An Overview of Information-Theoretic Security and Privacy: Metrics, Limits and Applications

Matthieu Bloch, *Senior Member, IEEE*, Onur Günlü, *Member, IEEE*, Aylin Yener, *Fellow, IEEE*, Frédérique Oggier, H. Vincent Poor, *Life Fellow, IEEE*, Lalitha Sankar, *Senior Member, IEEE*, and Rafael F. Schaefer, *Senior Member, IEEE*

***Abstract*—This tutorial reviews fundamental contributions to information security. An integrative viewpoint is taken that explains the security metrics, including secrecy, privacy, and others, the methodology of information-theoretic approaches, along with the arising system design principles, as well as techniques that enable the information-theoretic designs to be applied in real communication and computing systems. The tutorial, while summarizing these contributions, argues for the simultaneous pivotal role of fundamental limits and coding techniques for secure communication system design.**

***Index Terms*—Information-theoretic security, privacy, wiretap channel, secret key agreement, coding, physical-layer security, security and privacy metrics, adversarial models.**

I. Introduction

INFORMATION security, a broad umbrella term that includes attributes including secrecy, privacy, and trust, has arguably become as important as information reliability in system design, especially so, as society at large conducts most operations virtually and as future generations of applications and devices emerge that amalgamates communication, sensing, computing, and control. In current systems, information security is largely treated as an addition to the network operations rather than a foundational design constraint at the outset. Consequently, securing information that flows over networked systems is largely guaranteed by higher network layer protocols.

While this layered approach has had undeniable success, future and emerging systems exhibit unique characteristics that challenge this prevalent view of security. The deployment of 5G, the advent of the IoT, the current and upcoming cyber-physical autonomous systems, and the envisioned all connected 6G world have all exacerbated the concerns for security and privacy in communication networks. In the next decade and beyond, tens of billions of devices are expected to be collecting and transmitting data over networks. The heterogeneity of these devices in terms of resources and capabilities, e.g., battery power, computational power, communication and storage capabilities, renders the approach to date of relying solely on computational approaches for security, e.g., cryptographic solutions, difficult. For example, networks with energy and computational power-limited IoT devices would benefit from lightweight security mechanisms that do not incur the overhead of traditional public-key infrastructures. Similarly, the stringent performance constraints of cyber-physical systems make increasingly apparent that security cannot be handled independently of other parameters, such as power consumption and latency, leading to unavoidable application dependent trade-offs. Cyber-physical systems would then benefit from bringing security closer to control in order to reduce overhead and latency in operation. Finally, all future massively connected systems would benefit from security mechanisms built into their foundation, e.g., to avoid the costly software updates required when new more powerful attacks emerge as a result of increasing computing power. Noting information security and privacy has a much larger domain of interest and impact, this tutorial focuses on communications as an exemplar to highlight recent advances in information-theoretic security.

Information-theoretic security [1], [2] aims at providing solutions to the aforementioned challenges, by offering a framework in which the security of information flows can be *measured* with quantitative information-theoretic metrics and *enforced* using a combination of signaling and coding mechanisms at the lower layers of the communication protocols. At its core, information-theoretic security embraces the observation structures inherent to communication systems. Specifically, acknowledging that legitimate users and adversaries obtain distinct signals through noisy and lossy channels, the asymmetry is harnessed through signal processing and coding mechanisms to control information

Manuscript received February 12, 2021; revised February 23, 2021; accepted February 24, 2021. Date of current version March 16, 2021. This work was supported in part by the U.S. National Science Foundation under Grant CCF-1749665, Grant CCF-2105872, Grant CCF-1955401, Grant CIF-1901243, Grant CIF-1815361, Grant CCF-1908308, and Grant CIF-2007688; and in part by the German Federal Ministry of Education and Research (BMBF) under Grant 16KIS1004 and Grant 16KIS1242. *(Corresponding author: H. Vincent Poor.)*

Matthieu Bloch is with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332 USA (e-mail: matthieu.bloch@ece.gatech.edu).

Onur Günlü is with the Information Theory and Applications Chair, Technische Universität Berlin, 10623 Berlin, Germany (e-mail: guenlue@tu-berlin.de).

Aylin Yener is with the Department of Electrical and Computer Engineering, The Ohio State University, Columbus, OH 43210 USA, also with the Department of Integrated Systems Engineering, The Ohio State University, Columbus, OH 43210 USA, and also with the Department of Computer Science and Engineering, The Ohio State University, Columbus, OH 43210 USA (e-mail: yener@ece.osu.edu).

Frédérique Oggier is with the School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore (e-mail: frederique@ntu.edu.sg).

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

Lalitha Sankar is with the School of Electrical, Computer, and Energy Engineering, Arizona State University, Tempe, AZ 85281 USA (e-mail: lalithasankar@asu.edu).

Rafael F. Schaefer is with the Lehrstuhl für Nachrichtentechnik/Kryptographie und Sicherheit, Universität Siegen, 57076 Siegen, Germany (e-mail: rafael.schaefer@uni-siegen.de).

Digital Object Identifier 10.1109/JSAIT.2021.3062755

2641-8770 © 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: California State University Fresno. Downloaded on June 21,2021 at 09:31:09 UTC from IEEE Xplore. Restrictions apply.

flows and information leakage. This tutorial provides a comprehensive review of information-theoretic security from the foundational concepts to the advances of the past two decades. Moreover, the tutorial seeks to highlight three crucial aspects of information-theoretic security that justify its relevance for securing information systems.

First, the tutorial makes the case that information-theoretic secrecy and privacy metrics have well-grounded cryptographic properties (Section II). Information-theoretic security metrics have naturally started out by measuring and controlling the mutual information *rate*. In recent years, however, information-theoretic security and privacy metrics have evolved significantly and are now defined in a much more principled way from a cryptographic perspective. In particular, *semantic security* precisely measures the ability of an adversary to infer information in secret communication setups, while *maximum information leakage* and its tunable variants offer a principled and operationally motivated way of measuring information leakage in privacy problems.

Second, the tutorial reviews how models for information-theoretic security have evolved since the beginning of the field (Section III). In particular, we make the point that the fundamental limits of models under which information-theoretic security holds have been characterized to accommodate increasingly more powerful adversaries. It is now known how to communicate secretly in the presence of adversaries that are not merely passive, but strategic in how they choose to acquire signals and even adversarial in their manipulation of the information.

Third, the tutorial emphasizes the meaningful connections between the foundational results and the tools that would accurately reflect the foundational insights in system design (Section IV). More specifically, we highlight coding and randomization as the mains tool towards realizing the potential of information-theoretic security. A main reason for doing so is to emphasize the distinguishing feature of information-theoretic security and privacy as compared with reliability that drove communication system design for many decades. In essence, whereas for reliability, separation of physical layer and error-correction coding techniques is often possible, enabling design insights from uncoded communication systems to carry through, this is not the case for security guarantees. This fact, at the outset, establishes the need for coding techniques for security to be an integral part of any real communication system design that guarantees information security.

The scope of information-theoretic security is ever-growing as new challenges dictated by emerging applications arise. We very briefly review a select subset of these in this tutorial (Section V) and point to several we were not able to accommodate into this article in the Conclusions and Forward look (Section VI).

II. Information-Theoretic Metrics: Secrecy, Privacy, and Beyond

In this section, we introduce the metrics that are commonly used in information-theoretic security to quantify secrecy, privacy, authentication, and covertness. Conceptually, many of these metrics reduce to measuring distances between probability distributions using an f-divergence [3]; however, the operational interpretation of the metrics depends on the security objective and not all metrics are equally amenable to analysis. Our main objective here is to clearly articulate these ideas independently of the specific models in which the metrics would be analyzed.

A. Information-Theoretic Secrecy

Secrecy is concerned with the problem of keeping the information content of a signal confidential from unauthorized parties, e.g., an adversary that intercepts signals emitted from the transmitter(s). In information theory, the digital information content is represented by a message, described as random variable W taking a value from a discrete set $\mathcal{W} \triangleq \{1, \ldots, M\}$. The signal carrying the message and observed by the adversary is described as random vector Z^n, consisting of n symbols taking value in a set $\mathcal{Z}$. The parameter n, hereafter called the blocklength, captures the fact that messages are typically coded into sequences. In the simplest situation, the joint distribution p_{WZ^n} of W and Z^n is known, which implicitly assumes that i) the statistics of the source of information are fully controlled; and ii) the statistical models that describe the processes relating the observation Z^n to the message W are fully characterized. Contemporary approaches to information-theoretic secrecy offer solutions to deal with channel uncertainties [4], [5], examples of which are discussed in Sections V-A and V-B. *Perfect secrecy* mandates that W and Z^n be statistically independent, i.e.,[1]

$$\forall w \in \mathcal{W}, \forall z^n \in \mathcal{Z}^n \quad p_{WZ^n}\big(w, z^n\big) = p_W(w) p_{Z^n}\big(z^n\big), \\ \text{i.e.,} \quad I\big(W; Z^n\big) = 0 \tag{1}$$

where $I(W; Z^n)$ is the mutual information between the message and the adversary's observation. Operationally, perfect secrecy has several interpretations. Writing (1) equivalently as $p_{W|Z^n}(w|z^n) = p_W(w)$ shows that perfect secrecy guarantees that the best attack an eavesdropper may launch is to guess the message at random according to p_W. Writing (1) as $p_{Z^n|W}(z^n|w) = p_{Z^n}(z^n)$ shows that perfect secrecy ensures that every message induces the same statistical distribution of the eavesdropper's observation; this also implies that a coding scheme with perfect secrecy maintains its guarantees regardless of the specific distribution p_W. Finally, perfect secrecy already hints at the coding mechanisms that must be deployed for information-theoretic security. W cannot be a function of Z^n, which suggests that some form of randomization must be present for secrecy to hold. This aspect is further discussed in Section IV. Despite these appealing cryptographic properties, perfect secrecy is often of little practical use. As recognized by Shannon [1], perfect secrecy requires excessive additional secret resources, in the form of uniformly distributed secret keys shared by legitimate parties, to act as a one-time pad.

To make information-theoretic secrecy actionable as a system design methodology, metrics that relax perfect secrecy have been introduced. Wyner's *weak secrecy* [2], replaces (1) with

$$\frac{1}{n} I\big(W; Z^n\big) \leq \epsilon \text{ for some suitably small } \epsilon > 0. \tag{2}$$

[1] Without loss of generality, we consider that W and Z^n have full support, i.e., $p_{WZ^n}(w, z^n) > 0$ for all pairs (w, z^n).

Authorized licensed use limited to: California State University Fresno. Downloaded on June 21,2021 at 09:31:09 UTC from IEEE Xplore. Restrictions apply.

Since the mutual information can be expressed in terms of the relative entropy $D(p_{WZ^n}\|p_W p_{Z^n})$ between the joint distribution p_{WZ^n} and the product of marginals $p_W p_{Z^n}$, weak secrecy retains the spirit of perfect secrecy. The factor $\frac{1}{n}$, makes weak secrecy a measure of information leakage *rate*, that measures how many bits are leaked about the message W per symbol of the sequence Z^n. Consequently, no matter how small the parameter $\epsilon > 0$ is, one can construct schemes that guarantee weak secrecy while leaking many bits of information [6]. Despite this weakness, weak secrecy has enabled system design and coding mechanisms for secrecy, as further discussed in Sections III and IV. *Strong secrecy*, introduced in [7], strengthens (2) as:

$$I\big(W; Z^n\big) \leq \epsilon \text{ for some suitably small } \epsilon > 0. \tag{3}$$

By dropping the normalization $\frac{1}{n}$, strong secrecy measures an amount of leaked information instead of a rate, which strengthens the security guarantee. That said, as (3) is equivalently expressed as $\mathbb{E}_W(D(p_{Z^n|W}\|p_{Z^n})) \leq \epsilon$, strong secrecy is dependent on the message distribution p_W. This leaves open the possibility that some very unlikely messages may be poorly protected because $D(p_{Z^n|W=w}\|p_{Z^n})$ could be large while $p_W(w)$ would be small.

Semantic secrecy, named after its connection with semantic security in standard cryptography [8], closes the last loophole of strong secrecy by requiring

$$\max_{p_W} I\big(W; Z^n\big) \leq \epsilon \text{ for some suitably small } \epsilon > 0. \tag{4}$$

In essence, semantic secrecy requires strong secrecy to hold *regardless* of the distribution of the message p_W. Compared with perfect secrecy, the main relaxation of semantic secrecy consists of introducing some slack in the independence requirement. Operationally, one can show that, under semantic secrecy, an adversary cannot do much better than randomly guessing any function of the message W [8]. Semantic secrecy can be further strengthened by making ϵ vanish with n; in particular, most of the results surveyed in Section III hold with $\epsilon = 2^{-cn}$ for some $c > 0$.

While weak, strong, and semantic secrecy are here expressed in terms of a relative entropy, one can devise similar quantities based of other f-divergences. In particular, the total variation distance and Rényi entropies often appear [9]–[12]. While the exact dependence between the message set size M and the secrecy parameter ϵ depends on the chosen metric, the underlying coding mechanisms and the fundamental limits are surprisingly robust and often remain unchanged no matter which metric is used.

B. Information-Theoretic Privacy

Information leakage pervades all modern data applications that require a user to disclose data in order to receive utility; these applications pose a privacy risk through unwanted inferences [13]–[18]. Quantifying information leakage is the first step towards limiting such leakage. Finding solutions that strike an acceptable compromise between privacy and utility has been a long standing research problem, see, e.g., [19], which has attracted growing interest over the past decade with the introduction of several often overlapping definitions of privacy/information leakage. Differential privacy (DP), which was first introduced within the context of querying databases, has emerged as a widely adopted worst-case privacy measure [20], [21]. DP seeks to ensure that changes in the database entries do not significantly influence the value of a query thereby limiting the inference of any specific entry from the query output. DP makes such a guarantee uniformly (hence, worst-case measure) for all "adjacent"[2] entries, and thus, requires noising the data to avoid such a distinction.

Taking a more average-case approach, a variety of information-theoretic measures have also been proposed as leakage measures. Foremost among them is mutual information: its use as a privacy measure in [22]–[31] is inspired by the common appearance of mutual information as an operationally-meaningful quantity throughout the literature on communication systems. In a similar vein, divergence-based quantities such as total variation distance between the prior and posterior distributions of the released data [32] have also been proposed as leakage measures. In fact, information-theoretic measures have been studied in the DP community via Rényi differential privacy which, based on Rényi divergence [33], allows relaxing the original definition of DP in order to achieve utility guarantees.

Similar to the secrecy metrics described in Section II-A, privacy metrics can be operationally motivated. However, while secrecy exclusively focuses on a regime in which the information leakage is made negligible, privacy may more generally tolerate some leakage, if it is carefully controlled, to obtain some utility in return. Note that there is no universal privacy vs. utility tradeoff, and how much leakage about sensitive attributes is required (if at all) to obtain some utility is application dependent. Having an operational motivation of privacy is therefore crucial to appreciate and interpret the resulting tradeoffs. As an illustration, consider the following setup. Let $S \in \mathcal{S}$ and $X \in \mathcal{X}$ denote the sensitive and non-sensitive attributes of a dataset, respectively, and let $Y \in \mathcal{Y}$ denote the released data; without loss of generality, assume that S, X, and Y are all discrete. Denote the leakage of S via Y as $\mathcal{L}_{(\cdot)}(S \to Y)$ where $(\cdot)$ denotes a chosen adversarial model as detailed below. An operationally motivated privacy measure was introduced recently in [34] (see also [28], [35], [36]) as the information leaked to a "guessing" adversary. The authors measure the leakage $\mathcal{L}_c(S \to Y)$ in terms of an adversary's gain in the probability of correctly guessing S after observing the disclosed data as:

$$\mathcal{L}_c(S \to Y) \triangleq \frac{\mathsf{P_c}(S|Y)}{\mathsf{P_c}(S)} \tag{5}$$

where $\mathsf{P_c}(S|Y) := \sum_{y\in\mathcal{Y}} P_Y(y) \max_{s\in\mathcal{S}} P_{S|Y}(s|y) = \sum_{y\in\mathcal{Y}} \max_{s\in\mathcal{S}} P_S(s) P_{Y|S}(y|s)$. Measures based on probability of correctly guessing have also been considered in [37]. While $\mathcal{L}_c(S \to Y)$ focuses on quantifying leakage about a specific S, more generally, one could also quantify the leakage to an adversary that can guess any function of the sensitive S or just the non-sensitive X from Y. To this end,

[2]With respect to some measure of similarity.

Authorized licensed use limited to: California State University Fresno. Downloaded on June 21,2021 at 09:31:09 UTC from IEEE Xplore. Restrictions apply.

in [38] (see also, [39], [40]), *maximal leakage* (MaxL), $\mathcal{L}_{\text{MaxL}}(X \to Y)$, is introduced, as the maximal logarithmic gain in the probability of correctly guessing any arbitrary function of the original data X from the released data Y given by

$$\mathcal{L}_{\text{MaxL}}(X \to Y) \triangleq \sup_{U-X-Y} \log \frac{\max_{P_{\hat{U}|Y}} \mathbb{E}\Big[P_{\hat{U}|Y}(U|Y)\Big]}{\max_u P_U(u)} \quad (6)$$

where $\hat{U}$ represents an estimator taking values from the same arbitrary finite support as U and $U - X - Y$ is a Markov chain relating any (potentially random) function U of X to Y. It is shown that $\mathcal{L}_{\text{MaxL}}(X \to Y) = \log \sum_{y\in\mathcal{Y}} \max_{\substack{x\in\mathcal{X}:\\ P_X(x)>0}} P_{Y|X}(y|x) = I_\infty(X;Y)$, where $I_\infty(X;Y)$ is the Sibson mutual information of order ∞ [41], and that MaxL satisfies well-accepted desiderata for information measures including: (i) the data processing inequality, $\mathcal{L}_{\text{MaxL}}(X \to Z) \le \min\{\mathcal{L}_{\text{MaxL}}(X \to Y), \mathcal{L}_{\text{MaxL}}(Y \to Z)\}$ for a Markov chain $X - Y - Z$; (ii) the independence property: $\mathcal{L}_{\text{MaxL}}(X \to Y) = 0$ if and only if X and Y are independent; and (iii) the additivity property: if (X_1, Y_1) and (X_2, Y_2) are independent, then $\mathcal{L}_{\text{MaxL}}((X_1, X_2) \to (Y_1, Y_2)) = \mathcal{L}_{\text{MaxL}}(X_1 \to Y_1) + \mathcal{L}_{\text{MaxL}}(X_2 \to Y_2)$.

An adversarial model based on the probability of correctly guessing focuses on an adversary that makes a hard decision (see (5) and (6)). Yet, in many practical settings including machine learning, adversaries can make soft decisions prior to making a hard decision. Motivated by this, [42] introduces a parameterized class of adversarial models via a tunable loss function, α-loss, $\alpha \in [0, \infty]$, where each α captures a specific adversarial action. Thus, for X, Y and $\hat{X}$ such that $X - Y - \hat{X}$ form a Markov chain and $\hat{X}$ is an estimator of X, the α-loss, for $\alpha \in (1, \infty)$, of an adversarial strategy $P_{\hat{X}|Y}$ in estimating X from Y is

$$\ell_\alpha\Big(x, y, P_{\hat{X}|Y}\Big) = \frac{\alpha}{\alpha - 1}\Big(1 - P_{\hat{X}|Y}(x|y)^{\frac{\alpha-1}{\alpha}}\Big). \quad (7)$$

Specifically, for $\alpha = 1$ and $\alpha = \infty$, by continuous extension, we have $\ell_1(x, y, P_{\hat{X}|Y}) = -\log P_{\hat{X}|Y}(x|y)$ and $\ell_\infty(x, y, P_{\hat{X}|Y}) = 1 - P_{\hat{X}|Y}(x|y)$. An adversary minimizing this loss effectively maximizes the estimate $P_{\hat{X}|Y}^{\frac{\alpha-1}{\alpha}}$. By varying α, α-loss captures adversarial strategies ranging from the probability of correctly guessing for $\alpha = \infty$ to the posterior distribution for $\alpha = 1$ about data X from the disclosed Y. Using these loss functions, [42] introduces two kinds of leakage measures: α-leakage and maximal α-leakage (Max-αL), wherein the former captures the leakage of X from Y while the latter captures the maximal such leakage over all functions of X.

Formally, given a joint distribution P_{XY} and an estimator $\hat{X}$ with the same support as X, the α-leakage, $\mathcal{L}_\alpha(X \to Y)$, and Max-$\alpha$L, $\mathcal{L}_\alpha^{\max}(X \to Y)$, from X to Y are defined as for $\alpha \in (1, \infty)$ and by the continuous extension of (8) for $\alpha = 1$ and ∞ as

$$\mathcal{L}_\alpha(X \to Y) \triangleq \frac{\alpha}{\alpha - 1} \log \frac{\max_{P_{\hat{X}|Y}} \mathbb{E}\Big[P_{\hat{X}|Y}(X|Y)^{\frac{\alpha-1}{\alpha}}\Big]}{\max_{P_{\hat{X}}} \mathbb{E}\Big[P_{\hat{X}}(X)^{\frac{\alpha-1}{\alpha}}\Big]}, \quad (8)$$

$$\mathcal{L}_\alpha^{\max}(X \to Y) \triangleq \sup_{U-X-Y} \mathcal{L}_\alpha(U \to Y), \quad (9)$$

where $1 \le \alpha \le \infty$, and U is any function of X taking values from an arbitrary finite alphabet.

One can show that $\mathcal{L}_\alpha(X \to Y)$ and $\mathcal{L}_\alpha^{\max}(X \to Y)$ simplify to the Arimoto mutual information and the Sibson capacity of order α, respectively. Furthermore, Max-αL satisfies the data processing, independence, and additivity properties, is robust to adversarial side information [40], [43], and is monotonically increasing in α. For $\alpha = \infty$, $\mathcal{L}_\infty(S \to Y)$ is the guessing gain in (5) for an $S - X - Y$ setting while $\mathcal{L}_\infty^{\max}(X \to Y)$ is MaxL in (6). Finally, both measures also allow quantifying leakage between sensitive features S and the release Y.

While Max-αL, and therefore, MaxL, capture the worst case leakage over all distributions of X, [40] showed that local DP, a stronger version of DP, upper bounds MaxL, and therefore, $\mathcal{L}_\alpha^{\max}(X \to Y)$ for all $\alpha \in [1, \infty)$. Local DP is a variant of DP where privacy has to be guaranteed over all pair of data entries. Such relationships have also been studied in [44]. There continues to be interest in exploring both the information-theoretic foundations of DP (e.g., [45]) and understanding how maxαL and α-leakage relax the strong privacy requirements of DP thereby assuring more utility, particularly in context-aware settings [46]–[48].

The role of these measures in practical data sharing and learning settings continues to be studied including understanding how multiple queries or uses of the data (e.g., learning gradients privately over all samples in a dataset) requires the composition of privacy measures. A key challenge here is in understanding the limits of data usage for a fixed privacy budget or alternately, the allocation of the total budget to different private operations. While such bounds exist for DP, information-theoretic measures can enhance existing bounds as shown recently in [45].

C. Authentication, Stealth and Covertness

Information-theoretic metrics also capture security concerns beyond secrecy and privacy.

a) *Authentication:* Authentication aims at ensuring that a message received at a terminal is indeed the one transmitted by a legitimate transmitter [49], [50]. An attacker can thwart authentication by launching one of two attacks: i) an *impersonation* attack, by which the attacker forges a new message; ii) a *substitution* attack by which the attacker first intercepts a transmitted signal and tries to substitute it for another. Formally, the problem can be cast as a binary hypothesis test on a received signal Y^n to distinguish between a signal Y^n that has not been manipulated (hypothesis H_0) and a signal Y^n that has been tampered with (Hypothesis H_1). An effective authentication scheme is then one that achieves good detection performance for this hypothesis test. The main challenge behind authentication is that it is impossible to accomplish without using additional resources, either in the form of shared secret keys between the legitimate parties to facilitate the detection of tampering [49], or in the form of restrictions on the manipulation that an adversary can perform [51].

b) *Stealth and covertness:* Stealth and covertness aim at concealing the fact that communication is taking place and at

Authorized licensed use limited to: California State University Fresno. Downloaded on June 21,2021 at 09:31:09 UTC from IEEE Xplore. Restrictions apply.

ensuring that signals generated by a communicating terminal can be transmitted with low-probability of intercept (LPI) or a low probability of detection (LPD). Unlike secrecy and privacy, which are concerned about the *information content* of transmitted signals, stealth and covertness are constraints on the *signals themselves*. Although the systematic study of such security constraints in the context of communication channels is relatively recent [52], the problem can be traced back to steganography where the objective is to embed an undetectable stegotext into a covertext [53], [54]. Denoting the observations of the signals intercepted by an eavesdropper Z^n, stealth requires that the statistical distribution induced by a coding scheme, p_{Z^n}, be nearly indistinguishable from a reference innocent looking distribution q_{Z^n}, as

$$D(p_{Z^n} \| q_{Z^n}) \leq \epsilon \text{ for some suitably small } \epsilon > 0. \quad (10)$$

This measure of stealth assumes that the statistical distribution p_{Z^n} and q_{Z^n} are known. Operationally, ensuring that $D(p_{Z^n} \| q_{Z^n})$ is small ensures that no detector deployed by the eavesdropper can perform much better than a "blind guess" [55]. More formally, in Neyman-Pearson detection theory, the performance of any reasonable detector is characterized by a trade-off between probability of false alarm α (detecting P_Z^n when Q_{Z^n} is true) and probability of missed detection (detecting Q_{Z^n} when P_{Z^n} takes place) of the form $1 \geq \alpha + \beta \geq 1 - \sqrt{D(p_{Z^n} \| q_{Z^n})}$. Ensuring that $D(p_{Z^n} \| q_{Z^n})$ is small ensures that $\alpha + \beta \approx 1$ for any test, which is no better than the trade-off of a guess made without knowing Z^n. Covertness corresponds to a special case of stealth, in which the innocent looking distribution Q_{Z^n} is the one induced by the absence of communication, e.g., background noise. This subtle difference has important consequences when analyzing communication systems, as covertness is often much more stringent than stealth and leads to a so-called square-root law [56], by which the rate of communication scales as the inverse of the square root of the coding blocklength.

It is crucial to note that stealth and secrecy are not equivalent; said otherwise, being stealth does not necessarily protect information content and vice versa. One elegant way to combine requirements is to enforce *effective secrecy* [57] defined as

$$D(p_{MZ^n} \| p_M q_{Z^n}) \leq \epsilon \text{ for some suitably small } \epsilon > 0. \quad (11)$$

One can rewrite the effective secrecy criterion as $D(p_{MZ^n} \| p_M q_{Z^n}) = I(M; Z^n) + D(p_{Z^n} \| q_{Z^n})$, which highlights that effective secrecy combines strong secrecy and stealth in a single metric.

III. Information-Theoretic Security Models: Fundamental Limits

A. Wiretap Channel Models

The *wiretap channel* (WT) goes back to Wyner [2] and refers to the simplest building block that models secure communications over noisy channels. Specifically, Wyner considered that the adversary observes the communication between the legitimate parties through a channel that is degraded with respect to the legitimate channel, and showed that secure communication is possible irrespective of the computational power of the adversary. This model explicitly brings in the notion that if the channel between the legitimate entities has an advantage over the channel to an adversary, e.g., as measured in [58], then coding (more specifically stochastic encoding with carefully selected rates) leads to quantifiable guarantees that limit information leakage, specifically under the metric now known as *weak secrecy*, see Section II-A.

It is worth emphasizing that the significance of Wyner's original wiretap channel model is (1) to demonstrate the possibility of information theoretically secure transmission over noisy channels and (2) to establish the fundamental limits of reliable information transport under information leakage constraints to an external entity that has access to the receiver's observations (which the receiver obtains from the transmitter through a Discrete Memoryless Channel (DMC)) through a second DMC. The need for the explicit channel advantage of single user models [58], [59] should not be attributed as a limiting factor of information theoretic secrecy in general. Indeed, the advent of multiuser information theory, notably revived with the advent of wireless communication networks that operate in shared multiuser channels, has also led to a plethora of models where a network advantage can be created utilizing the broadcast nature of the wireless medium, see Section V-A.

About a decade later than the original wiretap channel, Ozarow and Wyner proposed the Wiretap Channel II (WT-II) [60]. The channel model in this case is even more specific than the wiretap channel, namely, the paper considers a noiseless channel between the legitimate transmitter and the receiver, and a specific erasure model for the adversary, i.e., the eavesdropper. At the same time a new capability is introduced to the eavesdropper which can be interpreted as the first *strategic* adversary model in information-theoretic security. More specifically, the significance of this second landmark paper lies in the additional ability of the eavesdropper to be able to tap noiselessly α fraction of the symbols, of its own choosing, sent by the transmitter, while seeing erasures in the remaining positions. It was shown that irrespective of the positions chosen by the adversary, coding guarantees secrecy capacity to be identical to that of the case if the erasures seen by the adversary happened randomly at the same rate, i.e., through a BEC with erasure probability identical to the fraction in the WT-II model, α.

Recently, a generalized wiretap channel model was introduced that unifies the two models. Specifically, the model considers a strategic adversary who can choose α fraction of symbols to tap in its observation, like WT-II, while observing the rest through a DMC with transition probability $P_{Z|X}$ (as opposed to them being erasures), providing the adversary with the capabilities of both WT and WT-II. The main channel between the legitimate transmitter and the receiver is a DMC with transition probability $P_{Y|X}$ as is the case in WT. In this generalized set up, and considering strong secrecy (see Section II-A), [61] established the following secrecy capacity result, for channel model details see also [61], [62].

Authorized licensed use limited to: California State University Fresno. Downloaded on June 21,2021 at 09:31:09 UTC from IEEE Xplore. Restrictions apply.

Theorem 1 [61, Th. 1]: For $0 \leq \alpha \leq 1$, the strong secrecy capacity of the generalized wiretap channel is given by

$$C_s(\alpha) = \max_{U-X-YV} [I(U;Y) - I(U;V) - \alpha I(U;X|V)]^+, \quad (12)$$

where the maximization is over all the distributions p_{UX} which satisfy the Markov chain $U - X - YV$, and the cardinality of U can be restricted as $|\mathcal{U}| \leq |\mathcal{X}|$.

An equivalent characterization for the strong secrecy capacity of the generalized wiretap channel is given by

$$C_s(\alpha) = \max_{U-X-YV} \begin{bmatrix} I(U;Y) - \alpha I(U;X) \\ -(1-\alpha) I(U;V) \end{bmatrix}^+, \quad (13)$$

which clarifies the cost of providing the strategic ability to the eavesdropper.

Corollary 1 [61, Corollary 1]: By setting the tapped subset by the wiretapper, S, to the null set, or equivalently $\alpha = 0$, the secrecy capacity in (12) is equal to the secrecy capacity of the discrete memoryless wiretap channel in [58, Corollary 2], i.e.,

$$C_s(0) = \max_{U-X-YV} [I(U;Y) - I(U;V)]^+. \quad (14)$$

Corollary 2 [61, Corollary 2]: By setting the wiretapper's DMC through which she observes the $(1-\alpha)n$ symbols she does not choose, $p_{V|X}$, to be an erasure channel with erasure probability one, the secrecy capacity in (12) is equal to the secrecy capacity of the wiretap channel II with a noisy main channel in [63, Th. 2], i.e.,

$$C_s(\alpha) = \max_{U-X-Y} [I(U;Y) - \alpha I(U;X)]^+. \quad (15)$$

Comparing (12) and (14), we observe that the secrecy cost, with respect to the classical wiretap channel, of the additional capability of the wiretapper to choose a subset of size αn of the codewords to access perfectly, is equal to $\alpha I(U;X|V)$. Comparing (13) and (15), the secrecy cost, with respect to the wiretap channel II with a noisy main channel, of the additional capability of the wiretapper of observing $(1-\alpha)$ fraction of the codeword through the DMC $p_{V|X}$, is equal to $(1-\alpha)I(U;V)$.

Secrecy capacity [61] captures the fundamental limit of confidential reliable communications. While this formulation considers the asymptotic blocklength regime, recent references have also analyzed wiretap channels in the finite blocklength regime, see, e.g., [64], [65].

B. Secret-Key Agreement Models

Another information-theoretic confidentiality problem aims to agree on a secret key by using a noisy channel in addition to a noiseless public channel. The aim of the legitimate parties is to extract a secret key from the noise in the channel such that the key is hidden from an adversary, which is different from communicating a message secretly over a noisy channel considered in Section III-A. The secret key can then be used, e.g., for authentication, identification, secure transmission with public key cryptography, etc. There are two main models for the secret-key agreement problem: *source model* and *channel model*, introduced in [66], [67]. A result in [68] shows that it is possible to authenticate the public channel between the legitimate parties by using a small amount of secret key, which follows steps that are entirely similar to quantum key distribution (QKD) protocols discussed in Section V-D.

In the source model, the two legitimate parties n i.i.d. symbols of random variables X and Y, respectively, while the adversary observes n i.i.d. symbols of a random variable Z. The model assumes that these random variables are dependent, i.e., they are distributed according to a given joint probability mass function (pmf) $p_{XYZ}(x,y,z)$ for $x \in \mathcal{X}$, $y \in \mathcal{Y}$, $z \in \mathcal{Z}$ with $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ finite sets. The legitimate parties exchange public messages $F_{1:k}$ sequentially based on both the previous messages exchanged and their random sequences, which can include local randomness, for k rounds. Each party then extracts a secret key S that is almost uniformly distributed over its set by using all locally available information. The reliability constraint requires the two keys to be equal with high probability, i.e., probability of not agreeing on the same key should tend to zero with increasing blocklength n. The secrecy criterion is to ensure that the secret key S is almost independent of the adversary's information $(Z^n, F_{1:k})$, which can be imposed as a weak or strong security constraint. Consider the *weak secrecy* constraint for the source model problem

$$\frac{1}{n} I\big(S; Z^n, F_{1:k}\big) \leq \epsilon. \quad (16)$$

Define the secret-key rate as $R_s = \frac{1}{n} H(S)$ and the supremum of all achievable key rates as the source model secret-key capacity $S(X;Y\|Z)$. We have the following upper and lower bounds on the source model secret-key capacity [66], [67]

$$\begin{aligned} &I(X;Y) - \min\{I(X;Z), I(Y;Z)\} \\ &\quad \leq S(X;Y\|Z) \leq \min\{I(X;Y), I(X;Y|Z)\}. \end{aligned} \quad (17)$$

The lower bounds can be achieved by using a one-way communication, which is possible in two different directions and this explains the two lower bounds. We remark that the secret-key capacity $S(X;Y\|Z)$ is not known for general probability distributions, but the lower and upper bounds given in (17) are tight for various cases. Furthermore, if the number of rounds is fixed to $k = 1$, the one-way secret-key capacity is given as [67]

$$S_{k=1}(X;Y\|Z) = \max_{(U,V)-X-(Y,Z)} I(U;Y|V) - I(U;Z|V) \quad (18)$$

which is a valid lower bound for the general case and does not require local randomness. As an extension of the coding method used to achieve the one-way secret-key capacity, a single letter interactive communication lower bound is obtained in [69, Th. 7].

There is a method to convert a coding method that achieves weak secrecy (16) into a code that achieves strong secrecy by applying the steps given in [7], which mainly follows because a secret key does not carry any information by itself. The steps to achieve strong secrecy follow a QKD-based protocol, called *sequential key distillation* that consists of three main steps: *advantage distillation*, *information reconciliation*, and *privacy amplification*. The first step is introduced to gain an advantage over an adversary by using multi-round communications, which allows to

Authorized licensed use limited to: California State University Fresno. Downloaded on June 21,2021 at 09:31:09 UTC from IEEE Xplore. Restrictions apply.

achieve non-zero secret-key rates that cannot be achieved by using one-way communication methods [66], [70]. Thus, *feedback improves the secret-key rate*. Powerful advantage distillation methods combined with matching information reconciliation methods are shown to improve the secret-key rates [71]–[76]. The last two steps are discussed in more details in Section IV-B.

Various improvements to the upper bounds on the source model secret-key capacity given in (17) have been provided. The *intrinsic mutual information* upper bound $B_0(X;Y||Z)$ follows from the basic idea that by degrading the observations of the adversary the secret-key capacity does not decrease, i.e., we have [67, Remark 2], [77]

$$S(X;Y\|Z) \leq \min_{P_{J|Z}} S(X;Y\|J) \leq B_0(X;Y||Z) = \min_{P_{J|Z}} I(X;Y|J). \tag{19}$$

Further improvements are given in [69], [78]–[80]; see also [71] for a new interpretation of the best known upper bound given in [69] by relating it to deviation from the *less noisy condition*, introduced in [81] originally for broadcast channels.

Unlike the source model, the channel model allows one of the legitimate parties to control an input sequence X^n that is the input to a DMC $P_{YZ|X}$ whose outputs Y^n and Z^n are observed by the other legitimate user and the adversary, respectively. In the channel model, the sequence X^n is not necessarily i.i.d., unlike in the source model. Similar to the source model, a public, noiseless, and authentic channel is assumed to be available between the legitimate users. Thus, the channel model can be modeled as a WTC, defined in Section III-A, with an additional public channel over which the legitimate parties can communicate in multiple rounds. Imposing the same reliability and secrecy constraints to the channel model as being imposed to the source model, one can observe that all source model achievable secret-key rates are achievable also for the channel model as the channel model is more general than the source model. Similarly, by following the same steps as for the source model, similar upper bounds can be given for the channel model. Furthermore, due to the generality of the channel model, it is generally harder to find the channel model secret-key capacity. However, the secret-key capacity of a specific channel model is established in [66] by converting the problem into a virtual WTC problem. This example also illustrates that the channel model secret-key capacity can be positive, even if the secrecy capacity is zero for a DMC $P_{YZ|X}$.

Various extensions to multiple parties, continuous random variables, and cases with limited public communications rates can be found, e.g., in [6], [82]–[88]. Furthermore, the source and channel model secret-key agreement problem assumes that the adversary is passive, i.e., it does not intervene the secret-key agreement process and simply observes what is available. However, there can be active adversaries or uncertainties in channel or source statistics as for example in [89], [90].

IV. Coding for Security: The Role of Randomness

The term coding broadly refers to any technique that involves mapping a set of elements (typically with a mathematical structure, e.g., the binary alphabet $\{0,1\}$, a finite field, lattice points) into a larger set. Coding problems traditionally emerge from communication systems, where a transmitter wishes to communicate messages to a receiver over a noisy communication channel, and coding is needed to combat the noise. Coding is however also useful in engineering applications that fit a communication model although the problem at hand may not be reliable communication per se. The objective of this section is to shed the light on how to code for security and achieve the limits identified in Section III, as well as to highlight the central role played by randomness.

A. Coding for the Wiretap Channel

In the wiretap channel model, the security objective is to ensure that a message W, encoded as a codeword $X^n = (X_1,\ldots,X_n)$ and observed by an eavesdropper as Z^n, is not leaked, as measured, e.g., by a strong secrecy constraint $I(W;Z^n) \leq \epsilon$. As alluded to in Section II-A, ensuring the secrecy constraint requires a non-bijective mapping between W and X^n, for otherwise the information leakage grows linearly with n in general. Specifically, writing $I(W;Z^n) = I(X^n;Z^n) - I(X^n;Z^n|W)$ shows that controlling $I(W;Z^n)$ requires $H(X^n|W)$ to be non zero. In other words, multiple codewords X^n should represent the same codeword W and randomness must be injected in the encoding process. To build further intuition, consider the following small example from an instance of Wiretap Channel II (see Section III-A). The channel between Alice and Bob is noiseless, while Eve's channel is described as follows: out of any n bits sent by Alice, she gets exactly μ of them. Alice knows it, but she does not know which symbols Eve will get. A wiretap coding strategy for this scenario consists in Alice mixing random bits with information bits. In the simplest case where $n=2$ and $\mu=1$, Alice sends $(s+r,r)$ where r is a random bit chosen uniformly at random, s is a secret bit of information. Whether Eve gets r or $r+s$, she knows nothing about u, which can be formalized as $I(S;S+R)=0$. When Alice wishes to send l secret bits $s_1,\ldots,s_l$, she appends $n-l$ random bits $r_1,\ldots,r_{n-l}$, chosen uniformly at random, and encodes them as follows:

$$\begin{aligned}&\left[s_1,\ldots,s_l,r_1,\ldots,r_{n-l}\right]\begin{bmatrix}M\\G\end{bmatrix}\\&\quad=\underbrace{[s_1,\ldots,s_l]M}_{\text{coset choice}}+\underbrace{[r_1,\ldots,r_{n-l}]G}_{\text{random codeword}}\end{aligned}$$

where G is chosen to be of rank $n-l$, so it forms a generator matrix of a linear code C (the subspace generated by the rows of G), to which the codeword $[r_1,\ldots,r_{n-l}]G$ belongs, and M contains l linearly independent vectors, which are not contained in C. Since we can write the whole space $\{0,1\}^n$ as a disjoint union of 2^l subsets, called *cosets* of C of the form $C+t$ (imagine all the points in the subspace C translated by t), for $t=[s_1,\ldots,s_l]M$, Alice's strategy is often called *coset coding*: it maps a secret to a coset, and then randomness is coming from choosing a codeword uniformly at

Authorized licensed use limited to: California State University Fresno. Downloaded on June 21,2021 at 09:31:09 UTC from IEEE Xplore. Restrictions apply.

random within the coset. When $n = 2$, the above example corresponds to $G = [1, 1]$ (a repetition code), $\{0, 1\}^2$ contains only $\{(0, 0), (0, 1), (1, 0), (1, 1)\}$, which contains the code $C = \{(0, 0), (1, 1)\}$ and its coset $C + (1, 0) = \{(1, 0), (0, 1)\}$. To send say $s = 0$, Alice picks uniformly at random a codeword of C. This can equivalently be expressed as: to send, say $s = 0$, Alice picks uniformly at random a vector among vectors $x = [x_1, x_2]$ satisfying $[1, 1]x^T = 0$. The matrix $[1, 1]$ here corresponds to the parity check of the code C (which so happens to be equal to G, this is an example of self-dual code). Description of coset coding in terms of parity check is common. Let H be an $(n-l) \times n$ parity check matrix for C, by definition this means that $Hx^T = 0$ exactly when $x \in C$. Alice chooses the secret s she wants to send, then solving $Hx^T = s$ will give her as solution for x all 2^l vectors in a given coset, then she is left to choose uniformly at random the vector x she will actually send.

The fundamental insight to take away is that from the moment there is noise (even small) in an eavesdropper's channel, the transmitter can amplify this noise by properly encoding its secrets, inserting its own controlled randomness. The concept of coset coding highlighted above generalizes beyond linear codes, as already established in the seminal works [2], [58], [59] using *bins* of codewords representing the same message.

In recent years, much efforts have been devoted to develop explicit codes for the wiretap channel with rates approaching the fundamental limits [91], [92]. Coset coding has been successfully analyzed with several families of codes, including low-density parity-check codes [93], polar codes [94]–[97], and lattice codes [98]. In particular, polar codes have proved useful to bridge the gap between information-theoretic limits and algorithms in a host of multi-user security models [99]–[105]. Another powerful approach has been to adopt a modular approach and combine invertible extractors with an error control code [8], [106]–[108] to create the bins of codewords representing the same message. For the special case of erasure channels, it is also possible to relate the information leakage to algebraic properties of the codes, such as generalized Hamming weights [109]. Very recently, a deep learning-based approach to the code design problem has been considered based on autoencoders [110]–[113]. The coding mechanisms for secrecy have also provided traction to enforce stealth and covertness (see Section II-C) [114], which although different from secrecy also require the introduction of randomization in the encoding [55], [115].

B. Coding for Secret-Key Agreement

In the secret key agreement model, the security objective is to ensure that a key K can be extracted from an observation X^n against an eavesdropper observing Z^n, in the sense of guaranteeing, e.g., $I(K; Z^n) < \epsilon$. Writing $I(K; Z^n) = I(X^n; Z^n) - I(X^n; Z^n|K)$ shows that controlling $I(K; Z^n)$ requires $H(X^n|K)$ to be non zero, i.e., multiple sequences should map to the same key. The major difference with the wiretap model is that the coding operation consists here of *extracting* the secret key rather than *encoding* a secret message.

Interestingly, this operation is simpler than the design of codes for the wiretap channel and is embodied in a result known as the left-over hash lemma [116], [117]; an extensive review of the left-over hash lemma and its variants in information theory is available in [118]. In simplified terms, the left-over hash lemma states that given the knowledge of the conditional entropy $H(X^n|Z^n)$, applying a randomly chosen universal hash function [119] with output size slightly smaller than $H(X^n|Z^n)$ to the sequence X^n results in an output that is secret from Z^n. There exist many powerful variations of the left-over hash lemma, e.g., [67], [120]–[122], in which the knowledge of the conditional entropy is expressed using different entropy metrics. The result of the left-over hash lemma is also known under the name *privacy amplification* [117] to emphasize its operational meaning, by which the privacy of the sequence X^n is amplified through the use of a hash function.[3] One key aspect of the left-over hash lemma is its *universality*, meaning that the secrecy of the resulting key is guaranteed knowing only the conditional entropy of X^n given Z^n, regardless of the actual joint distribution $p_{X^nZ^n}$. This makes it a powerful tool with many applications, such as quantum key distribution briefly discussed in Section V-D.

The secret key agreement model also includes a reliability objective, by which transmitting public messages collectively denoted F allows a terminal observing Y^n correlated to Z^n to reconstruct the key. This operation is effectively an instance of a source coding with side information problem [123], also known as *reconciliation*, for which many constructions are now known [124] and which can be easily combined with privacy amplification [125].

V. Contemporary Approaches to Information-Theoretic Security

A. Role of Wireless Medium: Multi-User Secure Physical Layer Design

The past two decades have seen a flurry of research activity in wiretap channels and wireless physical layer security, following wireless taking over as the dominant medium of communications [126]–[128]. Though being a broadcast medium is a vulnerability for wireless with respect to security attacks, e.g., eavesdropping, it was recognized that studying wiretap models in wireless channels could lead to design insights that effectively turn this vulnerability into an advantage. As such, properties of wireless medium can serve as security resources, and designing the physical layer accordingly provides information-theoretic security guarantees. Efforts along these lines include utilizing multiple antennas for improving secure communication rates [129]–[131] and utilizing channel variations in various time-scales (fading states) for creating a channel advantage [132]–[134]. Natural to the broadcast properties of wireless, multi-terminal wiretap channel models have been studied, e.g., [135] and led to new design insights such as cooperative jamming where some legitimate terminals can generate judicious interference tailored to harm the adversary for better network-wide secure communication

[3]The privacy referred to here should be understood colloquially and differs from the formal privacy discussed in Section II-B.

Authorized licensed use limited to: California State University Fresno. Downloaded on June 21,2021 at 09:31:09 UTC from IEEE Xplore. Restrictions apply.

rates [136]. A number of network information theoretic security models emerged in the past two decades focusing on the design principles that the models can offer with respect to interference alignment, broadcast and relaying, see for example, [137]–[147] and many others. Multi-terminal models with multiple antennas have been studied with [148], [149] or without channel state information where the latter relies on a network advantage with more antennas at the legitimate terminals and provides *universal strong secrecy* irrespective of eavesdropper's channel [4], [150], [151]. For other models of varying channel state information in wiretap channels, see also Section V-B. The impact of having a massive number of antennas has also been studied [152], [153], including connections to computational hardness [154] further discussed in Section V-E.

Finally, extensive experimental efforts have explored key generation from wireless channel states [155]–[160].

B. Role of Channel State Information: Compound and Arbitrarily Varying Models

Earlier wiretap studies often start with models where the channels to the adversaries and/or to the legitimate parties are known. As these are clearly assumptions whose validity can be questioned in practical networks, including those in wireless systems, information-theoretic security models have branched out to address uncertainties in channels.

The classical concept of compound channels [161], [162] provides a first step in the direction of more realistic and practically relevant assumptions on channel knowledge to capture the effects of channel uncertainty. Here, the actual channel that governs the transmission is unknown. Rather, the users only know that the true channel belongs to a known set of channels and that it remains constant for the whole duration of transmission. Secure communication over compound channels is then captured by the compound wiretap channel which has been studied in [133], [163]–[171]. Despite considerable effort, a single-letter characterization of the secrecy capacity is only known for special cases [133], [163], [166]–[169].

While for compound channels the unknown channel realization remains constant for the entire duration of transmission, the concept of an *arbitrarily varying channel (AVC)* [172]–[174] provides a model in which this realization may vary from channel use to channel use in an unknown and arbitrary manner. The corresponding *arbitrarily varying wiretap channel (AVWC)* has been studied in [171], [175]–[181] and it has been shown that it makes a difference whether unassisted or common randomness (CR) assisted codes are used by the transmitter and legitimate receiver. In particular, if the channel to the legitimate receiver possesses the so-called property of symmetrizability, the unassisted secrecy capacity is zero, while the CR-assisted secrecy capacity may be non-zero. A complete characterization of the relation between the unassisted and CR-assisted secrecy capacity is established in [176], [180]; but similar to the compound wiretap channel, a single-letter characterization of the secrecy capacity itself remains open. CR-assisted achievable secrecy rates are known only under certain circumstances [175], [176], [178]. Recently, a multi-letter description of the CR-assisted secrecy capacity has been found in [196].

The presence of feedback offers new avenues to deal with channel state information, e.g., by allowing legitimate terminals to learn the channel and adapt to changes without compromising secrecy [182].

C. Role of Digital Circuits: Physical Unclonable Functions (PUFs)

The problem of reliably identifying a human being by using biometric features (or *biometric identifiers* [183]) such as retina characteristics, iris color, fingerprint, palm print, voice characteristics, or signature has been an important security problem throughout the history. Biometric features are used for, e.g., identifying or authenticating a person according to a pre-determined set of permissions. Such applications require the feature used to be unique and reliable for every human being, which resulted in numerous signal processing, cryptographic, algebraic-code based, and information-theoretic algorithms and system designs especially in the last two decades; see [184]–[187]. Similar methods are proposed later to be used for correctly identifying a digital device, which helps solve the security and privacy problems faced in the digital transformation by defining unique and reliable physical identifiers as the outputs of a digital circuit embodied by the digital device. The first contemporary physical identifiers apply the cryptographic concept of "one-way functions", i.e., functions that are easy to evaluate but (on average) difficult to invert [188], to physical systems to implement "physical one-way functions" (POWFs). As the first example of POWFs, the speckle pattern obtained from coherent waves propagating through a disordered medium is a one-way function of both the physical randomness in the medium and the angle of the laser beam used to generate the optical waves [189]. To allow a widespread usage of such a security primitive, one needs to replace the disordered medium, used as a source of randomness in POWFs, with a digital component that can be used to provide security and privacy to (in principle) all digital devices with low-complexity. One auspicious solution is to determine physical identifiers for each digital device, similar to biometric identifiers of human beings. The most general name for such physical identifiers is "physical unclonable functions" (PUFs) [190], which mainly refers to a physical function embodied in a digital device such that its challenge-response (or input-output) pairs cannot be cloned physically or digitally.

A PUF is commonly defined as a complex challenge-response mapping determined by random and uncontrollable variations in a physical object. Contemporary applications of PUFs include the following scenarios.

- Consider 5G/6G mobile devices that embody a set of static random access memories (SRAMs), which put out random binary outputs. Randomness in SRAM outputs allows to use them as a PUF (i.e., SRAM PUF) such that each mobile device can be assigned an identifier that is the output bit sequence put out by its SRAMs. SRAM PUFs can be used as a local source of randomness, which

Authorized licensed use limited to: California State University Fresno. Downloaded on June 21,2021 at 09:31:09 UTC from IEEE Xplore. Restrictions apply.

can be used for data encryption or identification via channels [191] in combination with higher layer cryptographic security primitives.

- Consider any information-theoretic problem where it helps to use a local randomness, i.e., randomization either improves the performance or is required. For instance, since a WTC encoder is a digital device that can embody digital circuits that can be used as a PUF, the PUF outputs at the encoder can be used to confuse the eavesdropper.
- Consider an autonomous vehicle, whose controller area network (CAN) bus standard is illustrated in [192] to be vulnerable to denial-of-service attacks due to insufficiently-secured transmission of messages over the network. This problem threatens people's lives since critical inputs such as throttle and brakes would then be susceptible to attacks. Similar problems are faced in using unmanned military drones, recently addressed by PUF companies. Determining digital components in the corresponding hardware that are appropriate to be used as a PUF would allow to enforce a better authentication procedure that can save lives.

There are a massive number of PUF types and constraints imposed to use PUFs in different applications; see [193] for a summary. We consider only the information-theoretically relevant constraints to analyze PUFs that use digital circuit outputs and model the PUF usage problem as a secure, reliable, and private identifier (or secret key) agreement problem. The most common and practical PUFs that are of information-theoretical interest use oscillation frequencies of ring oscillators (ROs) or the random binary outputs of SRAMs as the source of randomness. Thus, for the remaining analysis we consider such PUFs for modeling. For this purpose, it is useful to follow Shannon's approach of removing the complex practical constraints of a problem until the remaining part can be tackled by using information-theoretic analyses in such a way that removed parts can be inserted back to extend the basic results. Therefore, the basic information-theoretic model of the PUF problem used in the literature considers two i.i.d. dependent sequences used to agree on a physical identifier. This basic model is shown in [194] to fit with the reality if transform-coding algorithms are applied, which is mainly borrowed from the biometrics literature [184], [187], [195].

The basic PUF model consists of two random sequences X^n and Y^n that are i.i.d. according to a joint probability distribution P_{XY} and that represent the noiseless and noisy PUF outputs, respectively. An encoder $\mathsf{Enc}(\cdot)$ that observes X^n generates a uniformly-random index (or an identifier) $S \in \mathcal{S}$ during an *enrollment* step, which represents that the identifier is being enrolled to a security system that will use it. At a later time, the noisy PUF outputs Y^n are observed by a decoder $\mathsf{Dec}(\cdot)$ (which is likely to be in the same digital device that embodies the PUF) to reconstruct S during a *reconstruction* step. To reliably reconstruct S, the decoder in general requires extra information from the encoder. In the biometrics and PUF literature, the extra public information $W \in \mathcal{W}$ provided to the decoder is called *helper data*, which is the only data accessible to an eavesdropper during key agreement in addition to fixed encoding and decoding operations. This model is depicted in Fig. 1. The reliability constraint imposes that $\Pr[S \neq \widehat{S}]$ should be negligible, the strong secrecy-leakage constraint that $I(S;W)$ should be negligible, and the storage-rate constraint that $\log|\mathcal{W}|/n$ should be minimized. These constraints illustrate the close connection of PUFs to the information-theoretic key agreement problem discussed in [66], [67], [85]. A privacy-rate constraint that minimizes $I(X^n;W)/n$ is introduced in [187], [196], shown in [197] to provide an upper bound on the overall secrecy leakage if the same PUF is used by other encoder-decoder pairs that were not considered during code and system design. Thus, such a privacy-leakage constraint might be useful to design key agreement schemes with varying number of security mechanisms that use the same PUF (or biometrics) as the source of randomness.

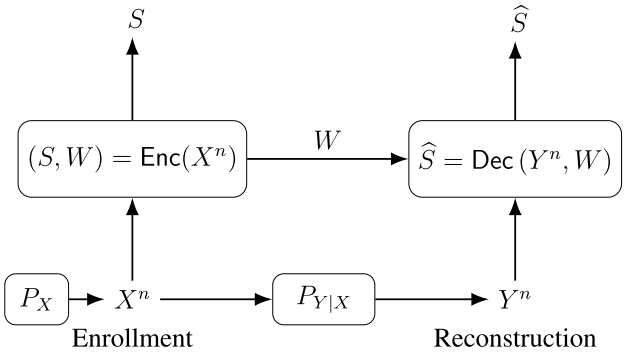

Fig. 1. Basic key agreement with PUFs problem model.

Comparisons between information-theoretic rate regions obtained and performance of available (cryptographic) code constructions such as code-offset fuzzy extractors [198] and the fuzzy commitment scheme [199] illustrate that to improve the privacy and storage performance new code constructions are necessary [99], [200]–[204]. Since in storage-limited key agreement models satisfying reliability and secrecy constraints separately is suboptimal [205], code constructions that satisfy all constraints jointly are proposed, including (nested) random linear codes, (nested) polar codes, invertible extractors, nested convolutional codes, and nested polar subcodes. Depending on the practical constraints such as the available number of PUF circuits, which affects the blocklength of the codes used, and assumed source and channel models, different code constructions are expected to be preferred for different applications.

The most interesting extensions of the basic model (from an information-theoretic optimality perspective with realistic assumptions) include the extra constraint of identifying the device or the user [206], [207], analysis of false-acceptance exponents [208], [209] and false-rejection exponents [210], multiple enrollments by using the same or different noisy PUF outputs with remote (or hidden) sources [197], [211]–[213], cost-constrained actions at the decoder to control the decoder-measurement channel quality [214], [215], compound sources to accommodate possible uncertainty in source statistics [90], measurement channels with correlated noise components [215], [216] caused by surrounding hardware logic [217], and an equivalent WTC

Authorized licensed use limited to: California State University Fresno. Downloaded on June 21,2021 at 09:31:09 UTC from IEEE Xplore. Restrictions apply.

model [218]. Following Shannon's approach towards problems with complex practical constraints, mentioned above, these extensions manage to solve the key agreement with PUFs problem accurately enough. However, there are further interesting open problems that should be addressed by using information- and coding-theoretic tools to gain deeper insights into hardware-intrinsic security and privacy. We provide an open information-theoretic problem below; see [219] for open problems related to signal-processing and coding-theoretic methods applied to the key agreement with PUFs problem.

- RO and SRAM PUFs discussed above are considered as "weak (or key obfuscating) PUFs" since there is only a single input-output pair for these PUFs, i.e., if there is no noise, then one can challenge only the same digital circuits and obtain the same response. However, "strong PUFs" such as optical PUFs (or optical POWFs) [189] allow multiple challenge-response pairs for each PUF, where the noiseless response can be modeled as $X^n[c]$ and the noisy response as $Y^n[c]$ given a challenge $c \in \mathcal{C}$. In practice, it is required that an attacker who observed a set of challenges $\{c_1, c_2, \ldots\}$ and corresponding noiseless responses $\{X^n[c_1], X^n[c_2], \ldots\}$ should not be able to guess a challenge-response pair $(\tilde{c}, X^n[\tilde{c}])$ for a challenge $\tilde{c}$ chosen uniformly at random from the set $\mathcal{C}\backslash\{c_1, c_2, \ldots\}$. Due to correlations between responses of each PUF, there is a need for a post-processing step to satisfy this requirement. Furthermore, correlations between the challenge-response pairs of different PUFs, embodied by different digital devices, should also be eliminated to protect PUF responses when an attacker obtains challenge-response pairs of multiple PUFs. Such security problems are tackled in the literature mostly by applying heuristic methods and metrics. Thus, there is a need to propose information-theoretic metrics with operational meanings to obtain the ultimate limits for the key agreement with strong PUFs problem and then to design code constructions that can achieve or approach the ultimate limits.

D. Role of Quantum: Quantum Key Distribution and Beyond

Perhaps one the most criticized aspect of information-theoretic security and privacy is the need for known statistical models. Coding for secure communication over the wiretap channel [2], key generation from common randomness [66], [67], and many privacy coding techniques [26] require knowledge of statistical distributions to properly set the design parameters of the coding schemes. This is especially problematic in presence of passive adversaries that do not disclose their presence and do not provide signals from which to infer statistical models of observations. Although uncertainty can be factored into the models [5], e.g., with compound channels [133], [161], state dependent channels [4], [179], [220], or layered-secrecy coding [221], such approaches still leave open the possibility that the true channel is not properly captured by the model, in which case none of the security guarantees hold. At a more conceptual level, the crux of the challenge is that the statistical models must be *postulated* rather than built from first principles.

One solution to resolve this conundrum, at least in the context of secure communication and key generation, is to leave the classical realm and embrace a quantum formalism for the models. The laws of quantum mechanics have consistently resisted theoretical and experimental attempts to break them, thereby offering a powerful framework in which to build information-theoretic security models from first principles. Quantum models offer two main advantages over classical ones: i) it is sometimes possible to indirectly infer bounds on the information leaked to unknown adversaries, which we shall see forms the cornerstone of Quantum Key Distribution (QKD); and ii) the presence of noise can be guaranteed by physics, such as the presence of thermal background noise or the presence of unavoidable quantum noise in detectors. While quantum information theory allows the study of models that exceed today's technological capabilities, quantum phenomena already appear in low-power free-space and fiber optical communication systems. Consequently, quantum-secured communication are already a reality and have "leaped out of the lab" [222], [223].

Historically, the discovery in 1984 by Bennett and Brassard [224], followed in 1991 by Ekert [225], that quantum mechanics would allow legitimate parties to indirectly infer bounds on the information leaked to an a priori unknown quantum adversary pioneered the field of QKD. QKD predates the information-theoretic works on secret-key generation from common randomness [66], [67] but we shall see that QKD is effectively a secret-key generation protocol that bootstraps 1) the laws of quantum mechanics to infer the information leaked to an eavesdropper; and 2) source coding with side information and privacy amplification to effectively extract a key. There exist many excellent reviews of QKD [226]–[228] and, rather than duplicate these, we offer here a concise description of typical QKD operation, tying in to some of the concepts exposed in earlier sections. Heuristically, QKD exploits the fact that quantum states cannot be perfectly cloned [229] to ensure that any measurement by an adversary attempting to eavesdrop would result in a measurable distortion by the legitimate parties. More formally, this can be achieved by sharing n maximally entangled two-qubit states between two legitimate parties. During this sharing phase, an eavesdropper may interact with the states in any way allowed by quantum mechanics. In a second phase, Alice and Bob publicly agree to measure each state a randomly chosen basis, denoted by Θ^n. Alice's classical measurements are denoted by X^n while Bob's classical measurements are denoted by Y^n. Eve has access to her quantum state E^n and Θ^n. Note that this protocol effectively induces a source model for key generation between Alice, Bob, and Eve as in Section III-B. Unlike the classical case, however, there is a limit to how much Bob and Eve can *simultaneously* know about Alice's measurements, captured by the entropic uncertainty relation

$$H\big(X^n|Y^n\big) + H\big(X^n|E^n\Theta^n\big) \geq n. \tag{20}$$

By disclosing a fraction of their measurements, Alice and Bob can estimate $H(X^n|Y^n)$ and thereby obtain a *lower bound* on $H(X^n|E^n\Theta^n)$. Alice and Bob can finally run a classical key generation protocol consisting of the two coding mechanisms

Authorized licensed use limited to: California State University Fresno. Downloaded on June 21,2021 at 09:31:09 UTC from IEEE Xplore. Restrictions apply.

of Section IV-B: 1) source coding with side information to correct the discrepancies between their measurements; and 2) privacy amplification, which can be shown to hold against quantum observations [230].

Since its inception, research in QKD has made significant strides both in theory and practice. On the practical side, technological advances have taken us closer to large scale QKD networks, as exemplified by a recent satellite-based demonstration of QKD [231]. On the theoretical side, security proofs have evolved to include the statistical finite length effect that affect the estimation of the leaked information [232], as well as situations in which the apparatus used by the legitimate parties is partially under the control of the adversary [228]. The fundamental limits of QKD rates as a function of distance are known [233], and much of the current research focuses on closing the remaining gaps between theory and practice and exploring multi-dimensional qubits protocols to increase rates.

The wiretap channel model also possesses a quantum equivalent for which [9], [234]–[236] characterize secrecy capacity. Recent efforts have also analyzed and demonstrated the usefulness of quantum noise for covert communications [237], [238], including early attempts at covert QKD [239]–[242] to combine secrecy and covertness constraints.

E. Role of Crypto: Bridging Computational and Information-Theoretic Security

A usual goal in information theory is finding the capacity of a communication scenario or, at least, some coding schemes that achieve a certain rate. Such a task is considered to be accomplished once a single-letter entropic expression of the capacity has been found as such a characterization is implicitly assumed to be numerically computable (or evaluable) on a digital computer. Surprisingly, the requirement of being algorithmically computable has not been specified explicitly in general, though the notion of computational information theory was already identified by [243], motivated by cryptography considerations.

To address this issue from a fundamental algorithmic point of view, the concept of a *Turing machine* [244]–[246] and the corresponding *computability framework* can be used. A Turing machine is a mathematical model of an abstract machine that manipulates symbols on a strip of tape according to certain given rules. It can simulate any given algorithm and therewith provides a simple but very powerful model of computation. Turing machines have no limitations on computational complexity, unlimited computing capacity and storage, and execute programs completely error-free. They are further equivalent to the von Neumann-architecture without hardware limitations and the theory of recursive functions, see also [247]–[251]. Accordingly Turing machines provide fundamental performance limits for today's digital computers. Therefore, they are the ideal concept to study whether or not certain capacity expressions can be algorithmically (i.e., numerically) computed and whether or not the corresponding optimal codes can be constructed algorithmically in principle (without putting any constraints on the computational complexity of such an algorithm).

Communication from a computability or algorithmic point of view has attracted some attention recently. In [252] the computability of the capacity functions of the wiretap channel under channel uncertainty and adversarial attacks is studied. The secrecy capacity of the wiretap channel is shown to be Turing computable so that its expression can be numerically evaluated. However, it is also observed that the secrecy capacity becomes non-computable in the case of adversarial attacks so that it is no longer numerically evaluable. These works have in common that they analyze the capacity function of various communication scenarios and analyze under which conditions the capacity function is non-computable. However, they tackle this is issue from a probabilistic or random coding point of view and do not consider actual code constructions.

A key observation from [243] is that the use of randomness in the context of computational information theory is the same as in the context of Wyner's wiretap channel in that it enhances the security of the system considered, e.g., a trapdoor function in the former case and a communication channel in the latter. Two examples of the use of noise to construct a hard computational problem from an easy one are McEliece's cryptosystem [253], and Regev's cryptosystem [254].

Public-key cryptosystems refer to a cryptography setting that involve two players, Alice and Bob, who are communicating using pairs of keys: public keys (for encryption, known to anyone) and private keys (for decryption, known only to the owner, meaning that Alice has her own key, and so does Bob). If Alice wants to write to Bob, she takes Bob's public key, encrypts her message and sends it to Bob who will use his private key to decrypt. A private key is usually obtained from a function computationally hard to compute, while the public key is easily computed.

McEliece cryptosystem is an example of code-based cryptosystem, in which the generator matrix of a Goppa code is hidden by scrambling/permuting its entries, which becomes a public key. A plaintext is encrypted by being encoded with this generator matrix, and then x-ored with some small (with respect to the code's parameters) weight error. The difficult part (leading to the private key) is to be able to decode, or more precisely, it is based on the hardness of decoding a random linear code, and depends on the introduction of noise (the small weight error). Its disadvantage though is the (huge) size of the keys.

Regev's cryptosystem is an example of a cryptosystem based on the so-called learning with errors (LWE) hard problem. The underlying problem behind LWE is solving a system of linear equations (an easy task) that becomes difficult once noise gets added. Namely, a secret s is fixed, and one can ask noisy linear equations in s, the goal of LWE being to find s. The LWE problem can be expressed as lattice problem, by introducing q-ary lattices, n-dimensional lattices that contain $q\mathbb{Z}^n$, in which case it becomes a bounded distance decoding on lattices. This variation of the LWE problem thus fits within the area of lattice-based cryptography.

Code-based and lattice-based cryptography [255] are two families that are considered in the area of post-quantum cryptography, where cryptography protocols that are resistant to quantum computing are studied.

Authorized licensed use limited to: California State University Fresno. Downloaded on June 21,2021 at 09:31:09 UTC from IEEE Xplore. Restrictions apply.

VI. Conclusion and Forward Look

In this tutorial, we have reviewed information-theoretic security and privacy approaches. Starting from initial formulations, we have provided the progressive development in metrics, problems and models that are increasingly connected to real systems and can provide foundational security and privacy guarantees for emerging applications going forward. We have covered the role of information-theoretic security and privacy approaches in communication system design as well as the relevant coding techniques needed in these designs. We have touched upon some of the contemporary directions in information-theoretic security, namely that of the roles of wireless medium, realistic channel assumptions, digital circuits, and provided connections to quantum and to computational security. The current and forward looking directions we were not able to cover include content security and privacy, e.g., secure caching and private information retrieval, privacy aided by and concerned by distributed, e.g., federated, learning, connections with adversarial machine learning and many others. We conclude the article by stating that information-theoretic approaches to security and privacy remain vibrant, as relevant metrics for emerging applications continue to encourage designs that focus on security and privacy as foundational necessity in networked information flow.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

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

[3] I. Sason and S. Verdú, "f-divergence inequalities," *IEEE Trans. Inf. Theory*, vol. 62, no. 11, pp. 5973–6006, Nov. 2016.

[4] X. He and A. Yener, "MIMO wiretap channels with unknown and varying eavesdropper channel states," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6844–6869, Nov. 2014.

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

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

[7] U. M. Maurer, "The strong secret key rate of discrete random triples," *Communication and Cryptography: Two Sides of One Tapestry*. Norwell, MA, USA: Kluwer, 1994, pp. 271–285.

[8] M. Bellare, S. Tessaro, and A. Vardy, "Semantic security for the wiretap channel," in *Advances in Cryptology—CRYPTO*, R. Safavi-Naini and R. Canetti, Eds. Berlin, Germany: Springer, 2012, pp. 294–311.

[9] J. M. Renes and R. Renner, "Noisy channel coding via privacy amplification and information reconciliation," *IEEE Trans. Inf. Theory*, vol. 57, no. 11, pp. 7377–7385, Nov. 2011.

[10] M. Iwamoto and K. Ohta, "Security notions for information theoretically secure encryptions," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2011, pp. 1777–1781.

[11] M. Iwamoto and J. Shikata, "Information theoretic security for encryption based on conditional Rényi entropies," in *Proc. Int. Conf. Inf. Theor. Security*, 2013, pp. 103–121.

[12] M. Hayashi and V. Y. F. Tan, "Equivocations, exponents, and second-order coding rates under various Rényi information measures," *IEEE Trans. Inf. Theory*, vol. 63, no. 2, pp. 975–1005, Feb. 2017.

[13] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," in *Proc. IEEE Symp. Security Privacy*, 2008, pp. 111–125.

[14] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds," in *Proc. 16th ACM Conf. Comput. Commun. Security*, 2009, pp. 199–212.

[15] D. Shah and T. Zaman, "Rumors in a network: Who's the culprit?" *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 5163–5181, Aug. 2011.

[16] G. Liang, W. He, C. Xu, L. Chen, and J. Zeng, "Rumor identification in microblogging systems based on users' behavior," *IEEE Trans. Comput. Soc. Syst.*, vol. 2, no. 3, pp. 99–108, Sep. 2015.

[17] A. Ghassami, X. Gong, and N. Kiyavash, "Capacity limit of queueing timing channel in shared FCFS schedulers," in *Proc. IEEE Int. Symp. Inf. Theory*, 2015, pp. 789–793.

[18] A. K. Biswas, "Efficient timing channel protection for hybrid (packet/circuit-switched) network-on-chip," *IEEE Trans. Parallel Distrib. Syst.*, vol. 29, no. 5, pp. 1044–1057, May 2018.

[19] A. C. Yao, "Protocols for secure computations," in *Proc. 23rd Annu. Symp. Found. Comput. Sci. (SFCS)*, Nov. 1982, pp. 160–164.

[20] C. Dwork, "Differential privacy," in *Proc. 33rd Int. Colloquium Automata Lang. Program.*, Venice, Italy, Jul. 2006, pp. 1–6.

[21] C. Dwork, "Differential privacy: A survey of results," in *Theory and Applications of Models of Computation: Lecture Notes in Computer Science*. New York, NY, USA: Springer, Apr. 2008.

[22] C. C. Aggarwal, "On k-anonymity and the curse of dimensionality," in *Proc. ACM 31st Int. Conf. Very Large Data Bases*, 2005, pp. 901–909.

[23] D. Rebollo-Monedero, J. Forne, and J. Domingo-Ferrer, "From t-closeness-like privacy to postrandomization via information theory," *IEEE Trans. Knowl. Data Eng.*, vol. 22, no. 11, pp. 1623–1636, Nov. 2010.

[24] G. Aggarwal *et al.*, "Achieving anonymity via clustering," in *Proc. Symp. Principles Database Syst.*, Dallas, TX, USA, Jun. 2006, pp. 153–162.

[25] F. du Pin Calmon and N. Fawaz, "Privacy against statistical inference," in *Proc. Allerton Conf. Commun. Control Comput.*, 2012, pp. 1401–1408.

[26] L. Sankar, S. R. Rajagopalan, and H. V. Poor, "Utility-privacy tradeoffs in databases: An information-theoretic approach," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 6, pp. 838–852, Jun. 2013.

[27] L. Sankar, S. K. Kar, R. Tandon, and H. V. Poor, "Competitive privacy in the smart grid: An information-theoretic approach," in *Proc. Smart Grid Commun.*, Brusells, Belgium, Oct. 2011, pp. 220–225.

[28] S. Asoodeh, F. Alajaji, and T. Linder, "On maximal correlation, mutual information and data privacy," in *Proc. IEEE 14th Can. Workshop Inf. Theory*, 2015, pp. 27–31.

[29] W. Wang, L. Ying, and J. Zhang, "On the relation between identifiability, differential privacy, and mutual-information privacy," *IEEE Trans. Inf. Theory*, vol. 62, no. 9, pp. 5018–5029, Sep. 2016.

[30] J. Liao, L. Sankar, V. Y. F. Tan, and F. P. Calmon, "Hypothesis testing under mutual information privacy constraints in the high privacy regime," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 4, pp. 1058–1071, Apr. 2018.

[31] S. Li, A. Khisti, and A. Mahajan, "Information-theoretic privacy for smart metering systems with a rechargeable battery," *IEEE Trans. Inf. Theory*, vol. 64, no. 5, pp. 3679–3695, May 2018.

[32] B. Rassouli and D. Gündüz, "Optimal utility-privacy trade-off with total variation distance as a privacy measure," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 594–603, 2020.

[33] I. Mironov, "Rényi differential privacy," in *Proc. IEEE 30th Comput. Security Found. Symp.*, 2017, pp. 263–275.

[34] S. Asoodeh, M. Diaz, F. Alajaji, and T. Linder, "Estimation efficiency under privacy constraints," *IEEE Trans. Inf. Theory*, vol. 65, no. 3, pp. 1512–1534, Mar. 2019.

[35] S. Asoodeh, F. Alajaji, and T. Linder, "Notes on information-theoretic privacy," in *Proc. Allerton Conf. Commun. Control Comput.*, Sep. 2014, pp. 1272–1278.

[36] S. Asoodeh, M. Diaz, F. Alajaji, and T. Linder, "Privacy-aware guessing efficiency," in *Proc. IEEE Int. Symp. Inf. Theory*, 2017, pp. 754–758.

[37] A. Nageswaran and P. Narayan, "Data privacy for a ρ-recoverable function," *IEEE Trans. Inf. Theory*, vol. 65, no. 6, pp. 3470–3488, Jun. 2019.

[38] I. Issa, S. Kamath, and A. B. Wagner, "An operational measure of information leakage," in *Proc. Annu. Conf. Inf. Sci. Syst.*, 2016, pp. 234–239.

[39] I. Issa and A. B. Wagner, "Operational definitions for some common information leakage metrics," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2017, pp. 769–773.

[40] I. Issa, A. B. Wagner, and S. Kamath, "An operational approach to information leakage," *IEEE Trans. Inf. Theory*, vol. 66, no. 3, pp. 1625–1657, Mar. 2020.

[41] R. Sibson, "Information radius," *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete*, vol. 14, no. 2, pp. 149–160, 1969.

Authorized licensed use limited to: California State University Fresno. Downloaded on June 21,2021 at 09:31:09 UTC from IEEE Xplore. Restrictions apply.

[42] J. Liao, O. Kosut, L. Sankar, and F. du Pin Calmon, "Tunable measures for information leakage and applications to privacy-utility tradeoffs," *IEEE Trans. Inf. Theory*, vol. 65, no. 12, pp. 8043–8066, Dec. 2019.

[43] J. Liao, L. Sankar, O. Kosut, and F. P. Calmon, "Robustness of maximal α-leakage to side information," 2019. [Online]. Available: arXiv:1901.07105.

[44] P. Cuff and L. Yu, "Differential privacy as a mutual information constraint," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security (CCS)*, 2016, pp. 43–54.

[45] S. Asoodeh, J. Liao, F. P. Calmon, O. Kosut, and L. Sankar, "A better bound gives a hundred rounds: Enhanced privacy guarantees via f-divergences," in *Proc. IEEE Int. Symp. Inf. Theory*, 2020, pp. 920–925.

[46] C. Huang, P. Kairouz, X. Chen, L. Sankar, and R. Rajagopal, "Context-aware generative adversarial privacy," *Entropy*, vol. 19, no. 12, p. 656, 2017.

[47] B. Jiang, M. Li, and R. Tandon, "Local information privacy and its application to privacy-preserving data aggregation," 2020. [Online]. Available: arXiv:2001.02385.

[48] M. Seif, R. Tandon, and M. Li, "Context aware Laplacian mechanism for local information privacy," in *Proc. IEEE Inf. Theory Workshop*, 2019, pp. 1–5.

[49] G. J. Simmons, "Authentication theory/coding theory," in *Proc. CRYPTO 84 Adv. Cryptol.*, 1985, pp. 411–431.

[50] R. A. Chou and A. Yener, "Strongly secure multiuser communication and authentication with anonymity constraints," *IEEE Trans. Inf. Theory*, vol. 66, no. 1, pp. 572–586, Jan. 2020.

[51] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels—Part II: The simulatability condition," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 832–838, Apr. 2003.

[52] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, "Hiding information in noise: Fundamental limits of covert wireless communication," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 26–31, Dec. 2015.

[53] P. Moulin and J. A. O'Sullivan, "Information-theoretic analysis of information hiding," *IEEE Trans. Inf. Theory*, vol. 49, no. 3, pp. 563–593, Mar. 2003.

[54] C. Cachin, "An information-theoretic model for steganography," *Inf. Comput.*, vol. 192, no. 1, pp. 41–56, Jul. 2004.

[55] M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2334–2354, May 2016.

[56] B. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1921–1930, Sep. 2013.

[57] J. Hou and G. Kramer, "Effective secrecy: Reliability, confusion and stealth," in *Proc. IEEE Int. Symp. Inf. Theory*, Honolulu, HI, USA, Jul. 2014, pp. 601–605.

[58] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–3487, May 1978.

[59] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[60] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *AT&T Bell Lab. Tech. J.*, vol. 63, no. 10, pp. 2135–2157, 1984.

[61] M. Nafea and A. Yener, "A new wiretap channel model and its strong secrecy capacity," *IEEE Trans. Inf. Theory*, vol. 64, no. 3, pp. 2077–2092, Mar. 2018.

[62] M. Nafea and A. Yener, "Generalizing multiple access wiretap and wiretap II channel models: Achievable rates and cost of strong secrecy," *IEEE Trans. Inf. Theory*, vol. 65, no. 8, pp. 5125–5143, Aug. 2019.

[63] Z. Goldfeld, P. Cuff, and H. H. Permuter, "Semantic-security capacity for wiretap channels of type II," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3863–3879, Jul. 2016.

[64] M. Hayashi, "General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channels," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1562–1575, Apr. 2006.

[65] W. Yang, R. F. Schaefer, and H. V. Poor, "Wiretap channels: Nonasymptotic fundamental limits," *IEEE Trans. Inf. Theory*, vol. 65, no. 7, pp. 4069–4093, Jul. 2019.

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

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

[68] D. R. Stinson, "Universal hashing and authentication codes," *Designs Codes Cryptography*, vol. 4, no. 3, pp. 369–380, 1994.

[69] A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals—Part I," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3973–3996, Aug. 2010.

[70] A. Orlitsky and A. Wigderson, "Secrecy enhancement via public discussion," in *Proc. IEEE Int. Symp. Inf. Theory*, San Antonio, TX, USA, Jan. 1993, p. 155.

[71] A. Gohari, O. Günlü, and G. Kramer, "Coding for positive rate in the source model key agreement problem," *IEEE Trans. Inf. Theory*, vol. 66, no. 10, pp. 6303–6323, Oct. 2020.

[72] U. M. Maurer, "Protocols for secret key agreement by public discussion based on common information," in *Proc. Annu. Int. Cryptol. Conf.*, Santa Barbara, CA, USA, Aug. 1992, pp. 461–470.

[73] M. J. Gander and U. M. Maurer, "On the secret-key rate of binary random variables," in *Proc. IEEE Int. Symp. Inf. Theory*, Trondheim, Norway, Jun./Jul. 1994, p. 351.

[74] S. Liu, H. C. V. Tilborg, and M. V. Dijk, "A practical protocol for advantage distillation and information reconciliation," *Designs Codes Cryptography*, vol. 30, no. 1, pp. 39–62, 2003.

[75] M. Naito, S. Watanabe, R. Matsumoto, and T. Uyematsu, "Secret key agreement by reliability information of signals in Gaussian maurer's model," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, ON, Canada, Jul. 2008, pp. 727–731.

[76] D. Jost, U. Maurer, and J. L. Ribeiro, "Information-theoretic secret-key agreement: The asymptotically tight relation between the secret-key rate and the channel quality ratio," in *Proc. Theory Crypt. Conf.*, Goa, India, Nov. 2018, pp. 345–369.

[77] U. M. Maurer and S. Wolf, "Unconditionally secure key agreement and the intrinsic conditional information," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 499–514, Mar. 1999.

[78] S. Watanabe, R. Matsumoto, T. Uyematsu, and Y. Kawano, "Key rate of quantum key distribution with hashed two-way classical communication," *Phys. Rev. A*, vol. 76, no. 3, Sep. 2007, Art. no. 32312.

[79] R. Renner and S. Wolf, "New bounds in secret-key agreement: The gap between formation and secrecy extraction," in *Proc. Int. Conf. Theory Appl. Cryptograph. Technol.*, Warsaw, Poland, May 2003, pp. 562–577.

[80] K. Keykhosravi, M. Mahzoon, A. Gohari, and M. R. Aref, "From source model to quantum key distillation: An improved upper bound," in *Proc. Iran Workshop Commun. Inf. Theory*, Tehran, Iran, May 2014, pp. 1–6.

[81] J. Körner and K. Marton, "Comparison of two noisy channels," in *Topics in Information Theory* (Coll. Math. Soc. J. Bolyai No. 16), P. Elias and I. Csiszar, Eds., North Holland, pp. 411–423.

[82] Q. Zhou and C. Chan, "Secret key generation for minimally connected hypergraphical sources," *IEEE Trans. Inf. Theory*, vol. 66, no. 7, pp. 4226–4244, Jul. 2020.

[83] C. Chan, M. Mukherjee, N. Kashyap, and Q. Zhou, "When is omniscience a rate-optimal strategy for achieving secret key capacity?" in *Proc. IEEE Inf. Theory Workshop*, Cambridge, U.K., Sep. 2016, pp. 354–358.

[84] S. Nitinawarat, C. Ye, A. Barg, P. Narayan, and A. Reznik, "Secret key generation for a pairwise independent network model," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6482–6489, Dec. 2010.

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

[86] H. Tyagi, "Common information and secret key capacity," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5627–5640, Sep. 2013.

[87] C. Chan and L. Zheng, "Multiterminal secret key agreement," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3379–3412, Jun. 2014.

[88] A. E. Gamal and Y.-H. Kim, *Network Information Theory*. New York, NY, USA: Cambridge Univ. Press, 2011.

[89] N. Tavangaran, H. Boche, and R. F. Schaefer, "Secret-key generation using compound sources and one-way public communication," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 1, pp. 227–241, Jan. 2017.

[90] N. Tavangaran, R. F. Schaefer, H. V. Poor, and H. Boche, "Secret-key generation and convexity of the rate region using infinite compound sources," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 2075–2086, Aug. 2018.

[91] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 41–50, Sep. 2013.

[92] M. Bloch, M. Hayashi, and A. Thangaraj, "Error-control coding for physical-layer secrecy," *Proc. IEEE*, vol. 103, no. 10, pp. 1725–1746, Oct. 2015.

Authorized licensed use limited to: California State University Fresno. Downloaded on June 21,2021 at 09:31:09 UTC from IEEE Xplore. Restrictions apply.

[93] V. Rathi, M. Andersson, R. Thobaben, J. Kliewer, and M. Skoglund, "Performance analysis and design of two edge-type lDPC codes for the bec wiretap channel," *IEEE Trans. Inf. Theory*, vol. 59, no. 2, pp. 1048–1064, Feb. 2013.

[94] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6428–6443, Oct. 2011.

[95] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, "Nested polar codes for wiretap and relay channels," *IEEE Commun. Lett.*, vol. 14, no. 4, pp. 752–754, Jun. 2010.

[96] E. Hof and S. Shamai, "Secrecy-achieving polar-coding," in *Proc. IEEE Inf. Theory Workshop*, Dublin, Ireland, Sep. 2010, pp. 1–5.

[97] O. O. Koyluoglu and H. E. Gamal, "Polar coding for secure transmission and key agreement," in *Proc. IEEE Int. Symp. Pers. Indoor Mobile Radio Commun.*, Istambul, Turkey, Sep. 2010, pp. 2698–2703.

[98] C. Ling, L. Luzzi, J. Belfiore, and D. Stehlé, "Semantically secure lattice codes for the Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 60, no. 10, pp. 6399–6416, Oct. 2014.

[99] R. A. Chou, M. R. Bloch, and E. Abbe, "Polar coding for secret-key generation," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 6213–6237, Nov. 2015.

[100] R. A. Chou and M. R. Bloch, "Polar coding for the broadcast channel with confidential messages: A random binning analogy," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2410–2429, May 2016.

[101] Y. P. Wei and S. Ulukus, "Polar coding for the general wiretap channel with extensions to multiuser scenarios," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 2, pp. 278–291, Feb. 2016.

[102] T. C. Gulcu and A. Barg, "Achieving secrecy capacity of the wiretap channel and broadcast channel with a confidential component," *IEEE Trans. Inf. Theory*, vol. 63, no. 2, pp. 1311–1324, Feb. 2017.

[103] R. A. Chou and A. Yener, "Polar coding for the multiple access wiretap channel via rate-splitting and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 64, no. 12, pp. 7903–7921, Dec. 2018.

[104] M. Andersson, R. F. Schaefer, T. J. Oechtering, and M. Skoglund, "Polar coding for bidirectional broadcast channels with common and confidential messages," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1901–1908, Sep. 2013.

[105] M. Zheng, W. Chen, and C. Ling, "Polar coding for the cognitive interference channel with confidential messages," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 762–774, Apr. 2018.

[106] M. Hayashi and R. Matsumoto, "Secure multiplex coding with dependent and non-uniform multiple messages," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2355–2409, May 2016.

[107] S. Sharifian, F. Lin, and R. Safavi-Naini, "Hash-then-Encode: A modular semantically secure wiretap code," in *Proc. Workshop Commun. Security*, Paris, France, Apr. 2018, pp. 49–63.

[108] R. A. Chou, "Explicit codes for the wiretap channel with uncertainty on the eavesdropper's channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Vail, CO, USA, Jun. 2018, pp. 476–481.

[109] V. K. Wei, "Generalized hamming weights for linear codes," *IEEE Trans. Inf. Theory*, vol. 37, no. 5, pp. 1412–1418, Sep. 1991.

[110] R. Fritschek, R. F. Schaefer, and G. Wunder, "Deep learning for the Gaussian wiretap channel," in *Proc. IEEE Int. Conf. Commun.*, Shanghai, China, Jun. 2019, pp. 1–6.

[111] R. Fritschek, R. F. Schaefer, and G. Wunder, "Deep learning based wiretap coding via mutual information estimation," in *Proc. ACM Workshop Wireless Security Mach. Learn.*, Linz, Austria, Jul. 2020, pp. 74–79.

[112] R. Fritschek, R. F. Schaefer, and G. Wunder, "Reinforce security: A model-free approach towards secure wiretap coding," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2021, pp. 1–5.

[113] K.-L. Besser, P.-H. Lin, C. R. Janda, and E. A. Jorswieck, "Wiretap code design by neural network autoencoders," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3374–3386, 2020.

[114] I. A. Kadampot, M. Tahmasbi, and M. R. Bloch, "Multilevel-coded pulse-position modulation for covert communications over binary-input discrete memoryless channels," *IEEE Trans. Inf. Theory*, vol. 66, no. 10, pp. 6001–6023, Oct. 2020.

[115] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental limits of communication with low probability of detection," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3493–3503, Jun. 2016.

[116] R. Impagliazzo, L. A. Levin, and M. Luby, "Pseudo-random generation from one-way functions," in *Proc. ACM Symp. Theory Comput.*, 1989, pp. 12–24.

[117] C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

[118] H. Tyagi and A. Vardy, "Universal hashing for information-theoretic security," *Proc. IEEE*, vol. 103, no. 10, pp. 1781–1795, Oct. 2015.

[119] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *J. Comput. Syst. Sci.*, vol. 18, no. 2, pp. 143–154, 1979.

[120] T. Holenstein and R. Renner, "On the randomness of independent experiments," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 1865–1871, Apr. 2011.

[121] J. Muramatsu, "Channel coding and lossy source coding using a generator of constrained random numbers," *IEEE Trans. Inf. Theory*, vol. 60, no. 5, pp. 2667–2686, May 2014.

[122] M. H. Yassaee, M. R. Aref, and A. Gohari, "Achievability proof via output statistics of random binning," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6760–6786, Nov. 2014.

[123] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. IT-19, no. 4, pp. 471–480, Jul. 1973.

[124] J. Martinez-Mateo, D. Elkouss, and V. Martin, "Key reconciliation for high performance quantum key distribution," *Sci. Rep.*, vol. 3, p. 1576, Apr. 2013.

[125] C. Cachin and U. M. Maurer, "Linking information reconciliation and privacy amplification," *J. Cryptol.*, vol. 10, no. 2, pp. 97–110, Mar. 1997.

[126] A. Yener and S. Ulukus, "Wireless physical layer security: Lessons learned from information theory," *Proc. IEEE*, vol. 103, no. 10, pp. 1814–1825, Oct. 2015.

[127] R. Bassily *et al.*, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 16–28, Sep. 2013.

[128] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. Nat. Acad. Sci. USA*, vol. 114, no. 1, pp. 19–26, 2017.

[129] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[130] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[131] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[132] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[133] Y. Liang, G. Kramer, H. V. Poor, and S. S. Shitz, "Compound wiretap channels," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, no. 1, Oct. 2009.

[134] M. Bloch and J. N. Laneman, "On the secrecy capacity of arbitrary wiretap channels," in *Proc. Allerton Conf. Commun. Control Comput.*, Sep. 2008, pp. 818–825.

[135] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.

[136] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[137] X. He and A. Yener, "Providing secrecy with structured codes: Two-user Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 60, no. 4, pp. 2121–2138, Apr. 2014.

[138] O. O. Koyluoglu and H. E. Gamal, "Cooperative encoding for secrecy in interference channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 9, pp. 5682–5694, Sep. 2011.

[139] X. He and A. Yener, "The Gaussian many-to-one interference channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2730–2745, May 2011.

[140] L. Lai and H. E. Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[141] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.

[142] X. He and A. Yener, "Strong secrecy and reliable byzantine detection in the presence of an untrusted relay," *IEEE Trans. Inf. Theory*, vol. 59, no. 1, pp. 177–192, Jan. 2013.

[143] X. He and A. Yener, "End-to-end secure multi-hop communication with untrusted relays," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 1–11, Jan. 2013.

Authorized licensed use limited to: California State University Fresno. Downloaded on June 21,2021 at 09:31:09 UTC from IEEE Xplore. Restrictions apply.

[144] X. He and A. Yener, "The role of feedback in two-way secure communications," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 8115–8130, Dec. 2013.

[145] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[146] E. Ekrem and S. Ulukus, "Capacity-equivocation region of the Gaussian MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 58, no. 9, pp. 5699–5710, Sep. 2012.

[147] A. A. Zewail and A. Yener, "Multi-terminal two-hop untrusted-relay networks with hierarchical security guarantees," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 9, pp. 2052–2066, Sep. 2017.

[148] M. Nafea and A. Yener, "Secure degrees of freedom for the MIMO wire-tap channel with a multi-antenna cooperative jammer," *IEEE Trans. Inf. Theory*, vol. 63, no. 11, pp. 7420–7441, Nov. 2017.

[149] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, Apr. 2011.

[150] X. He, A. Khisti, and A. Yener, "MIMO multiple access channel with an arbitrarily varying eavesdropper," *IEEE Trans. Inf. Theory*, vol. 59, no. 8, pp. 4733–4745, Aug. 2013.

[151] X. He, A. Khisti, and A. Yener, "MIMO broadcast channel with an unknown eavesdropper: Secrecy degrees of freedom," *IEEE Trans. Commun.*, vol. 62, no. 1, pp. 246–255, Jan. 2014.

[152] S. Asaad, A. Bereyhi, A. M. Rabiei, R. R. Müller, and R. F. Schaefer, "Optimal transmit antenna selection for massive MIMO wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 817–828, Apr. 2018.

[153] A. Bereyhi, S. Asaad, R. R. Müller, R. F. Schaefer, G. Fischer, and H. V. Poor, "Securing massive MIMO systems: Secrecy for free with low-complexity architectures," 2020. [Online]. Available: arXiv:1912.02444.

[154] T. R. Dean and A. J. Goldsmith, "Physical-layer cryptography through massive MIMO," *IEEE Trans. Inf. Theory*, vol. 63, no. 8, pp. 5419–5436, Aug. 2017.

[155] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Trans. Antennas Propag.*, vol. 53, no. 11, pp. 3776–3784, Nov. 2005.

[156] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a cryptographic key from an un-authenticated wireless channels," in *Proc. 14th Annu. Int. Conf. Mobile Comput. Netw.*, San Francisco, CA, USA, Sep. 2008, pp. 128–139.

[157] A. J. Pierrot, R. A. Chou, and M. R. Bloch, "Experimental aspects of secret-key generation in indoor wireless environments," in *Proc. Signal IEEE 4th Workshop Signal Process. Adv. Wireless Commun.*, Apr. 2013, pp. 669–673.

[158] S. N. Premnath *et al.*, "Secret key extraction from wireless signal strength in real environments," *IEEE Trans. Mobile Comput.*, vol. 12, no. 5, pp. 917–930, May 2013.

[159] H. Liu, J. Yang, Y. Wang, Y. Chen, and C. Koksal, "Group secret key generation via received signal strength: Protocols, achievable rates, and implementation," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, pp. 2820–2835, Dec. 2014.

[160] C. T. Zenger, M. Pietersz, and C. Paar, "Preventing relay attacks and providing perfect forward secrecy using PHYSEC on 8-bit μC," in *Proc. IEEE Int. Conf. Commun. Workshops*, May 2016, pp. 110–115.

[161] D. Blackwell, L. Breiman, and A. J. Thomasian, "The capacity of a class of channels," *Ann. Math. Stat.*, vol. 30, no. 4, pp. 1229–1241, Dec. 1959.

[162] J. Wolfowitz, "Simultaneous channels," *Arch. Rational Mech. Anal.*, vol. 4, no. 4, pp. 371–386, 1960.

[163] I. Bjelaković, H. Boche, and J. Sommerfeld, "Secrecy results for compound wiretap channels," *Probl. Inf. Transm.*, vol. 49, no. 1, pp. 73–98, Jan. 2013.

[164] E. Ekrem and S. Ulukus, "On Gaussian MIMO compound wiretap channels," in *Proc. Conf. Inf. Sci. Syst.*, Baltimore, MD, USA, Mar. 2010, pp. 1–6.

[165] A. Khisti, "Interference alignment for the multiantenna compound wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2976–2993, May 2011.

[166] R. F. Schaefer and S. Loyka, "The secrecy capacity of a compound MIMO Gaussian channel," in *Proc. IEEE Inf. Theory Workshop*, Seville, Spain, Sep. 2013, pp. 104–108.

[167] R. F. Schaefer and S. Loyka, "The compound secrecy capacity of a class of non-degraded MIMO Gaussian channels," in *Proc. Allerton Conf. Commun. Control Comput.*, Monticello, IL, USA, Oct. 2014, pp. 1004–1010.

[168] R. F. Schaefer and S. Loyka, "On the secrecy capacity of rank-deficient compound wiretap channels," in *Proc. IEEE Global Commun. Conf. Workshops*, San Diego, CA, USA, Dec. 2015, pp. 1–6.

[169] R. F. Schaefer and S. Loyka, "The secrecy capacity of compound MIMO Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 61, no. 10, pp. 5535–5552, Dec. 2015.

[170] R. F. Schaefer and H. V. Poor, "Robust transmission over wiretap channels with secret keys," in *Proc. Asilomar Conf. Signals Syst. Comput.*, Pacific Grove, CA, USA, Nov. 2014, pp. 60–64.

[171] H. Boche, R. F. Schaefer, and H. V. Poor, "On the continuity of the secrecy capacity of compound and arbitrarily varying wiretap channels," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2531–2546, Dec. 2015.

[172] D. Blackwell, L. Breiman, and A. J. Thomasian, "The capacities of certain channel classes under random coding," *Ann. Math. Stat.*, vol. 31, no. 3, pp. 558–567, 1960.

[173] R. Ahlswede, "Elimination of correlation in random codes for arbitrarily varying channels," *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete*, vol. 44, pp. 159–175, Jun. 1978.

[174] I. Csiszár and P. Narayan, "The capacity of the arbitrarily varying channel revisited: Positivity, constraints," *IEEE Trans. Inf. Theory*, vol. IT-34, no. 2, pp. 181–193, Mar. 1988.

[175] E. MolavianJazi, M. Bloch, and J. N. Laneman, "Arbitrary jamming can preclude secure communication," in *Proc. Allerton Conf. Commun. Control Comput.*, Monticello, IL, USA, Sep. 2009, pp. 1069–1075.

[176] I. Bjelaković, H. Boche, and J. Sommerfeld, "Capacity results for arbitrarily varying wiretap channels," in *Information Theory, Combinatorics, and Search Theory*. Heidelberg, Germany: Springer, 2013, pp. 123–144.

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

[178] H. Boche, R. F. Schaefer, and H. V. Poor, "On arbitrarily varying wiretap channels for different classes of secrecy measures," in *Proc. IEEE Int. Symp. Inf. Theory*, Honolulu, HI, USA, Jun. 2014, pp. 2376–2380.

[179] 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.

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

[181] R. F. Schaefer, H. Boche, and H. V. Poor, "Super-activation as a unique feature of secure communication in malicious environments," *Information*, vol. 7, no. 2, p. 24, May 2016.

[182] M. Tahmasbi, M. R. Bloch, and A. Yener, "Learning an adversary's actions for secret communication," *IEEE Trans. Inf. Theory*, vol. 66, no. 3, pp. 1607–1624, Mar. 2020.

[183] R. Plamondon, "The handwritten signature as a biometric identifier: Psychophysical model and system design," in *Proc. Eur. Convention Security Detect.*, Brighton, U.K., May 1995, pp. 23–27.

[184] P. Campisi, *Security and Privacy in Biometrics*. London, U.K.: Springer-Verlag, 2013.

[185] S. Rane, Y. Wang, S. C. Draper, and P. Ishwar, "Secure biometrics: Concepts, authentication architectures, and challenges," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 51–64, Sep. 2013.

[186] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process.*, vol. 2008, no. 113, pp. 1–17, Jan. 2008.

[187] T. Ignatenko and F. M. J. Willems, "Biometric systems: Privacy and secrecy aspects," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 4, pp. 956–973, Dec. 2009.

[188] O. Goldreich, *Modern Cryptography, Probabilistic Proofs and Pseudorandomness*, vol. 17. Berlin, Germany: Springer-Verlag, 1998.

[189] R. Pappu, *Physical One-Way Functions*. Cambridge, MA, USA: MIT Press, Oct. 2001.

[190] B. Gassend, D. Clarke, M. V. Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. ACM Conf. Comput. Commun. Security*, Washington, DC, USA, Nov. 2002, pp. 148–160.

[191] R. Ahlswede and G. Dueck, "Identification via channels," *IEEE Trans. Inf. Theory*, vol. 35, no. 1, pp. 15–29, Jan. 1989.

Authorized licensed use limited to: California State University Fresno. Downloaded on June 21,2021 at 09:31:09 UTC from IEEE Xplore. Restrictions apply.

[192] A. Palanca, E. Evenchick, F. Maggi, and S. Zanero, "A stealth, selective, link-layer denial-of-service attack against automotive networks," in *Proc. Int. Conf. Detection Intrusions Malware Vulnerability Assessment*, Bonn, Germany, Jul. 2017, pp. 185–206.

[193] C. Böhm and M. Hofer, *Physical Unclonable Functions in Theory and Practice*. New York, NY, USA: Springer, Oct. 2012.

[194] O. Günlü, "Key agreement with physical unclonable functions and biometric identifiers," Ph.D. dissertation, Dept. Elect. Comput. Eng., TU Munich, Munich, Germany, Nov. 2018.

[195] J. Wayman, A. Jain, D. Maltoni, and D. Maio, Eds., *Biometric Systems: Technology, Design and Performance Evaluation*. London, U.K.: Springer-Verlag, Feb. 2005.

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

[197] O. Günlü and G. Kramer, "Privacy, secrecy, and storage with multiple noisy measurements of identifiers," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 11, pp. 2872–2883, Nov. 2018.

[198] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. Comput.*, vol. 38, no. 1, pp. 97–139, Jan. 2008.

[199] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. ACM Conf. Comp. Commun. Security*, New York, NY, USA, Nov. 1999, pp. 28–36.

[200] T. Ignatenko and F. M. J. Willems, "Information leakage in fuzzy commitment schemes," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 337–348, Mar. 2010.

[201] T. Jerkovits, O. Günlü, V. Sidorenko, and G. Kramer, "Nested tail-biting convolutional codes for secrecy, privacy, and storage," in *Proc. ACM Workshop Inf. Hiding Multimedia Security*, Denver, CO, USA, Jun. 2020, pp. 79–89.

[202] B. Chen, T. Ignatenko, F. M. Willems, R. Maes, E. van der Sluis, and G. Selimis, "A robust SRAM-PUF key generation scheme based on polar codes," in *Proc. IEEE Global Commun. Conf.*, Singapore, Dec. 2017, pp. 1–6.

[203] O. Günlü, O. İşcan, V. Sidorenko, and G. Kramer, "Code constructions for physical unclonable functions and biometric secrecy systems," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 11, pp. 2848–2858, Nov. 2019.

[204] O. Günlü, P. Trifonov, M. Kim, R. F. Schaefer, and V. Sidorenko, "Randomized nested polar subcode constructions for privacy, secrecy, and storage," in *Proc. IEEE Int. Symp. Inf. Theory Appl.*, Kapolei, HI, USA, Oct. 2020, pp. 475–479.

[205] R. A. Chou and M. R. Bloch, "Separation of reliability and secrecy in rate-limited secret-key generation," *IEEE Trans. Inf. Theory*, vol. 60, no. 8, pp. 4941–4957, Aug. 2014.

[206] K. Kittichokechai and G. Caire, "Secret key-based identification and authentication with a privacy constraint," *IEEE Trans. Inf. Theory*, vol. 62, no. 11, pp. 6189–6203, Nov. 2016.

[207] T. Ignatenko and F. M. J. Willems, "Fundamental limits for biometric identification with a database containing protected templates," in *Proc. IEEE Int. Symp. Inf. Theory Appl.*, Taichung, Taiwan, Oct. 2010, pp. 54–59.

[208] F. M. J. Willems and T. Ignatenko, "Authentication based on secret-key generation," in *Proc. IEEE Int. Symp. Inf. Theory*, Cambridge, MA, USA, Jul. 2012, pp. 1792–1796.

[209] K. Kittichokechai and G. Caire, "Optimal tradeoff of secure PUF-based authentication," in *Proc. IEEE Conf. Commun. Netw. Security*, Florence, Italy, Sep. 2015, pp. 83–88.

[210] N. Merhav, "False-accept/false-reject trade-offs for ensembles of biometric authentication systems," *IEEE Trans. Inf. Theory*, vol. 65, no. 8, pp. 4997–5006, Aug. 2019.

[211] L. Lai, S. W. Ho, and H. V. Poor, "Privacy-security trade-offs in biometric security systems—Part II: Multiple use case," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 140–151, Mar. 2011.

[212] L. Kusters and F. M. J. Willems, "Secret-key capacity regions for multiple enrollments with an SRAM-PUF," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 9, pp. 2276–2287, Sep. 2019.

[213] O. Günlü, "Multi-entity and multi-enrollment key agreement with correlated noise," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1190–1202, 2021.

[214] O. Günlü, K. Kittichokechai, R. F. Schaefer, and G. Caire, "Controllable identifier measurements for private authentication with secret keys," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 1945–1959, Aug. 2018.

[215] O. Günlü, R. F. Schaefer, and H. V. Poor, "Biometric and physical identifiers with correlated noise for controllable private authentication," in *Proc. IEEE Int. Symp. Inf. Theory*, Los Angeles, CA, USA, Jun. 2020, pp. 874–878.

[216] O. Günlü, R. F. Schaefer, and G. Kramer, "Private authentication with physical identifiers through broadcast channel measurements," in *Proc. IEEE Inf. Theory Workshop*, Visby, Sweden, Aug. 2019, pp. 1–5.

[217] S. Eiroa and I. Baturone, "An analysis of ring oscillator PUF behavior on FPGAs," in *Proc. IEEE Int. Conf. Field Program. Techn.*, New Delhi, India, Dec. 2011, pp. 1–4.

[218] A. J. H. Vinck, "Applications of coding and information theory in biometrics," in *Proc. Eur. Signal Process. Conf.*, Aug./Sep. 2011, pp. 2254–2258.

[219] O. Günlü and R. F. Schaefer, "An optimality summary: Secret key agreement with physical unclonable functions," *Entropy*, vol. 23, no. 1, p. 16, Jan. 2021.

[220] Z. Goldfeld, P. Cuff, and H. H. Permuter, "Arbitrarily varying wiretap channels with type constrained states," *IEEE Trans. Inf. Theory*, vol. 62, no. 12, pp. 7216–7244, Dec. 2016.

[221] S. Zou, Y. Liang, L. Lai, H. V. Poor, and S. Shamai, "Broadcast networks with layered decoding and layered secrecy: Theory and applications," *Proc. IEEE*, vol. 103, no. 10, pp. 1841–1856, Oct. 2015.

[222] J. Qiu, "Quantum communications leap out of the lab," *Nature*, vol. 508, no. 7497, pp. 441–442, Apr. 2014.

[223] E. Diamanti, "Quantum signals could soon span the globe," *Nature*, vol. 549, no. 7670, pp. 41–42, Sep. 2017.

[224] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.*, Bangalore, India, Dec. 1984, pp. 175–179.

[225] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991.

[226] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, Mar. 2002.

[227] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, "Entropic uncertainty relations and their applications," *Rev. Mod. Phys.*, vol. 89, no. 1, Feb. 2017, Art. no. 015002.

[228] V. Scarani *et al.*, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, Sep. 2009.

[229] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, Oct. 1982.

[230] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, "Leftover hashing against quantum side information," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 5524–5535, Aug. 2011.

[231] S.-K. Liao *et al.*, "Satellite-relayed intercontinental quantum network," *Phys. Rev. Lett.*, vol. 120, Jan. 2018, Art. no. 030501.

[232] R. Renner, "Security of quantum key distribution," Ph.D. dissertation, Dept. Comput. Sci., ETH Zürich, Zürich, Switzerland, 2005.

[233] M. Takeoka, S. Guha, and M. M. Wilde, "Fundamental rate-loss tradeoff for optical quantum key distribution," *Nat. Commun.*, vol. 5, no. 1, p. 5235, Oct. 2014.

[234] B. Schumacher and M. D. Westmoreland, "Quantum privacy and quantum coherence," *Phys. Rev. Lett.*, vol. 80, no. 25, pp. 5695–5697, Jun. 1998.

[235] N. Cai, A. Winter, and R. W. Yeung, "Quantum privacy and quantum wiretap channels," *Probl. Inf. Transm.*, vol. 40, no. 4, pp. 318–336, Oct. 2004.

[236] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 44–55, Jan. 2005.

[237] B. A. Bash *et al.*, "Quantum-secure covert communication on bosonic channels," *Nat. Commun.*, vol. 6, p. 8626, Oct. 2015.

[238] M. S. Bullock, C. N. Gagatsos, S. Guha, and B. A. Bash, "Fundamental limits of quantum-secure covert communication over bosonic channels," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 3, pp. 471–482, Mar. 2020.

[239] J. M. Arrazola and V. Scarani, "Covert quantum communication," *Phys. Rev. Lett.*, vol. 117, Dec. 2016, Art. no. 250503.

[240] J. M. Arrazola and R. Amiri, "Secret-key expansion from covert communication," *Phys. Rev. A*, vol. 97, Feb. 2018, Art. no. 022325.

[241] M. Tahmasbi and M. R. Bloch, "Framework for covert and secret key expansion over classical-quantum channels," *Phys. Rev. A*, vol. 99, May 2019, Art. no. 052329.

[242] M. Tahmasbi and M. R. Bloch, "Towards undetectable quantum key distribution over bosonic channels," *IEEE J. Sel. Areas Inf. Theory*, vol. 1, no. 2, pp. 585–598, Aug. 2020.

[243] A. C. Yao, "Theory and application of trapdoor functions," in *Proc. 23rd Annu. Symp. Found. Comput. Sci. (SFCS)*, 1982, pp. 80–91.

Authorized licensed use limited to: California State University Fresno. Downloaded on June 21,2021 at 09:31:09 UTC from IEEE Xplore. Restrictions apply.

[244] A. M. Turing, "On computable numbers, with an application to the Entscheidungsproblem," *London Math. Soc.*, vol. 2, no. 42, pp. 230–265, 1936.
[245] A. M. Turing, "On computable numbers, with an application to the Entscheidungsproblem. A correction," *London Math. Soc.*, vol. 2, no. 43, pp. 544–546, 1937.
[246] K. Weihrauch, *Computable Analysis—An Introduction*. Berlin, Germany: Springer-Verlag, 2000.
[247] J. Avigad and V. Brattka, "Computability and analysis: The legacy of Alan Turing," in *Turing's Legacy: Developments From Turing's Ideas in Logic*, R. Downey, Ed. Cambridge, U.K.: Cambridge Univ. Press, 2014.
[248] K. Gödel, "Die Vollständigkeit der Axiome des logischen Funktionenkalküls," *Monatshefte für Mathematik*, vol. 37, no. 1, pp. 349–360, 1930.
[249] K. Gödel, "On undecidable propositions of formal mathematical systems," in *Notes by Stephen C. Kleene and Barkely Rosser on Lectures at the Institute for Advanced Study*. Princeton, NJ, USA: Inst. Adv. Study, 1934.
[250] S. C. Kleene, *Introduction to Metamathematics*. New York, NY, USA: Wolters-Noordhoffv, 1952.
[251] M. Minsky, "Recursive unsolvability of Post's problem of 'tag' and other topics in theory of Turing machines," *Ann. Math.*, vol. 74, no. 3, pp. 437–455, 1961.
[252] H. Boche, R. F. Schaefer, and H. V. Poor, "Secure communication and identification systems—Effective performance evaluation on Turing machines," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1013–1025, 2020.
[253] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," Jet Propulsion Lab., Pasadena, CA, USA, DSN Progr., Rep. 42-44, 1978.
[254] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *J. ACM*, vol. 56, no. 6, pp. 1–40, Sep. 2009.
[255] C. Peikert, "A decade of lattice cryptography," *Found. Trends Theor. Comput. Sci.*, vol. 10, no. 4, pp. 283–424, Mar. 2016.

Authorized licensed use limited to: California State University Fresno. Downloaded on June 21,2021 at 09:31:09 UTC from IEEE Xplore. Restrictions apply.