Code Constructions for Physical Unclonable Functions and Biometric Secrecy Systems

Onur Günlü, *Member, IEEE,* Onurcan İşcan, Vladimir Sidorenko, *Member, IEEE,* and Gerhard Kramer, *Fellow, IEEE*

***Abstract*—The two-terminal key agreement problem with biometric or physical identifiers is considered. Two linear code constructions based on Wyner-Ziv coding are developed. The first construction uses random linear codes and achieves all points of the key-leakage-storage regions of the generated-secret and chosen-secret models. The second construction uses nested polar codes for vector quantization during enrollment and error correction during reconstruction. Simulations show that the nested polar codes achieve privacy-leakage and storage rates that improve on existing code designs. One proposed code achieves a rate tuple that cannot be achieved by existing methods.**

***Index Terms*—Information theoretic security, key agreement, physical unclonable functions, Wyner-Ziv coding.**

I. Introduction

Biometric features like fingerprints can be used to authenticate and identify individuals, and to generate secret keys. Similarly, one can generate secret keys with physical unclonable functions (PUFs) that are used as sources of randomness. For example, fine variations of ring oscillator (RO) outputs and the start-up behavior of static random access memories (SRAM) can serve as PUFs [1]. Fingerprints and PUFs are identifiers with high entropy and reliable outputs [2], [3], and one can consider them as physical "one-way functions" that are easy to compute and difficult to invert [4].

There are several requirements that a PUF-based key agreement method should fulfill. First, the method should not leak information about the secret key (no *secrecy leakage*). Second, the method should leak little information about the identifier (limited *privacy leakage*). For example, in most applications the same identifier is used multiple times. If the eavesdropper can extract information about the identifier each time the identifier is used, then the eavesdropper might be able to learn the secret key of a second system that uses the same identifier. Third, one should limit the *storage* rate because storage is generally expensive and limited.

In this work, we focus on the key agreement problem and develop an information-theoretically optimal linear code construction. We then design nested polar codes that achieve better rate tuples than existing code constructions.

A. Related Work and on Basic PUF Models

There are two common models for the key agreement problem: the *generated-secret (GS)* and the *chosen-secret (CS) models*. For the GS model, an encoder extracts a secret key from an identifier measurement, while for the CS model a secret key that is independent of the identifier measurements is given to the encoder by a trusted entity. For the key-agreement model introduced in [5] and [6], two terminals observe dependent random variables and have access to an authenticated, public, one-way communication link; an eavesdropper observes the public messages, called *helper data*. The GS model is treated in [7, Thm. 2.6] as a special case of a more general key agreement problem with eavesdropper side information and a helper. However, [5]–[7] do not consider privacy leakage. The regions of achievable secret-key vs. privacy-leakage (key-leakage) rates for the GS and CS models are given in [2], [8]. The storage rates for general (non-negligible) secrecy-leakage levels are analyzed in [9], while the rate regions with multiple encoder and decoder measurements of a hidden source are treated in [10].

The above papers consider identifier measurements that are independent and identically distributed (i.i.d.) according to a probability distribution with a discrete alphabet. We remark that raw identifier outputs usually have memory but there are transform coding algorithms [11]–[13] that can extract almost i.i.d. and uniformly distributed bits from identifier outputs.

B. Other Models

There are many other key-agreement models. For instance, key agreement and device authentication with an eavesdropper that has access to a sequence correlated with the identifier outputs has been studied in [7], [14]–[16]. The model with eavesdropper side information may be unrealistic, unlike physical-layer security primitives and some biometric identifiers that are continuously available for physical attacks. This is because many physical identifiers and some biometric identifiers are used for *on-demand* key reconstruction, i.e., the attack should be performed during execution, and an invasive attack applied to obtain a correlated sequence permanently changes the identifier output [3].

A closely related problem to the key agreement problem is Wyner's wiretap channel [17], for which code constructions are studied in, e.g., [18]–[20]. The main aim in this problem

The work of O. Günlü was supported by the German Research Foundation (DFG) through the Project HoliPUF under the grant KR3517/6-1. V. Sidorenko is on leave from the Institute for Information Transmission Problems, Russian Academy of Science. The work of G. Kramer was supported by an Alexander von Humboldt Professorship endowed by the German Federal Ministry of Education and Research.

O. Günlü, V. Sidorenko, and G. Kramer are with the Chair of Communications Engineering, Technical University of Munich, 80333 Munich, Germany (e-mail: {onur.gunlu, vladimir.sidorenko, gerhard.kramer}@tum.de).

O. İşcan is with Huawei Technologies Duesseldorf GmbH, 80992 Munich, Germany (email: onurcan.iscan@huawei.com).

is to hide a transmitted message from the eavesdropper that observes a channel output correlated with the observation of a legitimate receiver.

C. Code Constructions

Several practical code constructions for key-agreement with identifiers have been proposed in the literature. For instance, the code-offset fuzzy extractor (COFE) [21] and the fuzzy-commitment scheme (FCS) [22] both require an error-correcting code to satisfy the constraints of, respectively, the key generation (GS model) and key embedding (CS model) problems. Similarly, a polar code construction is proposed in [23] for the GS model. We show that these constructions are suboptimal in terms of the privacy-leakage and storage rates.

The binary Golay code is used in [2] as a vector quantizer (VQ) in combination with Slepian-Wolf (SW) codes [24] to illustrate that the key vs. storage (or key vs. leakage) rate ratio can be increased via quantization. This observation motivates the use of a VQ to improve the performance of previous constructions. In this work, we apply VQ by using Wyner-Ziv (WZ) coding [25] to decrease storage rates, as suggested in [26, Remark 4.5].

The WZ-coding construction turns out to be optimal, which is not coincidental. For instance, the bounds on the storage rate of the GS model and on the WZ rate (storage rate) have the same mutual information terms optimized over the same conditional probability distribution. This similarity suggests an *equivalence* that is closely related to *formula duality* defined, e.g., in [27]. In fact, the optimal random code construction, encoding, and decoding operations are identical for both problems. We therefore call the GS model and WZ problem *functionally equivalent*. Such a strong connection suggests that there might exist constructive methods that are optimal for both problems for all measurement channels, which is closely related to *operational duality*; see [27].

D. Summary of Contributions and Organization

We propose code constructions for the key agreement models of [2], [8], [10] and illustrate that they are asymptotically optimal and improve on all existing methods. A summary of the main contributions is as follows.

- The GS and WZ problems are shown to be functionally equivalent, in the sense that the constraints of both problems are satisfied simultaneously by using the same random code construction.
- We describe two WZ-coding constructions for binary symmetric sources and binary symmetric channels (BSCs). Such sources and channels are often used for physical identifiers such as RO PUFs [12] and SRAM PUFs [28]. The first WZ-coding construction is based on [29] and achieves all points of the key-leakage-storage regions of the GS and CS models. The second construction uses nested polar codes.
- We design and simulate our polar codes for standard parameter ranges for SRAM PUFs under ideal environmental conditions, and for RO PUFS under varying environmental conditions. The target block error probability is $P_B = 10^{-6}$ and the target secret-key size is 128 bits. One of the codes achieves key-leakage-storage rates that cannot be achieved by existing methods.
- In Appendix A, we prove that there are random binning and random coding based approaches that achieve all points of the key-leakage-storage regions of the GS and CS models and that result in strong secrecy.
- In Appendix B, we consider a hidden identifier source whose noisy measurements via BSCs are observed at the encoder and decoder. The WZ-coding construction is shown to be optimal also for such identifiers.

E. Organization

This paper is organized as follows. In Sections II-A and II-B, we describe the GS and CS models, the WZ problem, and give their rate regions. In Section II-C, we show that there is a random code construction that satisfies the constraints of the WZ problem and the GS model simultaneously to motivate using a WZ-coding construction for key generation and embedding. We show that existing methods are suboptimal even after applying improvements described in Section III. Section IV describes a random linear code construction based on WZ-coding. Section V describes a nested polar code design for the GS model and illustrates that it improves on existing code designs.

F. Notation

Upper case letters represent random variables and lower case letters their realizations. A superscript denotes a string of variables, e.g., $X^n = X_1 \dots X_i \dots X_n$, and a subscript denotes the position of a variable in a string. A random variable X has probability distribution P_X. Calligraphic letters such as $\mathcal{X}$ denote sets, and set sizes are written as $|\mathcal{X}|$. Bold letters such as $\mathbf{H}$ represent matrices. $\mathcal{T}_\epsilon^n(P_X)$ denotes the set of length-n letter-typical sequences with respect to the probability distribution P_X and the positive number ϵ [30]. $\mathsf{Enc}(\cdot)$ is an encoder mapping and $\mathsf{Dec}(\cdot)$ is a decoder mapping. $H_b(x) = -x\log x - (1-x)\log(1-x)$ is the binary entropy function, where we take logarithms to the base 2. The $*$-operator is defined as $p * x = p(1-x) + (1-p)x$. The operator $\oplus$ represents the element-wise modulo-2 summation. A BSC with crossover probability p is denoted by $\mathrm{BSC}(p)$. $X^n \sim \mathrm{Bern}^n(\alpha)$ is an i.i.d. binary sequence of random variables with $\Pr[X_i = 1] = \alpha$ for $i = 1, 2, \dots, n$. $\mathbf{H}^T$ represents the transpose of $\mathbf{H}$. A linear error-correction code with parameters (n, k) has block length n and dimension k.

II. Problem Formulations

A. Generated-secret and Chosen-secret Models

Consider the GS model in Fig. $1(a)$, where a secret key is generated from a biometric or physical source. The source, measurement, secret key, and storage alphabets $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{S}$, and $\mathcal{W}$ are finite sets. During enrollment, the encoder observes an i.i.d. sequence X^n, generated by the identifier (source) according to some P_X, and computes a secret key S and public helper data W as $(S, W) = \mathsf{Enc}(X^n)$. During reconstruction,

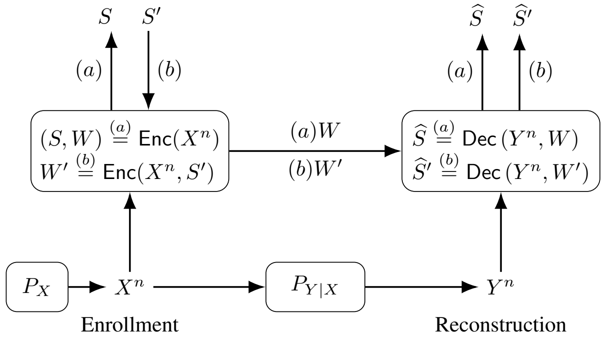
S
S'
(a)
(b)
$\widehat{S}$
$\widehat{S}'$
(a)
(b)
$(S,W)\overset{(a)}{=}\mathsf{Enc}(X^n)$
$W'\overset{(b)}{=}\mathsf{Enc}(X^n,S')$
$(a)W$
$(b)W'$
$\widehat{S}\overset{(a)}{=}\mathsf{Dec}\,(Y^n,W)$
$\widehat{S}'\overset{(b)}{=}\mathsf{Dec}\,(Y^n,W')$
P_X
X^n
$P_{Y|X}$
Y^n
Enrollment
Reconstruction

Fig. 1. The (a) GS and (b) CS models.

the decoder observes a noisy source measurement Y^n of X^n through a memoryless channel $P_{Y|X}$ together with the helper data W. The decoder estimates the secret key as $\widehat{S}=\mathsf{Dec}(Y^n,W)$. Similarly, Fig. 1$(b)$ shows the CS model, where a secret key $S'\in\mathcal{S}$ that is independent of (X^n,Y^n) is embedded into the helper data as $W'=\mathsf{Enc}(X^n,S')$. The decoder for the CS model estimates the secret key as $\widehat{S}'=\mathsf{Dec}(Y^n,W')$.

Definition 1. *A key-leakage-storage tuple* (R_s,R_ℓ,R_w) *is* achievable *for the GS model if, given any* $\epsilon>0$*, there is some* $n\geq 1$*, an encoder, and a decoder such that* $R_s=\frac{\log|\mathcal{S}|}{n}$ *and*

$$\begin{aligned}
&\Pr[\widehat{S}\neq S]\leq\epsilon && (\textit{reliability}) && (1)\\
&\frac{1}{n}I(S;W)\leq\epsilon && (\textit{weak secrecy}) && (2)\\
&\frac{1}{n}H(S)\geq R_s-\epsilon && (\textit{key uniformity}) && (3)\\
&\frac{1}{n}\log|\mathcal{W}|\leq R_w+\epsilon && (\textit{storage}) && (4)\\
&\frac{1}{n}I(X^n;W)\leq R_\ell+\epsilon && (\textit{privacy}). && (5)
\end{aligned}$$

Similarly, a tuple (R_s,R_ℓ,R_w) *is* achievable *for the CS model if, given any* $\epsilon>0$*, there is some* $n\geq1$*, an encoder, and a decoder such that* $R_s=\frac{\log|\mathcal{S}'|}{n}$ *and (1)-(5) are satisfied when* S *and* W *in the constraints are replaced by, respectively,* S' *and* W'*.*

The key-leakage-storage *regions* $\mathcal{R}_{gs}$ *and* $\mathcal{R}_{cs}$ *for the GS and CS models, respectively, are the closures of the sets of achievable tuples for the corresponding models.* ◊

Theorem 1 ([2])**.** *The key-leakage-storage regions for the GS and CS models as in Fig. 1, respectively, are*

$$\begin{aligned}
\mathcal{R}_{gs}=\bigcup_{P_{U|X}}\Big\{&(R_s,R_\ell,R_w)\colon 0\leq R_s,R_\ell,R_w,\\
&R_s\leq I(U;Y),\\
&R_\ell\geq I(U;X)-I(U;Y),\\
&R_w\geq I(U;X)-I(U;Y)\ \textit{for}\\
&P_{UXY}=P_{U|X}P_XP_{Y|X}\Big\},
\end{aligned}\qquad(6)$$

$$\begin{aligned}
\mathcal{R}_{cs}=\bigcup_{P_{U|X}}\Big\{&(R_s,R_\ell,R_w)\colon 0\leq R_s,R_\ell,R_w,\\
&R_s\leq I(U;Y),\\
&R_\ell\geq I(U;X)-I(U;Y),\\
&R_w\geq I(U;X)\ \textit{for}\\
&P_{UXY}=P_{U|X}P_XP_{Y|X}\Big\}.
\end{aligned}\qquad(7)$$

These regions are convex sets. The alphabet $\mathcal{U}$ *of the auxiliary random variable* U *can be limited to have size* $|\mathcal{U}|\leq|\mathcal{X}|+1$ *for both regions* $\mathcal{R}_{gs}$ *and* $\mathcal{R}_{cs}$*.*

B. Wyner-Ziv Problem

Consider two dependent random variables X and Y with joint distribution P_{XY}. Fig. 2 depicts the WZ problem. The source, side information, and message alphabets $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{W}$ are finite sets. An encoder that observes X^n generates the message $W\in[1,2^{nR_w}]$. The decoder observes Y^n and W and puts out a quantized version $\widehat{X}^n$ of X^n. Define the average distortion between X^n and the reconstructed sequence $\widehat{X}^n$ as

$$\frac{1}{n}\sum_{i=1}^{n}E[d(X_i,\widehat{X}_i(Y^n,W))]\qquad(8)$$

where $d(x,\hat{x})$ is a distortion function and $\widehat{X}_i(y^n,w)$ is a reconstruction function. For simplicity, assume that $d(x,\hat{x})$ is bounded.

Definition 2. *A WZ rate-distortion pair* (R_w,D) *is* achievable *for a distortion measure* $d(x,\hat{x})$ *if, given any* $\epsilon>0$*, there is some* $n\geq1$*, an encoder, and a decoder that satisfy the inequalities (4) and*

$$\frac{1}{n}\sum_{i=1}^{n}E[d(X_i,\widehat{X}_i(Y^n,W))]\leq D+\epsilon.\qquad(9)$$

The WZ rate-distortion region $\mathcal{R}_{\text{WZ}}$ *is the closure of the set of achievable rate-distortion pairs.* ◊

Theorem 2 ([25])**.** *The WZ rate-distortion region is*

$$\begin{aligned}
\mathcal{R}_{\text{WZ}}=\bigcup_{P_{U|X}}\ \bigcup_{\widehat{X}(Y,U)}\Big\{&(R_w,D)\colon 0\leq R_w,\\
&R_w\geq I(U;X)-I(U;Y),\\
&D\geq E[d(X,\widehat{X}(Y,U))]\ \textit{for}\\
&P_{UXY}=P_{U|X}P_{XY}\Big\}
\end{aligned}\qquad(10)$$

where $\widehat{X}(Y,U)$ *is a reconstruction function used at the decoder. One can limit the alphabet* $\mathcal{U}$ *of the auxiliary random variable* U *to have size* $|\mathcal{U}|\leq|\mathcal{X}|+1$*. The region* $\mathcal{R}_{\text{WZ}}$ *is convex.*

C. Functional Equivalence

The duality of two problems is sometimes useful because it can help to find optimal code constructions for otherwise difficult-looking problems. Similar to duality, we call the

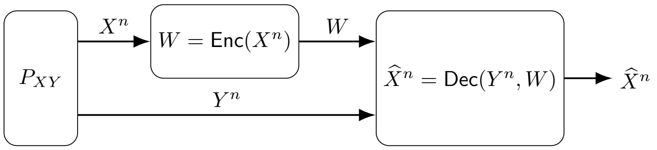

Fig. 2. The WZ problem.

problems given in Definitions 1 and 2 *functionally equivalent* because the optimal random code constructions for the GS model and WZ problem are the same. More precisely, we say that the problems are functionally equivalent for some specified (R_s, R_ℓ, R_w, D) if there is a random code construction that satisfies (1)-(5) and (9) simultaneously. Functional duality is closely related to functional equivalence, but we do not exchange the encoders and decoders for the latter, unlike for the functional duality.

Theorem 3. *The GS model with the probability distributions P_X and $P_{Y|X}$, and the WZ problem with the joint probability distribution $P_{XY} = P_X P_{Y|X}$ and a distortion function $d(x, \hat{x})$ are functionally equivalent.*

Proof Sketch: Fix a $P_{U|X}$ and $\widehat{X}(y, u)$ such that $E[d(X, \hat{X}(Y, U))] \leq D + \epsilon$ for some distortion $D > 0$ and $\epsilon > 0$. Randomly and independently generate codewords $u^n(w, s)$, $w = 1, 2, \dots, 2^{nR_w}$, $s = 1, 2, \dots, 2^{nR_s}$ according to $\prod_{i=1}^{n} P_U(u_i)$, where $P_U(u_i) = \sum_{x \in \mathcal{X}} P_{U|X}(u|x) P_X(x)$. These codewords define the random codebook

$$\mathcal{C} = \{U^n(w, s)\}_{(w,s)=(1,1)}^{(2^{nR_w}, 2^{nR_s})}. \qquad (11)$$

Let $0 < \epsilon' < \epsilon$.

Encoding: Given x^n, the encoder looks for a codeword that is jointly typical with x^n, i.e., $(u^n(w, s), x^n) \in \mathcal{T}_{\epsilon'}^n(P_{UX})$. If there is one or more such codeword, the encoder chooses one of them and puts out (w, s). If there is no such codeword, set $w = s = 1$. The encoder publicly stores w.

Decoding: The decoder puts out $\hat{s}$ if there is a unique key label $\hat{s}$ that satisfies the typicality check $(u^n(w, \hat{s}), y^n) \in \mathcal{T}_{\epsilon}^n(P_{UY})$; otherwise, it sets $\hat{s} = 1$. The decoder then puts out $\widehat{X}(y_i, u_i(w, \hat{s})) = \hat{x}_i$ for all $i = 1, 2, \dots, n$.

Using covering and packing lemmas [31, Lemmas 3.3 and 3.1], there is a code that satisfies (1)-(5) and (9) if we consider large n and approximately $2^{n(I(U;X) - I(U;Y))}$ storage labels w and $2^{nI(U;Y)}$ key labels s. This code asymptotically achieves the key-leakage-storage tuple $(R_s, R_\ell, R_w) = (I(U;Y), I(U;X) - I(U;Y), I(U;X) - I(U;Y))$. Using the typical average lemma [31, Section 2.4], the rate-distortion (R_w, D) pair can be achieved as well. ■

Note that by using the coding scheme defined in the proof of Theorem 3 and by taking the union of the achieved rate tuples over all $P_{U|X}$, one can achieve the key-leakage-storage region $\mathcal{R}_{\text{gs}}$. Achieving the region $\mathcal{R}_{\text{cs}}$ follows by adding a one-time pad step to the proof of the GS model [2]. Similarly, by using the same coding scheme and by taking the union of the achieved tuples over all $P_{U|X}$ and all reconstruction functions $\widehat{X}(\cdot)$, one can achieve the rate-distortion region $\mathcal{R}_{\text{WZ}}$.

Motivated by Theorem 3, we show in Section IV that a linear WZ-coding construction achieves all boundary points of the key-leakage-storage regions of the GS and CS models for uniform binary sources measured through a BSC.

III. Prior Art and Comparisons

There are several existing code constructions proposed for the GS and CS models. We here consider the three best methods: FCS [22] for the CS model, and COFE [21] and the polar code construction in [23] for the GS model.

During enrollment with the FCS, an encoder takes a uniformly distributed secret key S' as input to generate a codeword C^n. The codeword and the binary source output X^n are summed modulo-2, and the sum is stored as helper data W'. During reconstruction, W' and another binary sequence Y^n, correlated with X^n through, e.g., a BSC(p_A), are summed modulo-2 and this sum is used by a decoder to estimate S'. Similar steps are applied in the COFE, except that the secret key is a hashed version of X^n. The FCS achieves the single optimal point in the key-leakage region with the maximum secret-key rate $R_s^* = I(X;Y)$; the privacy-leakage rate is $R_\ell^* = H(X|Y)$ [32]. Similarly, the COFE achieves the same boundary point in the key-leakage region. This is, however, the only boundary point of the key-leakage regions that these methods can achieve.

We can improve both methods by adding a VQ step: instead of X^n we use its quantized version X_q^n during enrollment. This asymptotically corresponds to summing the original helper data and an independent random variable $J^n \sim \text{Bern}^n(q)$ such that $W'' = X^n \oplus C^n \oplus J^n$ is the new helper data so that we create a virtual channel $P_{Y|X \oplus J}$ and apply the FCS or COFE to this virtual channel. The modified FCS and COFE can achieve all points of the key-leakage region if we take a union of all rate pairs achieved over all $q \in [0, 0.5]$. However, the helper data has n bits for both methods, and the resulting storage rate of 1 bit/symbol is not necessarily optimal.

The polar code construction in [23] requires less storage rate than the FCS and COFE. However, this approach improves only the storage rate and cannot achieve all points of the key-leakage-storage region. Furthermore, in [23] some code designs assume that there is a "private" key shared only between the encoder and decoder, which is not realistic since a private key requires hardware protection against invasive attacks. If such a protection is possible, then there is no need to use an on-demand key reconstruction method like a PUF.

The existing methods cannot, therefore, achieve all points of the key-leakage-storage region for a BSC, unlike the WZ-coding constructions we describe in Sections IV and V.

In previous works such as [33], only the secret-key rates of the proposed codes are compared because the sum of the secret-key and storage (or privacy-leakage) rates is one. This constraint means that increasing the key vs. storage (or key vs. leakage) rate ratio is equivalent to increasing the key rate. Instead, our code constructions are more flexible than the existing methods in terms of achievable rate tuples. We will use the key vs. storage rate ratio as a metric to control the storage and privacy leakage in our code designs.

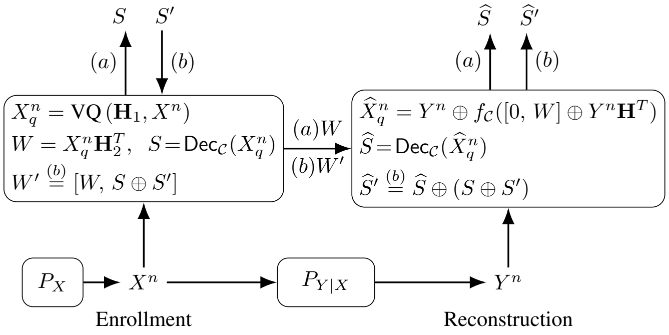
S
S'
(a)
(b)
$X_q^n = \mathsf{VQ}(\mathbf{H}_1, X^n)$
$W = X_q^n\mathbf{H}_2^T,\ S = \mathsf{Dec}_{\mathcal{C}}(X_q^n)$
$W' \overset{(b)}{=} [W, S \oplus S']$
$(a)W$
$(b)W'$
$\widehat{S}$
$\widehat{S}'$
$\widehat{X}_q^n = Y^n \oplus f_{\mathcal{C}}([0, W] \oplus Y^n\mathbf{H}^T)$
$\widehat{S} = \mathsf{Dec}_{\mathcal{C}}(\widehat{X}_q^n)$
$\widehat{S}' \overset{(b)}{=} \widehat{S} \oplus (S \oplus S')$
P_X
X^n
$P_{Y|X}$
Y^n
Enrollment
Reconstruction

Fig. 3. First WZ-coding construction for the (a) GS and (b) CS models, where VQ represents the vector quantization and $\mathsf{Dec}_{\mathcal{C}}$ represents the demapping operation between a codeword of the code $\mathcal{C}$ and the corresponding information sequence.

IV. First WZ-coding Construction

Consider the lossy source coding construction proposed in [29] that achieves the boundary points of the WZ rate-distortion region by using linear codes. We use this code construction to achieve the boundary points of $\mathcal{R}_{\text{gs}}$ and $\mathcal{R}_{\text{cs}}$ for a binary uniform identifier source P_X and a BSC $P_{Y|X}$ with crossover probability p_A (see [11]–[13] for algorithms to obtain approximately such outputs from correlated and biased identifier outputs). Fig. 3(a) and Fig. 3(b) plot the proposed code construction, respectively, for the GS and CS models.

Code Construction: Choose uniformly at random full-rank parity-check matrices $\mathbf{H}_1$, $\mathbf{H}_2$, and $\mathbf{H}$ as

$$\mathbf{H} = \begin{bmatrix}\mathbf{H}_1\\ \mathbf{H}_2\end{bmatrix} \tag{12}$$

where $\mathbf{H}_1$ with dimensions $m_1 \times n$ defines a binary $(n, n-m_1)$ linear code $\mathcal{C}_1$ and $\mathbf{H}_2$ with dimensions $m_2 \times n$ defines another binary $(n, n-m_2)$ linear code $\mathcal{C}_2$. The $(n, n-m_1-m_2)$ code $\mathcal{C}$ defined by $\mathbf{H}$ in (12) is thus a subcode of $\mathcal{C}_1$ such that $\mathcal{C}_1$ is partitioned into 2^{m_2} cosets of $\mathcal{C}$. For some distortion $q \in [0, 0.5]$ and $\delta > 0$, impose the conditions

$$\frac{m_1}{n} = H_b(q) + \delta \tag{13}$$

$$\frac{m_1 + m_2}{n} = H_b(q * p_A) + 2\delta. \tag{14}$$

Enrollment: The vector quantizer (VQ) in Fig. 3 quantizes the source output X^n into the closest codeword X_q^n in $\mathcal{C}_1$ in Hamming metric. If there are two or more codewords with the minimum Hamming distance, the VQ chooses one of them uniformly at random. Define the error sequence

$$E_q^n = X^n \oplus X_q^n \tag{15}$$

which resembles an i.i.d. sequence $\sim \text{Bern}^n(q)$ when $n \to \infty$ due to uniformity of X^n and the linearity of $\mathcal{C}_1$ [29].

In the GS model, we publicly store the side information

$$W = X_q^n \mathbf{H}_2^T \tag{16}$$

which corresponds to a coset of $\mathcal{C}$. We sum modulo-2 the bit sequence that is in the coset W and that has the minimum Hamming weight with X_q^n to obtain a codeword X_c^n of $\mathcal{C}$. Then, we assign the information sequence that is encoded to the codeword X_c^n as the secret key S such that $X_c^n = S\mathbf{G}$, where $\mathbf{G}$ is the generator matrix of $\mathcal{C}$. The secret key has length $n - m_1 - m_2$ bits. We denote this operation as $\mathsf{Dec}_{\mathcal{C}}(\cdot)$.

Consider the secrecy leakage for the GS model:

$$\begin{aligned}
\lim_{n\to\infty}\frac{1}{n}I(S;W) &= \lim_{n\to\infty}\frac{1}{n}\big(H(S)+H(W)-H(W,S)\big)\\
&\overset{(a)}{\le} \lim_{n\to\infty}\frac{1}{n}\big(\log|\mathcal{S}| + \log|\mathcal{W}| - H(W,S,X_q^n)\big)\\
&\le \lim_{n\to\infty}\frac{1}{n}\big((n-m_1-m_2) + m_2 - H(X_q^n)\big)\\
&\overset{(b)}{\le} \lim_{n\to\infty}\frac{1}{n}\big(n - m_1 - (n - m_1 - n\delta_n)\big) = 0
\end{aligned} \tag{17}$$

where (a) follows because (W, S) determines X_q^n and (b) follows with high probability for some δ_n such that $\lim_{n\to\infty}\delta_n = 0$ due to the translation invariance of the linear code $\mathcal{C}_1$ and the uniformity of X^n (see also the discussions in [34, Section I]).

For the CS model shown in Fig. 3(b), we have access to an embedded (chosen) secret key S' that is independent of (X^n, Y^n) and such that $|\mathcal{S}| = |\mathcal{S}'|$. We store the helper data $W' = [W, S \oplus S']$. The secrecy leakage for the CS model is

$$\begin{aligned}
&\lim_{n\to\infty}\frac{1}{n}I(S';W') = \lim_{n\to\infty}\frac{1}{n}I(S';W,S\oplus S')\\
&\overset{(a)}{=} \lim_{n\to\infty}\frac{1}{n}\Big(H(S') + H(W,S\oplus S') - H(W,S) - H(S')\Big)\\
&\le \lim_{n\to\infty}\frac{1}{n}\Big(H(W) + H(S\oplus S') - H(W,S)\Big)\\
&\overset{(b)}{\le} \lim_{n\to\infty}\frac{1}{n}\big(\log|\mathcal{W}| + \log|\mathcal{S}| - H(W,S,X_q^n)\big)\\
&\overset{(c)}{\le} \lim_{n\to\infty}\frac{1}{n}\big(m_2 + (n-m_1-m_2) - (n-m_1-n\delta_n)\big) = 0
\end{aligned} \tag{18}$$

where (a) follows because S' is independent of (W, S), (b) follows because $|\mathcal{S}| = |\mathcal{S}'|$ and (W, S) determines X_q^n, and (c) follows with high probability for some δ_n such that $\lim_{n\to\infty}\delta_n = 0$ due to the translation invariance of the linear code $\mathcal{C}_1$ and uniformity of X^n.

Remark 1. *We can improve the weak-secrecy results in (17) and (18) to strong-secrecy results, i.e., we replace (2) with*

$$I(S;W) \le \epsilon \qquad \textit{(strong secrecy)} \tag{19}$$

by applying information reconciliation and privacy amplification steps to multiple blocks of identifier outputs as described in [35], e.g., by using multiple PUFs in a device for key agreement.

Remark 2. *We prove in Appendix A that there are code constructions that provide strong secrecy for general probability distributions P_{XY} without additional information reconciliation and privacy amplification steps.*

Reconstruction: The noisy identifier output observed during reconstruction is $Y^n = X^n \oplus Z^n$, where Z^n is independent of X^n and $Z^n \sim \text{Bern}^n(p_A)$. The error sequence E_q^n and the noise sequence Z^n are independent. Furthermore, E_q^n asymptotically resembles an i.i.d. sequence $\sim \text{Bern}^n(q)$ when $n \to \infty$, as discussed above. Therefore, when $n \to \infty$, the sequence $E_q^n \oplus Z^n$, which corresponds to the noise sequence of the equivalent channel $P_{Y^n|X_q^n}$, is distributed according to $\text{Bern}^n(q * p_A)$ since the equivalent channel is a concatenation of two BSCs. One can thus reconstruct X_q^n with high probability when $n \to \infty$ by using the syndrome decoder $f_{\mathcal{C}}(\cdot)$ of the code $\mathcal{C}$ as follows

$$\begin{aligned}\widehat{X}_q^n &= Y^n \oplus f_{\mathcal{C}}([0,\,W] \oplus Y^n\mathbf{H}^T)\\ &\overset{(a)}{=} Y^n \oplus f_{\mathcal{C}}(X_q^n\mathbf{H}^T \oplus Y^n\mathbf{H}^T)\\ &\overset{(b)}{=} (X_q^n \oplus E_q^n \oplus Z^n) \oplus f_{\mathcal{C}}((E_q^n \oplus Z^n)\mathbf{H}^T)\\ &\overset{(c)}{=} (X_q^n \oplus E_q^n \oplus Z^n) \oplus (E_q^n \oplus Z^n)\\ &= X_q^n \end{aligned} \tag{20}$$

where (a) follows by (16) and because X_q^n is a codeword of $\mathcal{C}_1$, (b) follows by (15), and (c) follows with high probability because, asymptotically, $E_q^n \oplus Z^n \sim \text{Bern}^n(q * p_A)$ so that the syndrome decoder $f_{\mathcal{C}}(\cdot)$ determines the noise sequence $E_q^n \oplus Z^n$. This is because the constraint in (14) indicates that the code rate of $\mathcal{C}$ is below the capacity of the BSC$(q * p_A)$.

The secret-key is reconstructed in the GS model as

$$\widehat{S} = \mathsf{Dec}_{\mathcal{C}}(\widehat{X}_q^n) \tag{21}$$

and in the CS model as

$$\widehat{S}' = \widehat{S} \oplus (S \oplus S') \tag{22}$$

both of which result in the same error probability.

A. Optimality of the Proposed Construction for the GS Model

Recall that $X^n \sim \text{Bern}^n(\frac{1}{2})$ and that the channel $P_{Y|X}$ is a BSC(p_A), where $p_A \in [0, 0.5]$. Using Mrs. Gerber's lemma [36], the key-leakage-storage region of the GS model is

$$\begin{aligned}\mathcal{R}_{\text{gs,bin}} = \bigcup_{q \in [0,0.5]} \Big\{ &(R_s, R_\ell, R_w)\colon\\ &0 \leq R_s \leq 1 - H_b(q * p_A),\\ &R_\ell \geq H_b(q * p_A) - H_b(q),\\ &R_w \geq H_b(q * p_A) - H_b(q) \Big\}. \end{aligned} \tag{23}$$

Theorem 4. *The key-leakage-storage region $\mathcal{R}_{gs,bin}$ for the GS model is achieved by using the WZ-coding construction proposed above.*

Proof: By (13) and (14), we have

$$\frac{\log|\mathcal{W}|}{n} = \frac{m_2}{n} = H_b(q * p_A) - H_b(q) + \delta \leq R_w + \delta \tag{24}$$

if $R_w \geq H_b(q * p_A) - H_b(q)$.

The secret key satisfies

$$\begin{aligned}\frac{H(S)}{n} &\geq \frac{n - m_1 - m_2}{n} - \delta = 1 - H_b(q * p_A) - 3\delta\\ &\geq R_s - 3\delta \end{aligned} \tag{25}$$

if $R_S \leq 1 - H_b(q * p_A)$. Furthermore, we have

$$\begin{aligned}\frac{I(X^n; W)}{n} &\overset{(a)}{=} \frac{H(W)}{n} \leq \frac{\log|\mathcal{W}|}{n} = \frac{m_2}{n}\\ &= H_b(q * p_A) - H_b(q) + \delta \leq R_\ell + \delta \end{aligned} \tag{26}$$

if $R_\ell \geq H_b(q * p_A) - H_b(q)$, where (a) follows because X^n determines W. ■

B. Optimality of the Proposed Construction for the CS Model

The key-leakage-storage region of the CS model for a uniform binary source measured through a BSC(p_A) is

$$\begin{aligned}\mathcal{R}_{\text{cs,bin}} = \bigcup_{q \in [0,0.5]} \Big\{ &(R_s, R_\ell, R_w)\colon\\ &0 \leq R_s \leq 1 - H_b(q * p_A),\\ &R_\ell \geq H_b(q * p_A) - H_b(q),\\ &R_w \geq 1 - H_b(q) \Big\}. \end{aligned} \tag{27}$$

Theorem 5. *The key-leakage-storage region $\mathcal{R}_{cs,bin}$ for the CS model is achieved by using the WZ-coding construction proposed above.*

Proof: The storage rate for the CS model is the sum of the storage and secret-key rates of the GS model. By choosing achievable storage and key rates for the GS model, we can achieve for the CS model a storage rate of

$$R_w \geq 1 - H_b(q). \tag{28}$$

Since $H(S') = \log|\mathcal{S}'|$, $|\mathcal{S}| = |\mathcal{S}'|$, and S' is independent of (X^n, Y^n), the secret-key and privacy-leakage rates are the same as in the GS model, i.e., we have

$$R_s \leq 1 - H_b(q * p_A) \tag{29}$$

$$R_\ell \geq H_b(q * p_A) - H_b(q). \tag{30}$$

■

Remark 3. *We show in Appendix B that the above WZ-coding construction is optimal also for hidden sources, i.e., the encoder observes a noisy measurement of the source rather than the source itself.*

V. Second WZ-coding Construction with Polar Codes

Polar codes [37] have a low encoding/decoding complexity, asymptotic optimality for various problems, and good finite length performance if a list decoder is used. Furthermore, they have a structure that allows simple nested code design, and they can be used for WZ-coding [38].

Polar codes rely on the *channel polarization* phenomenon, where a channel is converted into polarized bit channels by a polar transform. This transform converts an input sequence U^n with frozen and unfrozen bits to a codeword of the same length n. A polar decoder processes a noisy observation of the codeword together with the frozen bits to estimate U^n.

Let $\mathcal{C}(n, \mathcal{F}, G^{|\mathcal{F}|})$ denote a polar code of length n, where $\mathcal{F}$ is the set of indices of the frozen bits and $G^{|\mathcal{F}|}$ is the sequence of frozen bits. In the following, we use the nested polar code construction proposed in [38].

A. Polar Code Construction for the GS Model

We use two polar codes $\mathcal{C}_1(n, \mathcal{F}_1, V)$ and $\mathcal{C}(n, \mathcal{F}, \overline{V})$ with $\mathcal{F} = \mathcal{F}_1 \cup \mathcal{F}_w$ and $\overline{V} = [V, W]$, where V has length m_1 and W has length m_2 such that m_1 and m_2 satisfy (13) and (14). The indices in $\mathcal{F}_1$ represent frozen channels with assigned values

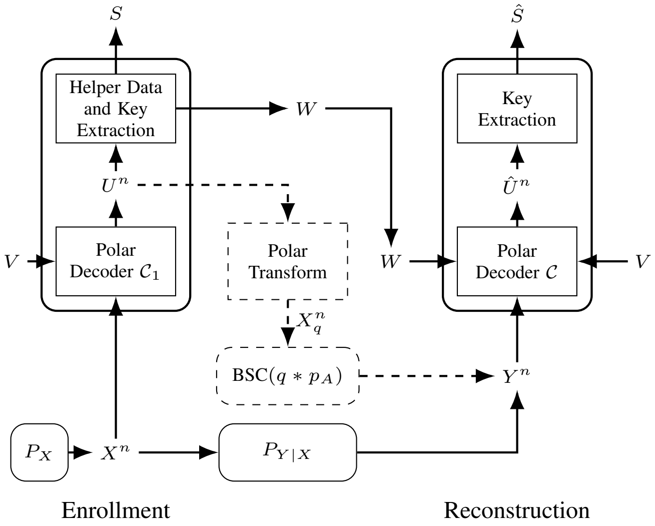

Fig. 4. Second WZ-coding construction for the GS model.

V for both codes and $\mathcal{C}$ has additional frozen channels with assigned values W denoted by $\mathcal{F}_w$, i.e., the codes are nested.

The code $\mathcal{C}_1$ serves as a VQ with a desired distortion q, and the code $\mathcal{C}$ serves as the error correcting code for a BSC$(q * p_A)$. The idea is to obtain W during enrollment and store it as public helper data. For reconstruction, W is used by the decoder to estimate the secret key S of length $n - m_1 - m_2$. Fig. 4 shows the block diagram of the proposed construction. In the following, suppose V is the all-zero vector so that no additional storage is necessary. This choice has no effect on the average distortion $E[q]$ between X^n and X_q^n defined below; see [38, Lemma 10].

Enrollment: The uniform binary sequence X^n generated by a PUF during enrollment is treated as the noisy observation of a BSC(q). X^n is quantized by a polar decoder of $\mathcal{C}_1$. We extract from the decoder output U^n the bits at indices $\mathcal{F}_w$ and store them as the helper data W. The bits at the indices $i \in \{1, 2, \dots, n\} \backslash \mathcal{F}$ are used as the secret key. Note that applying a polar transform to U^n generates X_q^n, which is a distorted version of X^n. The distortion between X^n and X_q^n is modeled as a BSC(q) because the error sequence $E_q^n = X^n \oplus X_q^n$ resembles an i.i.d. sequence $\sim$ Bern$^n(q)$ when $n \to \infty$ [38, Lemma 11].

Reconstruction: During reconstruction, the polar decoder of $\mathcal{C}$ observes the binary sequence Y^n, which is a noisy measurement of X^n through a BSC(p_A). The frozen bits $\overline{V} = [V, W]$ at indices $\mathcal{F}$ are input to the polar decoder. The output $\widehat{U}^n$ of the polar decoder is the estimate of U^n and contains the estimate $\widehat{S}$ of the secret key at the unfrozen indices of $\mathcal{C}$, i.e., $i \in \{1, 2, \dots, n\} \setminus \mathcal{F}$.

We next give a method to design practical nested polar codes for the GS model.

Construction of $\mathcal{C}$ and $\mathcal{C}_1$: Since $\mathcal{C} \subseteq \mathcal{C}_1$ are nested codes, they must be constructed jointly. $\mathcal{F}$ and $\mathcal{F}_1$ should be selected such that the reliability and security constraints are satisfied. For a given secret key size $n - m_1 - m_2$, block length n, crossover probability p_A, and target block-error probability $P_B = \Pr[S \neq \widehat{S}]$, we propose the following procedure.

1) Construct a polar code of rate $(n-m_1-m_2)/n$ and use it as the code $\mathcal{C}$, i.e., define the set of frozen indices $\mathcal{F}$.
2) Evaluate the error correction performance of $\mathcal{C}$ with a decoder for a BSC over a range of crossover probabilities to obtain the crossover probability p_c, resulting in a target block-error probability of P_B. Using $p_c = E[q] * p_A$, we obtain the target distortion $E[q]$ averaged over a large number of realizations of X^n.
3) Find an $\mathcal{F}_1 \subset \mathcal{F}$ that results in an average distortion of $E[q]$ with a minimum possible amount of helper data. Use $\mathcal{F}_1$ as the frozen set of $\mathcal{C}_1$.

Step 1 is a conventional polar code design task and step 2 is applied by Monte-Carlo simulations. For step 3, we start with $\mathcal{F}_1^{'} = \mathcal{F}$ and compute the resulting average distortion $E[q']$ via Monte-Carlo simulations. If $E[q']$ is not less than $E[q]$, we remove elements from $\mathcal{F}_1^{'}$ according to the reliabilities of the polarized bit channels and repeat the procedure until we obtain the desired average distortion $E[q]$.

We remark that the distortion level introduced by the VQ is an additional degree of freedom in choosing the code design parameters. For instance, different values of P_B can be targeted with the same code by changing the distortion level. Alternatively, devices with different p_A values can be supported by using the same code. This additional degree of freedom makes the proposed code design suitable for a wide range of applications.

B. Proposed Codes for the GS Model

Consider, for instance, the GS model where S is used in the advanced encryption standard (AES) with length 128, i.e., $\log |\mathcal{S}| = n - m_1 - m_2 = 128$ bits. If we use PUFs in a field-programmable gate array (FPGA) as the randomness source, we must satisfy a block-error probability P_B of at most 10^{-6} [39]. Consider a BSC $P_{Y|X}$ with crossover probability $p_A = 0.15$, which is a common value for SRAM PUFs under ideal environmental conditions [28] and for RO PUFs under varying environmental conditions [1]. We design nested polar codes for these parameters to illustrate that we can achieve better key-leakage-storage rate tuples than previously proposed codes.

Code 1: Consider $n = 1024$ and recall that $n - m_1 - m_2 = 128$, $P_B = 10^{-6}$, and $p_A = 0.15$. Polar successive cancellation list (SCL) decoders with list size 8 are used as the VQ and channel decoder. We first design the code $\mathcal{C}$ of rate 128/1024 and evaluate its performance with the SCL decoder for a BSC with a range of crossover probabilities, as shown in Fig. 5. We observe a block-error probability of 10^{-6} at a crossover probability of $p_c = 0.1819$. Since $p_A = 0.15$, this corresponds to an average distortion of $E[q] = 0.0456$, i.e., $E[q] * p_A = 0.1819$.

Fig. 6 shows the average distortion $E[q]$ with respect to $n - m_1 = n - |\mathcal{F}_1|$, obtained by Monte-Carlo simulations. We observe from Fig. 6 that the target average distortion is obtained at $n - m_1 = 778$ bits. Thus, $m_2 = 650$ bits of helper data suffice to obtain a block-error probability of $P_B = 10^{-6}$ to reconstruct a $n - m_1 - m_2 = 128$-bit secret key.

We observe that the parameter p_c is less than $p_A = 0.15$ when we apply the procedure in Section V-A to $n = 512$ with

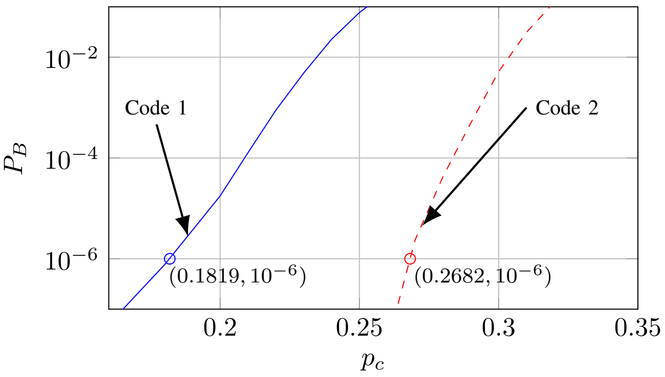

Fig. 5. Block error probability of $\mathcal{C}$ over a BSC(p_c) with an SCL decoder (list size 8) for codes 1 and 2 of length 1024 and 2048, respectively.

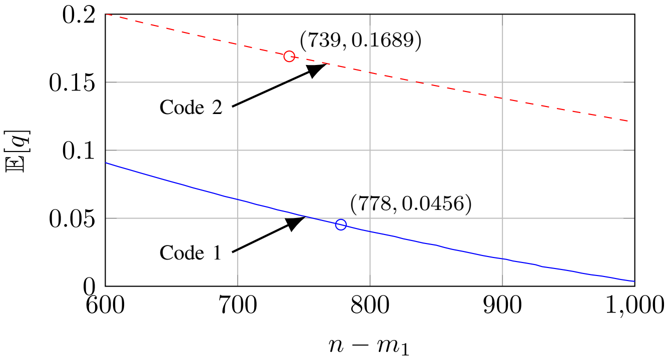

Fig. 6. Average distortion $E[q]$ with respect to $n - m_1$ with an SCL decoder (list size 8) for codes 1 and 2 of length 1024 and 2048, respectively.

the same P_B. Therefore, it is not possible to construct a code with our procedure for $n \leq 512$ since $q * p_A$ is an increasing function of q for any $q \in [0, 0.5]$. Such a code construction for $n = 512$ might be possible if one improves the code design and the decoder.

Code 2: Consider the same parameters as in code 1, except $n = 2048$. We apply the same steps as above and plot the performance of an SCL decoder for a BSC with a range of crossover probabilities in Fig. 5. A crossover probability of $p_c = 0.2682$ is required to obtain a block-error probability of 10^{-6}, which gives an average distortion of $E[q] = 0.1689$. As depicted in Fig. 6, we achieve the target average distortion with $n - m_1 = 739$ bits so that helper data of length 611 bits is required to satisfy $P_B = 10^{-6}$ for a secret key of length 128 bits.

Remark 4. *Our assumptions on the channel statistics are not necessarily satisfied for the model depicted in Fig. 4 for finite n since, e.g., the channel $P_{X^n|X_q^n}$ is not $\sim$ Bern$^n(q)$. However, our code designs and analysis are based on simulations made over a large number of possible inputs at fixed lengths, which allows us to give reliability guarantees to a set of input realizations. The results of such guarantees are given below.*

The error probability P_B is calculated as an average over a large number of PUF realizations, i.e., over a large number of PUF devices with the same circuit design. To satisfy the block-error requirement for each PUF realization, one could consider using the maximum distortion instead of $E[q]$ as a metric in step 3 in Section V-A. This would increase the amount of helper data. We can guarantee a block-error probability of at most 10^{-6} for 99.99% of all realizations x^n of X^n by adding 32 bits to the helper data for code 1 and 33 bits for code 2. The numbers of extra helper data bits required are small since the variance of the distortion q over all PUF realizations is small for the blocklengths considered. For comparisons, we use the helper data sizes required to guarantee $P_B = 10^{-6}$ for 99.99% of all PUF realizations.

C. Code Comparisons and Discussions

We show in Fig. 7 the storage-key (R_w, R_s) projection of the boundary points of the region $\mathcal{R}_{\text{gs}}$ for $p_A = 0.15$. Furthermore, we show the point with the maximum secret-key rate R_s^* and the minimum storage rate R_w^* to achieve R_s^*. For the FCS and COFE, we use the random coding union bound [40, Thm. 16] to confirm that the plotted rate pairs are achievable for a secret-key length of 128 bits, an error probability of $P_B = 10^{-6}$, and blocklengths of $n = 1024$ and $n = 2048$. These rate pairs are shown in Fig. 7 to the right of the dashed line representing $R_w + R_s = 1$. Similarly, the rate pairs achieved by the previous polar code design, and codes 1 and 2 are shown in Fig. 7.

The storage rates of the FCS and COFE are 1 bit/symbol, which is suboptimal as discussed in Section III. The previous polar code construction in [23] achieves a rate point with $R_s + R_w = 1$ bit/symbol, which is expected since this is a SW-coding construction. The polar code construction improves on the rate pairs achieved by the FCS and COFE in terms of the key vs. storage ratio.

We achieve the key-leakage-storage rates of approximately $(0.125, 0.666, 0.666)$ bits/symbol by code 1 and $(0.063, 0.315, 0.315)$ bits/symbol by code 2, projections of which are depicted in Fig. 7. These rates are significantly better than the best rate tuple $(0.125, 0.875, 0.875)$ bits/symbol in the literature, i.e., the previous polar code construction in [23], for the same parameters and without any private key assumption. We increase the key vs. storage rate ratio R_s/R_w from 0.188 for code 1 to 0.199 for code 2, which suggests to increase the blocklength to obtain better ratios. Furthermore, code 2 achieves privacy-leakage and storage rates that cannot be achieved by existing methods without applying *time sharing* (see, e.g., [31, Section 4.4]). This is because code 2 achieves privacy-leakage and storage rates of 0.315 bits/symbol that are significantly less than the minimum privacy-leakage and storage rates $R_w^* = R_\ell^* = H_b(p_A) \approxeq 0.610$ bits/symbol that can be asymptotically achieved by existing methods at the maximum secret-key rate $R_s^* \approxeq 0.390$ bits/symbol.

We use the sphere packing bound [41, Eq. (5.8.19)] to upper bound the key vs. storage rate ratio that can be achieved by SW-coding constructions for the maximum secret-key rate point. Consider $p_A = 0.15$, $n = 1024$, and $P_B = 10^{-6}$, for which the sphere packing bound requires that the rate of the code $\mathcal{C}$ satisfies $R_{\mathcal{C}} \leq 0.273$. If we assume that the key rate is given by its maximal value $R_s = R_{\mathcal{C}}$ and the

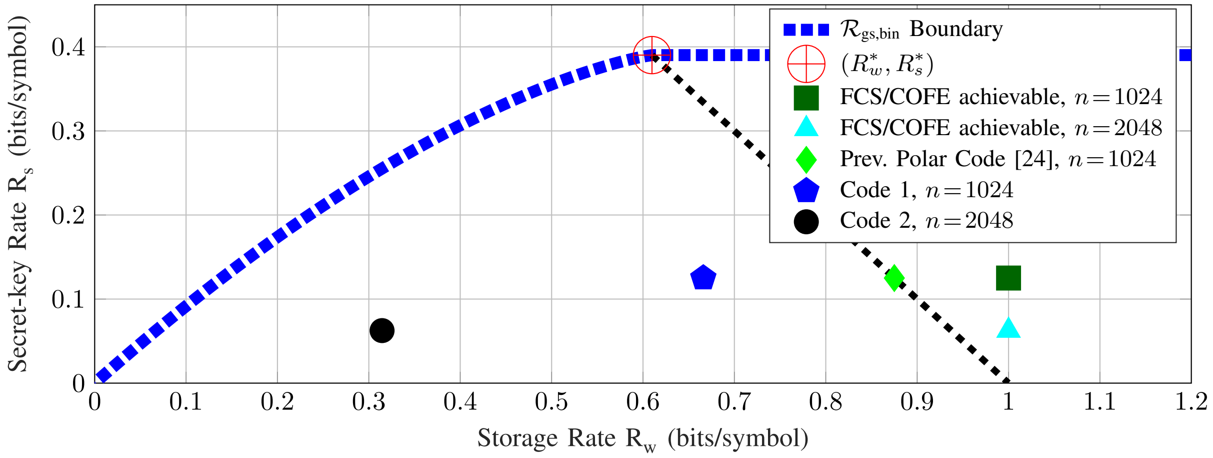

Fig. 7. Storage-key rates for the GS model with $p_A = 0.15$. The (R_w^*, R_s^*) point is the best possible point achieved by SW-coding constructions, which lies on the dashed line representing $R_w + R_s = H(X)$. The block error probability satisfies $P_B \leq 10^{-6}$ and the key length is 128 bits for all code points.

storage rate is given by its minimal value $R_w = 1 - R_{\mathcal{C}}$, then we arrive at $R_s/R_w \leq 0.375$. A similar calculation for $n = 2048$ yields $R_s/R_w \leq 0.437$. These results indicate that there are still gaps between the maximum key vs. storage rate ratios achieved by WZ-coding constructions, which might achieve higher ratios than SW-coding constructions, and the ratios achieved by codes 1 and 2. The gaps can be reduced by using, e.g., larger list sizes at the decoder, which is not desired for applications that require low hardware complexity. For other PUF applications, codes that satisfy $P_B \leq 10^{-9}$ should be designed [13], for which either laborious decoder simulations or analytical block-error probability bounds seem to be required.

VI. Conclusion

We showed that there are random codes that asymptotically achieve all points of the rate regions of the WZ problem and GS model simultaneously, i.e., these problems are functionally equivalent. Extending the functional equivalence, we argued that a first WZ-coding construction based on random linear codes is asymptotically optimal for the GS and CS models with uniform binary sources with decoder measurements through a BSC. These source and channel models are the standard models for RO PUFs and SRAM PUFs. We implemented a second WZ-coding construction with nested polar codes that achieve better rate tuples than existing methods, and one of our codes achieves a rate tuple that cannot be achieved by existing methods without time sharing. Gaps to the maximum key vs. storage rate ratios were illustrated.

Acknowledgment

O. Günlü thanks Amin Gohari and Navin Kashyap for their insightful comments, and also Matthieu Bloch for his help and useful suggestions that significantly improved this work.

Appendix A
Strong Secrecy

Theorem 6. *For the GS model (or CS model), given any $\epsilon > 0$, there exist some $n \geq 1$, an encoder, and a decoder that achieve the key-leakage-storage region $\mathcal{R}_{gs}$ (or $\mathcal{R}_{cs}$) and that satisfy the strong-secrecy constraint (19).*

We prove Theorem 6 for the GS model by using two approaches; the first proof uses output statistics of random binning (OSRB) [42] and the second uses resolvability [43] and a likelihood encoder [44]. The proofs for the CS model follow by applying a one-time pad step, as in Section II-C.

Proof Sketch 1: We first give a random binning based proof by following the steps in [42]. Fix a $P_{U|X}$ and let (U^n, X^n, Y^n) be i.i.d. according to $P_{U|X}P_X P_{Y|X}$. For each u^n, assign three random bin indices $S \in [1 : 2^{nR_s}]$, $W \in [1 : 2^{nR_w}]$, and $C \in [1 : 2^{nR_c}]$, which represent, respectively, the secret key, helper data, and randomness shared by encoder, decoder, and eavesdropper (similar to W).

We use a SW decoder to estimate $\widehat{U}^n$ from (C, W, Y^n), which satisfies (1) if (see [42, Lemma 1])

$$R_c + R_w > H(U|Y). \tag{31}$$

We further have that (S, W, C) are almost mutually independent and uniform so that (3) and (19) are satisfied if we have (see [42, Theorem 1])

$$R_s + R_w + R_c < H(U). \tag{32}$$

Similarly, the shared randomness C is almost independent of X^n, suggesting that it is almost independent of Y^n also, if

$$R_c < H(U|X). \tag{33}$$

Applying Fourier-Motzkin elimination [45, Section 12.2] to (31)-(33) and following a similar privacy-leakage rate analysis as in Theorem 3, there exists a binning with a fixed value of C and that achieves all rate tuples (R_s, R_ℓ, R_w) in the key-leakage-storage region $\mathcal{R}_{\text{gs}}$ with strong secrecy. ■

Proof Sketch 2: We next give a random coding based proof by following the steps in [44] and [46, Section 1.6.2]. Consider the allied channel coding problem where $S \in [1 : 2^{nR_s}]$ and $W \in [1 : 2^{nR_w}]$ are uniform and independent inputs of an encoder $\mathsf{Enc}(\cdot)$ with the output codeword U^n that passes through a channel $P_{X|U}$ to obtain X^n, which further passes through the channel $P_{Y|X}$ to obtain Y^n. Applying the resolvability result from [43, Theorem 1], one can simulate $X^n \sim \prod_{i=1}^n P_X(x_i)$ if

$$R_s + R_w > I(U;X). \tag{34}$$

Furthermore, one can reliably estimate $\widehat{U}^n$ from (W, Y^n) if

$$R_s < I(U;Y). \tag{35}$$

Note that this channel coding problem defines a joint probability distribution

$$\begin{aligned}&\widetilde{P}_{SWX^nY^n}(s,w,x^n,y^n)\\ &= Q_S^{\text{Unif}}(s) Q_W^{\text{Unif}}(w) \mathbb{1}\{x^n = \mathsf{Enc}(w,s)\} \prod_{i=1}^n P_{Y|X}(y_i|x_i)\end{aligned} \tag{36}$$

where Q_S^{Unif} and Q_W^{Unif} are uniform probability distributions over the sets, respectively, $[1:2^{nR_s}]$ and $[1:2^{nR_w}]$, and $\mathbb{1}\{\cdot\}$ is the indicator function.

However, for the original problem, we should invert the random coding and use a stochastic encoder according to the conditional probability distribution $\widetilde{P}_{SW|X^n}$ obtained from (36), which is induces a joint distribution

$$\begin{aligned}&P_{SWX^nY^n}(s,w,x^n,y^n)\\ &\quad= \widetilde{P}_{SW|X^n}(s,w|x^n) \prod_{i=i}^n P_X(x_i) P_{Y|X}(y_i|x_i).\end{aligned} \tag{37}$$

It follows from the above channel coding problem that (1), (3), (4), and (19) are satisfied. Following similar privacy-leakage rate analysis as in Theorem 3, there exist some $n \geq 1$, an encoder, and a decoder that achieve all rate tuples (R_s, R_ℓ, R_w) in the key-leakage-storage region $\mathcal{R}_{\text{gs}}$ with strong secrecy. ■

Remark 5. *Resolvability can be achieved by a random linear code (RLC) construction for binary input channels $P_{X|U}$ [47], so one can use the decoder for such an RLC during enrollment to obtain the bins (S,W) with strong secrecy. A binary U is optimal for the rate regions $\mathcal{R}_{gs}$ and $\mathcal{R}_{cs}$ if, e.g., $P_{Y|X}$ can be decomposed into a mixture of BSCs [10, Theorem 3].*

Remark 6. *In [48, Theorem 10], a polar code construction based on OSRB is shown to be optimal for the GS model with strong secrecy. This construction requires chains of identifier-outputs, each of which has size n, and a secret seed shared between the encoder and decoder. Furthermore, the constructions used in Proofs 1 and 2 of Theorem 6 are stochastic and such code constructions do not seem to be practical.*

Appendix B
Extensions to Hidden Sources with Multiple Decoder Measurements

The GS and CS models in Fig. 1 are extended in [10] by having the encoder measure a noisy version $\widetilde{X}^n$ of a hidden, or remote, identifier source X^n. The encoder generates or embeds a secret key and sends a public message W or W' to the decoder. The decoder observes another noisy measurement Y^n of the source and estimates the secret key. The key-leakage-storage regions that satisfy (1)-(5) for the GS and CS models with a hidden source are given in the following theorem.

Theorem 7 ([10])**.** *The key-leakage-storage regions for the GS and CS models with a hidden source, respectively, are*

$$\begin{aligned}\widetilde{\mathcal{R}}_{gs} = \bigcup_{P_{U|\widetilde{X}}} \Big\{ &(R_s, R_\ell, R_w) : 0 \leq R_s, R_\ell, R_w,\\ &R_s \leq I(U;Y),\\ &R_\ell \geq I(U;X) - I(U;Y),\\ &R_w \geq I(U;\widetilde{X}) - I(U;Y) \quad \textit{for}\\ &P_{U\widetilde{X}XY} = P_{U|\widetilde{X}} P_{\widetilde{X}|X} P_X P_{Y|X} \Big\},\end{aligned} \tag{38}$$

$$\begin{aligned}\widetilde{\mathcal{R}}_{cs} = \bigcup_{P_{U|\widetilde{X}}} \Big\{ &(R_s, R_\ell, R_w) : 0 \leq R_s, R_\ell, R_w,\\ &R_s \leq I(U;Y),\\ &R_\ell \geq I(U;X) - I(U;Y),\\ &R_w \geq I(U;\widetilde{X}) \quad \textit{for}\\ &P_{U\widetilde{X}XY} = P_{U|\widetilde{X}} P_{\widetilde{X}|X} P_X P_{Y|X} \Big\}.\end{aligned} \tag{39}$$

These regions are convex sets. The alphabet $\mathcal{U}$ of the auxiliary random variable U can be limited to have size $|\mathcal{U}| \leq |\widetilde{\mathcal{X}}| + 2$ for both regions $\widetilde{\mathcal{R}}_{gs}$ and $\widetilde{\mathcal{R}}_{cs}$.

Suppose next the encoder measures a binary hidden source X^n through a channel $P_{\widetilde{X}|X}$ such that the inverse channel $P_{X|\widetilde{X}}$ is a BSC, and the decoder measures the source through a channel $P_{Y|X}$ that is a BSC.

Theorem 8 ([10])**.** *Assume $P_{X|\widetilde{X}}$ is a BSC and $P_{Y|X}$ is a binary-input symmetric memoryless channel; see [49], [50]. The boundary points of $\widetilde{\mathcal{R}}_{gs}$ and $\widetilde{\mathcal{R}}_{cs}$ are achieved by channels $P_{\widetilde{X}|U}$ that are BSCs.*

We next argue the optimality of the first WZ-coding construction given in Section IV for the GS and CS models with the hidden source model considered above.

Theorem 9. *The WZ-coding construction given in Section IV achieves the regions $\widetilde{\mathcal{R}}_{gs}$ and $\widetilde{\mathcal{R}}_{cs}$ for a uniform source X^n, an inverse channel $P_{X|\widetilde{X}}$ that is a BSC, and a decoder-measurement channel $P_{Y|X}$ that is also a BSC.*

Proof: We first modify the WZ-coding construction in Section IV by defining the new error sequence

$$\widetilde{E}_q^n = \widetilde{X}^n \oplus \widetilde{X}_q^n \tag{40}$$

which resembles an i.i.d. sequence $\sim \text{Bern}^n(q)$ for some $q \in [0, 0.5]$ when $\widetilde{X}_q^n$ is the closest codeword of $\mathcal{C}_1$ to $\widetilde{X}^n$ in Hamming distance and $n \to \infty$. The new error sequence represents the BSCs $P_{\widetilde{X}|U}$ since the new common randomness $\widetilde{X}_q^n$ asymptotically represents the auxiliary random variable U^n. Therefore, we asymptotically obtain i.i.d. channels $P_{\widetilde{X}|U} \sim \text{BSC}(q)$. It follows from Theorem 8 that applying the code construction and taking a union of the rate tuples achieved over all $q \in [0, 0.5]$, we can achieve the boundary points of $\widetilde{\mathcal{R}}_{\text{gs}}$ and $\widetilde{\mathcal{R}}_{\text{cs}}$. ■

Remark 7. *Applying additional information reconciliation and privacy amplification steps to multiple identifier blocks, as in Remark 1, provides strong secrecy also for hidden sources. Alternatively, random binning and random coding based approaches can be applied, as in Theorem 6, to show that there exist code constructions that provide strong secrecy for the GS and CS models with a hidden source.*

REFERENCES

[1] O. Günlü, O. İşcan, and G. Kramer, "Reliable secret key generation from physical unclonable functions under varying environmental conditions," in *IEEE Int. Workshop Inf. Forensics Security*, Rome, Italy, Nov. 2015, pp. 1–6.

[2] 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.

[3] B. Gassend, "Physical random functions," Master's thesis, M.I.T., Cambridge, MA, Jan. 2003.

[4] R. Pappu, "Physical one-way functions," Ph.D. dissertation, M.I.T., Cambridge, MA, Oct. 2001.

[5] 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, July 1993.

[6] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 2733–742, May 1993.

[7] 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.

[8] 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.

[9] M. Koide and H. Yamamoto, "Coding theorems for biometric systems," in *IEEE Int. Symp. Inf. Theory*, Austin, TX, June 2010, pp. 2647–2651.

[10] 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.

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

[12] O. Günlü and O. İşcan, "DCT based ring oscillator physical unclonable functions," in *IEEE Int. Conf. Acoustics Speech Sign. Process.*, Florence, Italy, May 2014, pp. 8198–8201.

[13] O. Günlü, T. Kernetzky, O. İşcan, V. Sidorenko, G. Kramer, and R. F. Schaefer, "Secure and reliable key agreement with physical unclonable functions," *Entropy*, vol. 20, no. 5, May 2018.

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

[15] 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.

[16] 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.

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

[18] 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.

[19] 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. 8, pp. 752–754, Aug. 2010.

[20] O. O. Koyluoglu and H. El Gamal, "Polar coding for secure transmission and key agreement," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 5, pp. 1472–1483, Oct. 2012.

[21] 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.

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

[23] 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 *IEEE Global Commun. Conf.*, Singapore, Dec. 2017, pp. 1–6.

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

[25] A. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Trans. Inf. Theory*, vol. 22, no. 1, pp. 1–10, Jan. 1976.

[26] M. Bloch and J. Barros, *Physical-layer Security*. Cambridge, U.K.: Cambridge Uni. Press, 2011.

[27] A. Gupta and S. Verdú, "Operational duality between Gelfand-Pinsker and Wyner-Ziv coding," in *IEEE Int. Symp. Inf. Theory*, Austin, TX, June 2010, pp. 530–534.

[28] R. Maes, P. Tuyls, and I. Verbauwhede, "A soft decision helper data algorithm for SRAM PUFs," in *IEEE Int. Symp. Inf. Theory*, Seoul, Korea, June-July 2009, pp. 2101–2105.

[29] S. Shamai, S. Verdú, and R. Zamir, "Systematic lossy source/channel coding," *IEEE Trans. Inf. Theory*, vol. 44, no. 2, pp. 564–579, Mar. 1998.

[30] A. Orlitsky and J. R. Roche, "Coding for computing," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 903–917, Mar. 2001.

[31] A. E. Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge, U.K.: Cambridge Uni. Press, 2011.

[32] 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.

[33] R. Maes, A. V. Herrewege, and I. Verbauwhede, "PUFKY: A fully functional PUF-based cryptographic key generator," in *Int. Workshop Cryp. Hardware Embedded Sys.*, Leuven, Belgium, Sep. 2012, pp. 302–319.

[34] V. Guruswami, J. Hastad, and S. Kopparty, "On the list-decodability of random linear codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 718–725, Feb. 2011.

[35] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Int. Conf. Theory Appl. Cryptographic Techn.*, Bruges, Belgium, May 2000, pp. 351–368.

[36] A. D. Wyner and J. Ziv, "A theorem on the entropy of certain binary sequences and applications: Part I," *IEEE Trans. Inf. Theory*, vol. 19, no. 6, pp. 769–772, Nov. 1973.

[37] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, July 2009.

[38] S. B. Korada and R. L. Urbanke, "Polar codes are optimal for lossy source coding," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1751–1768, Apr. 2010.

[39] C. Bösch, J. Guajardo, A.-R. Sadeghi, J. Shokrollahi, and P. Tuyls, "Efficient helper data key extractor on FPGAs," Washington, D.C., Aug. 2008, pp. 181–197.

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

[41] R. G. Gallager, *Information theory and reliable communication*. New York, Chichester, Brisbane, Toronto, Singapore: John Wiley & Sons Inc., 1968.

[42] 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.

[43] J. Hou and G. Kramer, "Informational divergence approximations to product distributions," in *Canadian Workshop Inf. Theory*, Toronto, ON, Canada, June 2013, pp. 76–81.

[44] E. C. Song, P. Cuff, and H. V. Poor, "The likelihood encoder for lossy compression," *IEEE Trans. Inf. Theory*, vol. 62, no. 4, pp. 1836–1849, Apr. 2016.

[45] A. Schrijver, *Theory of linear and integer programming*. Chichester, West Sussex, England: John Wiley & Sons Ltd, 1998.

[46] M. Bloch, *Lecture Notes in Information-Theoretic Security*. Atlanta, GA: Georgia Inst. Technol., July 2018.

[47] R. A. Amjad and G. Kramer, "Channel resolvability codes based on concatenation and sparse linear encoding," in *IEEE Int. Symp. Inf. Theory*, Hong Kong, China, June 2015, pp. 2111–2115.

[48] 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.

[49] R. Gallager, "Low-density parity-check codes," *IRE Trans. Inf. Theory*, vol. 8, no. 1, pp. 21–28, Jan. 1962.

[50] N. Chayat and S. Shamai, "Extension of an entropy property for binary input memoryless symmetric channels," *IEEE Trans. Inf. Theory*, vol. 35, no. 5, pp. 1077–1079, Sep. 1989.