function $\delta(k)$ with

$$\mathrm{diam}_{\tau_k}\left((f_{0:k}^{-1}\circ\mathbf{T}_C^{-t_k})(c(0:t_k-1))\right)\ge\delta(k)$$

for all $c(0:\infty)\in\mathrm{ran}(\mathbf{T}_C^{\infty}\circ f_{0:\infty})$ and $\delta(k)\to\infty$ as $k\to\infty$.

Upon receiving any sequence $c(0:\infty)$ of channel outputs generated by a d-secure transmission scheme, the eavesdropper's estimate of the system path $x(0:\infty)$ that generated $c(0:\infty)$ grows to infinity[2] uniformly in $c(0:\infty)$. Note that since $\mathcal{X}_{0:t}$ is bounded for every $t\ge0$, the diameter of $(f_{0:k}^{-1}\circ\mathbf{T}_C^{-t_k})(c(0:t_k-1))$ cannot be infinite for any k. Thus, the eavesdropper's estimation error will always be finite, though increasingly large, in finite time.

Next, one can ask the question of how many system paths could be the possible generators of an eavesdropper sequence $c(0:\infty)$. This is considered in the following secrecy criterion. For a set $\mathcal{E}$ of real sequences of finite length $T+1$ and $0\le t\le T$, we write $\mathcal{E}|_t := \{x\in\mathbb{R}: x=x(t)\text{ for some } x(0:T)\in\mathcal{E}\}$. The volume $\mathrm{vol}(\mathcal{E}')$ of a subset $\mathcal{E}'$ of the real numbers is measured in terms of the Lebesgue measure.

Definition 4: A transmission scheme $(f_k,\varphi_k)_{k=0}^{\infty}$ is called *v-secure* if there exists a function $\nu(k)$ such that

$$\mathrm{vol}((f_{0:k}^{-1}\circ\mathbf{T}_C^{-t_k})(c(0:t_k-1))|_{\tau_k-1})\ge\nu(k)$$

for all $c(0:\infty)\in\mathrm{ran}(\mathbf{T}_C^{\infty}\circ f_{0:\infty})$ and $\nu(k)\to\infty$ as $k\to\infty$.

Similar to the definition of d-security, we require a uniform divergence to infinity. Since $\mathcal{X}_{0:t}$ is bounded for all $t\ge0$, the volume in Definition 4 cannot be infinite in finite time.

Remark 4: Clearly, v-security implies d-security. The volume is measured at time τ_k-1 because it would trivially tend to infinity if the τ_k-dimensional volume of the set $(f_{0:k}^{-1}\circ\mathbf{T}_C^{-t_k})(c(0:t_k-1))$ was measured. If the volume of the set of states tends to infinity along τ_k-1 as $k\to\infty$, then the same holds for the volume measured at all other infinite, increasing sequences of time instances.

Remark 5: Note that reliability only concerns $\mathbf{T}_B$, while both notions of security only concern $\mathbf{T}_C$. The task will be to find a transmission scheme that simultaneously is reliable with respect to $\mathbf{T}_B$ and (d-/v-) secure with respect to $\mathbf{T}_C$. The challenge is the combination of these properties.

B. Results for Secure Estimation

We first state a sufficient condition that the uncertain wiretap channel has to satisfy for reliability as well as d- or v-security to be possible.

Theorem 3: There exists a transmission scheme that is reliable, d-secure, and v-secure if $C_0(\mathbf{T}_B,\mathbf{T}_C)>\log\lambda$.

[1] Due to the application of the ∞-norm, the reliability criterion is a "pointwise" criterion. Using p-norms of the form $\|y(0:T)\|_p := (\sum_{t=0}^{T}|y(t)|^p)^{1/p}$ for some $1\le p<\infty$ would always lead to an infinite estimation error if $\Omega>0$ and $\mathbf{T}_B$ can transmit at most a finite number of messages in finite time, since the sequence $|x(t)-\hat{x}(t)|: t\ge0$ would not tend to zero for all state sequences $x(0:\infty)$.

[2] Note that d-security, as defined via the ∞-norm, is stronger than the analogous criteria with the p-norm instead of the ∞-norm for all $1\le p<\infty$ because $\|x(0:\infty)\|_\infty\le\|x(0:\infty)\|_p$.

The proof of Theorem 3 can be found in Section V-A. The transmission schemes applied there separate the quantization/estimation from the coding for uncertain wiretap channels by concatenating a quantizer defined, in the following, with a wiretap zero-error code. Note that the condition $C_0(\mathbf{T}_B, \mathbf{T}_C) > 0$ is weak; Nair [5] proved that $C_0(\mathbf{T}_B) > \log\lambda$ is sufficient and $C_0(\mathbf{T}_B) \geq \log\lambda$ is necessary to achieve reliability. Thus, by Theorem 1, the additional requirement in Theorem 3 is nothing but $C_0(\mathbf{T}_B, \mathbf{T}_C) > 0$. This is the minimal condition one would expect to be necessary to also achieve security. For general $(\mathbf{T}_B, \mathbf{T}_C)$, we do not know that $C_0(\mathbf{T}_B, \mathbf{T}_C) > 0$ really has to be satisfied for secure estimation to be possible.

For injective channels, however, the condition from Theorem 3 is "almost" necessary to achieve reliability and d-security, hence also for v-security.

Theorem 4: If $\mathbf{T}_B$ is injective and $\mathcal{C}$ finite, then the existence of a reliable and d-secure transmission scheme implies $\sharp\mathcal{A} \geq \lambda$ and $C_0(\mathbf{T}_B, \mathbf{T}_C) > 0$.

The proof of this theorem can be found in Section V-B. Since $\mathbf{T}_B$ is injective, the condition $\sharp\mathcal{A} \geq \lambda$ means nothing but $C_0(\mathbf{T}_B) \geq \log\lambda$. As noted previously, $C_0(\mathbf{T}_B) \geq \log\lambda$ was shown by Nair [5] to follow from reliability for general uncertain channels. The additional condition $C_0(\mathbf{T}_B, \mathbf{T}_C) > 0$, which follows from d-security, implies $C_0(\mathbf{T}_B, \mathbf{T}_C) \geq \log\lambda$ by Theorem 1. The problem of finding a tight necessary condition for secure estimation over general uncertain wiretap channels $(\mathbf{T}_B, \mathbf{T}_C)$ remains open. We conjecture that it depends on a criterion for $C_0(\mathbf{T}_B, \mathbf{T}_C)$ to be positive. We only have such a criterion when $\mathbf{T}_B$ is injective from Theorem 2.

As a refinement of Theorem 3, we have a closer look at the exponential rate at which the estimation error or the volume of the set of states at a given time that are possible according to the eavesdropper's information tends to infinity. The higher the speed of divergence, the higher is the degree of security.

Lemma 1: There exists a reliable transmission scheme $(f_k, \varphi_k)_{k=0}^{\infty}$ such that for every $c(0\!:\!\infty) \in \operatorname{ran}(\mathbf{T}_C^{\infty} \circ f_{0:\infty})$, there exist system paths $x(0\!:\!\infty), x'(0\!:\!\infty) \in (f_{0:\infty}^{-1} \circ \mathbf{T}_C^{-\infty})(c(0\!:\!\infty))$ satisfying the following:

$$\lim_{t\to\infty} \frac{\log \|x(0\!:\!t) - x'(0\!:\!t)\|_\infty}{t} = \log\lambda. \tag{8}$$

This lemma is proved in Section V-A3. Clearly, $\log\lambda$ is the largest exponential rate at which two trajectories can diverge. For v-security, the speed of increase of the volume of the set of possible states, according to the eavesdropper's information, will in general increase at an exponential rate smaller than $\log\lambda$.

Lemma 2: For every zero-error wiretap (n, M, γ)-code $\mathbf{F}$, upon setting

$$\frac{\log M}{n} =: R, \qquad \frac{\log\gamma}{n} =: \Gamma \tag{9}$$

there exists a reliable transmission scheme $(f_k, \varphi_k)_{k=0}^{\infty}$ with blocklength n such that for all $c(0\!:\!\infty) \in \operatorname{ran}(\mathbf{T}_C^{\infty} \circ f_{0:\infty})$, we have

$$\lim_{k\to\infty} \frac{\log \operatorname{vol}((f_{0:k}^{-1} \circ \mathbf{T}_C^{-t_k})(c(0\!:\!t_k - 1))|_{\tau_k - 1})}{\tau_k} \geq \begin{cases} \Gamma + \log\lambda - R, & \text{if } \Omega = 0 \\ \frac{\Gamma\log\lambda}{R + 2\log\lambda + \varepsilon_n}, & \text{if } \Omega > 0 \end{cases} \tag{10}$$

where $\varepsilon_n = \varepsilon_n(R, \lambda)$ is positive and $\varepsilon_n \to 0$ as $n \to \infty$.

This lemma is proved in Section V-A. For $\Omega = 0$, a positive rate is achievable by choosing $R < \Gamma + \log\lambda$. Lemmas 1 and 2 are discussed in detail in Section VI.

IV. Quantizer Analysis

Both Lemmas 1 and 2 follow from analyzing the transmission scheme we apply in the proof of Theorem 3. For proving Theorem 3, we separate the quantization/estimation from the channel coding. Next, we will, therefore, describe the quantizer used in the proof of Theorem 3. More precisely, we analyze the behavior of the system (6) with an appropriate quantization of every single state $x(t)$. Later, when concatenating the quantizer with a channel code of blocklength $n > 1$, we will use an analogous quantizer for the n-sampled version of (6).

Note that this quantizer is only one of possibly many that can form part of a transmission scheme, achieving the performance claimed in Theorem 3. Definition 1 does not put any restriction on the quantizers one might want to use in a transmission scheme. Since the state space of (6) is compact at every time step, a finite-level quantizer is sufficient for reliability. In addition, an infinite-level quantizer could pose problems in proving v-security, since the volume of the quantizer intervals might tend to zero too quickly.

Definition 5: Consider the system (6) and let $M \geq 2$ be an integer, called the *number of quantizer levels*. Let $\hat{x}(m(0\!:\!-1))$ be the midpoint of $\mathcal{I}(m(0\!:\!-1)) := \mathcal{I}_0$. For every integer $t \geq 0$ and every sequence $m(0\!:\!t) \in \{0, \ldots, M-1\}^{t+1}$, we then recursively set

$$\mathcal{P}(m(0\!:\!t)) := \mathcal{I}(m(0\!:\!t-1))_{\min} + \frac{|\mathcal{I}(m(0\!:\!t-1))|}{M}[m(t), m(t)+1] \tag{11}$$

$$\hat{x}(m(0\!:\!t)) := \text{midpoint of } \mathcal{P}(m(0\!:\!t)) \tag{12}$$

$$\mathcal{I}(m(0\!:\!t)) := \lambda\mathcal{P}(m(0\!:\!t)) + \left[-\frac{\Omega}{2}, \frac{\Omega}{2}\right] \tag{13}$$

[in (11), recall our notation for intervals]. Finally, we define for every $t \geq 0$ the tth *quantizer channel*, an uncertain channel $\mathbf{Q}_t$ that maps any message sequence $m(0\!:\!t-1)$ and any $x(t) \in \mathcal{I}(m(0\!:\!t-1))$ to an element of

$$\mathbf{Q}_t(x(t), m(0\!:\!t-1)) = \{m : x(t) \in \mathcal{P}(m(0\!:\!t-1), m)\}. \tag{14}$$

The sets $\mathcal{P}(\cdot)$ will be referred to as *quantizer intervals*. The numbers $0, \ldots, M-1$ are *messages*. Equations (11)–(14) define the *quantizer of the system (6) with M quantizer levels*.

Every state sequence $x(0\!:\!\infty)$ generates a message sequence $m(0\!:\!\infty)$ via the uncertain channels $\mathbf{Q}_t$. Assume that the state sequence $x(0\!:\!t-1)$ has generated a message sequence $m(0\!:\!t-1)$ until time $t-1$. The interval $\mathcal{I}(m(0\!:\!t-1))$ consists of all states $x(t)$ that are possible in the next time step. Upon observation of $x(t)$, the message $m(t)$ is generated as an element[3] of $\mathbf{Q}_t(x(t), m(0\!:\!t-1))$. From the sequence $m(0\!:\!t)$, one can then infer that $x(t) \in \mathcal{P}(m(0\!:\!t))$. Accordingly, the estimate of $x(t)$ is $\hat{x}(m(0\!:\!t))$. Note that for every message sequence $m(0\!:\!\infty)$, there exists a system path $x(0\!:\!\infty)$ that generates $m(0\!:\!\infty)$.

[3] $m(t)$ is not determined deterministically from $x(t)$ and $m(0\!:\!t-1)$ because in this way we can have all intervals $\mathcal{P}(m(0\!:\!t))$ closed. Note that $\sharp\,\mathbf{Q}_t(x(t), m(0\!:\!t-1)) \geq 2$ only if $x(t)$ is on the boundary of two neighboring quantizer intervals.

Most of the quantizer analysis we do in the following serves the proof of Lemma 2. We are interested in the disjointness of quantizer intervals at a given time in order to find a lower bound on the volume of the set of states that are possible according to the eavesdropper's information. If a set of quantizer intervals at a common time instant is disjoint, the volume covered by their union equals the sum over their individual volumes. Thus, two questions need to be answered: 1) What is the volume of a quantizer interval? 2) How many disjoint quantizer intervals are there (from the eavesdropper's view)? An answer to the first question is the following lemma.

Lemma 3: If $\lambda \neq M$, then for every $t \in \mathbb{N}$ and $m(0{:}t) \in \{0,\dots,M-1\}^{t+1}$, we have

$$|\mathcal{P}(m(0{:}t))| = \frac{\lambda^t}{M^t}\left(\frac{|\mathcal{I}_0|}{M} - \frac{\Omega}{M-\lambda}\right) + \frac{\Omega}{M-\lambda}. \tag{15}$$

In particular, we have $\sup_t |\mathcal{P}(m(0{:}t))| < \infty$ for every infinite message sequence $m(0{:}\infty)$ if $\lambda < M$. In that case, we have

$$\sup_{t\geq 0} |\mathcal{P}(m(0{:}t))| = \max\left\{\frac{|\mathcal{I}_0|}{M}, \frac{\Omega}{M-\lambda}\right\}.$$

Further, the length of $\mathcal{P}(m(0{:}t))$ only depends on t, not on $m(0{:}t)$. Thus, we can define

$$\ell_t := |\mathcal{P}(m(0{:}t))|. \tag{16}$$

The proof can be found in Appendix B. Lemma 3 not only is useful in the security analysis but it also essentially establishes the reliability for $M > \lambda$, a result that, of course, is not surprising in view of the existing literature. Concerning question 2), life is simple when $\Omega = 0$ because of the following lemma.

Lemma 4: If $\Omega = 0$, then at each time $t \geq 0$, the interiors of the intervals $\mathcal{P}(m(0{:}t))$ are disjoint, where $m(0{:}t)$ ranges over $\{0,\dots,M-1\}^{t+1}$.

For the proof, see Appendix B. Thus, at time t, we have M^{t+1} disjoint quantizer intervals of the same length. If $\Omega > 0$, then the situation is more complicated; quantizer intervals belonging to different message sequences of the same length can overlap. This is the reason for the two different lower bounds on the rate of volume increase in (10).

Example 1: Consider the system (6) with $\lambda = 1.2$, $\Omega = .1$, $\mathcal{I}_0 = [-1, 1]$, and its quantizer with $M = 3$. Then, $\mathcal{P}(0) = [-1, -1/3]$ and $\mathcal{P}(1) = [-1/3, +1/3]$. In the next time step, one has

$$\mathcal{P}(0,1) = [-.6, -.35]\,, \quad \mathcal{P}(1,0) = [-.45, -.15]\,.$$

Thus, $\mathcal{P}(0,1)$ and $\mathcal{P}(1,0)$ are not disjoint. The closer a state $x(t)$ is to the origin (and the larger t), the more paths there are which can be in this particular state at time t.

Example 1 shows that one can only hope to obtain disjoint quantizer sets for a strict subset of all message sequences. To find such a subset, we derive an important formula for the sequence $\hat{x}(m(0{:}\infty))$, given a message sequence $m(0{:}\infty)$.

Lemma 5: Consider the system (6) and the quantizer for (6) with M quantizer levels. Let $m(0{:}\infty)$ be a message sequence. Then, for every $t = 0, 1, 2, \dots$, we have

$$\begin{aligned}&\hat{x}(m(0{:}t))\\ &= \lambda^t\Bigg\{\hat{x}(m(0{:}-1))\\ &+\frac{1}{2}\sum_{i=0}^{t}\left(\frac{\Omega M}{M-\lambda}\left(\frac{1}{\lambda^i}-\frac{1}{M^i}\right)+\frac{|\mathcal{I}_0|}{M^i}\right)\left(\frac{2m(i)+1}{M}-1\right)\Bigg\}.\end{aligned} \tag{17}$$

See Appendix B for the proof. In order to find disjoint quantizer intervals, the idea is to look at the distance between points $\hat{x}(m(0:t))$ and $\hat{x}(m'(0:t))$ and ask how the distances between the estimate sequences will evolve in future.

Lemma 6: Assume that $M > \lambda$. Let $m(0{:}\infty)\ and\ m'(0{:}\infty)$ be two message sequences, and let $T \geq 0$. If

$$|\hat{x}(m(0{:}T)) - \hat{x}(m'(0{:}T))| \geq \frac{\Omega}{M-\lambda}\,\frac{M-1}{\lambda-1} + \ell_T \tag{18}$$

then, for every $t \geq 0$, the interiors of the intervals $\mathcal{P}(m(0{:}T+t))$ and $\mathcal{P}(m'(0{:}T+t))$ are disjoint.

The proof can be found in Appendix B. Finally, assume that at each time instant at least γ different messages are possible according to the eavesdropper's view. For every $t \geq 0$, let $\mathcal{M}_t := \{m_{t,1} < m_{t,2} < \cdots < m_{t,\gamma}\} \subseteq \{0,\dots,M-1\}$ be a subset of the possible messages at time t, which has exactly γ elements. In particular, $\mathcal{M}_t$ may differ from $\mathcal{M}_{t'}$ for $t \neq t'$. Now, fix a $T \geq 1$. For $j \geq 1$ and $\xi(1{:}j) \in \{1,\dots,\gamma\}^j$, we define the message sequence $m_{\xi(1:j)}(0{:}jT-1)$ as follows:

$$m_{\xi(1:j)}(s) = m_{s,\xi(i)} \in \mathcal{M}_s$$

if $1 \leq i \leq j$ and $(i-1)T \leq s \leq iT-1$. On the jth block of times $(j-1)T,\dots,jT-1$, the sequences $m_{\xi(1:j)}(0{:}jT-1)$, where $\xi(1{:}j-1)$ is kept fixed and $\xi(j)$ ranges over $\{1,\dots,\gamma\}$, are an ordered set of γ message sequences with the order induced by a componentwise ordering. The corresponding quantizer intervals $\mathcal{P}(m_{\xi(1:j)}(0{:}jT-1))$, where $1 \leq \xi(j) \leq \gamma$, will therefore diverge due to the instability of the system (6). The following lemma is proved in Appendix B.

Lemma 7: Let $\Omega > 0$ and $M > \lambda$, and choose a $T \in \mathbb{N}$ satisfying

$$T \geq 1 + \frac{\log(M-1) + \log(M+\lambda-1) - \log(M-\lambda)}{\log\lambda}. \tag{19}$$

Then, for every $j \geq 1$, the interiors of the sets $\mathcal{P}(m_{\xi(1:j)}(0{:}jT-1))$, where $\xi(1{:}j)$ ranges over $\{1,\dots\gamma\}^j$, are disjoint.

Thus, we have obtained a lower bound on the number of disjoint quantizer intervals at times $t = jT-1$, for positive j. This will be sufficient when we put everything together in Section V to prove v-security and obtain the lower bound of Lemma 2 when $\Omega > 0$.

V. Secure Estimation—Proofs

A. Proof of Theorem 3 and Lemmas 1 and 2

1) Definition of the Transmission Scheme: We start by defining a transmission scheme $(f_k, \varphi_k)_{k=0}^{\infty}$. We choose its blocklength n such that $M := N_{(\mathbf{T}_B,\mathbf{T}_C)}(n) > \lambda^n$, which is possible because $C_0(\mathbf{T}_B, \mathbf{T}_C) > \log\lambda$. Let $\gamma \geq 2$ be chosen such that there exists a zero-error wiretap (n, M, γ)-code $\mathbf{F}$.

Since we use the channel in blocks of length n, we also observe the system only at intervals of length n. If we look at the outputs of (6) at times $0, n, 2n, \ldots$, we obtain a new dynamical system that satisfies the following:

$$x^{(n)}(k+1) = \lambda^n x^{(n)}(k) + w^{(n)}(k) \tag{20a}$$

$$x^{(n)}(0) \in \mathcal{I}_0 \tag{20b}$$

where

$$w^{(n)}(k) = \sum_{j=0}^{n-1} \lambda^{n-j-1} w(kn+j).$$

Note that $w^{(n)}(k)$ is a nonstochastic disturbance in the range $[-\Omega^{(n)}/2, \Omega^{(n)}/2]$ for

$$\Omega^{(n)} = \frac{\Omega}{\lambda - 1}(\lambda^n - 1). \tag{21}$$

Therefore, the quantizer for (20) with M quantization levels is well defined as in Definition 5, and all results derived in Section IV for (6) and its quantizer carry over to (20) with the obvious modifications of the parameters.

We define the encoding and decoding functions of our transmission scheme by separating the quantization/estimation from the channel coding similar to how it has been done frequently in settings without security, e.g., [21]. For every $k \geq 0$, let $\mathbf{Q}_k^{(n)}$ be the kth quantizer channel of the quantizer of (20) [see (14)]. The transmission scheme is defined by recursively concatenating the $\mathbf{Q}_k^{(n)}$ with $\mathbf{F}$. We set $f_0(x(0)) = \mathbf{F}(\mathbf{Q}_0^{(n)}(x(0)))$ and for $k \geq 1$, assuming that the quantizer channels have produced the message sequence $m(0\!:\!k-1)$ so far, we set

$$f_k(x(0\!:\!\tau_k - 1)) = \mathbf{F}(\mathbf{Q}_k^{(n)}(x^{(n)}(k), m(0\!:\!k-1))).$$

For the definition of the decoding functions, recall that $\mathbf{F}$ is a zero-error code. Thus, for every $k \geq 0$ and $b(0\!:\!t_k - 1) \in \mathrm{ran}(\mathbf{T}_B^{t_k} \circ \mathbf{F}^{k+1})$, the set $(\mathbf{F}^{-(k+1)} \circ \mathbf{T}_B^{-t_k})(b(0\!:\!t_k - 1))$ contains precisely one element, namely the message sequence $m(0\!:\!k)$ sent by the encoder. The zeroth decoding function has a one-dimensional output, which is defined by $\varphi_0(b(0\!:\!t_0 - 1)) = \hat{x}^{(n)}((\mathbf{F}^{-1} \circ \mathbf{T}_B^{-t_0})(b(0\!:\!t_0 - 1)))$. Here, $\hat{x}^{(n)}(m(0:k))$, for any $m(0:k)$, is the midpoint of the quantizer interval $\mathcal{P}^{(n)}(m(0:k))$ belonging to the quantizer of (20). For $k \geq 1$, the output of the kth decoding function φ_k is n dimensional. If, with a little change of notation, we write $\varphi_k(b(0\!:\!t_k - 1)) =: (\hat{x}_{\tau_{k-1}}(b(0\!:\!t_k - 1)), \ldots, \hat{x}_{\tau_k - 1}(b(0\!:\!t_k - 1)))$, then we set

$$\hat{x}_{\tau_k - 1}(b(0\!:\!t_k - 1)) = \hat{x}^{(n)}((\mathbf{F}^{-(k+1)} \circ \mathbf{T}_B^{-t_k})(b(0\!:\!t_k - 1))).$$

Since (6) does not grow to infinity in finite time, the values $\hat{x}_{\tau_{k-1}}(b(0\!:\!t_k - 1)), \ldots, \hat{x}_{\tau_k - 2}(b(0\!:\!t_k - 1))$ can be defined in an arbitrary way, as long as their distance from $\hat{x}_{\tau_k - 1}(b(0\!:\!t_k - 1))$ is uniformly bounded in k and $b(0\!:\!\infty)$.

2) Reliability: Although it is not surprising and well known in the literature, we show the reliability of the transmission scheme for completeness. Since the states of (6) cannot diverge to infinity in finite time, we only need to make sure that the estimation errors at the observation times $\tau_0 - 1, \tau_1 - 1, \ldots$ are bounded. To see this, let $k \geq 0$ and $m(0\!:\!k)$ be any message sequence and observe that

$$(f_{0:k}^{-1} \circ \mathbf{T}_B^{-t_k} \circ \varphi_{0:k}^{-1})(\hat{x}^{(n)}(m(0\!:\!k)))|_{\tau_k - 1} = \mathcal{P}^{(n)}(m(0\!:\!k)).$$

Since $M > \lambda^n$, the length of $\mathcal{P}^{(n)}(m(0\!:\!k))$ is bounded by Lemma 3. This shows that the transmission scheme is reliable.

3) d-Security and Lemma 1: Let $c(0\!:\!\infty) \in \mathrm{ran}(\mathbf{T}_C^{\infty} \circ f_{0:\infty})$. Let $m(0) \neq m'(0) \in \mathbf{F}^{-1}(\mathbf{T}_C^{-n}(c(0\!:\!t_0 - 1)))$ and $m(k) \in \mathbf{F}(\mathbf{T}_C^{-n}(c(t_{k-1}\!:\!t_k - 1)))$. Then, there are two system trajectories $x(0\!:\!\infty), x'(0\!:\!\infty)$ such that $x(\tau_k - 1) = \hat{x}^{(n)}(m(0\!:\!k))$ and $x'(\tau_k - 1) = \hat{x}^{(n)}(m'(0)m(1\!:\!k))$ for all $k \geq 0$. With Lemma 5, one immediately sees that $x(0\!:\!\infty)$ and $x'(0\!:\!\infty)$ diverge at an exponential rate of $\log \lambda$. Thus, $x(0\!:\!\infty)$and $x'(0\!:\!\infty)$ satisfy (8). This proves Lemma 1 and the achievability of d-security.

4) v-Security and Lemma 2: For the proof of v-security of the transmission scheme, we consider two subcases with $\Omega = 0$ and $\Omega > 0$. We first assume $\Omega = 0$; hence, $|\mathcal{I}_0| > 0$. In this case, hardly anything remains to be proved. By Lemma 4, for given $k \geq 0$, the interiors of all $\mathcal{P}^{(n)}(m(0\!:\!k))$ are disjoint. Now, assume that the eavesdropper receives the sequence $c(0\!:\!t_k - 1)$. Since $\mathbf{F}$ is an (n, M, γ)-code, $\sharp(\mathbf{F}^{-(k+1)} \circ \mathbf{T}_C^{-t_k})(c(0\!:\!t_k - 1)) \geq \gamma^{k+1}$. Hence, we have the following:

$$\begin{aligned}
&\mathrm{vol}((f_{0:k}^{-1} \circ \mathbf{T}_C^{-t_k})(c(0\!:\!t_k - 1))|_{\tau_k - 1}) \\
&= \sum_{m(0:k) \in (\mathbf{F}^{-(k+1)} \circ \mathbf{T}_C^{-t_k})(c(0:t_k - 1))} \ell_k^{(n)} \\
&\geq \gamma^{k+1} \ell_k^{(n)} = \left(\frac{\gamma\lambda^n}{M}\right)^k \frac{\gamma|\mathcal{I}_0|}{M}
\end{aligned}$$

where $\ell_k^{(n)}$ is the length of the quantizer intervals at time k of the quantizer of (20). This gives the possibly negative growth rate $(\log \gamma)/n + \log \lambda - (\log M)/n$, as claimed in Lemma 2 for the case with $\Omega = 0$. Since $(\log M)/n$ can be chosen as strictly smaller than $(\log \gamma)/n + \log \lambda$, this also proves that v-security is achievable for $\Omega = 0$, and thus completes the proof of Theorem 3 for the case with $\Omega = 0$.

Next, we assume that $\Omega > 0$. Define

$$T^{(n)} := \left\lceil 1 + \frac{\log M}{n \log \lambda} + \frac{\log(M + \lambda^n) - \log(M - \lambda^n)}{n \log \lambda} \right\rceil.$$

Choose a $j \geq 1$, and set $k(j) := jT^{(n)} - 1$. Let $c(0\!:\!t_{k(j)} - 1)$ be an eavesdropper output sequence. Then, by choice of $\mathbf{F}$, we have

$$\sharp(\mathbf{F}^{-(k(j)+1)} \circ \mathbf{T}_C^{-t_{k(j)}})(c(0\!:\!t_{k(j)} - 1)) \geq \gamma^{k(j)+1}. \tag{22}$$

$T^{(n)}$ satisfies (19) for (20). By applying Lemma 7 to (20), within the set on the left-hand side of (22), the γ^j message sequences of the form $m_{\xi(1:j)}(0\!:\!k(j))$ produce sets $\mathcal{P}^{(n)}(m_{\xi(1:j)}(0\!:\!k(j)))$ with disjoint interiors. Therefore, we have

$$\begin{aligned}
&\mathrm{vol}((f_{0:k(j)}^{-1} \circ \mathbf{T}_C^{-t_{k(j)}})(c(0\!:\!t_{k(j)} - 1))|_{\tau_{k(j)} - 1}) \\
&\geq \sum_{\xi(1:j) \in \{1,\ldots,\gamma\}^j} \ell_{k(j)}^{(n)} = \gamma^j \ell_{k(j)}^{(n)}.
\end{aligned} \tag{23}$$

Since $\ell_{k(j)}^{(n)}$ tends to a constant as j tends to infinity, the asymptotic rate of volume growth is lower bounded by

$$\lim_{k \to \infty} \frac{\log(\gamma^j \ell_{k(j)}^{(n)})}{\tau_k} = \frac{\log \gamma}{nT^{(n)}}.$$

With the notation (9) and setting

$$\varepsilon_n := \frac{\log(M+\lambda^n) - \log(M-\lambda^n)}{n}$$

we obtain

$$\frac{\log\gamma}{nT^{(n)}} \geq \frac{\Gamma\log\lambda}{R + 2\log\lambda + \varepsilon_n}.$$

Clearly, ε_n is positive and tends to 0 as n tends to infinity. This proves that v-security can be achieved in the case with $\Omega > 0$ as well and at the rate claimed in Lemma 2. Altogether, this completes the proof of Theorem 3 and Lemmas 1 and 2.

B. Proof of Theorem 4

Assume that $\mathbf{T}_B$ is injective and $\mathcal{C}$ is finite. Let $(f_k, \varphi_k)_{k=0}^{\infty}$ be a reliable and d-secure transmission scheme with blocklength n. In particular, choose $\kappa > 0$ in such a way that (7) is satisfied for every possible sequence of estimates $\hat{x}(0\!:\!\infty)$. The necessity of $C_0(\mathbf{T}_B) \geq \log\lambda$ was shown in [5]. Due to the injectivity of $\mathbf{T}_B$, this condition can be reformulated as $\sharp\mathcal{A} \geq \lambda$. It remains to show that $C_0(\mathbf{T}_B, \mathbf{T}_C) > 0$.

By the uniform divergence requirement in the definition of d-security, it is possible to choose a k such that

$$\operatorname{diam}_{\tau_k}((f_{0:k}^{-1} \circ \mathbf{T}_C^{-t_k})(c(0\!:\!t_k - 1))) > \kappa \tag{24}$$

for every $c(0\!:\!t_k - 1) \in \operatorname{ran}(\mathbf{T}_C^{t_k} \circ f_{0:k})$. Let $\tilde{c}(0\!:\!t_k - 1) \in \operatorname{ran}(\mathbf{T}_C^{t_k} \circ f_{0:k})$. Recursively, we define the sets $\mathcal{T}_0(\tilde{c}(0\!:\!t_k - 1)) := \operatorname{ran}(f_{0:k}) \cap \mathbf{T}_C^{-t_k}(\tilde{c}(0\!:\!t_k - 1))$ and $\mathcal{T}_j(\tilde{c}(0\!:\!t_k - 1)) := \operatorname{ran}(f_{0:k}) \cap (\mathbf{T}_C^{-t_k} \circ \mathbf{T}_C^{t_k})(\mathcal{T}_{j-1}(\tilde{c}(0\!:\!t_k - 1)))$ for $j \geq 1$. Let j_* be the maximal j, which satisfies[4] $\mathcal{T}_j(\tilde{c}(0\!:\!t_k - 1)) \supsetneq \mathcal{T}_{j-1}(\tilde{c}(0\!:\!t_k - 1))$. If $a_0(0\!:\!t_k - 1), \ldots, a_{M-1}(0\!:\!t_k - 1)$ is an enumeration of the elements of $\mathcal{T}_{j_*}(\tilde{c}(0\!:\!t_k - 1))$, then the (M, t_k)-code $\mathbf{G}_k$ defined by $\mathbf{G}_k(m) = \{a_m(0\!:\!t_k - 1)\}$ is a zero-error code. This is due to the injectivity of $\mathbf{T}_B$.

However, $\mathbf{G}_k$ is also a wiretap zero-error code. To show this, let $c(0\!:\!t_k - 1) \in \operatorname{ran}(\mathbf{T}_C^{t_k} \circ \mathbf{G}_k)$. The definition of j_* implies that $\mathbf{T}_C^{-t_k}(c(0\!:\!t_k - 1)) \subseteq \mathcal{T}_{j_*}(\tilde{c}(0\!:\!t_k - 1)) = \operatorname{ran}(\mathbf{G}_k)$. Due to (24) and since $(f_k, \varphi_k)_{k=0}^{\infty}$ satisfies (7), we have $\sharp(\mathbf{G}_k^{-1} \circ \mathbf{T}_C^{-t_k})(c(0\!:\!t_k - 1)) = \sharp\mathbf{T}_C^{-t_k}(c(0\!:\!t_k - 1)) \geq 2$. Hence, $c(0\!:\!t_k - 1)$ can be generated by at least two different messages. This implies that $\mathbf{G}_k$ is also a wiretap zero-error code; hence, $C_0(\mathbf{T}_B, \mathbf{T}_C) > 0$.

VI. Discussion: d- and v-Security

We have a closer look at d- and v-security, in particular the rates derived in Lemmas 1 and 2. First, consider the system (6) with $\Omega = 0$. Let $(\mathbf{T}_B, \mathbf{T}_C)$ be any uncertain wiretap channel and $\mathbf{F}$ an (n, M, γ)-code for $(\mathbf{T}_B, \mathbf{T}_C)$. Then, the proof of Lemma 2 shows that the lower bound on the right-hand side of (10) is tight. On the other hand, the growth rate $\log\lambda$ of the eavesdropper's estimation error, derived in Lemma 1, will in general be strictly larger. This means that the set $(f_{0:k}^{-1} \circ \mathbf{T}_C^{-t_k})(c(0 : t_k - 1))$ is not connected, i.e., it has holes.

If $\Omega > 0$, we have seen in Example 1 and the proof of Lemma 2 that the situation is more complicated than for $\Omega = 0$.

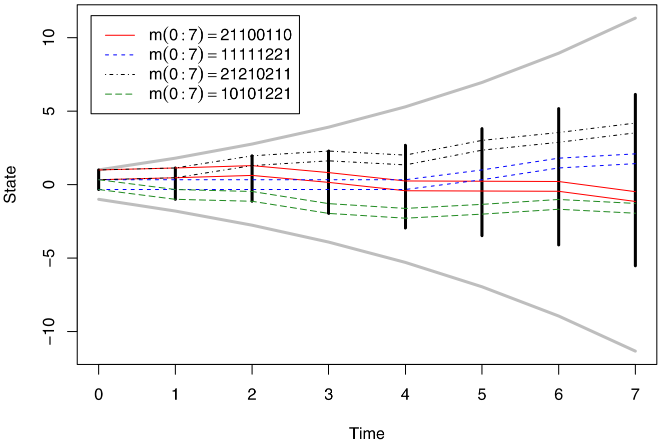

Fig. 4. State space of (6) with parameters as in the text. The thick gray lines mark the outer bounds of the state space. For the received eavesdropper sequence $c(0\!:\!7)$ as in the text, the vertical black lines show the set of states that are possible according to the eavesdropper's view. Further, for four possible message sequences $m(0 : 7)$, the evolution of the corresponding $\mathcal{P}(m(0 : 7))$ is shown for illustration purposes.

For an illustration, let $(\mathbf{T}_B, \mathbf{T}_C)$ and $\mathbf{F}$ be the channel and code from Fig. 2(b). Assume the system (6) with $\lambda = 1.2, \mathcal{I}_0 = [-1, 1]$, and $\Omega = 1.2$. As in the proof of Theorem 3, we construct a blocklength-1 transmission scheme $(f_k, \varphi_k)_{k=0}^{\infty}$ by concatenating the quantizer for (6) with $\mathbf{F}$ by mapping the quantizer message m to $\mathbf{F}(m)$. For example, if $x(0) \in [1/3, 1]$, the quantizer outputs message 2, which $\mathbf{F}$ maps to the set $\mathbf{F}(2) = \{a_4\}$. Sending a_4 through $\mathbf{T}_C$ generates the output c_2, from which the eavesdropper concludes that message 1 or 2 has been sent. By the choice of parameters, the length of the quantizer intervals remains constant over time. Fig. 4 illustrates this situation under the assumption that the eavesdropper receives the symbols $c(0\!:\!7) = c_2c_1c_2c_1c_1c_2c_2c_1$. There are 2^8 possible message sequences from the eavesdropper's point of view, one of which corresponds to the actual sequence generated by the quantizer. Notice the growth of $\operatorname{vol}((f_{0:7}^{-1} \circ \mathbf{T}_C^{-8})(c(0\!:\!7)))$, which also implies the growth of the eavesdropper's estimation error in the sense of d-security. Further, observe how quantizer intervals overlap and even "cross paths."

Generally, if $\Omega > 0$ and $\Gamma = R$, then the eavesdropper has no information about the transmitted message, and $\operatorname{vol}((f_{0:k}^{-1} \circ \mathbf{T}_C^{-t_k})(c(0\!:\!t_k - 1)))$ grows at the rate $\log\lambda$. The ratio of the left- and the right-hand sides of (10) tends to 1 as $\lambda \searrow 1$. Thus, the lower bound of Lemma 2 is asymptotically tight for λ tending to the boundary of the instability region.

Moreover, the lower bound (10) for $\Omega > 0$ is independent of Ω and $\mathcal{I}_0$. This behavior can be due to the asymptotic dominance of λ in the system dynamics. Fig. 5 shows the numerical evidence for the correctness of this independence. For the system parameters, we fix $\lambda = 1.2$ and consider four variations of Ω and $\mathcal{I}_0$, as shown in Fig. 5. We assume the same uncertain wiretap channel as in Fig. 4 and apply the same blocklength-1 transmission scheme. Because of the symmetry of the channel and the transmission scheme, $\operatorname{vol}((f_{0:k}^{-1} \circ \mathbf{T}_C^{-(k+1)})(c(0\!:\!k)))$ is independent of the eavesdropper's received sequence and can be calculated in closed form. For each of the four combinations of Ω and $\mathcal{I}_0$, we plot the ratio of the left-hand side of (10) (empirical rate) and the right-hand side of (10) (rate) versus time. After

[4] Without going into the details, we would like to mention here that $\mathcal{T}_{j_*}(c(0\!:\!t_k - 1))$ is an equivalence class in the taxicab partition of the joint range of $f_{0:k}$ and the corresponding outputs of $\mathbf{T}_C$, see [5].

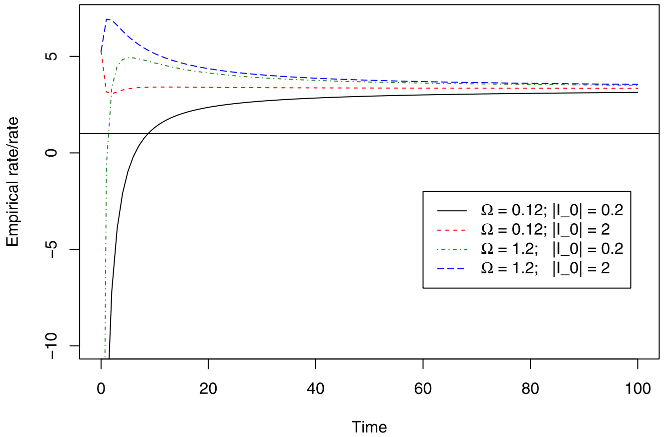

Fig. 5. Ratio of the left- and right-hand sides of (10) for different combinations of Ω and $\mathcal{I}_0$, with other parameters as in the text.

different initial values, mainly due to the differing lengths of the initial interval, the ratios converge. At time 100, the maximal absolute value of all differences between them equals 0.417; at time 1000, it reduces to 0.042.

The maximum ratio of empirical rate and rate in the previous example at time 1000 equals 3.36, quite a bit away from 1. This is due to the fact that $\mathrm{vol}((f_{0:k}^{-1} \circ \mathbf{T}_C^{-(k+1)})(c(0:k)))$ grows at the rate $\log \lambda$. The reason for this is that the symmetry of the situation allows, without loss of generality, to assume that the eavesdropper always receives the symbol c_1. The volume of states compatible with this sequence is essentially given by the difference between the largest and smallest paths that are possible according to this information, which by Lemma 5 grows at the rate $\log \lambda$. Since the extreme paths compatible with a given eavesdropper information always diverge at the rate $\log \lambda$ by Lemma 1, a smaller volume growth rate is only possible if there are gaps in the set of possible states, as in the case with $\Omega = 0$ (see above). We expect these gaps to increase if the difference between Γ and R increases.

A major problem for the general analysis of $\mathrm{vol}((f_{0:k}^{-1} \circ \mathbf{T}_C^{-t_k})$ $(c(0:t_k - 1)))$ is that a brute-force approach quickly becomes infeasible because with every secure transmission scheme, at least 2^{t+1} different message sequences are possible at time t from the eavesdropper's point of view. A general analysis without relying on symmetry might require techniques from fractal set theory. Symmetry, as in the previous example, is simpler to analyze. To achieve this symmetry, the association of quantizer messages with the code sets is crucial, an issue we have neglected here. We also expect the gap between the left- and the right-hand sides of (10) to decrease at higher blocklengths, not least because the ε_n term in the lower bound, at blocklength $n = 1$ and with $M = 3, \lambda = 1.2$ as in the example, equals 1.22 and is not negligible.

VII. Conclusion

In this paper, we introduced uncertain wiretap channels and their zero-error secrecy capacity. We introduced methods from hypergraph theory, which together with the already established graph theoretic methods for the zero-error capacity of uncertain channels facilitate the analysis of zero-error secrecy capacity. We showed how the zero-error secrecy capacity of an uncertain wiretap channel relates the zero-error capacity of the uncertain channel to the intended receiver of the wiretap channel. In the case where the uncertain channel to the intended receiver is injective, we gave a full characterization of the zero-error secrecy capacity of the corresponding uncertain wiretap channel.

We also analyzed how unstable linear systems can be estimated if the system state information has to be transmitted to the estimator through an uncertain wiretap channel, such that the eavesdropper should obtain as little information about the system states as possible. We introduced two security criteria, called d-security and v-security. We gave a sufficient criterion that uncertain channels have to satisfy in order for the estimator to obtain a bounded estimation error as well as for both d- and v-security to hold. In the case of an injective uncertain channel from the encoder to the estimator, we showed that this sufficient criterion essentially is necessary as well. We gave lower bounds on the exponential rates at which the eavesdropper's state information diverges under the two security criteria.

Some problems have been left open in the paper, such as a complete characterization of the zero-error secrecy capacity of uncertain wiretap channels, a characterization of when a secure estimation of unstable systems is possible over uncertain wiretap channels, and a complete answer to the question of optimality of the lower bounds from Lemma 2. Apart from that, there are several points that can be extended in future. One would be that the encoder has less knowledge about the uncertain wiretap channel. Another one would be an extension to multidimensional secure estimation, possibly with distributed observations. Finally, it would be interesting to link the zero-error secrecy capacity of uncertain wiretap channels to Nair's nonstochastic information theory [5] (cf. Footnote 5).

Appendix A
Uncertain Wiretap Channels: Proofs and Further Discussion

This appendix contains the proofs of Theorems 1 and 2 and some additional discussion. First, we prove Theorem 1. For the proof of Theorem 2, we then introduce a graph and a hypergraph structure on the input alphabet induced by the uncertain wiretap channel. Using these structures, we prove Theorem 2.

1) Proof of Theorem 1: Assume that $C_0(\mathbf{T}_B, \mathbf{T}_C) > 0$, which implies $C_0(\mathbf{T}_B) > 0$. Let $\mathbf{F}$ be a zero-error wiretap (n_1, M_1)-code, and let $\mathbf{G}$ be a zero-error (n_2, M_2)-code, where $M_1 = N_{(\mathbf{T}_B, \mathbf{T}_C)}(n_1) \geq 2$ and $M_2 = N_{\mathbf{T}_B}(n_2)$. Consider the concatenated $(n_1 + n_2, M_1 M_2)$-code $\mathbf{F} \times \mathbf{G}$. Clearly, it is a zero-error code, but it also is a zero-error wiretap code. Choose $(m_1, m_2) \in \{0, \ldots, M_1 - 1\} \times \{0, \ldots, M_2 - 1\}$, and choose $c(1 : n_1) \in \mathbf{T}_C^{n_1}(\mathbf{F}(m_1))$ and $c(n_1 + 1 : n_2) \in \mathbf{T}_C^{n_2}(\mathbf{G}(m_2))$. Since $\mathbf{F}$ is a zero-error wiretap code, there exists an $m_1' \in (\mathbf{F}^{-1} \circ \mathbf{T}_C^{-n_1})(c(1 : n_1))$ with $m_1' \neq m_1$. Therefore, the two different message pairs (m_1, m_2) and (m_1', m_2) can generate the output $c(1 : n_1 + n_2)$. Thus, $\mathbf{F} \times \mathbf{G}$ is a zero-error wiretap code. This construction implies

$$\frac{\log N_{(\mathbf{T}_B, \mathbf{T}_C)}(n_1 + n_2)}{n_1 + n_2} \geq \frac{\log N_{(\mathbf{T}_B, \mathbf{T}_C)}(n_1) + \log N_{\mathbf{T}_B}(n_2)}{n_1 + n_2}$$

and the term on the right-hand side tends to $C_0(\mathbf{T}_B)$ as n_2 tends to infinity. This proves Theorem 1.

2) Zero-error capacity and graphs: It was observed by Shannon [2] that the zero-error capacity of an uncertain channel $\mathbf{T}:\mathcal{A}\to 2^{\mathcal{B}}_*$ can be determined from a graph structure induced on the input alphabet $\mathcal{A}$ by $\mathbf{T}$. To see this, let n be a blocklength. Two words $a(1:n), a'(1:n)\in\mathcal{A}^n$ cannot be used as codewords for the same message if they have a common output word $b(1:n)\in\mathcal{B}^n$. If we draw a line between every two elements of $\mathcal{A}^n$ that generate a common output message $b(1:n)$, we obtain a *graph* on $\mathcal{A}^n$, which we denote by $G(\mathbf{T}^n)$. Thus, $G(\mathbf{T}^n)$ is nothing but a binary relation $\sim$ on $\mathcal{A}^n$, where $a(1:n)\sim a'(1:n)$ if and only if $\mathbf{T}^n(a(1:n))\cap\mathbf{T}^n(a(1:n))\neq\varnothing$. Since the blocklength should always be clear from the context, we omit it in the $\sim$ notation.

We call a family $\{\mathbf{F}(0),\dots,\mathbf{F}(M-1)\}$ of disjoint subsets of $\mathcal{A}^n$ an *independent system in* $G(\mathbf{T}^n)$ if for all $m,m'\in\{0,\dots,M-1\}$ with $m\neq m'$, we have $a(1:n)\not\sim a'(1:n)$ for all $a(1:n)\in\mathbf{F}(m), a'(1:n)\in\mathbf{F}(m')$. Clearly, every independent system consisting of M disjoint subsets of $\mathcal{A}$ is a zero-error (n,M)-code for $\mathbf{T}$ and vice versa. Finding the zero-error capacity of $\mathbf{T}$, therefore, amounts to finding the asymptotic behavior, as $n\to\infty$, of the sizes of maximum independent systems of the graphs $G(\mathbf{T}^n)$.

Given two blocklengths n_1 and n_2 and elements $a(1:n_1+n_2)$ and $a'(1:n_1+n_2)$ of $\mathcal{A}^{n_1+n_2}$, note that $a(1:n_1+n_2)\sim a'(1:n_1+n_2)$ if and only if one of the following holds:

1) $a(1:n_1)=a'(1:n_1)$ and $a(n_1+1:n_2)\sim a'(n_1+1:n_2)$;
2) $a(1:n_1)\sim a'(1:n_1)$ and $a(n_1+1:n_2)=a'(n_1+1:n_2)$;
3) $a(1:n_1)\sim a'(1:n_1)$ and $a(n_1+1:n_2)\sim a'(n_1+1:n_2)$.

We can, therefore, say that $G(\mathbf{T}^{n_1+n_2})$ is the *strong graph product* of $G(\mathbf{T}^{n_1})$ and $G(\mathbf{T}^{n_2})$, see [22, Definition 1.9.4]. In particular, $G(\mathbf{T}^n)$ is the n-fold product of $G(\mathbf{T})$ with itself.

3) Zero-error secrecy capacity and hypergraphs: Let $(\mathbf{T}_B,\mathbf{T}_C)$ be an uncertain wiretap channel and n a blocklength. In order to use the above-mentioned graph-theoretic framework for zero-error capacity also in the treatment of the zero-error secrecy capacity of $(\mathbf{T}_B,\mathbf{T}_C)$, we introduce an additional structure on $\mathcal{A}^n$, which is induced by $\mathbf{T}_C$. Every output $c(1:n)$ of $\mathbf{T}_C^n$ generates the set $e^{(n)}(c(1:n)) := \mathbf{T}_C^{-n}(c(1:n))\subseteq\mathcal{A}^n$. We set $\mathcal{E}(\mathbf{T}_C^n) := \{e^{(n)}(c(1:n)) : c(1:n)\in\operatorname{ran}(\mathbf{T}_C^n)\}$. Every element $e^{(n)}$of $\mathcal{E}(\mathbf{T}_C^n)$ is called a *hyperedge* and the pair $(\mathcal{A}^n,\mathcal{E}(\mathbf{T}_C^n))$ a *hypergraph* denoted by $H(\mathbf{T}_C^n)$.

Now, let $\mathbf{F}$ be a zero-error (n,M)-code for $\mathbf{T}_B$. Then, by definition, it is a zero-error wiretap (n,M)-code for $(\mathbf{T}_B,\mathbf{T}_C)$ if and only if $\sharp\{m:\mathbf{F}(m)\cap e^{(n)}\}\geq 2$ for every $e^{(n)}\in\mathcal{E}(\mathbf{T}_C^n)$. In other words, together with the aforementioned observation about zero-error codes and graphs, we obtain the following lemma.

Lemma 8: A family $\{\mathbf{F}(0),\dots,\mathbf{F}(M-1)\}$ of disjoint subsets of $\mathcal{A}^n$ is a zero-error wiretap (n,M)-code for $(\mathbf{T}_B,\mathbf{T}_C)$ if and only if it is an independent system in $G(\mathbf{T}_B^n)$ and if $\sharp\{m:\mathbf{F}(m)\cap e^{(n)}\}\geq 2$ for every $e^{(n)}\in\mathcal{E}(\mathbf{T}_C^n)$.

Observe that every $e^{(n)}\in\mathcal{E}(\mathbf{T}_C^n)$ has the form $e_1\times\cdots\times e_n$ for some $e_1,\dots,e_n\in\mathcal{E}(\mathbf{T}_C)$, and that every Cartesian product $e_1\times\cdots\times e_n$ of elements of $\mathcal{E}(\mathbf{T}_C)$ is an element of $\mathcal{E}(\mathbf{T}_C^n)$. This means that $H(\mathbf{T}_C^n)$ is the *square product* of $H(\mathbf{T}_C)$ (see [23]). For the uncertain wiretap channel from Fig. 2(b), the corresponding graph/hypergraph pair at blocklength 1 and a zero-error wiretap code are illustrated in Fig. 6.

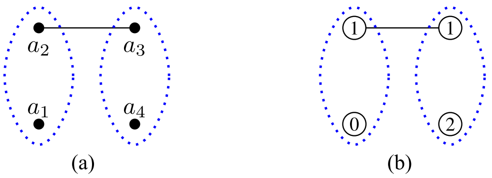

Fig. 6. (a) Pair $(G(\mathbf{T}_B),H(\mathbf{T}_C))$ corresponding to the uncertain wiretap channel $(\mathbf{T}_B,\mathbf{T}_C)$ from Fig. 2(b). The black, solid line means that a_2 and a_3 are adjacent to each other in $G(\mathbf{T}_B)$. The blue, dotted lines are the boundaries of the hyperedges of $H(\mathbf{T}_C)$. (b) Number inscribed on each node indicates to which set $\mathbf{F}(m)$ the node belongs, where $\mathbf{F}$ is the zero-error wiretap code defined in Fig. 2(b).

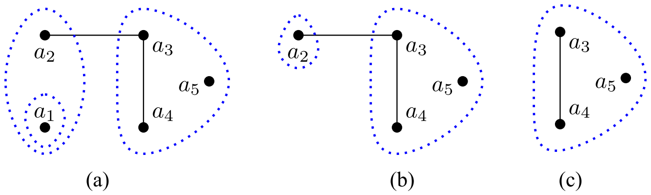

Fig. 7. (a) Original graph/hypergraph pair $(G(\mathbf{T}_B),H(\mathbf{T}_C))$ of some uncertain wiretap channel $(\mathbf{T}_B,\mathbf{T}_C)$. a_1 cannot be used in any zero-error wiretap code. (b) If a_1 is not used in any zero-error wiretap code, then a_2 is unusable as well. (c) Having eliminated a_1 and a_2, there are no singletons or cliques left among the hyperedges.

4) Proving Theorem 2: Theorem 2 will follow from a slightly more general lemma that holds for general wiretap channels. This lemma analyzes a procedure, to be presented next, which eliminates elements $a(1:n)$ from $\mathcal{A}^n$ that do not satisfy a necessary condition for being a codeword of a zero-error wiretap code. The idea behind the procedure is that by Lemma 8, no $a(1:n)\in\mathcal{A}^n$ can be a codeword that is contained in an $e^{(n)}\in\mathcal{E}(\mathbf{T}_C^n)$, which is a singleton or where all elements of $e^{(n)}$ are connected in $G(\mathbf{T}_B^n)$. Thus, these elements can be neglected when looking for a zero-error wiretap code. This amounts to deleting those elements from the input alphabet and to restricting the wiretap channel to the reduced alphabet, but not using a certain subset of the input alphabet may generate yet another set of unusable input words. Thus, a further reduction of the input alphabet may be necessary, and so on (see Fig. 7). We now formalize this procedure and analyze the result.

We apply the graph/hypergraph language developed above and start with introducing some terminology. Let $(\mathbf{T}_B,\mathbf{T}_C)$ be an uncertain wiretap channel with input alphabet $\mathcal{A}$. For any subset $\mathcal{A}'$ of $\mathcal{A}$, one can consider the uncertain wiretap channel restricted to inputs from $\mathcal{A}'$, thus creating an uncertain wiretap channel $(\mathbf{T}_B|_{\mathcal{A}'}:\mathcal{A}'\to 2^{\mathcal{B}}_*, \mathbf{T}_C|_{\mathcal{A}'}:\mathcal{A}'\to 2^{\mathcal{C}}_*)$ satisfying $\mathbf{T}_B|_{\mathcal{A}'}(a)=\mathbf{T}_B(a)$ and $\mathbf{T}_C|_{\mathcal{A}'}(a)=\mathbf{T}_C(a)$ for all $a\in\mathcal{A}'$. Thus, $\mathbf{T}_B|_{\mathcal{A}'}$ generates a graph $G(\mathbf{T}_B|_{\mathcal{A}'})$ on $\mathcal{A}'$ and $\mathbf{T}_C|_{\mathcal{A}'}$ generates a hypergraph $H(\mathbf{T}_C|_{\mathcal{A}'})$ on $\mathcal{A}'$. If we say that we *eliminate* a set $\mathcal{V}$ from $G(\mathbf{T}_B)$ or $H(\mathbf{T}_C)$, we mean that we pass from $G(\mathbf{T}_B)$ to $G(\mathbf{T}_B|_{\mathcal{A}\setminus\mathcal{V}})$ or from $H(\mathbf{T}_C)$ to $H(\mathbf{T}_C|_{\mathcal{A}\setminus\mathcal{V}})$, respectively. Further, a *clique in* $G(\mathbf{T}_B)$ is a subset $\mathcal{V}\subseteq\mathcal{A}$ such that

$a \sim a'$ for all $a, a' \in \mathcal{V}$. We write

$$\begin{aligned}&\mathcal{E}(G(\mathbf{T}_B), H(\mathbf{T}_C))_{s,c}\\ &:= \{e \in \mathcal{E}(\mathbf{T}_C) : \sharp e = 1 \text{ or } e \text{ is clique in } G(\mathbf{T}_B)\}.\end{aligned}$$

Finally, we can formalize the procedure of deleting some of the unusable input words from the input alphabet of an uncertain wiretap channel. Let $(\mathbf{T}_B, \mathbf{T}_C)$ be an uncertain wiretap channel with input alphabet $\mathcal{A}$, and fix a blocklength $n \geq 1$. For the sake of shorter notation, we use the notation a^n for the elements of $\mathcal{A}^n$ in the rest of the section. Put $\mathcal{A}^{(n)}_{s,c}(-1) = \varnothing$ and for $i \geq 0$, set

$$G^{(n)}(i) := G(\mathbf{T}^n_B|_{\mathcal{A}^n \setminus \mathcal{A}^{(n)}_{s,c}(i-1)}) \tag{25}$$

$$H^{(n)}(i) := H(\mathbf{T}^n_C|_{\mathcal{A}^n \setminus \mathcal{A}^{(n)}_{s,c}(i-1)}) \tag{26}$$

$$\begin{aligned}\mathcal{A}^{(n)}_{s,c}(i) := \{a^n \colon \exists\, e^{(n)} \in \mathcal{E}(G^{(n)}(i), H^{(n)}(i))_{s,c} : a^n \in e^{(n)}\}\\ \cup\, \mathcal{A}^{(n)}_{s,c}(i-1).\end{aligned} \tag{27}$$

Note that $\mathcal{A}^{(n)}_{s,c}(-1) \subseteq \mathcal{A}^{(n)}_{s,c}(0) \subseteq \mathcal{A}^{(n)}_{s,c}(1) \subseteq \cdots$. Define

$$\begin{aligned}I^{(n)} &:= [\min\{i \geq -1 : \mathcal{A}^{(n)}_{s,c}(i+1) = \mathcal{A}^{(n)}_{s,c}(i)\}]_+\\ \mathcal{A}^{(n)}_{s,c} &:= \mathcal{A}^{(n)}_{s,c}(I^{(n)})\end{aligned}$$

where we set $[x]_+ = \max\{x, 0\}$ for any real number x. Thus, $I^{(n)} + 1$ is the number of steps of the procedure (25)–(27), where the input alphabet is strictly reduced. The reason for defining $I^{(n)}$ in the way we have done will become clear in the proof of Lemma 10. Since $\mathcal{A}$ is finite, clearly $I^{(n)} < \infty$.

The next lemma states that not being an element of $\mathcal{A}^{(n)}_{s,c}$ is a necessary condition for any $a^n \in \mathcal{A}^n$ to be the codeword of a zero-error wiretap code.

Lemma 9: If $\mathbf{F}$ is a zero-error wiretap (n, M)-code for $(\mathbf{T}_B, \mathbf{T}_C)$ and any $M \geq 2$, then $\operatorname{ran}(\mathbf{F}) \cap \mathcal{A}^{(n)}_{s,c} = \varnothing$.

Proof: We use induction over the reduction steps i. Let $M \geq 2$ and assume that $\mathbf{F}$ is a zero-error wiretap (n, M)-code for $(\mathbf{T}_B, \mathbf{T}_C)$. By Lemma 8, it is clear that $\operatorname{ran}(\mathbf{F}) \cap \mathcal{A}^{(n)}_{s,c}(0) = \varnothing$. Thus, $\mathbf{F}$ is also a zero-error wiretap M-code for the reduced uncertain wiretap channel $(\mathbf{T}^n_B|_{\mathcal{A}^n \setminus \mathcal{A}^{(n)}_{s,c}(0)}, \mathbf{T}^n_C|_{\mathcal{A}^n \setminus \mathcal{A}^{(n)}_{s,c}(0)})$. In particular, if $e^{(n)} \in \mathcal{E}(G^{(n)}(1), H^{(n)}(1))_{s,c}$, then $e^{(n)} \cap \operatorname{ran}(\mathbf{F}) = \varnothing$. Now, note that the union of all $e^{(n)} \in \mathcal{E}(G^{(n)}(1), H^{(n)}(1))_{s,c}$ equals $\mathcal{A}^{(n)}_{s,c}(1) \setminus \mathcal{A}^{(n)}_{s,c}(0)$. Therefore, $\operatorname{ran}(\mathbf{F}) \cap \mathcal{A}^{(n)}_{s,c}(1) = \varnothing$. Repeating this argument $I^{(n)}$ times, one obtains the statement of the lemma. ■

The crucial point about the above-mentioned elimination procedure is that one can relate $\mathcal{A}^{(n)}_{s,c}$ to $\mathcal{A}^{(1)}_{s,c}$, which in turn will give us Theorem 2.

Lemma 10: For any uncertain wiretap channel $(\mathbf{T}_B, \mathbf{T}_C)$ and every blocklength $n \geq 1$, the corresponding set $\mathcal{A}^{(n)}_{s,c}$ satisfies $\mathcal{A}^{(n)}_{s,c} = (\mathcal{A}^{(1)}_{s,c})^n$.

Before proving Lemma 10, we show how Theorem 2 follows from it.

Proof of Theorem 2: Observe that one can restrict attention to singleton zero-error wiretap codes because the injectivity of $\mathbf{T}_B$ implies that no vertices are connected in $G(\mathbf{T}^n_B)$ for any n. Further, since $H(\mathbf{T}_C|_{\mathcal{A}^n \setminus \mathcal{A}^{(n)}_{s,c}})$ has no singletons as hyperedges by the construction of $\mathcal{A}^{(n)}_{s,c}$, we conclude that $N_{(\mathbf{T}_B, \mathbf{T}_C)}(n) = (\sharp\,\mathcal{A})^n - \sharp\,\mathcal{A}^{(n)}_{s,c}$. By Lemma 10, we have $\sharp\,\mathcal{A}^{(n)}_{s,c} = (\sharp\,\mathcal{A}^{(1)}_{s,c})^n$. Thus, if $\mathcal{A}^{(1)}_{s,c}$ is a strict subset of $\mathcal{A}$, then

$$C_0(\mathbf{T}_B, \mathbf{T}_C) = \lim_{n\to\infty} \frac{\log N_{(\mathbf{T}_B, \mathbf{T}_C)}(n)}{n} = \log \sharp\,\mathcal{A}.$$

Otherwise, $C_0(\mathbf{T}_B, \mathbf{T}_C)$ obviously equals 0. ■

Proof of Lemma 10: Fix $n \geq 2$. We set $\sigma := I^{(1)}$ and define a mapping $\iota : \mathcal{A} \to \{0, \ldots, \sigma\} \cup \{\infty\}$

$$\iota(a) = \begin{cases}\text{the } i \text{ with } a \in \mathcal{A}^{(1)}_{s,c}(i) \setminus \mathcal{A}^{(1)}_{s,c}(i-1), & \text{if } a \in \mathcal{A}^{(n)}_{s,c}\\ \infty & \text{otherwise.}\end{cases}$$

We also define

$$\iota^{(n)}(a^n) = (\iota(a_1), \ldots, \iota(a_n)).$$

Similarly, for $e \in \mathcal{E}(\mathbf{T}_C)$ with $e \subset \mathcal{A}^{(1)}_{s,c}$, we set $\iota(e) := \max\{\iota(a) : a \in e\}$, and for any $e^{(n)} \in \mathcal{E}(\mathbf{T}^n_C)$, we define $\iota^{(n)}(e^{(n)}) = (\iota(e_1), \ldots, \iota(e_n))$.

For any $i^n \in (\{0, \ldots, \sigma\} \cup \{\infty\})^n$, we set

$$f(i^n) = \{a^n \in (\mathcal{A}^{(1)}_{s,c})^n : \iota^{(n)}(a^n) = i^n\}, \quad w(i^n) = \sum_{t=1}^{n} i_t$$

and for $\mu \geq 0$

$$F(\mu) := \bigcup_{i^n \in \{0,\ldots,\sigma\}^n : w(i^n) \leq \mu} f(i^n).$$

Note that $F(n\sigma) = (\mathcal{A}^{(1)}_{s,c})^n$. We will now prove that

$$F(\mu) = \mathcal{A}^{(n)}_{s,c}(\mu), \quad \text{for } 0 \leq \mu \leq n\sigma \tag{28}$$

$$I^{(n)} = n\sigma = nI^{(1)}. \tag{29}$$

Together, (28) and (29) imply $(\mathcal{A}^{(1)}_{s,c})^n = F(nI^{(1)}) = \mathcal{A}^{(n)}_{s,c}$, which is what we want to prove.

We first prove (28) by induction over μ. Let $\mu = 0$. Then, $F(0) = (\mathcal{A}^{(1)}_{s,c}(0))^n$. This is equal to $\mathcal{A}^{(n)}_{s,c}(0)$.

Next, let $0 \leq \mu \leq n\sigma - 1$ and assume (28) has been proven for all $0 \leq \mu' \leq \mu$. We need to show that (28) holds for $\mu + 1$. First, we show that $F(\mu + 1) \subseteq \mathcal{A}^{(n)}_{s,c}(\mu + 1)$.

Let $i^n \in \{0, \ldots, \sigma\}^n$ with $w(i^n) = \mu + 1$. We have to show that $f(i^n) \subseteq \mathcal{A}^{(n)}_{s,c}(\mu + 1)$. Choose an a^n with $\iota(a^n) = i^n$. Then, by (27), for every $1 \leq t \leq n$, there exists an $e_t \in \mathcal{E}(\mathbf{T}_C)$ such that $a^n \in e^{(n)} = e_1 \times \cdots \times e_n$ and $\iota^{(n)}(e^{(n)}) = i^n$. Therefore, we have

$$\begin{aligned}&e^{(n)} \setminus \mathcal{A}^{(n)}_{s,c}(\mu) \overset{(a)}{=} e^{(n)} \setminus F(\mu)\\ &\overset{(b)}{=} (e_1 \setminus \mathcal{A}^{(1)}_{s,c}(\iota(e_1) - 1)) \times \cdots \times (e_n \setminus \mathcal{A}^{(1)}_{s,c}(\iota(e_n) - 1))\end{aligned} \tag{30}$$

where (a) is due to the induction hypothesis and (b) holds because $e_t \setminus \mathcal{A}^{(1)}_{s,c}(\iota(e_t)) = \varnothing$. By the definition of the mapping ι, every set $e_t \setminus \mathcal{A}^{(1)}_{s,c}(\iota(e_t) - 1)$ is a singleton or a clique, hence, so is the right-hand side of (30). Thus, $e^{(n)} \setminus \mathcal{A}^{(n)}_{s,c}(\mu) \in \mathcal{E}(G^{(n)}(\mu + 1), H^{(n)}(\mu + 1))_{s,c}$; hence, $a^n \in \mathcal{A}^{(n)}_{s,c}(\mu + 1)$. This proves $F(\mu + 1) \subseteq \mathcal{A}^{(n)}_{s,c}(\mu + 1)$.

Now, we prove that $\mathcal{A}_{s,c}^{(n)}(\mu+1)\subseteq F(\mu+1)$, which is equivalent to showing that $\mathcal{A}^n\setminus F(\mu+1)\subseteq\mathcal{A}^n\setminus\mathcal{A}_{s,c}^{(n)}(\mu+1)$. Let $a^n\in\mathcal{A}^n\setminus F(\mu+1)$. Thus, $a^n\in\mathcal{A}^n\setminus F(\mu)=\mathcal{A}^n\setminus\mathcal{A}_{s,c}^{(n)}(\mu)$, where the equality is due to the induction hypothesis. We need to show that $e^{(n)}\setminus\mathcal{A}_{s,c}^{(n)}(\mu)\not\subseteq\mathcal{A}_{s,c}^{(n)}(\mu+1)$ for every $e^{(n)}\in\mathcal{E}(\mathbf{T}_C^n)$ containing a^n; hence, $a^n\in\mathcal{A}^n\setminus\mathcal{A}_{s,c}^{(n)}(\mu+1)$.

Choose any $e^{(n)}=e_1\times\cdots\times e_n\in\mathcal{E}(\mathbf{T}_C^n)$ containing a^n. Let $i^n=\iota^{(n)}(a^n)$. Thus, $\iota(e_t)\ge i_t$ for every $t\in\{1,\dots,n\}$. Choose any $t_*\in\{1,\dots,n\}$. If $0\le i_{t_*}\le\sigma$, there exists an $a'_{t_*}\in e_{t_*}\setminus\mathcal{A}_{s,c}^{(1)}(i_{t_*}-2)$ with $a_{t_*}\not\sim a'_{t_*}$. Otherwise, $e_t\setminus\mathcal{A}_{s,c}^{(1)}(i_{t_*}-2)$ would be a singleton or a clique in $G^{(1)}(i_{t_*}-1)$; hence, a subset of $\mathcal{A}_{s,c}^{(1)}(i_{t_*}-1)$ contradicting $\iota(e_{t_*})\ge i_{t_*}$. A similar argument shows that there exists an $a'_{t_*}\in\mathcal{A}\setminus\mathcal{A}_{s,c}^{(1)}$ with $a'_{t_*}\not\sim a_{t_*}$ if $i_{t_*}=\infty$. Consequently, the sequence $\tilde{a}^n=(a_1,\dots,a_{t_*-1},a'_{t_*},a_{t_*+1},\dots,a_n)$ is an element of $e^{(n)}$ satisfying $a^n\not\sim\tilde{a}^n$ because $G(\mathbf{T}_B^n)$ is the n-fold strong graph product of $G(\mathbf{T}_B)$. Notice that $w(\tilde{a}^n)\ge w(a^n)-1\ge\mu+1$ because $\iota(a'_{t_*})\ge i_{t_*}-1$. In particular, $\tilde{a}^n\notin F(\mu)=\mathcal{A}_{s,c}^{(n)}(\mu)$. Thus, we have found two different $a^n,\tilde{a}^n\in e^{(n)}\setminus\mathcal{A}_{s,c}^{(n)}(\mu)$ that are not adjacent to each other, which implies $e^{(n)}\setminus\mathcal{A}_{s,c}^{(n)}(\mu)\not\subseteq\mathcal{A}_{s,c}^{(n)}(\mu+1)$. Therefore, $\mathcal{A}^n\setminus F(\mu+1)\subseteq\mathcal{A}^n\setminus\mathcal{A}_{s,c}^{(n)}(\mu+1)$, and this proves (28).

To show (29), observe that by the same argument as in the previous step, $\mathcal{A}_{s,c}^{(n)}(n\sigma+1)\subseteq F(n\sigma+1)=F(n\sigma)$. Therefore, $\mathcal{A}_{s,c}^{(n)}(n\sigma+1)=\mathcal{A}_{s,c}^{(n)}(n\sigma)$; hence, $I^{(n)}=n\sigma=nI^{(n)}$. ■

5) Examples and discussion: Example 2 The uncertain wiretap channel $(\mathbf{T}_B,\mathbf{T}_C)$ shown in Fig. 2(b) is an example of the fact that at finite blocklengths n, nonsingleton zero-error wiretap codes may be necessary to achieve $N_{(\mathbf{T}_B,\mathbf{T}_C)}(n)$. If one applies the zero-error wiretap code $\mathbf{F}=\{\{a_1\},\{a_2,a_3\},\{a_4\}\}$, then three messages can be distinguished at the intended receiver's output, and every eavesdropper output can be generated by two different messages. Hence, $\mathbf{F}$ is a zero-error wiretap $(1,3)$-code. On the other hand, the maximal M for which a singleton zero-error wiretap $(1,M)$-code exists is $M=2$; for example, $\mathbf{F}=\{\{a_1\},\{a_4\}\}$. $M=4$ is not possible because $N_{\mathbf{T}_B}(1)=3$. For $M=3$, either c_1 or c_2 would be generated by only one message.

We conjecture that nonsingleton zero-error wiretap codes are also necessary to achieve $C_0(\mathbf{T}_B,\mathbf{T}_C)$.

One can also construct examples that show the following: If there exists a zero-error wiretap (n,M)-code, then it is necessary to have nonsingleton codes to also find a zero-error wiretap (M',n)-code for every $2\le M'\le M$.

Another open question is when the zero-error wiretap capacity of general uncertain wiretap channels is positive.

Example 3: Consider the wiretap channel $(\mathbf{T}_B,\mathbf{T}_C)$ from Fig. 8 (a). Fig. 8(b) shows $\mathcal{A}$ with $G(\mathbf{T}_B)$ and $H(\mathbf{T}_C)$, and Fig. 8(c) shows $\mathcal{A}^2$ with $G(\mathbf{T}_B^2)$ and $H(\mathbf{T}_C^2)$. The code shown in Fig. 8(c) shows that $C_0(\mathbf{T}_B,\mathbf{T}_C)\ge 1$. Since $C_0(\mathbf{T}_B)=1$ by [2], we can even conclude $C_0(\mathbf{T}_B,\mathbf{T}_C)=1$.

Note that $N_{(\mathbf{T}_B,\mathbf{T}_C)}(1)=1$. Thus, the number of messages that can be transmitted securely jumps from none at blocklength 1 to 4 at blocklength 2. This behavior is remarkable when compared with the behavior of zero-error codes for uncertain channels; an uncertain channel $\mathbf{T}$ has $C_0(\mathbf{T})>0$ if and only if $N_{\mathbf{T}}(1)\ge 2$. This is a simple criterion to decide at blocklength 1, whether or not the zero-error capacity of an uncertain channel is positive. We do not yet have a general simple criterion for deciding whether or not the zero-error secrecy capacity of an uncertain wiretap channel is positive. Of course, if $\mathbf{T}_B$ is injective, then Theorem 2 provides such a criterion.

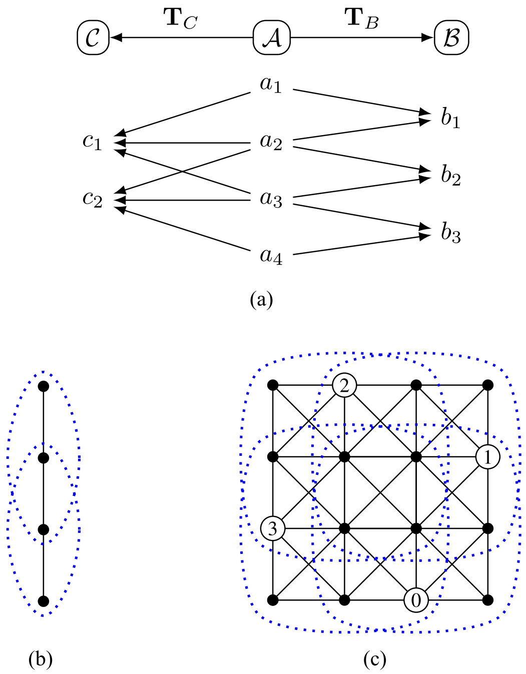

Fig. 8. (a) Uncertain wiretap channel $(\mathbf{T}_B,\mathbf{T}_C)$. (b) $\mathcal{A}$ with $G(\mathbf{T}_B)$ and $H(\mathbf{T}_C)$. (c) $\mathcal{A}^2$ with $G(\mathbf{T}_B^2)$ and $H(\mathbf{T}_C^2)$. Vertices connected by a solid black line are connected in $G(\mathbf{T}_B)$ or $G(\mathbf{T}_B^2)$, respectively. Vertices within the boundary of a blue dotted line belong to the same hyperedge of $H(\mathbf{T}_C)$ or $H(\mathbf{T}_C^2)$, respectively. A zero-error wiretap $(2,4)$-code is indicated on the right-hand figure.

Appendix B
Proofs from Quantizer Analysis

For reference, we note the following simple lemma, which is easily proved by induction.

Lemma 11: Let μ be a real number, and let $y(0\!:\!\infty)$, $v(0\!:\!\infty)$ be two sequences of real numbers satisfying $y(t+1)=\mu y(t)+v(t)$ for every $t\ge 0$. Then, for every $t\ge 0$, we have

$$y(t)=\mu^t y(0)+\sum_{i=0}^{t-1}\mu^{t-i-1}v(i).$$

Proof of Lemma 3: Note that the quantizer set $\mathcal{P}(m(0\!:\!t))$ is an interval. Thus, (13) implies $|\mathcal{I}(m(0\!:\!t+1))|=\lambda|\mathcal{P}(m(0\!:\!t))|+\Omega$. Hence, by (11), we obtain

$$|\mathcal{P}(m(0\!:\!t{+}1))|=\frac{|\mathcal{I}(m(0\!:\!t{+}1))|}{M}=\frac{\lambda}{M}|\mathcal{P}(m(0\!:\!t))|+\frac{\Omega}{M}. \tag{31}$$

Therefore, by Lemma 11, we get

$$\begin{aligned}|\mathcal{P}(m(0\!:\!t))| &= \left(\frac{\lambda}{M}\right)^t |\mathcal{P}(m(0\!:\!0))| + \frac{\Omega}{M}\sum_{i=0}^{t-1}\left(\frac{\lambda}{M}\right)^{t-i-1}\\ &= \left(\frac{\lambda}{M}\right)^t \left(\frac{|I_0|}{M} - \frac{\Omega}{M-\lambda}\right) + \frac{\Omega}{M-\lambda}\end{aligned}$$

which proves (15). The other statements of the lemma are immediate from (15). ■

Proof of Lemma 4: Let $m(0\!:\!t) \neq m'(0\!:\!t)$. It is sufficient to show that the minimal distance between $\hat{x}(m(0\!:\!t))$ and $\hat{x}(m'(0\!:\!t))$ is lower bounded by ℓ_t. By Lemma 5, we obtain

$$\hat{x}(m(0\!:\!t)) - \hat{x}(m'(0\!:\!t)) = \lambda^t \frac{|\mathcal{I}_0|}{M} \underbrace{\sum_{i=0}^{t} \frac{m(i)-m'(i)}{M^i}}_{=:n(m,m',t)}. \tag{32}$$

Since $m(i) - m'(i) \neq 0$ for at least one $i \in \{0,\ldots,t\}$, the absolute value of $n(m,m',t)$ is at least $1/M^t$. Thus, by (32), we have

$$|\hat{x}(m(0\!:\!t)) - \hat{x}(m'(0\!:\!t))| \geq \frac{|\mathcal{I}_0|}{M}\left(\frac{\lambda}{M}\right)^t. \tag{33}$$

By Lemma 3, the right-hand side of (33) equals ℓ_t. ■

Proof of Lemma 5: Recall the notation $\mathcal{I} = [\mathcal{I}_{\min}, \mathcal{I}_{\max}]$ for real intervals $\mathcal{I}$. For $t \geq 0$, we obtain

$$\begin{aligned}&\hat{x}(m(0\!:\!t+1))\\ &\overset{(a)}{=} \mathcal{I}(m(0\!:\!t))_{\min} + \left(m(t+1) + \frac{1}{2}\right)\ell_{t+1}\\ &\overset{(b)}{=} \lambda\mathcal{P}(m(0\!:\!t))_{\min} - \frac{\Omega}{2} + \left(m(t+1) + \frac{1}{2}\right)\ell_{t+1}\\ &\overset{(c)}{=} \lambda\hat{x}(m(0\!:\!t)) - \frac{\lambda\ell_t}{2} - \frac{\Omega}{2} + \left(m(t+1) + \frac{1}{2}\right)\ell_{t+1} \qquad (34)\\ &\overset{(d)}{=} \lambda\hat{x}(m(0\!:\!t)) - \frac{\lambda\ell_t}{2} - \frac{\Omega}{2} + \left(m(t+1) + \frac{1}{2}\right)\left(\frac{\lambda}{M}\ell_t + \frac{\Omega}{M}\right)\\ &= \lambda\hat{x}(m(0\!:\!t)) + \frac{\lambda\ell_t + \Omega}{2}\left(\frac{2m(t+1)+1}{M} - 1\right) \qquad (35)\end{aligned}$$

where (a) is due to (11) and (12), (b) is due to (13), (c) is again due to (12), and (d) is due to (31). Therefore, we have

$$\begin{aligned}&\hat{x}(m(0\!:\!t+1))\\ &\overset{(e)}{=} \lambda\hat{x}(m(0\!:\!t)) + \left(\frac{\lambda^{t+1}|\mathcal{I}_0|}{2M^{t+1}} - \frac{\lambda^{t+1}}{2M^t}\frac{\Omega}{M-\lambda} + \frac{\lambda}{2}\frac{\Omega}{M-\lambda} + \frac{\Omega}{2}\right)\\ &\qquad\qquad \times \left(\frac{2m(t+1)+1}{M} - 1\right)\\ &= \lambda\hat{x}(m(0\!:\!t)) + \frac{1}{2}\left(\frac{\lambda^{t+1}}{M^{t+1}}|\mathcal{I}_0| + \frac{\Omega M}{M-\lambda}\left(1 - \frac{\lambda^{t+1}}{M^{t+1}}\right)\right)\\ &\qquad\qquad \times \left(\frac{2m(t+1)+1}{M} - 1\right) \qquad (36)\end{aligned}$$

where (e) is due to (35) and (16). Consequently, we get

$$\begin{aligned}&\hat{x}(m(0\!:\!t))\\ &\overset{(f)}{=} \lambda^t\Bigg\{\hat{x}(m(0\!:\!0))\\ &\quad + \frac{1}{2}\sum_{i=0}^{t-1}\frac{1}{\lambda^{i+1}}\left(\frac{\lambda^{i+1}}{M^{i+1}}|\mathcal{I}_0| + \frac{\Omega M}{M-\lambda}\left(1 - \frac{\lambda^{i+1}}{M^{i+1}}\right)\right)\\ &\qquad\qquad \times\left(\frac{2m(i+1)+1}{M} - 1\right)\Bigg\}\\ &\overset{(g)}{=} \lambda^t\Bigg\{\hat{x}(m(0\!:\!-1)) + \frac{|\mathcal{I}_0|}{2}\left(\frac{2m(0)+1}{M} - 1\right)\\ &\quad + \frac{1}{2}\sum_{i=1}^{t}\left(\frac{|\mathcal{I}_0|}{M^i} + \frac{\Omega M}{M-\lambda}\left(\frac{1}{\lambda^i} - \frac{1}{M^i}\right)\right)\left(\frac{2m(i)+1}{M} - 1\right)\Bigg\}\\ &= \lambda^t\Bigg\{\hat{x}(m(0\!:\!-1))\\ &\quad + \frac{1}{2}\sum_{i=0}^{t}\left(\frac{\Omega M}{M-\lambda}\left(\frac{1}{\lambda^i} - \frac{1}{M^i}\right) + \frac{|\mathcal{I}_0|}{M^i}\right)\left(\frac{2m(i)+1}{M} - 1\right)\Bigg\}\end{aligned}$$

where (f) is due to Lemma 11, and the recursion formula for $\hat{x}(m(0\!:\!t))$ derived in (36) and in (g), we applied (11) to find the relation between $\hat{x}(m(0\!:\!0))$ and $\hat{x}(m(0\!:\!-1))$. ■

Proof of Lemma 6: Without loss of generality, we may assume that $\hat{x}(m(0\!:\!T)) > \hat{x}(m'(0\!:\!T))$. Then, it is sufficient to show that if (18) is satisfied, then $\hat{x}(m(0\!:\!T+t)) - \hat{x}(m'(0\!:\!T+t)) \geq \ell_{T+t}$ for all $t \geq 0$. We have

$$\begin{aligned}&\hat{x}(m(0\!:\!T+t)) - \hat{x}(m'(0\!:\!T+t))\\ &\overset{(a)}{=} \lambda^t\Bigg\{\hat{x}(m(0\!:\!T)) - \hat{x}(m'(0\!:\!T))\\ &\quad + \lambda^T\sum_{i=T+1}^{T+t}\left(\frac{\Omega}{M-\lambda}\left(\frac{1}{\lambda^i} - \frac{1}{M^i}\right) + \frac{|\mathcal{I}_0|}{M^{i+1}}\right)(m(i) - m'(i))\Bigg\}\\ &\overset{(b)}{\geq} \lambda^t\Bigg\{\hat{x}(m(0\!:\!T)) - \hat{x}(m'(0\!:\!T))\\ &\quad - \lambda^T(M-1)\sum_{i=T+1}^{T+t}\left(\frac{\Omega}{M-\lambda}\left(\frac{1}{\lambda^i} - \frac{1}{M^i}\right) + \frac{|\mathcal{I}_0|}{M^{i+1}}\right)\Bigg\}\\ &= \lambda^t\Bigg\{\hat{x}(m(0\!:\!T)) - \hat{x}(m'(0\!:\!T)) - \frac{\Omega(M-1)}{(M-\lambda)(\lambda-1)}(1 - \lambda^{-t})\\ &\quad - \frac{\lambda^T}{M^T}\left(\frac{|\mathcal{I}_0|}{M} - \frac{\Omega}{M-\lambda}\right)(1 - M^{-t})\Bigg\} \qquad (37)\end{aligned}$$

where (a) is due to Lemma 5 and (b) holds because $m(i) - m'(i) \geq -(M-1)$ for all i. Thus, one obtains

$$\frac{\hat{x}(m(0\!:\!T+t)) - \hat{x}(m'(0\!:\!T+t)) - \ell_{T+t}}{\lambda^t} \tag{38}$$

$$\begin{aligned}
&\overset{(c)}{\geq} \hat{x}(m(0{:}T)) - \hat{x}(m'(0{:}T)) - \frac{\Omega}{M-\lambda} \\
&\quad\times\left(\frac{M-1}{\lambda-1}(1-\lambda^{-t}) - \frac{\lambda^T}{M^T}(1-M^{-t}) + \frac{1}{\lambda^t} - \frac{\lambda^T}{M^{T+t}}\right) \\
&\quad - \frac{|\mathcal{I}_0|}{M}\left(\frac{\lambda^T}{M^T}(1-M^{-t}) + \frac{\lambda^T}{M^{T+t}}\right) \\
&= \hat{x}(m(0{:}T)) - \hat{x}(m'(0{:}T)) \\
&\quad - \frac{\Omega}{M-\lambda}\left(\frac{M-1}{\lambda-1}(1-\lambda^{-t}) - \frac{\lambda^T}{M^T} + \frac{1}{\lambda^t}\right) - \frac{|\mathcal{I}_0|}{M}\frac{\lambda^T}{M^T}
\end{aligned} \tag{39}$$

where (37) and Lemma 3 were used in (c). Since we want (38) to be positive for every $t \geq 0$, it is sufficient by (39) to have

$$\begin{aligned}
&\hat{x}(m(0{:}T)) - \hat{x}(m'(0{:}T)) \\
&\geq \max_{t\geq 0}\left\{\frac{\Omega}{M-\lambda}\left(\frac{M-1}{\lambda-1}(1-\lambda^{-t}) - \frac{\lambda^T}{M^T} + \frac{1}{\lambda^t}\right) + \frac{|\mathcal{I}_0|}{M}\frac{\lambda^T}{M^T}\right\} \\
&= \frac{\Omega}{M-\lambda}\left(\frac{M-1}{\lambda-1} - \frac{\lambda^T}{M^T} + 1\right) + \frac{|\mathcal{I}_0|}{M}\frac{\lambda^T}{M^T} \\
&\overset{(d)}{=} \frac{\Omega}{M-\lambda}\frac{M-1}{\lambda-1} + \ell_T
\end{aligned}$$

where (d) is due to Lemma 3. Thus, the inequality holds if (18) is satisfied. ■

Proof of Lemma 7: If we can show that

$$\begin{aligned}
&\hat{x}(m_{\xi(1:j-1)\xi(j)}(0{:}jT-1)) - \hat{x}(m_{\xi(1:j-1)\xi'(j)}(0{:}jT-1)) \\
&> \frac{\Omega}{M-\lambda}\frac{M-1}{\lambda-1} + \ell_{jT-1}
\end{aligned} \tag{40}$$

for every $j \geq 1$, every $\xi(1{:}j-1) \in \{1,\dots,\gamma\}^{j-1}$, and every $\xi(j), \xi'(j) \in \{1,\dots,\gamma\}$ with $\xi(j) > \xi'(j)$, then the claim of the lemma follows from Lemma 6. We have

$$\begin{aligned}
&\hat{x}(m_{\xi(1:j-1)\xi(j)}(0{:}jT-1)) - \hat{x}(m_{\xi(1:j-1)\xi'(j)}(0{:}jT-1)) \\
&\overset{(a)}{=} \lambda^{jT-1}\sum_{i=(j-1)T}^{jT-1}\left(\frac{\Omega M}{M-\lambda}\left(\frac{1}{\lambda^i} - \frac{1}{M^i}\right) + \frac{|\mathcal{I}_0|}{M^i}\right) \\
&\qquad \frac{m_{\xi(j)}(i) - m_{\xi'(j)}(i)}{M} \\
&\overset{(b)}{\geq} \frac{\Omega}{M-\lambda}\frac{\lambda^T-1}{\lambda-1} + \left(\frac{|\mathcal{I}_0|}{M} - \frac{\Omega}{M-\lambda}\right)\frac{\lambda^{jT-1}}{M^{(j-1)T-1}}\frac{1-M^{-T}}{M-1} \\
&\overset{(c)}{=} \frac{\Omega}{M-\lambda}\frac{M-1}{\lambda-1} + \ell_{jT-1} + \frac{\Omega}{M-\lambda}\frac{\lambda^T-M-\lambda+1}{\lambda-1} \\
&\quad + \left(\frac{|\mathcal{I}_0|}{M} - \frac{\Omega}{M-\lambda}\right)\left(\frac{\lambda}{M}\right)^{jT-1}\frac{M^T-M}{M-1} \\
&=: \frac{\Omega}{M-\lambda}\frac{M-1}{\lambda-1} + \ell_{jT-1} + A_{jT}
\end{aligned} \tag{41}$$

where (a) is due to Lemma 5, (b) uses $m_{\xi(j)}(i) - m_{\xi'(j)}(i) \geq 1$, which holds due to the choice of $\xi(j), \xi'(j)$, and Lemma 3 was used in (c). It remains to show that $A_{jT} \geq 0$. Since $\lambda^T \geq M + \lambda - 1$ for T satisfying (19), this is clear in the case where $|\mathcal{I}_0|/M \geq \Omega/(M-\lambda)$. Otherwise, we lower bound A_{jT} by A_T, for which we have

$$\begin{aligned}
&A_T + \frac{\Omega(M+\lambda-1)}{(M-\lambda)(\lambda-1)} \\
&\geq \frac{\Omega}{M-\lambda}\lambda^T\left(\frac{1}{\lambda-1} - \frac{M}{\lambda(M-1)}\right) \\
&\overset{(d)}{\geq} \frac{\Omega}{M-\lambda}\frac{\lambda(M-1)(M+\lambda-1)}{M-\lambda}\frac{M-\lambda}{\lambda(\lambda-1)(M-1)} \\
&= \frac{\Omega(M+\lambda-1)}{(M-\lambda)(\lambda-1)}
\end{aligned}$$

where (d) is due to (19). This implies $A_T \geq 0$; hence, $A_{jT} \geq 0$ for all $j \geq 1$. With (41), this implies (40) for all choices of j, $\xi(1{:}j-1)$, and $\xi(j) > \xi'(j)$ and hence, completes the proof of the lemma. ■

References

[1] H. Sandberg, S. Amin, and K. H. Johansson, “Cyberphysical security in networked control systems: An introduction to the issue,” *IEEE Control Syst.*, vol. 35, no. 1, pp. 20–23, Feb. 2015.

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

[3] A. S. Matveev and A. V. Savkin, “Shannon zero error capacity in the problems of state estimation and stabilization via noisy communication channels,” *Int. J. Control*, vol. 80, no. 2, pp. 241–255, 2007.

[4] G. N. Nair, F. Fagnani, S. Zampieri, and R. J. Evans, “Feedback control under data rate constraints: An overview,” *Proc. IEEE*, vol. 95, no. 1, pp. 108–137, Jan. 2007.

[5] G. N. Nair, “A nonstochastic information theory for communication and state estimation,” *IEEE Trans. Autom. Control*, vol. 58, no. 6, pp. 1497–1510, Jun. 2013.

[6] Y. Liang, H. V. Poor, and S. Shamai, “Information theoretic security,” *Found. Trends Commun. Inf. Theory*, vol. 5, no. 4–5, pp. 355–580, 2009.

[7] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[8] A. D. Wyner, “The wire-tap channel,” *The Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[9] C. De Persis and P. Tesi, “Input-to-state stabilizing control under denial-of-service,” *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 2930–2944, Nov. 2015.

[10] H. Fawzi, P. Tabuada, and S. Diggavi, “Secure estimation and control for cyber-physical systems under adversarial attacks,” *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1454–1467, Jun. 2014.

[11] A. Gupta, A. Nayyar, C. Langbort, and T. Başar, “A dynamic transmitter-jammer game with asymmetric information,” in *Proc. 51st IEEE Conf. Decision Control*, pp. 6477–6482, Dec. 2012.

[12] M. Pajic, P. Tabuada, I. Lee, and G. J. Pappas, “Attack-resilient state estimation in the presence of noise,” in *Proc. 54th IEEE Conf. Decision Control*, 2015, pp. 5827–5832.

[13] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, “A secure control framework for resource-limited adversaries,” *Automatica*, vol. 51, pp. 135–148, 2015.

[14] H. Li, L. Lai, and W. Zhang, “Communication requirement for reliable and secure state estimation and control in smart grid,” *IEEE Trans. Smart Grid*, vol. 2, no. 3, pp. 476–486, Sep. 2011.

[15] A. Tsiamis, K. Gatsis, and G. P. Pappas, “State estimation with secrecy against eavesdroppers,” *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 8385–8392, Jul. 2017.

[16] J. Körner and A. Orlitsky, “Zero-error information theory,” *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2207–2229, Oct. 1998.

[17] M. Fekete, “Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten,” *Math. Z.*, vol. 17, no. 1, pp. 228–249, 1923.

[18] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[19] M. R. Bloch and J. N. Laneman, "Strong secrecy from channel resolvability," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 8077–8098, Dec. 2013.

[20] M. Wiese, J. Nötzel, and H. Boche, "A channel under simultaneous jamming and eavesdropping attack—Correlated random coding capacities under strong secrecy criteria," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3844–3862, Jul. 2016.

[21] W. S. Wong and R. W. Brockett, "Systems with finite communication bandwidth constraints—Part I: State estimation problems," *IEEE Trans. Autom. Control*, vol. 42, no. 9, pp. 1294–1299, Sep. 1997.

[22] R. Balakrishnan and K. Ranganathan, *A Textbook of Graph Theory*. New York, NY, USA: Springer-Verlag, 2012.

[23] M. Hellmuth, L. Ostermeier, and P. Stadler, "A survey on hypergraph products," *Math. Comput. Sci.*, vol. 6, no. 1, pp. 1–32, 2012.

Moritz Wiese (S'09–M'15) received the Dipl.-Math. degree in mathematics from the University of Bonn, Bonn, Germany, in 2007, and the Ph.D. degree in information theory from Technische Universität München, Munich, Germany, in 2013.

From 2007 to 2010, he was a Research Assistant with Technische Universität Berlin, Berlin, Germany. From 2010 to 2014, he was with Technische Universität München. From 2014 to 2016, he was with the KTH Royal Institute of Technology, Stockholm, Sweden. He is now with Technische Universität München, Munich, Germany.

Tobias J. Oechtering (S'01–M'08–SM'12) received the Dipl-Ing degree in electrical engineering and information technology in 2002 from RWTH Aachen University, Aachen, Germany, the Dr-Ing degree in electrical engineering in 2007 from Technische Universität Berlin, Berlin, Germany, and the Docent degree in communication theory in 2012 from KTH Royal Institute of Technology, Stockholm, Sweden.

He joined the Communication Theory Lab at KTH Royal Institute of Technology in 2008 and has been an Associate Professor there since May 2013. His research interests include networked control, physical layer security and privacy, information theory, wireless communication, and statistical signal processing.

Dr. Oechtering was the recipient of the "Förderpreis 2009" Award from the Vodafone Foundation. Since June 2016, he has been an Associate Editor for the IEEE Transactions on Information Forensic and Security. From 2012 to 2015, he was an Editor for the IEEE Communications Letters.

Karl Henrik Johansson (F'13) received the M.Sc. and Ph.D. degrees in electrical engineering from Lund University, Lund, Sweden, in 1992 and 1997, respectively.

He is currently the Director of the Strategic Research Area ICT The Next Generation, Stockholm, Sweden, and also a Professor with the School of Electrical Engineering, KTH Royal Institute of Technology, Stockholm, Sweden. He has held visiting positions at UC Berkeley, Caltech, NTU, HKUST Institute of Advanced Studies, and NTNU. His research interests are in networked control systems, cyberphysical systems, and applications in transportation, energy, and automation.

Dr. Johansson was a recipient of several Best Paper Awards and other distinctions, including a ten-year Wallenberg Scholar Grant, a Senior Researcher position with the Swedish Research Council, and the Future Research Leader Award from the Swedish Foundation for Strategic Research. He is a member of the IEEE Control Systems Society Board of Governors and the European Control Association Council. He is a Distinguished Lecturer with the IEEE Control Systems Society.

Panagiotis (Panos) Papadimitratos (M'00–SM'17) received the Ph.D. degree in electrical and computer engineering from Cornell University, Ithaca, NY, USA, in 2005.

He is currently a tenured Professor with KTH Royal Institute of Technology, Stockholm, Sweden, where he leads the Networked Systems Security group. At KTH, he is affiliated with the ACCESS center, leading its security, privacy, and trust thematic area, as well as with the ICES center, where he leads the Industrial Competence Group on Security. He has held positions at Virginia Tech, EPFL, and Politecnico of Torino. His research interests include a gamut of security and privacy problems, with emphasis on wireless networks.

Dr. Papadimitratos is a Knut and Alice Wallenberg Academy fellow and a member of the Young Academy of Europe. He was the recipient of the Swedish Science Foundation Young Researcher Award. He has delivered numerous invited talks, keynotes, and panel addresses, as well as tutorials in flagship conferences. He currently serves as an Associate Editor for the IEEE Transactions on Mobile Computing and the ACM/IEEE Transactions on Networking. He has served in numerous program committees, with leading roles in numerous occasions; recently, in 2016, as the Program Co-Chair for the ACM WiSec and the TRUST conferences; he serves as the General Chair of the ACM WISec (2018) and PETS (2019) conferences.

Henrik Sandberg (S'01–M'07) received the M.Sc. degree in engineering physics and the Ph.D. degree in automatic control from Lund University, Lund, Sweden, in 1999 and 2004, respectively.

He is currently a Professor with the Department of Automatic Control, KTH Royal Institute of Technology, Stockholm, Sweden. From 2005 to 2007, he was a Postdoctoral Scholar with the California Institute of Technology, Pasadena, CA, USA. In 2013, he was a visiting scholar with the Laboratory for Information and Decision Systems (LIDS), MIT, Cambridge, MA, USA. He has also held visiting appointments at the Australian National University and the University of Melbourne, Australia. His research interests include security of cyberphysical systems, power systems, model reduction, and fundamental limitations in control.

Dr. Sandberg was a recipient of the Best Student Paper Award from the *IEEE Conference on Decision and Control* in 2004 and an Ingvar Carlsson Award from the Swedish Foundation for Strategic Research in 2007. He is Associate Editor for the *IFAC Journal Automatica* and the IEEE Transactions on Automatic Control.

Mikael Skoglund (S'93–M'97–SM'04) received the Ph.D. degree in information theory from the Chalmers University of Technology, Gothenburg, Sweden, in 1997.

In 1997, he joined the Royal Institute of Technology (KTH), Stockholm, Sweden, where he was appointed as the Chair in Communication Theory in 2003. At KTH, he heads the Communication Theory Division and he is also an Assistant Dean in electrical engineering. He is also a founding faculty member of the ACCESS Linnaeus Center and the Director of the Center Graduate School. He has authored and co-authored more than 130 journal and 300 conference papers, and he holds six patents. His research interests include problems in source-channel coding, coding and transmission for wireless communications, communication and control, Shannon theory, and statistical signal processing.

Dr. Skoglund has served on numerous technical program committees for IEEE sponsored conferences. From 2003 to 2008, he was an Associate Editor for the IEEE Transactions on Communications, and from 2008 to 2012, he was on the editorial board of the IEEE Transactions on Information Theory.