entropy

MDPI

Review

The Odyssey of Entropy: Cryptography

Behrouz Zolfaghari [1], Khodakhast Bibak [2,*] and Takeshi Koshiba [3]

[1] Cyber Science Lab, School of Computer Science, University of Guelph, Guelph, ON N1G 2W1, Canada; behrouz@cybersciencelab.org
[2] Department of Computer Science and Software Engineering, Miami University, Oxford, OH 45056, USA
[3] Department of Mathematics, Faculty of Education and Integrated Arts and Sciences, Waseda University, Tokyo 169-8050, Japan; tkoshiba@waseda.jp
* Correspondence: bibakk@miamioh.edu

Abstract: After being introduced by Shannon as a measure of disorder and unavailable information, the notion of entropy has found its applications in a broad range of scientific disciplines. In this paper, we present a systematic review on the applications of entropy and related information-theoretical concepts in the design, implementation and evaluation of cryptographic schemes, algorithms, devices and systems. Moreover, we study existing trends, and establish a roadmap for future research in these areas.

Keywords: entropy; cryptography; security; information theory; trend analysis

check for updates

Citation: Zolfaghari, B.; Bibak, K.; Koshiba, T. The Odyssey of Entropy: Cryptography. *Entropy* **2022**, *24*, 266. https://doi.org/10.3390/e24020266

Academic Editor: Raúl Alcaraz

Received: 6 January 2022
Accepted: 1 February 2022
Published: 12 February 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

1. Introduction

In thermodynamics and statistical mechanics, the internal disorder of a system in a given macroscopic state is stated as a logarithmic function of the number Ω of possible microscopic system configurations as follows,

$$S = k_B \ln \Omega. \quad (1)$$

In Equation (1), S is referred to as the *entropy* of the system, and k_B is called the *Boltzmann constant*. Under the equiprobability assumption, it is obvious that Ω is an exponential function of the number of particles that can randomly move within the system. In other words, $\ln \Omega$ is proportional to the number of random particles inside the system, which is a measure of randomness. The Boltzmann constant converts this number to the total uncontrolled kinetic energy of the random particles. On the other hand, the number of randomly moving particles inside a system can be considered to be representative of the amount of information that is needed to define the exact state of a system given its macroscopic state.

According to the above discussions, the thermodynamic concept of entropy connects uncontrolled energy inside a system to disorder, randomness and unavailable information. However, the term entropy has found its applications with different notions in a variety of scientific disciplines, ranging from cosmology and meteorology to economics, biology, medicine and sociology. In particular, Shannon paved the way ahead of this concept via information theory into communication theory and related fields, such as cryptography.

Information entropy (information theoretic entropy) was first introduced by Shannon in 1948 [1,2]. It can be assigned to a random variable as the average level of *self-information* in each possible event of the variable, which shows the inherent level of uncertainty or surprise in the event. In Shannon's theory, for a random variable X, the self-information I_X of an event x_i with probability $P_X(x_i)$ is defined as

$$I_X(x_i) = -\log_b P_X(x_i). \quad (2)$$

In Equation (2), the base b determines the unit of information. In particular, if $b = 2$, $I_X(x_i)$ is calculated in bits. Moreover, the entropy H of X is defined as

$$H(X) = E[I_X] = \sum_i P_X(x_i) I_X(x_i) = -\sum_i P_X(x_i) \log_b P_X(x_i). \tag{3}$$

In Equation (3), $E[I_X]$ is the mathematical expectation of I_X. Von Neumann suggested the name "entropy" for the concept introduced by Shannon because of its similarity to thermodynamic entropy in notion as well as related equations. In fact, information-theoretic entropy is used as a measure of randomness, disorder and unavailable information, like the case of thermodynamic entropy. Shannon discussed the role of entropy and related concepts in the modeling of cryptosystems. Further, he introduced the notion of a perfectly secure cryptosystem on the basis of entropy.

Some different notions of information entropy were introduced by other researchers before [3] and after [4] Shannon. In the rest of this paper, the term "entropy" refers to information-theoretic entropy, unless we clearly specify thermodynamic entropy. Entropy has found its applications in a variety of scientific and technological areas [5–7]. Many research reports have addressed the role of entropy in the design, implementation and analysis of cryptosystems as well as cryptographic applications and environments. Several survey reports have reviewed the applications of entropy in a variety of areas, such as economics [8], image processing [9], discrete mathematics [10], signal processing [11], etc.

There are some research reports that establish connections between the notion of entropy and elements or requirements of cryptosystems. For example, the role of entropy in the calculation of the lower bounds on key size as well as the relation between entropy and perfect secrecy were studied by Maurer [12]. Moreover, a quick introduction to some entropy-related notions in cryptosystems was presented by Reyzby [13]. The relation between entropy and true randomness as well as key unpredictability was studied by Vassilev and Hall [14]. However, to the best of our knowledge, there is no up-to-date, systematic and comprehensive review on the applications of entropy in cryptography and related areas. Thus, a systematic and comprehensive survey in this area can help researchers by shedding light on hot topics as well as the ones that need more research focus.

In this paper, we review and classify the roles and applications of entropy and related concepts in different branches of cryptography. We analyze the existing research trends in this area, and establish a future roadmap for further research in this area. In this survey, we divide the papers into those focused on the applications of entropy in encryption and those focused on other related cryptographic concepts, such as obfuscation, watermarking, etc. We classify encryption-related research works on the basis of the phases in a typical life cycle of a cryptosystem, namely, design, implementation, evaluation and application as shown in Figure 1.

The rest of this paper is organized as follows. Some entropy measures and related concepts are studied in Section 2. Section 3 studies the applications of entropy in encryption, and Section 4 reviews the applications of entropy in other cryptographic areas. Section 5 analyses the current trends, and presents a roadmap for future research on the applications of entropy in cryptography.

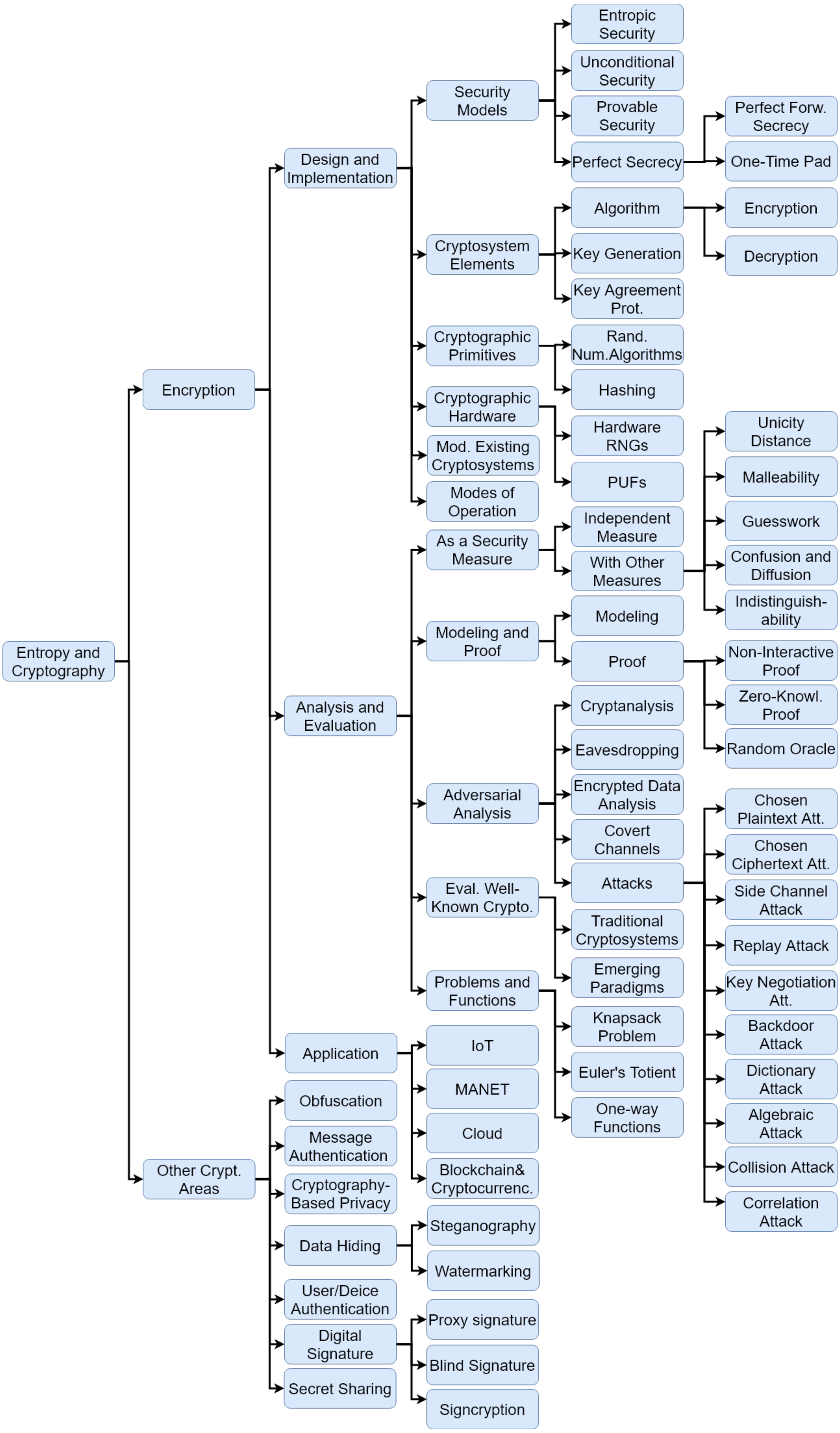

Figure 1. The classification of cryptographic concepts with entropy-related aspects.

2. Entropy Measures and Related Concepts

In the next sections of this paper, we review the roles of different entropy measures and related concepts in research on cryptography. Some of the most important measures and concepts are briefly introduced in this section.

2.1. Entropy Measures

In addition to Shannon entropy, some other measures for entropy have been introduced by different researchers. For example, for a random variable X with events $x_i = i$ ($i \in \{1, 2, \ldots, n\}$) of probability $P_X(x_i)$, Rényi entropy $H_\alpha^{(R)}$ of order $\alpha \in \mathbb{R}^+ \setminus \{1\}$ is defined as [4],

$$H_\alpha^{(R)}(X) = \frac{1}{1-\alpha} \log_2 \sum_{i=1}^{n} (P_X(x_i))^\alpha. \tag{4}$$

It is well known that $\lim_{\alpha \to 1} H_\alpha^{(R)}(X) = H(X)$, where $H(X)$ is the Shannon entropy given by Equation (3). Moreover, $H_0^{(R)}(X) = H^{(H)}(X)$, where $H^{(H)}(X)$ is the Hartley entropy (sometimes called max entropy) defined as

$$H^{(H)}(X) = \max_\alpha H_\alpha^{(R)}(X) \log_2 n = \log_2 |X|. \tag{5}$$

Collision entropy, defined below, is used by many researchers in cryptography,

$$H^{(C)}(X) = H_2^{(R)}(X) = -\log_2 \sum_{i=1}^{n} (P_X(x_i))^2. \tag{6}$$

The security of cryptosystems is measured by the expectation of certain function, which is called *perfect expectation* (in the ideal model, where perfect randomness is available) or *weak expectation* (in the real model, where perfect randomness is not available). Yao and Li [15] used Rényi entropy to derive some results and inequalities, which show that weak expectation is not much worse than perfect expectation. For a cryptosystem $\mathcal{C}$, let resource $\mathcal{R}$ be a tuple containing the values of all efficiency measures, such as running time, circuit size, the number of oracle queries, etc. For a secret key $k \in \{0,1\}^m$, let $f(k)$ be the advantage of adversary $\mathcal{A}$ conditioned on k. In addition, let U_m be the uniform distribution over $\{0,1\}^m$. Then $\mathcal{C}$ is $(\mathcal{R}, \varepsilon)$-secure if for any adversary $\mathcal{A}$ with resource $\mathcal{R}$, the expectation of $f(U_m)$ (called *perfect expectation*) is upper bounded by ε [16]. When the key is sampled from some non-uniform distribution W, the resulting security is the expectation of $f(W)$ (called *weak expectation,Weak-Expect-Conf001*). The result of Yao and Li [15] was motivated by the fact that while cryptographic schemes ideally assume highly random secret keys, true random number generation is so costly and sometimes not feasible in the real world, which causes weak expectation to be substituted for the ideal perfect expectation. As another example, Rényi entropy was used by Boztas [17] in order to analyze the success parameters of guess attacks.

The relation between the results of evaluating a cryptosystem using Shannon entropy and collision entropy was studied by Skorski [18], and the worst possible collision entropy for random variables with a given Shannon entropy was calculated.

Another well-known entropy measure is *min entropy*, $H^{(M)}$, which is calculated as

$$H^{(M)}(X) = \min_\alpha H_\alpha^{(R)}(X) = \lim_{\alpha \to \infty} H_\alpha^{(R)}(X) = -\log_2 \left(\max_i P_X(x_i) \right). \tag{7}$$

Min entropy has been used in studies related to cryptographic primitives, such as hash functions [19,20], in developing cryptographic hardware such as PUFs (physically unclonable functions) [21], and in authentication [22,23] and secret sharing [24].

For a probability distribution $P = \{p_1, p_2, \ldots, p_n\}$ and $R \in \mathbb{R}^+ \setminus \{1\}$, *R-norm entropy* $H_n^{(R)}(P)$ is defined as [25],

$$H_n^{(R)}(P) = \frac{R}{1-R}\left(1 - \left(\sum_{i=1}^{n}(p_i)^R\right)^{\frac{1}{R}}\right). \tag{8}$$

R-norm entropy is used in fuzzy probability spaces and related areas [26]. Kumar and Choudhary [27] considered Shannon entropy as a special case of R-norm entropy when parameter R in Equation (8) approaches unity. They defined conditional R-norm entropy as well as R-norm mutual information, and used the defined concepts to generalize the notion of random cipher introduced by Shannon.

For a continuous random variable X with a probability density function f whose support is set χ, the *differential entropy* $h(X)$ is defined as follows [1,2]:

$$h(X) = -\int_{\chi} f(x)\log_2 f(x). \tag{9}$$

Differential entropy has been suggested by some researchers as a measure of security. For example, it was used by Biryukova et al. [28] for cryptanalysis of the well-known IDEA block cipher.

2.2. Related Concepts

In addition to entropy measures, there are some related concepts that have played significant roles in research on cryptography. As an example, we can mention relative entropy, conditional entropy and mutual information; the latter is obtained using conditional entropy. For discrete probability distributions P and Q defined on the probability space $\mathcal{S}$, the *relative entropy* (i.e., the *Kullback–Leibler (KL) divergence*) from Q to P is defined as [29]

$$D_{\mathrm{KL}}(P \parallel Q) = \sum_{x\in\mathcal{S}} P(x)\log\left(\frac{P(x)}{Q(x)}\right). \tag{10}$$

Consider two random variables X and Y with outcomes x_i and y_i. The *conditional entropy* $H(Y|X)$ is defined as

$$\begin{aligned} H(Y|X) & \\ = & \quad -\sum_{x_i}\sum_{y_i}(P(x_i,y_i)\log_2 P(y_i|x_i)) \qquad (11)\\ = & \quad -\sum_{x_i}P_X(x_i)\sum_{y_i}(P(y_i|x_i)\log_2 P(y_i|x_i)). \qquad (12)\end{aligned}$$

$H(Y|X)$ represents the amount of uncertainty in Y given the value of X. *Mutual information* between X and Y is calculated as

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X). \tag{13}$$

$I(X;Y)$ quantifies the amount of information (in bits) obtained about X via observing Y or vice versa. Moreover, the *joint entropy* $H(X,Y)$ is calculated as

$$H(X,Y) = I(X;Y) + H(X|Y) + H(Y|X). \tag{14}$$

Moreover, for a distribution P_{XY} and $0 < \varepsilon < 1$, the *inf-spectral entropy* $H_s^{\varepsilon}(P)$ is defined as

$$H_s^{\varepsilon}(P) = \sup\{r \mid P_{XY}\{-\log P_{XY}(x,y) \le r\} \le \varepsilon\}. \tag{15}$$

A sequence of jointly distributed random variables $(X_1, X_2, \ldots, X_m)$ has *next-block pseudoentropy* of at least e if and only if there exist random variables $(Y_1, Y_2, \ldots, Y_m)$ jointly distributed with $(X_1, X_2, \ldots, X_m)$ such that, for every $i \in \{1, 2, \ldots, m\}$, $(X_1, \ldots, X_{i-1}, X_i)$ is computationally indistinguishable from $(X_1, \ldots, X_{i-1}, Y_i)$ and

$$\sum_{i=1}^{m} H(Y_i \mid X_1, X_2, \ldots, X_{i-1}) \geq e.$$

Further, the *conditional Rényi entropy* of order α is calculated as

$$H_\alpha^{(R)}(X|Y) = \frac{1}{1-\alpha} \max_{y_i} \left(\log_2 \sum_{x_i} (P(x_i|y_i))^\alpha \right). \tag{16}$$

Mutual information has played significant roles in several research works in the area of cryptology. For example, Rastegin [30] used it in quantum cryptography in order to measure the amount of information gained by an eavesdropper in each individual attack session. As another example, one can mention the research reported by Gierlichs et al. [31], in which mutual information was used for modeling the information leaked from an embedded device containing a secret key during a side channel attack. Conditional Rényi entropy was used by Iwamoto and Shikata [32] in developing generalizations for Shannon's secure encryption theorem.

In addition to statistical distributions, entropy can be calculated over different structures, such as graphs. For example, for an undirected graph $G(V, E)$, the *graph entropy* is defined as [33]

$$H(G) = \min_{X,Y} I(X;Y), \tag{17}$$

where X is uniformly distributed over V, and Y ranges over $I_S(G)$ defined as

$$I_S(G) = \{S | S \subset G, X \in S, \forall s_1, s_2 \in S : (s_1, s_1) \notin E\}. \tag{18}$$

Figure 2 shows the entropy measures and related concepts that have been used by researchers in the area of cryptography.

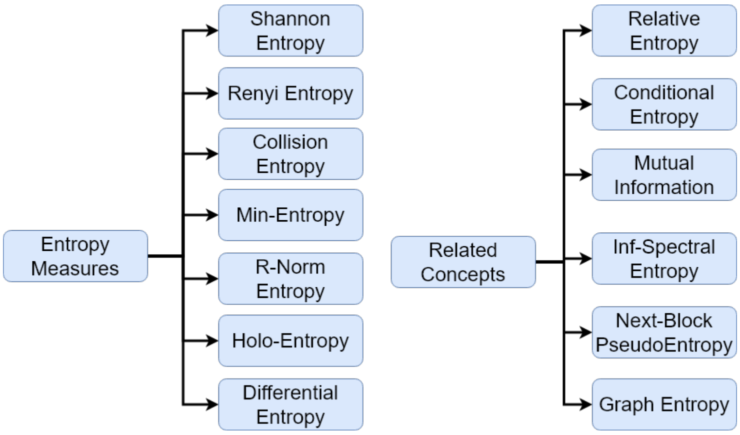

Figure 2. Entropy measures and related concepts used in cryptography.

3. Entropy and Encryption

This section reviews the role of entropy in research on the design, implementation, evaluation and applications of encryption modules and systems.

3.1. Modeling, Design and Implementation

In this section, we first study entropy-based security models. Afterwards, we review research works focusing on the role of entropy in the design and implementation of cryptosystem elements, cryptographic primitives and cryptographic hardware. In the next step, we study some entropy-aware modifications to existing cryptosystems. Lastly, we discuss the role of entropy in research on modes of operation, which are considered important implementation aspects of cryptosystems.

3.1.1. Security Models Related to Entropy

In the following, we discuss security models that can be analyzed using entropy, and we review some related research.

- **Entropic Security:** Entropic security is a relaxed version of semantic security. In *semantic security*, only negligible information about the plaintext can be extractable (in any feasible way) from the ciphertext. More specifically, suppose that a probabilistic polynomial time algorithm (PPTA) knows the ciphertext c generated from a message m (regardless of the related distribution) and the length of m. The algorithm should still be unable to extract any partial information regarding m with a probability that is non-negligibly larger than all other PPTAs that know only the length of m (and not c). In *entropic security*, the cryptosystem needs to guarantee that the entropy of the message space is high from the point of view of the adversary [34]. A few research reports have worked on entropic security for high-entropy plaintexts [35]. Moreover, this model was used in honey encryption [36]. In honey encryption, decrypting the ciphertext using an incorrect key (guessed by the adversary) leads to a meaningful, but incorrect plaintext, which fools the adversary.
- **Unconditional Security:** A cryptosystem is said to have *unconditional security* (also called *information-theoretic security*) if the system is secure against adversaries with unlimited computational power, resources, memory space, and time. Information-theoretic methods and techniques have been utilized in studying unconditionally secure cryptosystems [37]. Some researchers have focused on this security model. For example, Renner and Wolf [38] investigated the possibility of asymmetric unconditional security, which corresponds to asymmetric-key cryptography in the computational security model.
- **Provable Security:** Some researchers have used entropy in provable security. For example, Kim et al. [39] argued that the assumption of uniform key distribution, which is made in traditional provable security, is far from reality. They modeled realistic key distributions by entropy sources. As another example, it was shown by Ruana [40] that the explicit authenticated key agreement protocol presented by Zheng [41] is vulnerable to impersonation attack due to the low entropy of the keys.
- **Perfect Secrecy:** Perfect secrecy (defined by Shannon) guarantees that $H(P|C) = H(P)$, where P is the set of possible values for the plaintext and C denotes the set of possible values for the ciphertext. Put alternatively, a cryptosystem is perfectly secure if the adversary is unable to make any guesses about the plaintext, even in the case of full access to the channel (and, consequently, to the ciphertext). Several research works have focused on perfect secrecy. Gersho [42] argued that message quality degradation is inevitable for a perfectly secure cryptosystem that encrypts an analog message using a digital key with a finite size. He designed a perfectly secure analog signal encryption scheme that keeps the bandwidth of the encrypted signal from growing above that of the original analog signal without altering the key size or increasing the quality degradation incurred on the decrypted signal. The notion of "finite-state encryptability" for an individual plaintext sequence was introduced by Merhav [43] as the minimum asymptotic key rate required to guarantee perfect secrecy for that sequence. He demonstrated that the finite-state encryptability is equal to the finite-state compressibility (defined by Ziv and Lempel [44]) for every individual sequence. Perfect secrecy in radio signal encryption using DFT (discrete Fourier transform) was

studied by Bi et al. [45]. They proved perfect secrecy to be asymptotically achievable for any baseband signaling method, provided that the signal block length approaches infinity. It is well known that the only real-world implementation of perfect secrecy (in its pure notion) is one-time pad (OTP), wherein the key is at least as long as the plaintext and needs to be updated with each new plaintext. However, some variants of perfect secrecy have received research focus. In the following, we review some well-studied variants of perfect secrecy as well as some related research works.

- **Perfect Forward Secrecy:**
  Perfect forward secrecy depends on frequent changes in the encryption/decryption key (e.g., with each call or each message in a conversation, or each web page reload) in order to prevent the cryptosystem from being broken if a key is compromised. Several researchers have proposed encryption systems providing perfect forward secrecy to be used in different communication systems. For example, two email protocols with perfect forward secrecy were proposed by Sun et al. [46]. However, some flaws in the reasoning presented by Sun et al. [46] were reported by Dent [47], and two new robust email protocols with guaranteed perfect forward secrecy were introduced by Ziv and Lempel [48]. Later on, a method for cryptanalysis of the protocols proposed by Ziv and Lempel [48] was presented by Yoon and Yoo [49].
  In recent years, perfect forward secrecy has been considered in several other areas. For example, a lightweight transport layer security protocol with perfect secrecy was proposed by Pengkun et al. [50]. As another example, perfect secrecy is guaranteed to be provided by a high-performance key agreement protocol proposed by Yang et al. [51].
- **One-Time Pad (OTP):**
  OTP is the only perfectly secure cryptographic scheme used in real-world applications. Although some researchers believe that OTP is more of a key safeguarding scheme than a cryptosystem [52], a vast number of research works have considered OTP as (part of) the security solution in a broad spectrum of applications. The feasibility of perfectly secure cryptography using imperfect random sources was studied by Dodis and Spencer [53]. Liu et al. [54] proposed an OTP cryptosystem in which the receiver does not need the OTP to decrypt the ciphertext, while the OTP fully affects the plaintext from the adversaries point of view. The application of OTP in scenarios where the receiver may not be trustworthy was studied by Matt and Maurer [55].
  An OTP-based cryptosystem was proposed by Büsching and Wolf [56] for BANs (body area networks), wherein messages are short, and large volumes of NVM (non-volatile memory) are available. This cryptosystem stores pre-calculated OTPs in the NVM for future use. Moreover, OTPs have been used in a spectrum of environments, such as multi-user one-hop wireless networks [57], IMDs (implantable medical devices) [58], UAVs (ynmanned aerial vehicles) [59], medical images [60], mobile instant messaging [61], coded networks [62] and credit cards [63]. OTP has been also used in quantum computing, especially in QKD (quantum key distribution) [64–70].

3.1.2. Cryptosystem Elements

The security of a cryptosystem depends on the security of three main elements: the encryption and decryption algorithms, the key generation and management module, and the key agreement or exchange protocol [71]. In the following, we review the role of entropy and related concepts in the design and implementation of each of the aforementioned elements.

- **Encryption and Decryption Algorithms:** Entropy has played a role in several research reports focusing on the design of encryption and decryption algorithms. Some of these research works are discussed below.

  - **Encryption:**
    The role of image block entropy in image encryption was studied by researchers [72] just like the case of image steganography (reviewed in Section 4.3.1). A multimedia encryption scheme based on entropy coding with low computational overhead was proposed by Xie and Kuo [73]. A method for encrypting entropy-coded compressed video streams without the need for decoding was introduced by Almasalha et al. [74]. Moreover, the encryption of entropy-coded videos was studied in some other research works. To mention a few, one may refer to Refs. [75–78]. The impact of key entropy on the security of an image encryption scheme was studied by Ye et al. [79]. Külekci [80] investigated the security of high-entropy volumes, where the most typical sources are entropy-encoded multimedia files or compressed text sequences. Min entropy was used by Saeb [81] to reduce the size of the key search space of an encryption scheme to a value lower than that of a brute-force or birthday attack. A chaotic encryption scheme for low-entropy images was proposed by Yavuz et al. [82]. This method uses confusion and diffusion techniques to make it difficult for the adversary to perform statistical analysis on adjacent pixels, which are likely to have close values.
  - **Decryption:**
    There are few works focusing on the security of the encryption algorithm. For example, the multiple decryption problem was introduced by Domaszewicz and Vaishampayan [83] as a generalization of the problem of source coding subject to a fidelity criterion. They used entropy to evaluate the security of a multiple-channel system in this scenario.

- **Key Generation and Management Module:** Several research works have focused on the role of entropy in key generation and management. Some of these works are briefly reviewed in the following.
  The entropy of the key has been of interest to researchers as a measure of security for decades [84]. Golic and Baltatu [85] used Shannon entropy analysis to evaluate the security of their proposed biometric key generation scheme. Wang et al. [86] tried to alleviate the quantization discrepancy problem in quantization-based key generation methods using an ECQS (entropy-constrained-like quantization scheme).
  It was highlighted by Shikata [87] that the existing bounds on the key entropy for retaining information-theoretical security are not tight enough. The reason is that existing random number generators do not create truly random sequences. More realistic bounds for the key entropy were derived in this research. "Personal Entropy" was introduced by Ellison et al. [88] as a means for remembering personal passphrases based on which secret keys are generated. Personal entropy is created via asking the user several personal questions.
- **Key Agreement and Exchange Protocol:** There are a few research works focusing on the applications of entropy in key exchange protocols. Among these works, we can refer to a framework designed by Luo et al. [89] for fingerprinting key exchange protocols using their impact on high-entropy data blocks. Another example is the key transmission method presented by Boyer and Delpha [90] for MISO (multiple-input single-output) flat-fading channels. This method tries to increase relative entropy using an artificial noise in order to minimize the BER (bit error rate) for the key receiver, while keeping it close to unity (maximum) for the eavesdropper.

3.1.3. Cryptographic Primitives

Several researchers have used entropy in their research works focusing on the design and implementation of cryptographic primitives, such as random number generations and hashing. Some of these works are studied below.

- **Random Number Generation Algorithm:** Entropy has been considered by researchers as a measure for randomness for decades [91]. One well-known issue with pseudo-random number generators is that the entropy of their output depends on the entropy of the seed. This issue was reported by Kim et al. [92] to exist in entropy sources of random number generators used in real-world cryptographic protocols, such as SSL (secure socket layer). Several research works have proposed methods for increasing the entropy of the seed via harvesting entropy from execution times of programs [93] or chaotic functions [94]. In recent years, entropy has been used as an objective for improving different chaos-based random number generators [95,96] as well as randomness tests for image encryption [97,98]. The criticality of entropy in research on true random number generators is due to the fact that their susceptibility to process variations as well as intrusion attacks, degrades the generated entropy. This makes it necessary to include an on-the-fly mechanism for the detection and correction of bias variations [99].

- **Hashing Functions and Algorithms:** A hash function with maximized conditional entropy was used by Lin et al. [100] as part of the solution to the ANN (approximate nearest neighbor) problem. Later on, Wang et al. [101] suggested LSH (locality sensitive hashing) as a promising solution to the ANN problem. However, they argued that in LSH, points are often mapped to poor distributions. They proposed a number of novel hash map functions based on entropy to alleviate this problem. Maximum-entropy hash functions were used in some other applications, such as packet classification [102]. The role of graph entropy in perfect hashing was studied by Newman et al. [103]. Later on, a graph entropy bound was calculated by Arikan [104] for the size of perfect hash function families. A fuzzy hash method based on quantum entropy distribution was used to construct a biometric authentication algorithm by Cao and Song [105]. Entropy measurement and improvement techniques were used by Zhang et al. [106] along with perceptual hashing for key frame extraction in content-based video retrieval. Moreover, entropy reduction on layout data combined with lossless compression and cryptographic hashing was used by Koranne et al. [107] to manage IP (intellectual property) via tracking geometrical layout from design through manufacturing and into production. Inaccessible entropy was used in the design of one-way hash functions by Haitner et al. [108]. A generator G is said to have inaccessible entropy if the total accessible entropy (calculated over all blocks blocks) is considerably smaller than the real entropy of G's output. The possibility of designing a hash function with a hash-bit-rate equal to the conditional entropy was investigated by Li et al. [109].

3.1.4. Cryptographic Hardware

Entropy measures and related concepts have played important roles in the design and implementation of cryptographic hardware, such as hardware random number generators and physically unclonable functions. In the following, we study these roles.

- **Hardware Random Number Generators:** The metal oxide semi-conductor (CMOS) implementation of full-entropy true random number generators was investigated by Mathew et al. [110,110]. CMOS is a fabrication process used in integrated circuits with high noise immunity and low static power consumption. Cicek et al. [111] proposed architectures for the CMOS implementation of true random number generators with dual entropy cores. In these implementations, different entropy sources, such as MRAMs [112], beta radioisotopes [113], the jitter of event propagation in self-timed rings [114] or thermal phenomena [115], were examined by researchers. Other hardware implementations depend on field programmable gate arrays (FPGAs) [116,117] or system-on-chip (SoC) devices [115]. An FPGA is a programmable semiconductor device consisting of a matrix of configurable logic blocks connected via networks of bistate connections. Furthermore, an SoC is a single integrated circuit containing (almost) all components of a computer such as a central processing unit, secondary storage, input/output ports, memory, etc. In the hardware implementation of true random number generators, objectives, such as power consumption [118], were considered by researchers.

- **Physically Unclonable Functions (PUFs):** In recent years, it was shown that some unclonable properties in some elements such as devices, waves or materials can vary randomly in different experiments or uniquely between similar elements. PUFs use these properties to create random and/or unique signals. They are used in cryptographic primitives, such as random number generation as well as message/device authentication. PUFs have been of interest to researchers in recent years [119,120]. The architecture of a PUF is shown in Figure 3.

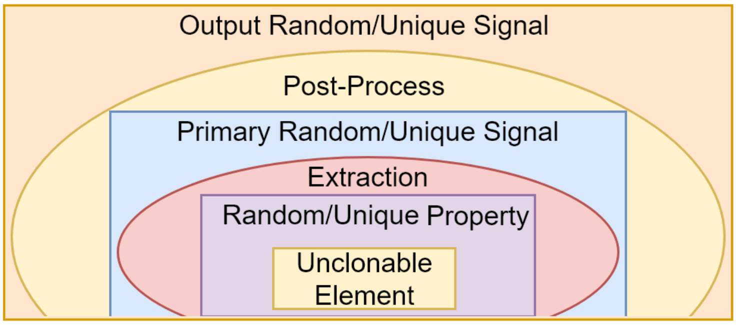

Figure 3. PUF architecture.

As shown in Figure 3, the core of a PUF is an unclonable element to which we simply refer as the element for short. The element can be a material, such as paper, carbon nanotube, etc. It can even be a wave, such as an optical or magnetic wave. However, most commonly, it is a device. It varies from sensors to microprocessors. The element along with its unique/random property (property for short) build the source of uniqueness/randomness (source for short). The property varies from eye-opening oscillation in humans to the geometry of the substrate in CMOS devices. As shown in Figure 3, an extraction circuit extracts this randomness, and (possibly) some post-processing improves the performance of the resulting signal to create the final output signal.

Entropy analysis has appeared in several research reports focusing on the implementation of PUFs. For example, a connection between the min entropy and the randomness of PUFs was established by Gu et al. [121]. Gu et al. [122] and Schaub et al. [123] used entropy to evaluate the randomness of PUFs. Similarly, Koyily et al. [124] used entropy to evaluate the non-linearity of PUFS. Upper bounds on the entropy of some types of PUFs were calculated by Delvaux et al. [21]. Some bounds on the conditional min entropy of PUFs were presented by Wilde et al. [125]. Liu et al. [119] argued that some previously calculated upper/lower bounds on the entropy of PUFs are too loose or too conservative. They proposed a method for calculating a new bound via predicting the expectation of the point where min entropy bounds obtained from different experiments will converge. The loss of entropy in key generation using PUFs was studied by Koeberl et al. [126]. Other research works used PUFs as pumps of entropy [120].

3.1.5. Modification and Use of Existing Cryptosystems

Some researchers have modified existing cryptosystems and used entropy (and related concepts) in part of their research. For example, a modified variant of the block encryption algorithm *Blowfish* was designed by Nagpal et al. [127] in order to be used in IoT (Internet of Things) platforms. The security of this variant was evaluated using entropy. ElGamal elliptic curves were used to improve the TLS (transport layer security) protocol in terms of entropy [128]. A chaotic image scrambling method based on DES was proposed by Zhang et al. [129] that uses image block entropy to select blocks for scrambling.

Entropy analysis was used in the design of an image encryption system aiming at the reduction of correlation between image blocks [130]. Moreover, entropy analysis has played roles in the design of elliptic curve point addition algorithms [131] and unconditionally secure encrypted authentication schemes [132].

3.2. Analysis and Evaluation

In this subsection, we first discuss entropy as a security measure. Afterwards, we review the research reports that have used entropy in the analysis of cryptographic systems, schemes, mechanisms, etc.

3.2.1. Entropy as a Security Measure

Some researchers used entropy as an independent measure, and others considered it in relation with other security measures. Some effort was spent on the formal assessment of the role of entropy in the evaluation of a cryptosystem [133]. Moreover, some research reports focused on developing methods for measuring the entropy of a cryptosystem [134]. In the following, we review the related research works.

- **As an Independent Measure:** Entropy is a widely used security measure. Among the research works that have used entropy as an independent measure for evaluating cryptographic schemes, one may refer to the following. A multichannel system was introduced by Voronych et al. [135] for the purpose of structuring and transmitting entropy-manipulated encrypted signals. Schulman [136] argued that entropy makes a cryptographic pseudo-random number generator indistinguishable from a truly random number generator. He studied different ways of creating and increasing entropy. A method was introduced by Wua et al. [97] to measure the entropy of small blocks in an encrypted image. The average of the entropy over the blocks of an image was suggested as an efficient measure for evaluating the security of an image encryption scheme.
- **Relation with Other Cryptographic Measures:** In the following, we study the research works that have established connections between entropy and other security measures, such as unicity distance, malleability, guesswork, confusion, diffusion and indistinguishability.
  - **Unicity Distance:**
    The unicity distance of a cryptosystem is defined as the minimum number of ciphertext bits needed for an adversary with unlimited computational power to recover the key. The connection between entropy and unicity distance has been of interest to some researchers. For example, an entropy analysis presented by AlJabri [137] highlighted the unicity distance as an upper bound on the probability of the key being guessed by an eavesdropper.
  - **Malleability:**
    Consider a cryptosystem $\mathcal{C}$ and a function f. Let us assume that $\mathcal{C}$ encrypts a plaintext p to a ciphertext c, and encrypts $f(p)$ to C'. If there is a transform g that guarantees $g(c) = c'$, then $\mathcal{C}$ is called a malleable cryptosystem with respect to the function f. The notion of non-malleable extractors was introduced by Dodis and Wichs [138] (inspired by the notion of malleability) for the purpose of symmetric-key cryptography from low-entropy keys. Later on, a widely believed conjecture on the distribution of prime numbers in arithmetic progressions was used by Dodis et al. [139] along with an estimate for character sums in order to build some new non-malleable extractors. Moreover, entropy analysis was used by Cohen et al. [140] to present an unconditional construction for non-malleable extractors with short seeds. Recently, some researchers worked on entropy lower bounds for non-malleable extractors [141].
  - **Guesswork:**
    There is a clear relation between entropy and guesswork. While entropy can be interpreted as the average number of guesses required by an optimal binary search attack to break a cryptosystem, guesswork is defined as the average number of guesses required in an optimal linear search attack scenario [142]. It was shown

by Christiansen and Duffy [143] that if appropriately scaled, when the key is long enough, the expectation of the logarithm of the guesswork approaches the Shannon entropy of the key selection process. A similar research work studied the relation between guesswork and Rényi entropy [144]. Pliam [145] demonstrated that there cannot be any general inequality between Shannon entropy and the logarithm of the minimum search space size necessary to guarantee a certain level of guesswork. Another research reported by Malone and Sullivan [146] showed that entropy and guesswork cannot be interchangeably used in normal conditions. The LDP (large deviation principle) was used by Malone and Sullivan [147] to derive the moments of the guesswork for a source of information determined by a Markov chain. It was shown by Lundin [148] how entropy and guesswork can be simultaneously used to evaluate the security of selectively encrypted information.

  - **Confusion and Diffusion:**
    Confusion and diffusion are two properties suggested by Shannon [1] in order to make the statistical analysis of a cryptosystem as difficult as possible. Confusion states that the ciphertext is a complex function of several portions of the key, and this function cannot be simplified to an easily analyzable function. On the other hand, diffusion requires that each plaintext symbol affects several symbols in the ciphertext and each ciphertext symbol is a function of several symbols in the plaintext. This property diffuses the statistical structures of the plaintext over the symbols of ciphertext. The relation between entropy and the mentioned two properties were studied in several research works. For example, entropy was used to evaluate the security of chaotic confusion–diffusion image encryption schemes [149,150]. Moreover, Wu et al. [151] used entropy improvement techniques in combination with confusion and diffusion mechanisms in their proposed cryptographic schemes.
  - **Indistinguishability:**
    Indistinguishability states that given the ciphertext corresponding to a plaintext randomly chosen from a plaintext space with only two elements (determined by the adversary), the adversary will not be able to identify the encrypted message with a probability significantly greater than that of random guessing ($\frac{1}{2}$). Indistinguishability plays a significant role in provable security. Some research works have investigated the relation between indistinguishability and entropy. As an example, one may refer the research reported by Hayashi [152]. In this research, smoothed Rényi entropy and min entropy were used to evaluate the indistinguishability of universal hash functions. Universal hash functions have many important applications in QKD (quantum key distribution), cryptography, privacy amplification (leftover hash lemma), error-correcting codes, parallel computing, complexity theory, pseudorandomness, randomness extractors, randomized algorithms, data structures, etc. (see [153–158] and the references therein).

3.2.2. Applications in Security Proof

Entropy has been used in several types of security proofs including zero-knowledge proof and random oracles. Some related works are briefly reviewed in the following.

- **Zero-Knowledge Proof:**
  Zero-knowledge proof is about proving the possession of some information by one party (the prover) to the other party (the verifier) without revealing the information itself. Zero-knowledge proofs are widely studied in cryptography. Goldreich et al. [159] further developed the notion of non-interactive statistical zero-knowledge proof introduces by De Santis et al. [160]. They used entropy measures to highlight some conditions under which every statistical zero-knowledge proof can be made non-interactive. Lovett and Zhang [161] studied some black box algorithms in order to be used in zero-knowledge proofs. These algorithms can reverse the entropy of a function. It was shown in this report that a black box function of this type incurs an

exponential loss of parameters, which makes it impossible for such an algorithm to be implemented in an efficient way. A new hard problem related to lattices, named ILP (isometric lattice problem) was introduced by Crépeau and Kazmi [162], who used entropy to show that there is an efficient zero-knowledge proof for this problem.

- **Random Oracle:**
  Random oracles are widely used in security proofs in order to model perfect hash algorithms. A random oracle is a hypothetical black box that responds to each query by producing a truly random number uniformly chosen from a predefined domain. There are a few research works that use entropy-related concepts in the analysis of random oracles. For example, it was demonstrated by Muchnik and Romashchenko [163] that random oracles cannot help the extraction of mutual information.

Moreover, Imai et al. [164] worked on information-theoretic proofs, and the relations among different information-theoretic security proofs were studied by Iwamoto et al. [165].

3.2.3. Applications in Adversarial Analysis

In the following, we review the role of entropy in adversarial analysis procedures, including cryptanalysis, eavesdropping, encrypted data analysis, covert channels and attacks.

- **Cryptanalysis:** Entropy measures have been frequently used in research works focusing on cryptanalysis [166]. In particular, chaotic image encryption methods were cryptanalyzed using entropy calculations [167]. Moreover, some researchers used different methods for the cryptanalysis of chaotic image encryption schemes that use entropy improvement techniques [168].
- **Eavesdropping:** Measures of mutual information in quantum key distribution and their applications in eavesdropping were investigated by Rastegin [30].
- **Encrypted Data Analysis:** The analysis of encrypted data is another relevant area of application for entropy. For example, entropy analysis was used for identifying encrypted malware [169], detecting encrypted executable files [170], and correcting noisy encrypted images [171]. Moreover, some researchers focused on entropy analysis of encrypted strings [172].
- **Covert Channel:** Entropy has played role in research on adversarial analysis of cryptosystems via covert channels. For example, entropy was used by Chen et al. [173] to analyze the capacity of a covert channel as well as the factors affecting it.
- **Attacks:** Entropy analysis was used as part of several kinds of attack scenarios. To mention a few, we can refer to the following.
  - **CPA (Chosen Plaintext Attack):**
    Kiltz et al. [174] used entropy measures in their analysis of instantiability of RSA and optimal asymmetric encryption padding (OAEP) under a chosen plaintext attack. OAEP is a padding scheme proposed by Bellare and Rogaway [175], which is often used along with RSA encryption. In another research reported by Bard [176], entropy was used in a CPA against SSL. Moreover, Bard [177] tested several modes of operation for resistance against a blockwise adaptive chosen plaintext attack.
  - **CCA (Chosen Ciphertext Attack):**
    Like the case of chosen plain text attack, entropy analysis has played role in chosen ciphertext attack adversarial analysis. For example, a public-key cryptosystem featuring resistance against CCA was introduced by Zhao et al. [178]. Entropy assessment was used in order to prove the security of this cryptosystem against after-the-fact leakage without non-interactive zero-knowledge proof. Similarly, Sun et al. [179] presented a CCA-secure identity-based encryption system and used entropy to show its resistance against key leakage attacks. Another research study on CCA-resistant and leakage-resistant cryptosystems was reported by Zhou et al. [180] in which entropy was used in the security proof.

- **Side Channel Attack:**
  Mutual information measure is frequently used in side channel attacks. The reason is that mutual information is capable of detecting any kind of statistical dependency, and many side channel analysis scenarios depend on a linear correlation coefficient as a wrong-key distinguisher [181]. Moreover, some research works have used entropy analyses to make cryptosystems more secure against side channel attacks. For example, a method for decreasing the entropy of the information leaked from side channels was introduced by Dhavlle et al. [182]. As another example, an information-theoretical model for side channel attacks was derived by Köpf and Basin [183]. The impact of the entropy of the masks in masking-based countermeasures against side channel attacks was studied by Nassar et al. [184]. This study shows that while these countermeasures are usually studied with the maximal possible entropy for the masks, some particular mask subsets may leak remarkably more as the entropy increases.
- **Replay Attack:**
  Entropy analysis has been used in the detection of replay attacks. As an example, we can mention the research reported by Liu et al. [185], wherein a novel feature based on spectral entropy was introduced for detecting replay attacks.
- **Key Negotiation Attack:**
  It was shown by Liu et al. [186] and Antonioli et al. [187] that an attacker can manipulate the key entropy negotiation protocols used by Bluetooth and Bluetooth low energy and notably reduce the encryption key space.
- **Backdoor Attack:**
  As an example of the applications of entropy in backdoor attacks, we can mention the research reported by Young and Yung [188]. They argued that some backdoor attacks, such as *Monkey*, require the attacker to obtain a large number of ciphertext blocks all encrypted by the same symmetric key, each containing one known plaintext bit. They proposed a new backdoor that eliminates the need for known plaintext while leaking a bound on the plaintext entropy to the reverse engineer.
- **Dictionary Attack:**
  Some researchers have worked on the role of entropy in dictionary attacks. For example, it was shown by Nam et al. [189] that low-entropy keys make some PAKE (password-authenticated key exchange) protocols, such as the one presented by Abdalla and Pointcheval [190], vulnerable to dictionary attacks.
- **Algebraic Attack:**
  In addition to dictionary attacks, low-entropy keys make cryptosystems vulnerable to algebraic attacks. For example, the complexity of finding low-entropy keys using SAT (Boolean satisfactory problem) solvers was studied by Hromada et al. [191].
- **Collision Attack:**
  It was demonstrated by Rock [192] that replacing random permutations by random functions for the update of a stream cipher causes entropy loss, which makes the cipher vulnerable to collision attacks.
- **Correlation Attack:**
  Wiemers and Klein [193] argued that the *correlation-enhanced power analysis collision attack* against AES proposed by Moradi et al. [194] usually yields a set of keys (instead of one) due to noise-related problems. To alleviate this problem, they proposed a practical search algorithm based on a theoretical analysis on how to quantify the remaining entropy.

3.2.4. Analysis of Well-Known Cryptographic Schemes

In the following, we review the applications of entropy in the analysis and evaluation of well-known traditional or modern cryptographic schemes, algorithms, systems and mechanisms.

- **Analysis of Traditional Cryptosystems:** Several researchers have made use of entropy analysis in their evaluations of well-known traditional cryptographic schemes. For example, Bivium [195], RSA [196], AES [197], DES [198] and SOBER-t [199] were subject to entropy analysis by different researchers.
- **Analysis of Emerging Cryptographic Paradigms:**
  In addition to traditional cryptographic schemes, entropy has been used in research on cutting edge cryptographic schemes and paradigms, such as quantum cryptography, homomorphic encryption, white-box cryptography and attribute-based encryption. Some related research works are briefly reviewed in the following.
  - **Quantum Cryptography:**
    Entropy was used by Bienfang et al. [200] and Bienfang et al. [201] in order to evaluate OTP video stream encryption that use quantum-generated secret keys. Arnon-Friedman et al. [202] used entropy to analyze the security of a device-independent quantum cryptography scheme. Moreover, entropy was used in several research works for the purpose of evaluating QKD (quantum key distribution) protocols [203,204].
  - **Attribute-Based Encryption:**
    A technique aimed at increasing the entropy available for proving the security of dual system encryption schemes under decisional linear assumption was presented by Kowalczyk and Lewko [205]. They showed the efficiency of their method in an attribute-based encryption scheme as a case study.

3.2.5. Analysis of Cryptographic Problems and Functions

Entropy was used in the analysis of several cryptographic functions. One-way functions (OWF) have many applications in cryptography [206]. Some of these functions were analyzed using different entropy notions. For instance, two computational notions of entropy, namely, "next-block pseudoentropy" and "inaccessible entropy" were used by Haitner and Vadhan [207] for analyzing and comparing some one-way functions.

3.3. Application

Cryptosystems and cryptographic schemes designed, implemented and evaluated using entropy, were used in a variety of platforms, environments, applications and computing paradigms, among which we can mention fog-based IoTs [208]. In fog-based IoT, a nearby light-weight middleware is used to bridge the gap between IoT deices and the far-away cloud. This helps provide the required support and communication between devices, sensors, receptors on one side and and the servers on the other side. Even entropy-as-a-service was proposed by some researchers [209]. However, among these environments, we will discuss blockchain and cryptocurrencies in more detail because of their importance in the modern world.

The possibility of using the inherent unpredictability of blockchains and especially Bitcoin as a source of randomness was investigated by Pierrot and Wesolowsk [210]. They demonstrated that random numbers generated by this method are malleable in the sense that an adversary will be able to manipulate them, even with limited computational power and financial budget. Some indicators for evaluating public blockchains were introduced by Yong and Peiwu [211]. They used entropy for ranking the indicators. Wu et al. [212] argued that while decentralization is a critical selling point of most public blockchain platforms, most research works on this property fail to quantify it and perform calculations on it. They presented a method based on entropy for quantification of the degree of decentralization in blockchains.

4. Entropy and Other Cryptographic Areas

There are several areas related to cryptography in the field of information security. In this subsection, we briefly review some of these areas along with the role of entropy in the research on each area.

4.1. *Obfuscation*

Obfuscation is the act of making a source of information difficult to understand without the use of a key or an external source of randomness (entropy). For example, in software development, vague names can be assigned to routines or variables in order to obfuscate the code. Entropy was used by Giacobazzi and Toppan [213] to model the uncertainty created by obfuscation and its impact on software security .

4.2. *Message Authentication Codes*

Cheng et al. [214] argued that entropy attacks can adversely affect the throughput of P2P live streaming systems that use network coding (entropy attacks are similar to pollution attacks, wherein the attacker fabricates and transmits polluted packets, avoiding linear combinations of previously sent original packets, but in this case, the attacker tries non-innovative packets containing information already known by the system). They proposed a message authentication system based on symmetric key homomorphic encryption to facilitate the detection of entropy attacks in these systems.

Entropy loss during generic distinguishing-H and state-recovery attacks against hash-based message authentication codes (such as HMAC and NMAC) above the birthday bound was studied by Leurent et al. [215]. Generic distinguishing-H attack aims at distinguishing between different MAC algorithms (e.g., between HMAC and NMAC) to pave the way for more complex attacks. State recovery attack against a cryptographic primitive, as suggested by the name, tries to recover the hidden internal state of an algorithm run by the primitive. Leurent et al. showed that trying to detect collisions by repetitive invocations of a random number generating function does not give a random collision, and this method makes some particular collision patterns much more likely to be detected than others.

4.3. *Cryptography-Based Privacy*

Entropy has played a significant role in several research works in the area of privacy. For example, Rényi entropy and inf-spectral entropy (defined by Bowen and Datta [216]) were used by Watanabe and Hayashi [217] for the purpose of non-asymptotic analysis of privacy amplification. They compared two existing bounds for the *"privacy amplification"* problem and used the mentioned entropy measures to present an interpolation-based method for achieving a new bound for this problem.

Both traditional and differential privacy were studied by Yao [218] from the perspective of α-mutual information (introduced in the same research report). They proposed a unified framework for analyzing the relations between statistical security and mutual information security for a number of different privacy schemes. A mechanism for achieving differential privacy in linear distributed control systems was presented by Wang et al. [219]. This mechanism is based on adding Laplace noise to the shared information depending on the sensitivity of the control system to the private data. They calculated a lower-bound for the entropy of any unbiased estimator of the private data from any noise-adding mechanism giving differential privacy.

4.3.1. Steganography and Steganalysis

Perfectly secure steganography takes great advantage of entropy analysis [220]. In this kind of steganography, the covertext keeps its statistical distribution despite the added hidden text. This makes the stegotext statistically indistinguishable from the covertext. The entropy of image blocks was used by Hu et al. [221] to define a novel distortion measure for steganographic schemes based on frequency domain transformations such as DCT (discrete cosine transform). A framework for blind decoding of image steganography was presented by Kim et al. [222] that is based on measuring the local entropy distributions of decoded images. It was shown in this report that the local entropy distributions of incorrectly decoded images are different from those of normal ones, and the reason is the abnormal structures in erroneously decoded images. Zheng and Cox [223] argued that the existence of a correlation between the cover image and the payload reduces the number of bits needed to hide a given message. They reasoned that this reduction is due to the fact that the correlation decreases the conditional entropy of the message given the cover. A variable-rate image steganography method was proposed by Roy and Changder [224] that tunes the data embedding rate in each image block based on the block entropy. In addition to steganography, some researchers investigated the use of entropy in steganalysis [225].

4.4. User/Device Authentication

Authentication is another cryptography-related area in which researchers used entropy for design and evaluation purposes. For example, entropy has played roles in some research works focusing on the trust evaluation of biometric user authentication systems [226]. As another example, one can mention the application of entropy in the design of image encryption, authentication and compression systems [227]. A comparative study of the applications of different entropy measures in the authentication of EEG (electroencephalogram) signals was presented by Mu et al. [228].

4.5. Digital Signature

Researchers have frequently used entropy in their research on digital signature. As an example, we can refer to the research reported by Atighehchi and Barbier [229], which focused on the problem of publicly authenticating low-entropy data, or data with slight variations over time. Moreover, entropy and related concepts were used in research reports focusing on proxy signature, blind signature and signcryption. For example, entropy was used by Verma and Dhir [230] as a performance measure for threshold proxy signature schemes based on RSA encryption. Rückert [231] used min entropy to evaluate lattice-based blind signatures. Dent et al. [232] presented formal security models for deterministic signcryption schemes with high/low-entropy input messages, and proved encrypt-and-sign to be a secure scheme for high-entropy messages.

4.6. Secret Sharing

Secret sharing is the science of dividing a secret into shares and distributing them among a number of participants in a way that the secret can be retrieved only when a predetermined minimum number of shares are collected from participants. For example, in Shamir's (k,n) secret sharing scheme, the secret s is distributed among n participants in a way that k of the participants can reconstruct s. The procedure is as follows. The dealer (the party who owns the secret) chooses $k-1$ random numbers $a_1, a_2, \dots, a_{k-1}$, and builds a polynomial $S(x) = a_0 + \sum_{i=1}^{k-1} a_i x^i$, where $a_0 = s$. Afterwards, the dealer calculates $S_i = S(i)$ for all $i \in \{1, 2, \dots, n\}$ and privately sends them to n participants $P_1, P_2, \dots, P_n$. The polynomial $S(x)$ and consequently the secret s can be reconstructed using any subset S' of $S = \{S_1, S_2, \dots, S_n\}$ via an interpolation method, such as Lagrange interpolation, provided that $|S'| \geq k$.

There are some secret recovery methods that eliminate the need for remembering the secret shares via making it possible to recover each share by asking the owning participant a number of personal questions [88]. Moreover, entropy was used to model and design more generalized secret sharing systems wherein more than one secret is shared, and each secret can be reconstructed only by a qualified set of participants [233].

5. Concluding Remarks

In the previous sections, we showed the importance of entropy and information theory in research on cryptography. In particular, modern cryptography highly depends on randomness extraction and truly random number generation [234]. PUFs are good examples of devices designed for these purposes (see Section 3.1.4). Furthermore, entropy plays a significant role in recent research on truly random number generation [96,99]. Future researchers may consider reviewing the role of other concepts, such as chaos and complexity, in cryptography. This trend is shown in Figure 4. In this figure, every circle represents the area mentioned, and the area highlighted by 'P' symbols shows the hot topic *'applications of entropy in truly random number generation'*. This is the research topic which is identified as a dominating trend.

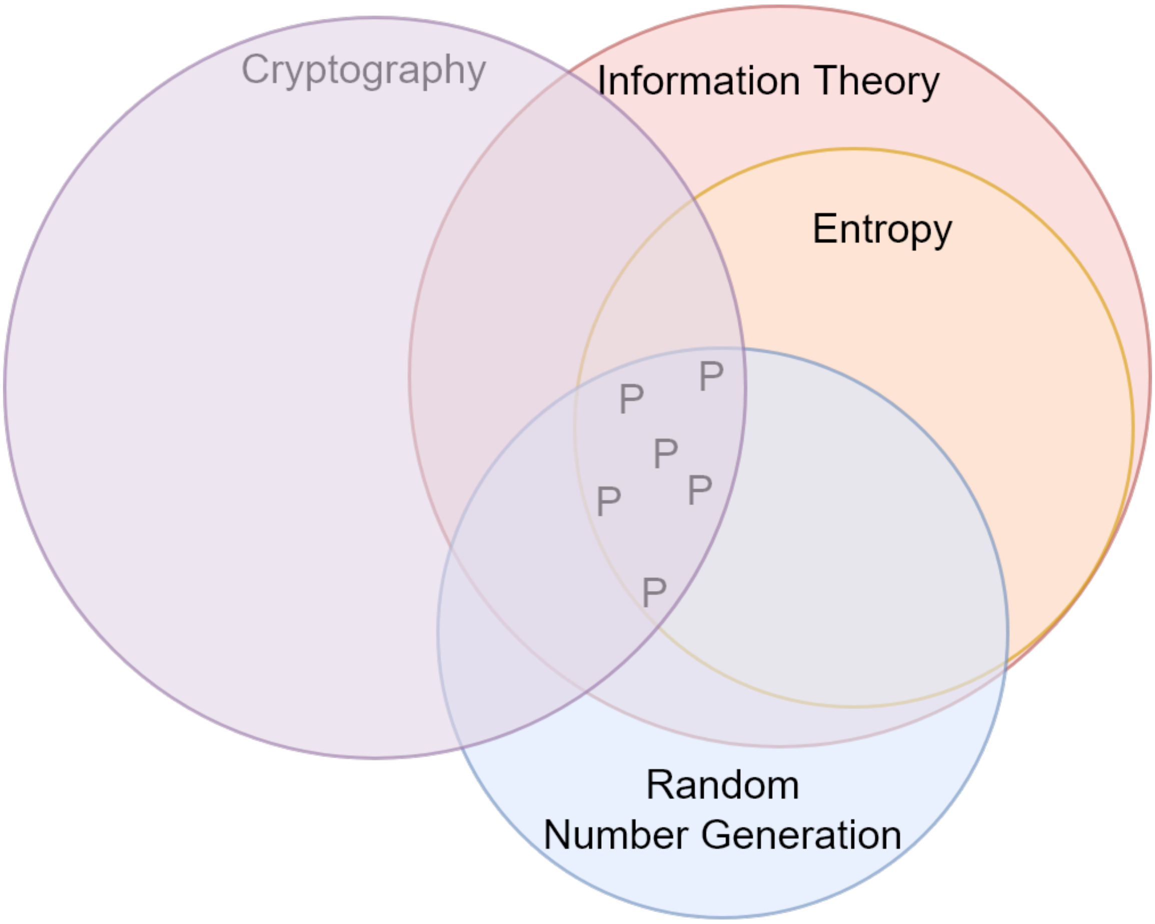

Figure 4. Current trends in the application of entropy in cryptography. Circles represent areas of research and the symbol 'P' denotes the hot topic *'applications of entropy in truly random number generation'*.

Author Contributions: Formal analysis, B.Z., K.B. and T.K.; Writing—original draft, B.Z., K.B. and T.K. All authors have read and agreed to the published version of the manuscript.

Funding: T.K. acknowledges support from MEXT Quantum Leap Flagship Program (MEXT Q-LEAP) Grant No. JPMXS0118067285 and No. JPMXS0120319794 and JSPS KAKENHI Grant Number 16H01705, 17H01695, 19K22849 and 21H04879.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank the referees for carefully reading the paper, and for their useful comments which helped improve the paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Shannon, C.E. A mathematical theory of communication. *Bell Syst. Tech. J.* **1948**, *27*, 379–423. [CrossRef]
2. Shannon, C.E.; Weaver, W. *The Mathematical Theory of Communication*; The University of Illinois Press: Champaign, IL, USA, 1949.
3. Hartley, R.V. Transmission of information 1. *Bell Syst. Tech. J.* **1928**, *7*, 535–563. [CrossRef]
4. Rényi, A. On measures of information and entropy. In *Proceedings of the fourth Berkeley Symposium on Mathematics, Statistics and Probability*; University of California Press: Berkeley, CA, USA, 1960.

5. Makkuva, A.V.; Wu, Y. Equivalence of additive-combinatorial linear inequalities for Shannon entropy and differential entropy. *IEEE Trans. Inf. Theory* **2018**, *64*, 3579–3589. [CrossRef]
6. Zhou, L.; Sood, K.; Xiang, Y. ERM: An accurate approach to detect DDoS attacks using entropy rate measurement. *IEEE Commun. Lett.* **2019**, *23*, 1700–1703. [CrossRef]
7. Yin, X.; Zhang, Q.; Wang, H.; Ding, Z. Rbfnn-based minimum entropy filtering for a class of stochastic nonlinear systems. *IEEE Trans. Autom. Control.* **2019**, *65*, 376–381. [CrossRef]
8. Hellman, Z.; Peretz, R. A survey on entropy and economic behaviour. *Entropy* **2020**, *22*, 157. [CrossRef]
9. Du, Y.; Wang, J.; Guo, S.-M.; Thouin, P. Survey and comparative analysis of entropy and relative entropy thresholding techniques. *IEE-Proc.-Vision Image Signal Process.* **2006**, *153*, 837–850.
10. Evans, L. A survey of entropy methods for partial differential equations. *Bull. Am. Math. Soc.* **2004**, *41*, 409–438. [CrossRef]
11. Lin, D.; Wong, E.K. A survey on the maximum entropy method and parameter spectral estimation. *Phys. Rep.* **1990**, *193*, 41–135. [CrossRef]
12. Maurer, U.M. The role of information theory in cryptography. In Proceedings of the Fourth IMA Conference on Cryptography and Coding, Cirencester, UK, 13–15 December 1993; pp. 49–71.
13. Reyzin, L. Some notions of entropy for cryptography. In *Proceedings of the International Conference on Information Theoretic Security*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 138–142.
14. Vassilev, A.; Hall, T.A. The importance of entropy to information security. *Computer* **2014**, *47*, 78–81. [CrossRef]
15. Yao, Y.; Li, Z. Security of weak secrets based cryptographic primitives via the Renyi entropy. *IET Inf. Secur.* **2016**, *10*, 442–450. [CrossRef]
16. Dodis, Y.; Yu, Y. Overcoming weak expectations. In Proceedings of the IEEE Information Theory Workshop, Lausanne, Switzerland, 3–7 September 2012.
17. Boztas, S. On Rényi entropies and their applications to guessing attacks in cryptography. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2014**, *97*, 2542–2548. [CrossRef]
18. Skórski, M. *Shannon Entropy Versus Renyi Entropy from a Cryptographic Viewpoint*; Springer: Cham, Switzerland, 2015; pp. 257–274.
19. Liu, Y.; Zhang, D.; Deng, Y.; Li, B. (Identity-based) dual receiver encryption from lattice-based programmable hash functions with high min-entropy. *Cybersecurity* **2019**, *2*, 18. [CrossRef]
20. Zhang, D.; Li, J.; Li, B.; Lu, X.; Xue, H.; Jia, D.; Liu, Y. Deterministic identity-based encryption from lattice-based programmable hash functions with high min-entropy. *Secur. Commun. Netw.* **2019**, *2019*, 1816393. [CrossRef]
21. Delvaux, J.; Gu, D.; Verbauwhede, I. Upper bounds on the min-entropy of RO Sum, Arbiter, Feed-Forward Arbiter, and S-ArbRO PUFs. In Proceedings of the IEEE Asian Hardware-Oriented Security and Trust (AsianHOST), Yilan, Taiwan, 19–20 December 2016.
22. Perazzone, J.B.; Paul, L.Y.; Sadler, B.M.; Blum, R.S. Physical layer authentication via fingerprint embedding: Min-entropy analysis: Invited presentation. In Proceedings of the 2019 53rd Annual Conference on Information Sciences and Systems (CISS), Baltimore, MD, USA, 20–22 March 2019; pp. 1–6.
23. Graves, E.; Kirby, B.; Yu, P. Messages per secret bit when authentication and a min-entropy secrecy criterion are required. In *Proceedings of the 2017 51st Annual Conference on Information Sciences and Systems (CISS)*; IEEE: Baltimore, MD, USA, 2017; pp. 1–6.
24. Iwamoto, M.; Shikata, J. Secret sharing schemes based on min-entropies. In *Proceedings of the 2014 IEEE International Symposium on Information Theory*; IEEE: Honolulu, HI, USA, 2014; pp. 401–405.
25. Arimoto, S. Information-theoretical considerations on estimation problems. *Inf. Control* **1971**, *19*, 181–194. [CrossRef]
26. Markechová, D.; Mosapour, B.; Ebrahimzadeh, A. R-norm entropy and R-norm divergence in fuzzy probability spaces. *Entropy* **2018**, *20*, 272. [CrossRef] [PubMed]
27. Kumar, S.; Choudhary, A. Shannon's random-cipher result and the generalized r-norm entropy of type b. *J. Cybersecur. Aware. Educ.*, **2019**, *1*, 768384.
28. Biryukov, A.; Nakahara J., Jr.; Yıldırım, H.M. Differential entropy analysis of the IDEA block cipher. *J. Comput. Appl. Math.* **2014**, *259*, 561–570. [CrossRef]
29. MacKay, D.J. *Information Theory, Inference and Learning Algorithms*; Cambridge University Press: Cambridge, UK, 2003.
30. Rastegin, A.E. On conclusive eavesdropping and measures of mutual information in quantum key distribution. *Quantum Inf. Process.* **2016**, *15*, 1225–1239. [CrossRef]
31. Gierlichs, B.; Batina, L.; Tuyls, P.; Preneel, B. Mutual information analysis: A generic side-channel distinguisher. In Proceedings of the Cryptographic Hardware and Embedded Systems (CHES 2008), Washington, DC, USA, 10–13 August 2008.
32. Iwamoto, M.; Shikata, J. Information theoretic security for encryption based on conditional Rényi entropies. In Proceedings of the Information Theoretic Security-7th International Conference (ICITS 2013), Singapore, 28–30 November 2013.
33. Körner, J. Coding of an information source having ambiguous alphabet and the entropy of graphs. In Proceedings of the 6th Prague Conference on Information Theory, Prague, Czech Republic, 19–25 June 1973.
34. Russell, A.; Wang, H. How to fool an unbounded adversary with a short key. In *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*; Springer: Amsterdam, The Netherlands, 2022; pp. 133–148.
35. Dodis, Y.; Smith, A. Entropic security and the encryption of high entropy messages. In *Proceedings of the Theory of Cryptography Conference*; Springer: Berlin, Germany, 2005; pp. 556–577.
36. Li, X.; Tang, Q.; Zhang, Z. Fooling an Unbounded Adversary with a Short Key, Repeatedly: The Honey Encryption Perspective. In Proceedings of the 2nd Conference on Information-Theoretic Cryptography (ITC 2021), Virtual, 19 July 2021.

37. Cachin, C. Entropy Measures and Unconditional Security in Cryptography. Ph.D. Thesis, Swiss Federal Institute of Technology, Zurich, Switzerland, 1997.
38. Renner, R.; Wolf, S. The exact price for unconditionally secure asymmetric cryptography. In *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*; Spring: Berlin, Germany, 2004.
39. Kim, N.; Kang, J.-S.; Yeom, Y. A synthetic provable security evaluation of cryptographic application with entropy sources. In Proceedings of the International Conference on Security and Management, Las Vegas, NV, USA, 27–30 July 2015.
40. Ruan, O.; Kumar, N.; He, D.; Lee, J.-H. Efficient provably secure password-based explicit authenticated key agreement. *Pervasive Mob. Comput.* **2015**, *24*, 50–60. [CrossRef]
41. Zheng, M.; Zhou, H.; Chen, J. An efficient protocol for two-party explicit authenticated key agreement. *Concurr. Comput. Pract. Exp.* **2015**, *27*, 2954–2963. [CrossRef]
42. Gersho, A. Perfect secrecy encryption of analog signals. *IEEE J. Sel. Areas Commun.* **1984**, *2*, 460–466. [CrossRef]
43. Merhav, N. Perfectly secure encryption of individual sequences. *IEEE Trans. Inf. Theory* **2012**, *59*, 1302–1310. [CrossRef]
44. Ziv, J.; Lempel, A. Compression of individual sequences via variable-rate coding. *IEEE Trans. Inf. Theory* **1978**, *24*, 530–536. [CrossRef]
45. Bi, S.; Yuan, X.; Zhang, Y.J.A. DFT-based physical layer encryption for achieving perfect secrecy. In *Proceedings of the 2013 IEEE International Conference on Communications (ICC)*; IEEE: Budapest, Hungary, 2013; pp. 2211–2216.
46. Sun, H.-M.; Hsieh, B.-T.; Hwang, H.-J. Secure e-mail protocols providing perfect forward secrecy. *IEEE Commun. Lett.* **2005**, *9*, 58–60.
47. Dent, A.W. Flaws in an e-mail protocol. *IEEE Commun. Lett.* **2005**, *9*, 718–719. [CrossRef]
48. Kim, B.H.; Koo, J.H.; Lee, D.H. Robust e-mail protocols with perfect forward secrecy. *IEEE Commun. Lett.* **2006**, *10*, 510–512.
49. Yoon, E.J.; Yoo, K.Y. Cryptanalysis of robust e-mail protocols with perfect forward secrecy. *IEEE Commun. Lett.* **2007**, *11*, 372–374. [CrossRef]
50. Li, P.; Su, J.; Wang, X. ITLS: lightweight transport-layer security protocol for IOT with minimal latency and perfect forward secrecy. *IEEE Internet Things J.* **2020**, *7*, 6828–6841. [CrossRef]
51. Yang, Z.; He, J.; Tian, Y.; Zhou, J. Faster authenticated key agreement with perfect forward secrecy for industrial internet-of-things. *IEEE Trans. Ind. Inform.* **2019**, *16*, 6584–6596. [CrossRef]
52. Blakley, G.R. One time pads are key safegaurding schemes, not cryptosystems. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, USA, 14–16 April 1980.
53. Dodis, Y.; Spencer, J. On the (non)universality of the one-time pad. In Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science, Vancouver, BC, Canada, 16–19 November 2002.
54. Liu, S.; Hong, Y.; Viterbo, E. Unshared secret key cryptography: Achieving shannon's ideal secrecy and perfect secrecy. In Proceedings of the IEEE Information Theory Workshop (ITW 2014), Hobart, TAS, Australia, 2–5 November 2014.
55. Matt, C.; Maurer, U. The one-time pad revisited. In Proceedings of the IEEE International Symposium on Information Theory, Istanbul, Turkey, 7–12 July 2013.
56. Büsching, F.; Wolf, L. The rebirth of one-time pads—Secure data transmission from ban to sink. *IEEE Internet Things J.* **2014**, *2*, 63–71. [CrossRef]
57. Xie, J.; Ulukus, S. Secure degrees of freedom of multiuser networks: One-time-pads in the air via alignment. *Proc. IEEE* **2015**, *103*, 1857–1873. [CrossRef]
58. Zheng, G.; Fang, G.; Shankaran, R.; Orgun, M.A. Encryption for implantable medical devices using modified one-time pads. *IEEE Access* **2015**, *3*, 825–836. [CrossRef]
59. Avdonin, I.; Budko, M.; Budko, M.; Grozov, V.; Guirik, A.A method of creating perfectly secure data transmission channel between unmanned aerial vehicle and ground control station based on one-time pads. In Proceedings of the 9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Munich, Germany, 6–8 November 2017.
60. Srivastava, A.; Awasthi, S.K.; Javed, S.; Gautam, S.; Kishore, N.; Bakthula, R. Seeded one time pad for security of medical images in health information. In Proceedings of the 4th International Conference on Computing Communication and Automation (ICCCA), Greater Noida, India, 14–15 December 2018.
61. Chen, H.-C.; Wijayanto, H.; Chang, C.-H.; Leu, F.-Y.; Yim, K. Secure mobile instant messaging key exchanging protocol with one-time-pad substitution transposition cryptosystem. In Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), San Francisco, CA, USA, 10–14 April 2016.
62. Zhang, Y.; Xu, C.; Wang, F. A novel scheme for secure network coding using one-time pad. In Proceedings of the International Conference on Networks Security, Wireless Communications and Trusted Computing, Wuhan, China, 25–26 April 2009.
63. Xu, D.; Lu, C.; Dos Santos, A. Protecting web usage of credit cards using one-time pad cookie encryption. In Proceedings of the 18th Annual Computer Security Applications Conference, Las Vegas, NV, USA, 9–13 December 2002.
64. Bennett, C.H.; Bessette, F.; Brassard, G.; Salvail, L.; Smolin, J. Experimental quantum cryptography. *J. Cryptol.* **1992**, *5*, 3–28. [CrossRef]
65. Peev, M.; Nölle, M.; Maurhardt, O.; Lorünser, T.; Suda, M.; Poppe, A.; Ursin, R.; Fedrizzi, A.; Zeilinger, A. A novel protocol-authentication algorithm ruling out a man-in-the middle attack in quantum cryptography. *Int. J. Quantum Inf.* **2005**, *3*, 225–231. [CrossRef]
66. Portmann, C. Key recycling in authentication. *IEEE Trans. Inf. Theory* **2014**, *60*, 4383–4396. [CrossRef]

67. Alléaume, R.; Branciard, C.; Bouda, J.; Debuisschert, T.; Dianati, M.; Gisin, N.; Godfrey, M.; Grangier, P.; Länger, T.; Lütkenhaus, N. Using quantum key distribution for cryptographic purposes: A survey. *Theor. Comput. Sci.* **2014**, *560*, 62–81. [CrossRef]
68. Li, Q.; Zhao, Q.; Le, D.; Niu, X. Study on the security of the authentication scheme with key recycling in QKD. *Quantum Inf. Process.* **2016**, *15*, 3815–3831. [CrossRef]
69. Bibak, K.; Ritchie, R.; Zolfaghari, B. Everlasting security of quantum key distribution with 1K-DWCDM and quadratic hash. *Quantum Inf. Comput.* **2021**, *21*, 181–202. [CrossRef]
70. Bibak, K.; Ritchie, R. Quantum key distribution with PRF (Hash, Nonce) achieves everlasting security. *Quantum Inf. Process.* **2021**, *20*, 1–18. [CrossRef]
71. Constantinesu, N. Estimators in cryptography. *Annals. Comput. Sci. Ser.* **2009**, *7*, 1–8. .
72. Al-Husainy, M.A.; Uliyan, D.M. Image encryption technique based on the entropy value of a random block. *Image* **2017**, *8*, 260–266.
73. Xie, D.; Kuo, C.-C. Multimedia encryption with joint randomized entropy coding and rotation in partitioned bitstream. *Eurasip J. Inf. Secur.* **2007**, *2007*, 1–18. [CrossRef]
74. Almasalha, F.; Hasimoto-Beltran, R.; Khokhar, A.A. Partial encryption of entropy-coded video compression using coupled chaotic maps. *Entropy* **2014**, *16*, 5575–5600. [CrossRef]
75. Mian, C.; Jia, J.; Lei, Y. An, H. 264 video encryption algorithm based on entropy coding. In Proceedings of the Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2007), Kaohsiung, Taiwan, 26–28 November 2007.
76. Wu, X.; Moo,P. Joint image/video compression and encryption via high-order conditional entropy coding of wavelet coefficients. In Proceedings of the IEEE International Conference on Multimedia Computing and Systems, Florence, Italy, 7–11 June 1999.
77. Wang, L.-F.; Wang, W.-D.; Ma, J.; Wang, K.-Q.; Xiao, C. Format-Compliant Entropy Coding Encryption Algorithms for Wireless Video System. In Proceedings of the 4th International Conference on Wireless Communications, Networking and Mobile Computing, Dalian, China, 12–17 October 2008.
78. Mostafa, M.; Fakhr, M.W. Joint image compression and encryption based on compressed sensing and entropy coding. In Proceedings of the IEEE 13th International Colloquium on Signal Processing & its Applications (CSPA), Batu Ferringhi, Malaysia, 10–12 March 2017.
79. Ye, G.; Pan, C.; Huang, X.; Zhao, Z.; He, J. A chaotic image encryption algorithm based on information entropy. *Int. J. Bifurc. Chaos* **2018**, *28*, 1850010. [CrossRef]
80. Külekci, M.O. An ambiguous coding scheme for selective encryption of high entropy volumes. In Proceedings of the 17th International Symposium on Experimental Algorithms (SEA 2018), L'Aquila, Italy, 27–29 June 2018.
81. Saeb, M. Reduction of Encryption Key Search Space Based on The Min-Entropy Approach. *Int. J. Comput. Sci. Commun. Secur. (Ijcscs)* **2018**, *6*, 77–80.
82. Yavuz, E.; Yazıcı, R.; Kasapbaşi, M.C.; Yamaç, E. Enhanced chaotic key-based algorithm for low-entropy image encryption. In Proceedings of the 22nd Signal Processing and Communications Applications Conference (SIU), Trabzon, Turkey, 23–25 April 2014.
83. Domaszewicz, J.; Vaishampayan, V. Design of Entropy Constrained Multiple-Decryption Scalar. In Proceedings of the IEEE International Symposium on Information Theory, San Antonio, TX, USA, 17–22 January 1993.
84. Kelsey, J.; Schneier, B.; Hall, C.; Wagner, D. Secure applications of low-entropy keys. In Proceedings of the Information Security Workshop, Beijing, China, 17–19 September 1997.
85. Golic, J.D.; Baltatu, M. Entropy analysis and new constructions of biometric key generation systems. *IEEE Trans. Inf. Theory* **2008**, *54*, 2026–2040. [CrossRef]
86. Wang, X.; Thiele, L.; Haustein, T.; Wang, Y. Secret key generation using entropy-constrained-like quantization scheme. In Proceedings of the 23rd International Conference on Telecommunications (ICT), Thessaloniki, Greece, 16–18 May 2016.
87. Shikata, J. Tighter bounds on entropy of secret keys in authentication codes. In Proceedings of the IEEE Information Theory Workshop (ITW), Kaohsiung, Taiwan, 6–10 November 2017.
88. Ellison, C.; Hall, C.; Milbert, R.; Schneier, B. Protecting secret keys with personal entropy. *Future Gener. Comput. Syst.* **2000**, *16*, 311–318. [CrossRef]
89. Luo, S.; Seideman, J.D.; Dietrich, S. Fingerprinting Cryptographic Protocols with Key Exchange using an Entropy Measure. In Proceedings of the IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 24–24 May 2018.
90. Boyer, R.; Delpha, C. Relative-entropy based beamforming for secret key transmission. In Proceedings of the IEEE 7th Sensor Array and Multichannel Signal Processing Workshop (SAM), Hoboken, NJ, USA, 17–20 June 2012.
91. Horibe, Y. Entropy and an optimal random number transformation (Corresp.). *IEEE Trans. Inf. Theory* **1981**, *27*, 527–529. [CrossRef]
92. Kim, H.; Oh, J.; Jang, C.; Yi, O.; Han, J.; Wi, H.; Park, C. Analysis of the noise source entropy used in openssl's random number generation mechanism. In Proceedings of the International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea, 16–18 October 2019.
93. Wang, J.; Pan, J.; Wu, X. The entropy source of pseudo random number generators: from low entropy to high entropy. In Proceedings of the IEEE International Conference on Intelligence and Security Informatics (ISI), Shenzhen, China, 1–3 July 2019.
94. Hart, J.D.; Roy, R.; Murphy, T.E. Optical random number generation-harvesting entropy from noise and chaos. In Proceedings of the 51st Annual Conference on Information Sciences and Systems (CISS), Baltimore, MD, USA, 22–24 March 2017.

95. Argyris, A.; Pikasis, E.; Syvridis, D. Gb/s one-time-pad data encryption with synchronized chaos-based true random bit generators. *J. Light. Technol.* **2016**, *34*, 5325–5331. [CrossRef]
96. Ma, Y.; Chen, T.; Lin, J.; Yang, J.; Jing, J. Entropy estimation for ADC sampling-based true random number generators. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2887–2900. [CrossRef]
97. Wu, Y.; Noonan, J.P.; Agaian, S. Shannon entropy based randomness measurement and test for image encryption. *Inf. Sci.* **2018**, 1–23. .
98. Wu, Y.; Noonan, J.P.; Agaian, S. A novel information entropy based randomness test for image encryption. In Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics, Anchorage, AK, USA, 9–12 October 2011.
99. Carreira, L.B.; Danielson, P.; Rahimi, A.A.; Luppe, M.; Gupta, S. Low-latency reconfigurable entropy digital true random number generator with bias detection and correction. *IEEE Trans. Circuits Syst. Regul. Pap.* **2020**, *67*, 1562–1575. [CrossRef]
100. Lin, R.-S.; Ross, D.A.; Yagnik, J. Spec hashing: Similarity preserving algorithm for entropy-based coding. In Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, San Francisco, CA, USA, 13–18 June 2010.
101. Wang, Q.; Guo, Z.; Liu, G.; Guo, J. Entropy based locality sensitive hashing. In Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Kyoto, Japan, 25–30 March 2012.
102. Choi, L.; Kim, H.; Kim, S.; Kim, M.H. Scalable packet classification through rulebase partitioning using the maximum entropy hashing. *IEEE/ACM Trans. Netw.* **2009**, *17*, 1926–1935. [CrossRef]
103. Newman, I.; Ragde, P.; Wigderson, A. Perfect hashing, graph entropy, and circuit complexity. In Proceedings of the Fifth Annual Structure in Complexity Theory Conference, Barcelona, Spain, 8–11 July 1990.
104. Arikan, E. An improved graph-entropy bound for perfect hashing. In Proceedings of the IEEE International Symposium on Information Theory, Trondheim, Norway, 27 June–1 July 1994.
105. Cao, D.; Song, Y. Biometric authentication constructed from quantum entropy distribution fuzzy hash. In Proceedings of the 12th International Conference on Signal Processing (ICSP), Hangzhou, China, 19–23 October 2014.
106. Zhang, M.; Tian, L.; Li, C. Key frame extraction based on entropy difference and perceptual hash. In Proceedings of the IEEE International Symposium on Multimedia (ISM), Taichung, Taiwan, 11–13 December 2017.
107. Koranne, S.; Ferguson, J.; Garg, B.; Khanna, M. Entropy-reduced hashing for physical IP management. In Proceedings of the 12th International Symposium on Quality Electronic Design, Santa Clara, CA, USA, 14–16 March 2011.
108. Haitner, I.; Holenstein, T.; Reingold, O.; Vadhan, S.; Wee, H. Universal one-way hash functions via inaccessible entropy. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, French, 30 May–3 June 2010.
109. Li, Z.; Wang, A.; Wang, H. Distributed video coding based on conditional entropy hash. In Proceedings of the International Conference on Computational Aspects of Social Networks, Taiyuan, China, 26–28 September 2010.
110. Mathew, S.K.; Johnston, D.; Satpathy, S.; Suresh, V.; Newman, P.; Anders, M.A.; Kaul, H.; Agarwal, A.; Hsu, S.K.; Chen, G. μ RNG: A 300–950 mV, 323 Gbps/W All-Digital Full-Entropy True Random Number Generator in 14 nm FinFET CMOS. *IEEE J. Solid State Circuits* **2016**, *51*, 1695–1704. [CrossRef]
111. Cicek, I.; Pusane, A.E.; Dundar, G. An integrated dual entropy core true random number generator. *IEEE Trans. Circuits Syst. Ii Express Briefs* **2016**, *64*, 329–333. [CrossRef]
112. Yang, K.; Dong, Q.; Wang, Z.; Shih, Y.-C.; Chih, Y.-D.; Chang, J.; Blaauw, D.; Svlvester, D. A 28NM integrated true random number generator harvesting entropy from MRAM. In Proceedings of the IEEE Symposium on VLSI Circuits, Honolulu, HI, USA, 18–22 June 2018.
113. Park, S.; Choi, B.; Kang, T.; Park, K.; Lee, J.; Kang, S.; Kim, J. Analysis of entropy estimator of true random number generation using beta source. In Proceedings of the 34th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC), Bucharest, Romania, 23–26 June 2019.
114. Cherkaoui, A.; Fischer, V.; Fesquet, L.; Aubert, A. A very high speed true random number generator with entropy assessment. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems (CHES), Santa Barbara, CA, USA, 19–22 December 2013.
115. Chindris, G.; Suciu, A.; Muresan, M. High-entropy random number generators using system on chip devices. In Proceedings of the 31st International Spring Seminar on Electronics Technology, Budapest, Hungary, 7–11 May 2008.
116. Lee, J.; Seo, Y.; Heo, J. Analysis of random number generated by quantum noise source and software entropy source. In Proceedings of the International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea, 17–19 October 2018.
117. Varchola, M.; Drutarovsky, M. New high entropy element for FPGA based true random number generators. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems (CHES), Santa Barbara, CA, USA, 17–20 August 2010.
118. Zhou, T.; Zhou, Z.; Yu, M.; Ye, Y. Design of a low power high entropy chaos-based truly random number generator. In Proceedings of the IEEE Asia Pacific Conference on Circuits and Systems, Singapore, 4–7 December 2006.
119. Liu, H.; Liu, W.; Lu, Z.; Tong, Q.; Liu, Z. Methods for estimating the convergence of inter-chip min-entropy of SRAM PUFs. *IEEE Trans. Circuits Syst. Regul. Pap.* **2017**, *65*, 593–605. [CrossRef]
120. Wang, Q.; Qu, G. A silicon PUF based entropy pump. *IEEE Trans. Dependable Secur. Comput.* **2018**, *16*, 402–414. [CrossRef]

121. Gu, C.; Liu, W.; Hanley, N.; Hesselbarth, R.; O'Neill, M. A theoretical model to link uniqueness and min-entropy for PUF evaluations. *IEEE Trans. Comput.* **2018**, *68*, 287–293. [CrossRef]
122. Gu, C.; Hanley, N.; O'Neill, M. FPGA-based strong PUF with increased uniqueness and entropy properties. In Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS), Baltimore, MD, USA, 28–31 May 2017.
123. Schaub, A.; Danger, J.-L.; Guilley, S.; Rioul, O. An improved analysis of reliability and entropy for delay PUFs. In Proceedings of the 21st Euromicro Conference on Digital System Design (DSD), Prague, Czech Republic, 29–31 August 2018.
124. Koyily, A.; Zhou, C.; Kim, C.H.; Parhi, K.K. An entropy test for determining whether a MUX PUF is linear or nonlinear. In Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS), Baltimore, MD, USA, 28–31 May 2017.
125. Wilde, F.; Frisch, C.; Pehl, M. Efficient bound for conditional min-entropy of physical unclonable functions beyond iid. In Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS), Delft, The Netherlands, 9–12 December 2019.
126. Koeberl, P.; Li, J.; Rajan, A.; Wu, W. Entropy loss in PUF-based key generation schemes: The repetition code pitfall. In Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), Arlington, VA, USA, 6–7 May 2014.
127. Nagpal, S.; Kumar, S.; Gupta, S.C. A new method for modifying blowfish algorithm for iot. *Comput. Secur.* **1998**, *8*, 331–334.
128. David, R.; Măluţan, R.; Borda, M. TLS protocol: Improving using ElGamal elliptic curves and one-time-pad. In Proceedings of the 11th International Symposium on Electronics and Telecommunications (ISETC), Timisoara, Romania, 14–15 November 2014.
129. Zhang, X.; Wang, L.; Cui, G.; Niu, Y. Entropy-based block scrambling image encryption using DES structure and chaotic systems. *Int. J. Opt.***2019**, *2019*, 3594534. [CrossRef]
130. Perrin, L.; Khovratovich, D. Collision spectrum, entropy loss, T-sponges, and cryptanalysis of GLUON-64. In Proceedings of the International Workshop on Fast Software Encryption, London, UK, 3–5 March 2014.
131. Leinweber, L.; Papachristou, C.; Wolff, F.G. An efficient elliptic curve cryptography processor using addition chains with high information entropy. In Proceedings of the 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Montreal, QC, Canada, 29 April –2 May 2012.
132. Hanaoka, G.; Hanaoka, Y.; Hagiwara, M.; Watanabe, H.; Imai, H. Unconditionally secure chaffing-and-winnowing: a relationship between encryption and authentication. In Proceedings of the International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, Las Vegas, NV, USA, 20–24 February 2006.
133. Brown, D.R. Formally assessing cryptographic entropy. *Cryptol. Eprint Arch.* **2011**, *659*, 1–98.
134. Dawson, E.; Gustafson, H. A method for measuring entropy of symmetric cipher key generators. *Comput. Secur.* **1998**, *17*, 177–184. [CrossRef]
135. Voronych, A.; Vozna, N.; Zastavnyy, O.; Pastukh, T.; Grynchyshyn, T. Multichannel system for structuring and transmission entropy-manipulated cipher signals. In Proceedings of the 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), Slavske, Ukraine, 20–24 February 2018.
136. Schulman, J.S. Entropy: An essential component of cryptographic security. *J. Cybersecur. Aware. Educ.* **2019**, *1*, 29–39.
137. Al Jabri, A.K. The unicity distance: An upper bound on the probability of an eavesdropper successfully estimating the secret key. *Inf. Process. Lett.* **1996**, *60*, 43–47. [CrossRef]
138. Dodis, Y.; Wichs, D. Non-malleable extractors and sym-metric key cryptography from weak secrets. In Proceedings of the 41st Annual ACM Symposium on Theory of Computing, Bethesda, MD, USA, 31 May 2009.
139. Dodis, Y.; Li, X.; Wooley, T.D.; Zuckerman, D. Privacy amplification and nonmalleable extractors via character sums. *Siam J. Comput.* **2014**, *43*, 800–830. [CrossRef]
140. Cohen, G.; Raz, R.; Segev, G. Nonmalleable extractors with short seeds and applications to privacy amplification. In Proceedings of the IEEE 27th Conference on Computational Complexity, Porto, Portugal, 26–29 June 2012.
141. Gur, T.; Shinkar, I. An entropy lower bound for non-malleable extractors. *IEEE Trans. Inf. Theory* **2019**, 1. (In Press)
142. Pliam, J.O. The Disparity between Work and Entropy in Cryptology. *IACR Cryptol. Eprint Arch.* **1998**, *1998*, 24.
143. Christiansen, M.M.; Duffy, K.R. Guesswork, large deviations, and Shannon entropy. *IEEE Trans. Inf. Theory* **2012**, *59*, 796–802. [CrossRef]
144. Pfister, C.E.; Sullivan, W.G. Renyi entropy, guesswork moments, and large deviations. *IEEE Trans. Inf. Theory* **2004**, *50*, 2794–2800. [CrossRef]
145. Pliam, J.O. On the incomparability of entropy and marginal guesswork in brute-force attacks. In Proceedings of the INDOCRYPT 2000: Progress in Cryptology, Calcutta, India, 10–13 December 2000.
146. Malone, D.; Sullivan, W. Guesswork is not a substitute for entropy. In Proceedings of the Irish Information Technology and Telecommunication conference, IT&T 2005, National Maritime College: Cork Institute of Technology, Dublin, Irland, 19 August 2005.
147. Malone, D.; Sullivan, W.G. Guesswork and entropy. *IEEE Trans. Inf. Theory* **2004**, *50*, 525–526. [CrossRef]
148. Lundin, R. Guesswork and Entropy as Security Measures for Selective Encryption. Ph.D. Thesis, Faculty of Economic Sciences, Communication and IT, Karlstad University, Karlstad, Sweden, 2012.
149. Afifi, A. A chaotic confusion-diffusion image encryption based on Henon map. *Int. J. Netw. Secur. Appl. (IJNSA)* **2019**, *11*, 19–30.
150. Som, S.; Kotal, A. Confusion and diffusion of grayscale images using multiple chaotic maps In Proceedings of the National Conference on Computing and Communication Systems, Durgapur, India, 21–22 November 2012.

151. Wu, X.; Wang, K.; Wang, X.; Kan, H. Lossless chaotic color image cryptosystem based on DNA encryption and entropy. *Nonlinear Dyn.* **2017**, *90*, 855–875. [CrossRef]
152. Hayashi, M. Security analysis of ε-almost dual universal 2 hash functions: Smoothing of min entropy versus smoothing of Rényi entropy of order 2. *IEEE Trans. Inf. Theory* **2016**, *62*, 3451–3476. [CrossRef]
153. Leiserson, C.E.; Schardl, T.B.; Sukha, J. Deterministic parallel random-number generation for dynamic-multithreading platforms. *Acm Sigplan Not.* **2012**, *47*, 193–204. [CrossRef]
154. Bibak, K.; Kapron, B.M.; Srinivasan, V. MMH* with arbitrary modulus is always almost-universal. *Inf. Process. Lett.* **2016**, *116*, 481–483. [CrossRef]
155. Bibak, K.; Kapron, B.M.; Srinivasan, V.; Tóth, L. On an almost-universal hash function family with applications to authentication and secrecy codes. *Int. J. Found. Comput. Sci.* **2018**, *29*, 357–375. [CrossRef]
156. Bibak, K. *Restricted Congruences in Computing*; CRC Press: Boca Raton, FL, USA, 2020.
157. Ritchie, R.; Bibak, K. SQUAREMIX: A faster pseudorandom number generator for dynamic-multithreading platforms. In Proceedings of the 2020 Data Compression Conference (DCC), Snowbird, UT, USA, 24–27 March 2020; p. 391.
158. Ritchie, R.; Bibak, K. DOTMIX-Pro: faster and more efficient variants of DOTMIX for dynamic-multithreading platforms. *J. Supercomput.* **2022**, *78*, 945–961. [CrossRef]
159. Goldreich, O.; Sahai, A.; Vadhan, S. Can statistical zero knowledge be made non-interactive? or on the relationship of SZK and NISZK. In Proceedings of the CRYPTO '99, Santa Barbara, CA, USA, 15–19 August 1999.
160. Santis, A.D.; Crescenzo, G.D.; Persiano, G.; Yung, M. Image density is complete for non-interactive-SZK. In Proceedings of the 25th International Col-loquium on Automata, Languages and Programming, Aalborg, Denmark, 13–17 July 1998.
161. Lovett, S.; Zhang, J. On the impossibility of entropy reversal, and itsapplication to zero-knowledge proofs. In Proceedings of the Theory of Cryptography Conference, Baltimore, MD, USA, 12–15 November 2017.
162. Crépeau, C.; Kazmi, R.A. Zero-knowledge interactive proof systems for new lattice problems. In Proceedings of the IMA International Conference on Cryptography and Coding, Oxford, UK, 15–17 December 2015.
163. Muchnik, A.; Romashchenko, A. A Random Oracle Does Not Help Extract the Mutual Information. In Proceedings of the International Symposium on Mathematical Foundations of Computer Science (MFCS 2008), Torun, Poland, 25–29 August 2008.
164. Imai, H.; Hanaoka, G.; Shikata, J.; Otsuka, A.; Nascimento, A. Cryptography with information theoretic security. In Proceedings of the IEEE Information Theory Workshop, Bangalore, India, 25 October 2002.
165. Iwamoto, M.; Ohta, K.; Shikata, J. Security formalizations and their relationships for encryption and key agreement in information-theoretic cryptography. *IEEE Trans. Inf. Theory* **2017**, *64*, 654–685. [CrossRef]
166. Li, C.; Lin, D.; Feng, B.; Lü, J.; Hao, F. Cryptanalysis of a chaotic image encryption algorithm based on information entropy. *IEEE Access* **2018**, *6*, 75834–75842. [CrossRef]
167. Reeds, J. Entropy calculations and particular methods of cryptanalysis. *Cryptologia* **1977**, *1*, 235–254. [CrossRef]
168. Su, X.; Li, W.; Hu, H. Cryptanalysis of a chaos-based image encryption scheme combining DNA coding and entropy. *Multimed. Tools Appl.* **2017**, *76*, 14021–14033. [CrossRef]
169. Lyda, R.; Hamrock, J. Using entropy analysis to find encrypted and packed malware. *IEEE Secur. Priv.* **2007**, *5*, 40–45. [CrossRef]
170. Alekseev, I.; Platonov, V. Detection of encrypted executable files based on entropy analysis to determine the randomness measure of byte sequences. *Autom. Control. Comput. Sci.* **2017**, *51*, 915–920. [CrossRef]
171. Puteaux, P.; Puech, W. Noisy encrypted image correction based on Shannon entropy measurement in pixel blocks of very small size. In Proceedings of the EUSIPCO: European Signal Processing Conference, Rome, Italy, 3–7 September 2018.
172. Lundin, R.; Lindskog, S. Entropy of selectively encrypted strings. In Proceedings of the 5th Workshop on Infor-mation Security Theory and Practices (WISTP), Heraklion, Crete, Greece, 1–3 June 2011.
173. Chen, L.; Ju, S.; Zhou, C.; Zhang, Y. Covert channel capacity analysis based on entropy. In Proceedings of the International Symposium on Information Science and Engineering, Shanghai, China, 20–22 December 2008.
174. Kiltz, E.; O'Neill, A.; Smith, A. Instantiability of RSA-OAEP under chosen-plaintext attack. *J. Cryptol.* **2017**, *30*, 889–919. [CrossRef]
175. Bellare, M.; Rogaway, P. Optimal asymmetric encryption–how to encrypt with rsa (extended abstract). In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt), Perugia, Italy, 9–12 May 1994.
176. Bard, G.V. A cahllenging but feasible blockwise-adaptive chosen-plaintext attac on ssl. In Proceedings of the International Conference on Security and Cryptography (SECRYPT 2006), Setúbal, Prtugal, 7–10 August 2006.
177. Bard, G. Blockwise-adaptive chosen-plaintext attack and online modes of encryption. In Proceedings of the Cryptography and Coding, 11th IMA International Conference, Cirencester, UK, 18–20 December 2007.
178. Zhao, Y.; Liang, K.; Yang, B.; Chen, L. CCA Secure Public Key Encryption against After-the-Fact Leakage without NIZK Proofs. *Secur. Commun. Netw.* **2019**, *2019*, 1–9. [CrossRef]
179. Sun, S.F.; Gu, D.; Liu, S. Efficient chosen ciphertext secure identity-based encryption against key leakage attacks. *Secur. Commun. Netw.* **2016**, *9*, 1417–1434. [CrossRef]
180. Zhou, Y.; Yang, B.; Yu, Y.; Khan, A. Efficient chosen-ciphertext secure hybrid encryption scheme tolerating continuous leakage attacks. *J. Chin. Inst. Eng.* **2019**, *42*, 39–47. [CrossRef]
181. Prouff, E.; Rivain, M. Theoretical and practical aspects of mutual information based side channel analysis. *Int. J. Appl. Cryptogr.* **2010**, *2*, 121–138. [CrossRef]

182. Dhavlle, A.; Bhat, S.; Rafatirad, S.; Homayoun, H.; Sai Manoj, P.D. Work-in-progress: Sequence-crafter: Side-channel entropy minimization to thwart timing-based side-channel attacks. In Proceedings of the International Conference on Compliers, Architectures and Synthesis for Embedded Systems (CASES), New York, NY, USA, 13–18 October 2019.
183. Köpf, B.; Basin, D.A. An information-theoretic model for adaptive side-channel attacks. In Proceedings of the 14th ACM conference on Computer and communications security, Alexandria, Virginia, USA, 31 October–2 November 2007.
184. Nassar, M.; Guilley, S.; Danger, J.-L. Formal analysis of the entropy/security trade-off in first-order masking countermeasures against side-channel attacks. In Proceedings of the International Conference on Cryptology in India (INDOCRYPT), Chennai, India, 11–14 August 2011.
185. Liu, Y.; Das, R.K.; Li, H. Multi-band spectral entropy information for detection of replay attacks. In Proceedings of the Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), Lanzhou, China, 18–21 November 2019.
186. Antonioli, D.; Tippenhauer, N.O.; Rasmussen, K. Key negotiation downgrade attacks on Bluetooth and Bluetooth low energy. *ACM Trans. Priv. Secur.* **2020**, *23*, 14:1–14:28. [CrossRef]
187. Antonioli, D.; Tippenhauer, N.O.; Rasmussen, K.B. The KNOB is Broken: Exploiting Low Entropy in the Encryption Key Negotiation Of Bluetooth BR/EDR. In Proceedings of the 28th USENIX Security Symposium, Santa Clara, CA, USA, 14–16 August 2019.
188. Young, A.; Yung, M. Backdoor attacks on black-box ciphers exploiting low-entropy plaintexts. In Proceedings of the Australasian Conference on Information Security and Privacy, Wollongong, NSW, Australia, 9–11 July 2003.
189. Nam, J.; Choo, K.-K.R.; Paik, J.; Won, D. An offline dictionary attack against a three-party key exchange protocol. *IEEE Commun. Lett.* **2009**, *13*, 205–207.
190. Abdalla, M.; Pointcheval, D. Simple password-based encrypted keyexchange protocols. In Proceedings of the RSA Conference, San Francisco, CA, USA, 14–18 February 2005.
191. Hromada, V.; Öllős, L.; Zajac, P. Using SAT solvers in large scale distributed algebraic attacks against low entropy keys. *Tatra Mt. Math. Publ.* **2015**, *64*, 187–203. [CrossRef]
192. Rock, A. Collision attacks based on the entropy loss caused by random functions. In Proceedings of the Second Western European Workshop on Research in Cryptology (WEWoRC), Bochum, Germany, 4–6 July 2007.
193. Wiemers, A.; Klein, D. Entropy reduction for the correlation-enhanced power analysis collision attack. In Proceedings of the International Workshop on Security, Sendai, Japan, 3–5 September 2018.
194. Moradi, A.; Mischke, O.; Eisenbarth, T. Correlation-enhanced power analysis collision attack. In Proceedings of the 12th international conference on Cryptographic hardware and embedded systems, Santa Barbara, CA, USA, 17–20 August 2010.
195. Rohani, N.; Noferesti, Z.; Mohajeri, J.; Aref, M.R. Guess and Determine Attack on Bivium. *J. Inf. Process. Syst.* **2011**, *7*, 151–158. [CrossRef]
196. Soder, N.; Deluca, C.; Biersach, D.; DePhillips, M. Assessing the Cryptographic Strength of RSA Moduli Using Algorithmic Entropy Reduction in Bivariate Polynomials. In Proceedings of the New York Scientific Data Summit (NYSDS), New York, NY, USA, 6–8 August 2018.
197. Lashermes, R.; Reymond, G.; Dutertre, J.-M.; Fournier, J.; Robisson, B.; Tria, A. A DFA on AES based on the entropy of error distributions. In Proceedings of the Workshop on Fault Diagnosis and Tolerance in Cryptography, (A DFA on AES Based on the Entropy of Error Distributions), Leuven, Belgium, 9 September 2012.
198. Patil, P.; Narayankar, P.; Narayan, D.; Meena, S.M. A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish. In Proceedings of the International Conference on Information Security & Privacy (ICISP2015), ESEO, Angers, Loire Valley, France, 11–12 February 2015.
199. Babbage, S.; Lano, J. Probabilistic factors in the sober-t stream ciphers. In Proceedings of the 3rd New European Schemes for Signatures, Integrity, and Encryption (NESSIE Workshop), Munich, Germany, 6–7 November 2002.
200. Bienfang, J.; Mink, A.; Hershman, B.; Nakassis, A.; Tang, X.; Boisvert, R.; Su, D.; Clark, C.W.; Williams, C.J.; Gross, A. Broadband quantum generated one-time-pad encryption. In Proceedings of the Quantum Electronics and Laser Science Conference, Shanghai, China, 22–27 December 2005.
201. Bienfang, J.; Mink, A.; Hershman, B.; Nakassis, A.; Tang, X.; Boisvert, R.; Su, D.; Clark, C.W.; Williams, C.J.; Gross, A. Quantum generated one-time-pad encryption with 1.25 Gbps clock synchronization. In Proceedings of the OFC/NFOEC Technical Digest. Optical Fiber Communication Conference, Anaheim, CA, USA, 7–10 March 2005.
202. Arnon-Friedman, R.; Dupuis, F.; Fawzi, O.; Renner, R.; Vidick, T. Practical device-independent quantum cryptography via entropy accumulation. *Nat. Commun.* **2018**, *9*, 1–11. [CrossRef]
203. Chen, Z.; Zhang, Y.; Wang, X.; Yu, S.; Guo, H. Improving parameter estimation of entropic uncertainty relation in continuous-variable quantum key distribution. *Entropy* **2019**, *21*, 652. [CrossRef] [PubMed]
204. Myers, J.M.; Wu, T.T.; Pearson, D.S. Entropy estimates for individual attacks on the BB84 protocol for quantum key distribution. In Proceedings of the Fourth IMA Conference on Cryptography and Coding, Orlando, FL, USA, 24 August 2004.
205. Kowalczyk, L.; Lewko, A.B. Bilinear entropy expansion from the decisional linear assumption. In Proceedings of the Annual Cryptology Conference, Santa Barbara, CA, USA, 16–20 August 2015.
206. Impagliazzo, R.; Luby, M. One-way functions are essential for complexity based cryptography. In Proceedings of the 30th Annual Symposium on Foundations of Computer Science, Research Triangle Park, NC, USA, 30 October–1 November 1989.

207. Haitner, I.; Vadhan, S. *Tutorials on the Foundations of Cryptography*; The Many Entropies in One-Way Functions; Springer: Berlin, Germany, 2017; pp. 159–217.
208. Boakye-Boateng, K.; Kuada, E.; Antwi-Boasiako, E.; Djaba, E. Encryption protocol for resource-constrained devices in fog-based IoT using one-time pads. *IEEE Internet Things J.* **2019**, *6*, 3925–3933. [CrossRef]
209. Vassilev, A.; Staples, R. Entropy as a service: Unlocking cryptography's full potential. *Computer* **2016**, *49*, 98–102. [CrossRef]
210. Pierrot, C.; Wesolowski, B. Malleability of the blockchain's entropy. *Cryptogr. Commun.* **2018**, *10*, 211–233. [CrossRef]
211. Tang, H.; Shi, Y.; Dong, P. Public blockchain evaluation using entropy and TOPSIS. *Expert Syst. Appl.* **2019**, *117*, 204–210. [CrossRef]
212. Wu, K.; Peng, B.; Xie, H.; Huang, Z. An information entropy method to quantify the degrees of decentralization for blockchain systems. In Proceedings of the IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC), Beijing, China, 12–14 July 2019.
213. Giacobazzi, R.; Toppan, A. On entropy measures for code obfuscation. In Proceedings of the Software Security and Protection Workshop, Orlando, FL, USA, 16 June 2012.
214. Cheng, C.; Jiang, T.; Zhang, Q. TESLA-based homomorphic MAC for authentication in P2P system for live streaming with network coding. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 291–298. [CrossRef]
215. Leurent, G.; Peyrin, T.; Wang, L. New generic attacks against hash-based MACs. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, 1–5 December 2013.
216. Bowen, G.; Datta, N. Beyond i.i.d. in quantum information theory. In Proceedings of the IEEE International Symposium on Information Theory, Seattle, WA, USA, 10 July 2006.
217. Watanabe, S.; Hayashi, M. Non-asymptotic analysis of privacy amplification via rényi entropy and inf-spectral entropy. In Proceedings of the IEEE International Symposium on Information Theory, Istanbul, Turkey, 7–12 July 2013.
218. Yao, Y. A generalized constraint of privacy: A-mutual information security. *IEEE Access*, **2019**, *7*, 36122–36131. . [CrossRef]
219. Wang, Y.; Huang, Z.; Mitra, S.; Dullerud, G.E. Differential privacy in linear distributed control systems: Entropy minimizing mechanisms and performance tradeoffs. *IEEE Trans. Control. Netw. Syst.*, **2017**, *4*, 118–130. [CrossRef]
220. Ryabko, B.; Ryabko, D. Information-theoretic approach to steganographic systems. In Proceedings of the IEEE International Symposium on Information Theory, Nice, France, 24–29 June 2007.
221. Hu, X.; Ni, J.; Shi, Y.-Q. Efficient JPEG steganography using domain transformation of embedding entropy. *IEEE Signal Process. Lett.* **2018**, *25*, 773–777. [CrossRef]
222. Kim, C.; Lee, S.; Lee, J.; Park, J.-I. Blind decoding of image steganography using entropy model. *Electron. Lett.* **2018**, *54*, 626–628. [CrossRef]
223. Zheng, L.; Cox, I.J. Jpeg based conditional entropy coding for correlated steganography. In Proceedings of the IEEE International Conference on Multimedia and Expo, Beijing, China, 2–5 July 2007.
224. Roy, R.; Changder, S. Image steganography with block entropy based segmentation and variable rate embedding. In Proceedings of the 2nd International Conference on Business and Information Management (ICBIM), Durgapur, India, 9–11 January 2014.
225. Malik, H.; Subbalakshmi, K.; Chandramouli, R. Nonparametric steganalysis of qim steganography using approximate entropy. *IEEE Trans. Inf. Forensics Secur.* **2011**, *7*, 418–431. [CrossRef]
226. Kim, J.H.; Kim, M.Y.; Youm, H.Y. Trust Elevation Scheme Based on Entropy-Specific Biometric Authentication Methods for the Financial Sector. In Proceedings of the 13th Asia Joint Conference on Information Security (AsiaJCIS), Guilin, China, 8–9 August 2018.
227. Nemavarkar, A.; Chakrawarti, R.K. A uniform approach for multilevel email security using image authentication, compression, otp & cryptography. In Proceedings of the International Conference on Computer, Communication and Control (IC4), Indore, India, 10–12 December 2015.
228. Mu, Z.; Hu, J.; Min, J.; Yin, J. Comparison of different entropies as features for person authentication based on EEG signals. *IET Biom.* **2017**, *6*, 409–417. [CrossRef]
229. Atighehchi , K.; Barbier, M. Signature renewal for low entropy data. In Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018.
230. Kumar, R.; Verma, H.K.; Dhir, R. Cryptanalysis and performance evaluation of enhanced threshold proxy signature scheme based on RSA for known signers. *Math. Probl. Eng.* **2013**, *2013*, 790257. [CrossRef]
231. Rückert, M. Lattice-based blind signatures. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Singapore, 5–9 December 2010.
232. Dent, A.W.; Fischlin, M.; Manulis, M.; Stam, M.; Schröder, D. Confidential signatures and deterministic signcryption. In Proceedings of the International Workshop on Public Key Cryptography, Paris, France, 26–28 May 2010.
233. Zou, S.; Liang, Y.; Lai, L.; Shamai, S. An information theoretic approach to secret sharing. In Proceedings of the IEEE International Symposium on Informa-tion Theory (ISIT), Saint Petersburg, Russia, 31 July–5 August 2011.
234. Zhao, Q.; Zheng, W.; Zhao, X.; Cao, Y.; Zhang, F.; Law, M.-K. A 108 F^2/bit fully reconfigurable RRAM PUF based on truly random dynamic entropy of jitter noise. *IEEE Trans. Circuits Syst.* **2020**, *67*, 3866–3879. [CrossRef]