applied system innovation

MDPI

Review

AI Makes Crypto Evolve

Behrouz Zolfaghari [1,*] and **Takeshi Koshiba** [2]

[1] Cyber Science Lab, University of Guelph, Guelph, ON N1G 2W1, Canada
[2] Department of Integrated Arts and Sciences, Waseda University, Tokyo 169-8050, Japan; tkoshiba@waseda.jp
* Correspondence: behrouz@cybersciencelab.org

Abstract: The recent literature reveals a dichotomy formed by a coevolution between cryptography and Artificial Intelligence (AI). This dichotomy consists of two sides, namely Crypto-Influenced AI (CIAI) and AI-Influenced Cryptography (AIIC). While it is pertinent to investigate this dichotomy from both sides, the first side has already been studied. In this review, we focused on AIIC. We identified and analyzed the stages on the evolutionary path of AIIC. Moreover, we attempted to anticipate what the future may hold for AIIC given the impact of quantum computing on the present and the future of AI.

Keywords: artificial antelligence; cryptography; evolution; AI-influenced cryptography; trend analysis; future raodmap

check for updates

Citation: Zolfaghari, B.; Koshiba, T. AI Makes Crypto Evolve. *Appl. Syst. Innov.* **2022**, *5*, 75. https://doi.org/10.3390/asi5040075

Received: 6 July 2022
Accepted: 26 July 2022
Published: 29 July 2022

1. Introduction

Cryptography (referred to as *Crypto*) has recently become a research focus [1–3]. It is the art and science of leveraging algorithms, mathematical problems and structures, secret keys, and complex transformations to maintain data confidentiality during storage or transmission. Cryptography plays significant roles in security-related scenarios including authentication [4], privacy [5] and information hiding [6]. This opens its way into numerous technological environments ranging from medical technology [7] to Internet of Things (IoT) [8] and Cloud computing [9]. There are many branches of science and technology that frequently appear in the ecosystem of modern cryptography. To mention a few, one may refer to chaos theory [10], information theory [11,12], quantum computing [13], hardware technology [14], and particularly AI [15–17].

Similar to the case of cryptography, AI has been of great interest to researchers in recent years [18–20]. It leverages computer and complex algorithms to mimic human decision making and problem solving. AI has been used in a variety of applications [21–23].

In recent years, cryptography and AI have formed a dichotomy that has led to their co-evolution [24]. The role of cryptography in the evolution of AI has already been studied [25]. However, to the best of our knowledge, the role of AI in the evolution of cryptography has not been studied in depth. This study is an attempt to address this gap. In this paper, we tried to provide a thorough overview and a comprehensive understanding of the role of AI in the evolution of cryptography. This role is illustrated in Figure 1.

The overlapping parallelograms in Figure 1 represent cryptography after evolving under the impact of AI, which we refer to as *AI-Influenced Crypto (AIIC)* in the rest of this paper.

Most cryptosystems depend on complex computing, and AI-based methods have already been proven to be efficient in any computation-intensive environment. Moreover, AI models can provide chaos [26], randomness [27], and many other properties, all of which are required by cryptosystems [28,29]. The above mentioned facts open the way for AI into cryptography and highlight the importance of AIIC. Moreover, AI has found its applications in some raising cryptography-related technologies such as blockchain, which can be studied in future research works.

While there may be existing surveys encompassing AI and cryptography, there are shortcomings within them, especially the lack of a detailed look at the evolutionary path of AIIC. These shortcomings (discussed in Section 2.4) motivated this research.

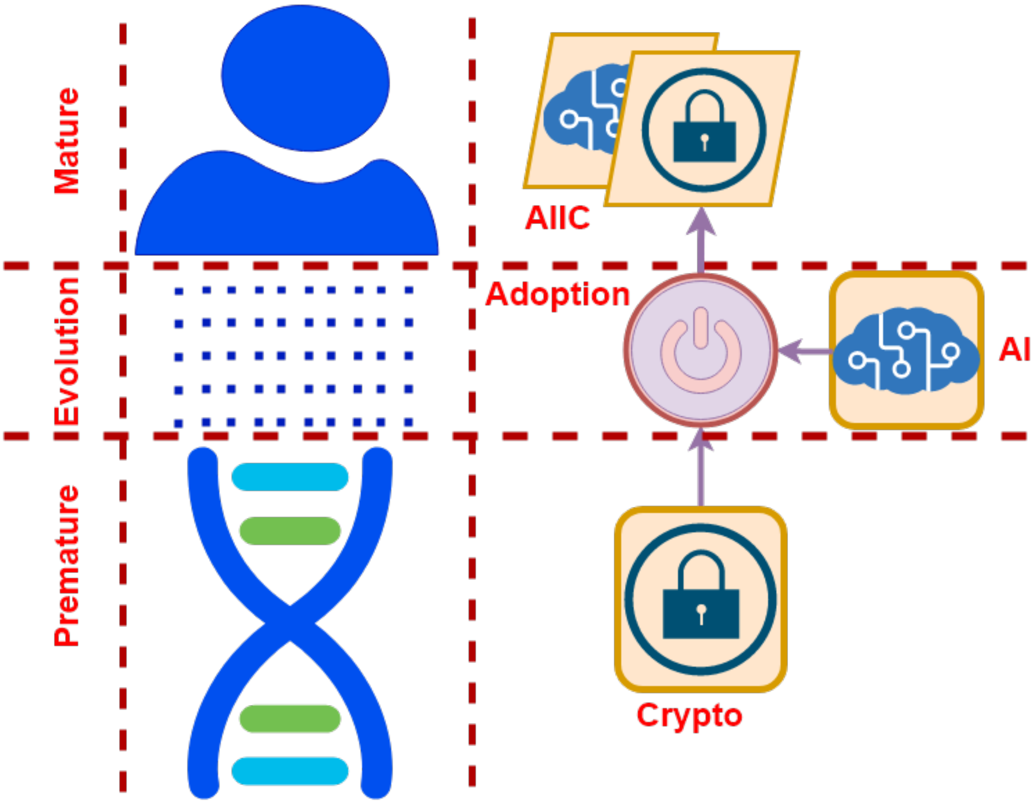

Figure 1. Crypto Makes AI Evolve.

1.1. Goals and Objectives

In this review, we explored the evolutionary path of AIIC as well as its future roadmap to answer the following questions:

- What stages should cryptography go through in order to adopt AI?
- What does AI add to the capabilities of cryptosystems in each of the identified stages?
- Which existing trends in the AI realm will affect the future of AIIC?
- What effects will AI trends have on the future of AIIC?

We sought to establish a comprehensive picture of the evolutionary path of cryptography under the impact of AI by providing answers to the above questions.

1.2. Achievements

Our achievements in this paper are as follows.

1. We recognized and defined the following five stages in the evolutionary path of AIIC.
    - *AI-Unaware Cryptography (AIUC)* (Section 3): At this stage, cryptography is vulnerable to Machine Learning (ML) and Deep Learning (DL) attacks. It can be targeted by AI-based attacks without any specialized defensive measure or mechanism.
    - *AI-Resilient Cryptography (AIRC)* (Section 4): This is the second evolutionary stage, wherein cryptosystems adopt caution towards ML and DL attacks. In this stage, cryptographic methods and devices are designed to be as resilient as possible against AI-based attacks.
    - *AI-Boosted Cryptography (AIBC)* (Section 5): In the third stage, cryptographic techniques, protocols, methods, devices, etc., are supported by AI models in two

possible ways. First, they might be improved with the help of AI in terms of different design objectives not including security. These objectives may include performance, efficiency, etc. Second, they might be assisted by AI for use in security-related scenarios not including cryptography. These scenarios include authentication, privacy, information hiding, etc.

- *AI-Assisted Cryptography (AIAC)* (Section 6): In this stage, as well as the next one, AI is utilized by one or more of the internal components of the cryptosystem, and directly for cryptographic purposes. What differentiates these two stages is the component where AI is used. A cryptosystem often consists of an encryption/decryption component along with some extra components, which perform cryptographic mechanisms such as hashing, random number generation, etc. In the AIAC stage, AI is used by the components running cryptographic mechanisms.
- *AI-Embedded Cryptography (AIEC)* (Section 7): In the last stage, AI is used by the encryption/decryption component.

The above stages are shown in Figure 2 along with the icon we used for each of them in the rest of this paper.

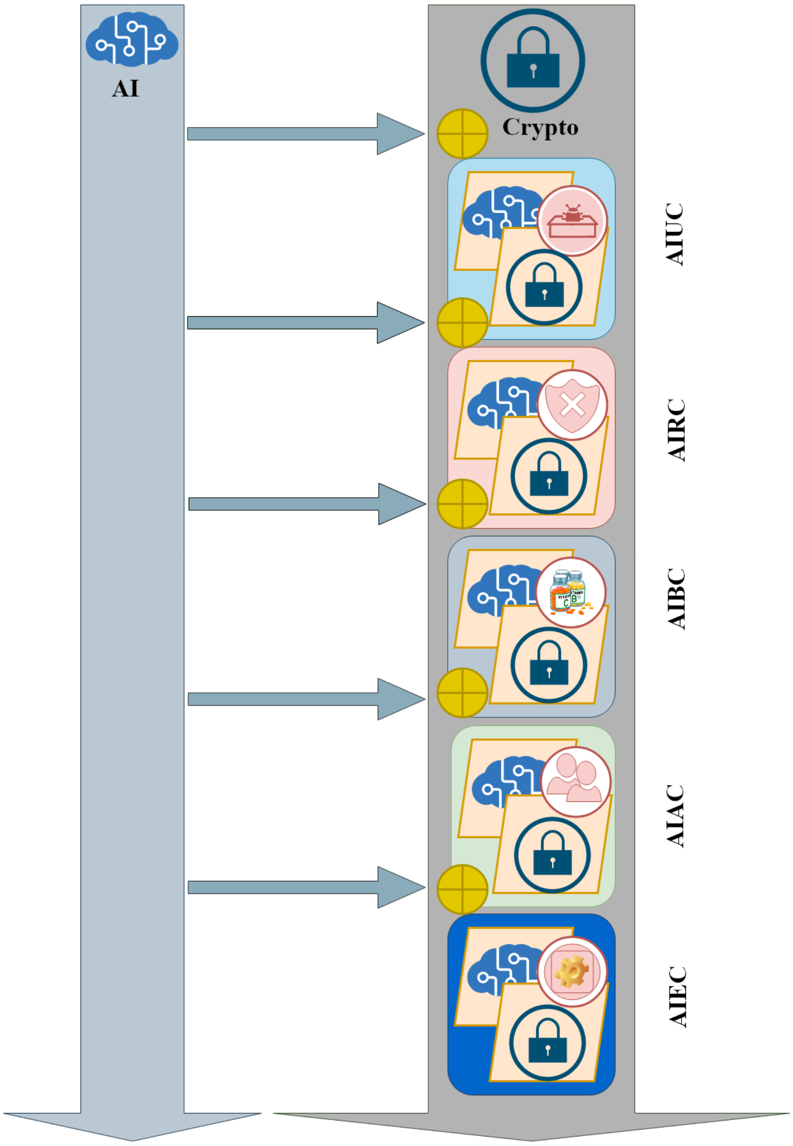

Figure 2. The Evolutionary Path of AIIC.

Table 1 summarizes the properties of the stages shown in Figure 2.

Table 1. Summary of AIIC Evolutionary States.

Stage	Resil.	Improve Non-Sec.	Support Scen.	Util. Non-Encrypt.	Util. Encrypt.
AIUC	No	No	No	No	No
AIRC	Yes	No	No	No	No
AIBC	Yes	Yes	Yes	No	No
AIAC	Yes	Yes	Yes	Yes	No
AIEC	Yes	Yes	Yes	Yes	Yes

In Table 1, the first entry in each row contains one of the evolutionary stages demonstrated in Figure 2. The second entry contains "Yes" if cryptographic modules and systems in the related stage are aware of and resilient against Ml and DL attacks. The third entry indicates whether or not cryptosystems in the related stage are improved via the use of AI in terms of objectives not related to security. The fourth entry shows the existence or lack of support from AI for cryptographic mechanisms in security-related scenarios. A "Yes" in the fifth entry shows that the stage mentioned in the first entry makes use of AI in some internal cryptographic components, but not exactly in the encryption/decryption module. The sixth entry indicates whether or not the related stage utilizes AI models exactly in the design and implementation of the encryption/decryption component.

As shown in Figure 2 and Table 1, each stage adds some new capabilities in addition to preserving the capabilities of the previous stages.

2. We reviewed current trends in research on AI such as bio-inspired and quantum-inspired AI, and attempted to anticipate the influence of these trends in terms of what the future may hold for AIIC. We developed a future roadmap for further research in this area (Section 8).

1.3. Organization

The rest of this paper is organized as follows. Section 2 studies existing surveys and their shortcomings in order to highlight our motivations for the work within this paper. Section 3 through Section 7 provides a study of the evolutionary path of AIIC. Sections 3–7 discuss AIIC, AIRC, AIBC, AIAC and AIEC, respectively. Section 8 develops the future roadmap and lastly, Section 9 concludes the paper and suggests further research.

2. Existing Surveys

The literature includes many surveys on the applications of AI in security. However, some of them are outdated for use in such a dynamic research area. Some of them do not specifically focus on the applications of AI in cryptography. Some relevant surveys study AI-assisted cryptography only in some specific environments. Others fail to develop a future roadmap. These surveys are analyzed below.

2.1. Surveys on AI in Security

This section explores surveys related to the use of AI tools including Neural Networks (NNs) which are also known as Artificial Neural Networks (ANNs), ML and DL in Cyber Security, but not directly in relation to their applications in cryptography.

Recent surveys identified many capabilities of AI that can be of assistance in security controls such as intrusion detection [30] and authentication [31,32]. These capabilities have paved the way for AI in many technological environments, which were reviewed in previous surveys. For example, with recent advances in the fields of blockchain and AI, both can be leveraged to secure communications in smart cars for inter-vehicle communication and vehicle to vehicle communication. These applications were reviewed in [33]. Other surveys explored the applications of ML in power systems [34] and smart grids [35].

As another example, the authors of [36] noted that although Edge computing can dramatically speed up and increase the performance of network applications, there are many security concerns (Edge computing can provide the integration for storage, processing, monitoring, and control of operations at the edge of a network). They studied several attacks including DDOS, eavesdropping and malware injection against Edge computing. These researchers showed by their reviews that NNs and other ML algorithms can provide strong mitigating factors for the detection and prevention of these attacks.

Several other surveys focused on the applications of AI in the security of IoT [37,38]. In this regard, the applications of ML and DL [39] as well as Reinforcement learning [40] have been of interest to the research community.

Moreover, the authors of [41] focused on the fact that while ML can be used as an effective technique for identifying some kinds of attacks, it is vulnerable to other kinds of attacks. They studied many attacks against naive Bayes, logistic regression, Support Vector Machine (SVM) and Deep Neural Networks (DNNs). Some defensive measures used to protect algorithms against well-known attacks include security assessment mechanisms, placing checks in the training stage, data security and ensuring privacy.

2.2. Surveys on AI in Cryptography (AIIC)

Most relevant surveys focus on the AIEC phase. Some of them focus on the applications of NNs in cryptography. These works typically discuss how NN can be used in the efficient and secure encryption and decryption of text [42–44]. There are also a few surveys available on the applications of NNs in image encryption [45].

Other surveys study the applications of ML in cryptography [46,47]. The latter surveys show how mutual learning provided by Tree Parity Machines (TPMs) can be useful in public key cryptosystems. Furthermore, they discuss how the classification capabilities of ML can be introduced into cryptography and how this may facilitate the classification of encrypted traffic.

There are only a few currently available surveys which discuss the role of quantum computing in AIIC [48]. These surveys failed to address the impact of quantum computing on the future of AIIC. The surveys reported some compatibility issues between NNs and quantum cryptography. These issues have their roots in the fact that quantum encryption and decryption methods based on *Heisenber's Principle* and *Photon Polarization* cannot match well with NN-based key generation.

2.3. Summary

Table 2 summarizes the surveys studied above for ease of comparison with our work in this paper.

In Table 2, the first entry in each row cites one of the surveys studied above. The second column shows the publication year of the survey. The third column contains a "Yes" for surveys that cover all branches of AI. It contains a "No" for those focusing on a specific topic such as ML or DL. The fourth column contains a "Yes" if the related survey focuses specifically on cryptography. A "No" in this column indicates a survey discussing all aspects of security, or focusing on a security aspect other than cryptography. The fifth column indicates whether the survey develops an evolutionary path or not. Th sixth column contains a "Yes" only for surveys that develop a future roadmap. The seventh column highlights surveys that discuss the role and the impact of quantum computing.

Table 2. Summary of Existing Surveys.

Survey	Year	Gen. AI	Crypto	Evol.	Roadmap	Quantum
[39]	2021	Yes	No	No	Yes	No
[30]	2021	No	No	No	No	No
[43]	2021	No	Yes	No	No	No
[34]	2020	No	No	No	Yes	No
[48]	2020	Yes	Yes	No	No	Yes
[42]	2020	No	No	No	Yes	No
[44]	2020	Yes	Yes	No	Yes	No
[37]	2020	Yes	No	No	Yes	No
[38]	2020	Yes	No	No	Yes	No
[33]	2020	No	No	No	Yes	No
[40]	2020	No	No	No	No	No
[36]	2020	No	No	No	Yes	No
[47]	2020	No	Yes	No	No	No
[45]	2020	No	Yes	No	No	No
[32]	2020	No	No	No	No	No
[49]	2019	Yes	Yes	No	No	No
[46]	2019	No	Yes	No	No	No
[35]	2019	No	No	No	Yes	No
[41]	2019	No	No	No	No	No
[31]	2010	No	No	No	No	No

2.4. Motivations

As seen in Table 2, although there are some surveys that are in some way relevant to the topic of this paper, none of them provide all the following properties:

- Covering all aspects of AI;
- Focusing specifically on cryptography among all security aspects and controls;
- Establishing an evolutionary path for the studied area;
- Developing a future roadmap;
- Discussing the role of quantum computing in the future of the studied area.

This paper attempted to address the above gap. We studied the evolutionary path of cryptography under the impact of AI, and established a future roadmap focusing on the role of quantum computing.

3. AIUC

In this stage, cryptosystems are unaware of vulnerabilities against AI-based attacks. AIUC can be easily affected by ML and DL attacks. Furthermore, AI models can be used to cryptanalyze cryptographic systems and mechanisms in this stage. Moreover, in this stage, encrypted data and code can be identified by AI models despite the desire of the designer. Figure 3 illustrates this stage.

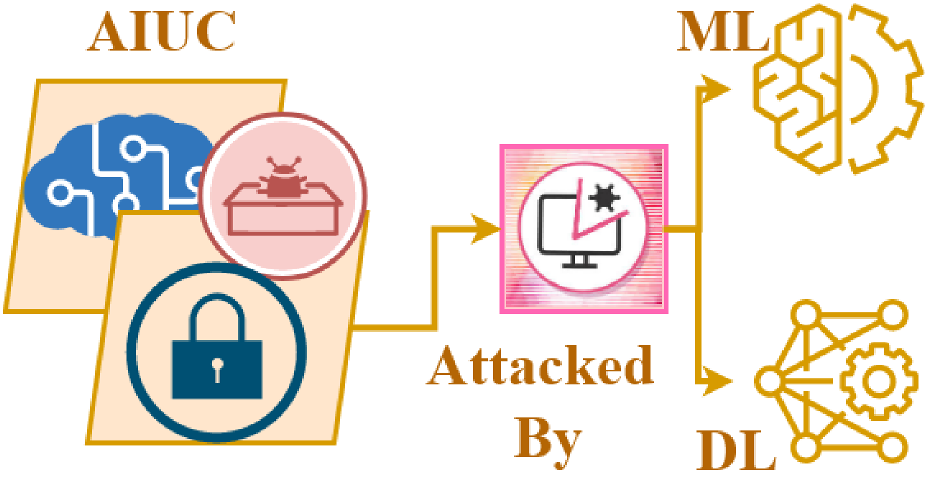

Figure 3. AIUC: Vulnerable to ML and DL Attacks.

In this section, we first present a brief review of encrypted data and code detection using AI (Section 3.1) as well as AI-based attacks against cryptosystems (Section 3.2). Then, we focus on AI-Unaware Physically Unclonable Functions (PUFs) because of their importance (Section 3.3).

3.1. Encryption Detection

In [50], NNs were utilized in a method called Neural Net for Locating Cryptography (NNLC) to classify functional blocks of a disassembled computer program into *Cryptographic* and *Non-Cryptographic*. Detecting encrypted code in malware programs has been of particular interest to the research community. To this end, NNS [51] and DL algorithms [52] have been used by researchers.

3.2. Attack and Cryptanalysis

The authors of [53] employed Convolutional Neural Networks (CNNs) to disclose the secret key of cryptographic circuits. In their method, a Sigmoid function and a step function were used to normalize and classify the power dissipation of the cryptographic circuit to generate the output training data of the CNNs. In another similar research work, NNs were applied to break a feistel type block cipher (a cryptographic method which alternates between confusion and diffusion of it's elements) [54]. Moreover, the authors of [55] showed that signals encrypted by Time Segment Permutation (TSP) can be cryptanalyzed through the hopfield NNs in order to extract intelligible information. This is achieved by looking at the distance between the coefficients of the segments and reordering them through the NN.

3.3. AI-Unaware PUF

In the following, we study AI-based attacks on PUFs. A PUF is an object that generates a random digital output referred to as a *response* serving as a unique identifier for every individual set of input and environmental conditions called *challenge*. A PUF can be uniquely identified by its set of Challenge–Response Pairs (CRPs). PUFs are most often based on natural uncertainties or unique physical variations appearing in semiconductor manufacturing, waves, noises, etc. PUFs are most often implemented by integrated circuits. They are commonly used in applications with high levels of security requirements, including cryptography.

In this subsection, we discuss how AI-based attacks can predict the outcomes of PUFs, individually or along with other kinds of attacks. ML attacks, DL attacks and hybrid attacks are analyzed in the following Sections 3.3.1–3.3.3, respectively.

3.3.1. ML Attacks

In this section, we analyzed the competition between ML attack-resistant PUFs and attacks on PUFs using traditional ML algorithms.

Some PUFs that were stated to have resistances against ML attacks were exposed. The proposed Ring Oscillator Physical Unclonable Function(ROPUF) used configurable XOR gates in the Field Programmable Gate Array [56]. These programmable XOR gates could be used for the selection of ROs during the activation period. After that, selected ROs would create a unique set of sample frequencies. Statics shows that it can only prevent attacks from Logistic Regression-based and SVM-based ML attacks. Furthermore, it failed to prevent attacks from ANNs with almost 90% accuracy for prediction.

Similar structures were shown in the proposed article [57]. It analyzed multiple arbiter PUFs with XOR gates by using NN-based ML attacks. A subspace pre-learner estimated the NN's weights by training on CRP data in subspaces corresponding to PUF components. It demonstrated 98% accuracy for the proposed PUF. However, it requires access to CRP in subspace which is not an easy condition to meet.

Moreover, the approach proposed in [58] used multiple ML attacks on Arbiter PUFs (APUF) on TSMC's 65 nm CMOS process. The CRPs were used again for training as in most attacks. The result shows that it can reach an accuracy of 90% when only 1000 CRPs are used for training. However, if there are two XOR gates APUF, 9000 CRPs are required to achieve an accuracy of 90%. Both results show that APUFs are not secure from modeled ML attacks. In addition, Double Arbiter PUFs (DAPUFs) were claimed to have good resistances against ML attacks. However, a study in [59] shows that they only resist attacks such as SVM but cannot prevent attacks such as NNs.

Some of the research works focus on lightweight PUFs. In this paper [60], two mathematical attack impulses related to the previously proposed light circuits PUF, namely the composite PUF and the Light-output rhythmic Secure PUF (LSPUF), were developed. It was shown that the different PUF components can be used to separate and capture attacks, which can determine the answers to unknown challenges. Using ML-based analysis, the attack complexity was reduced.

Additional techniques were applied to obtain a higher accuracy for the prediction of PUFs' results. An ML technique that uses the Multi-Layer Perceptron (MLP) method was proposed in the article [61]. The method used successfully broke APUFs but not XOR Arbiter PUFs. It was modified in the report with an Adaptive Moment Estimation optimizer for large CRPs. The results revealed at least 98% accuracy when predicting the response. Feed Forward APUFs (FFPUF) possess advantageous properties such as good resistance for ML attacks. They also have low complexity compared to other PUFs. In order to break this PUF, the MLP method was used again [62]. The accuracy for the NNthat using MLP was above 84%. Therefore, it increased accuracy by 16% compared to regular NNs.

Time-Delayed PUFs were also examined by others. For instance, another paper [63] investigated the delay model of the Hardware-Embedded Layout PUF (HELP) and applied ML algorithms to determine resilience to the built-in model. The delay model for HELP includes significant differences compared to other PUFs such as the PUF Arbiter grounded delay, especially with respect to the combined ways in which the response bits are tested.

Some of the studies also focused on examining PUFs' defence capability against ML attacks. Although metric criteria exist to evaluate the quality of PUFs, the most common empirical approaches to assess resistance to ML attacks need to be identified. Ref. [64] introduced the PUFmeter, a new toolbox consisting of publicly available in-house developed algorithms to provide a reliable foundation for robust estimations of PUFs against ML attacks.

3.3.2. DL Attacks

In addition to ML, DL attacks can target PUFs. Some PUFs that were thought to be robust against ML attacks were subsequently broken by DL attacks. For example, a DL attack was proposed and compared with traditional ML attacks based on SVM in [65].

The evaluations demonstrated that the proposed DL attack can achieve an accuracy of 58% compared with 50% for SVM on the target PUF. Moreover, the paper [66] provided an in-depth analysis of fabrication techniques using DL against APUFs. Compared with other traditional ML techniques such as Supported Logistic Regression (SLR) and SVM, the DL results revealed increased prediction accuracy. In a similar work, the authors of [67] conducted and evaluated DL attacks on nonlinear silicon photonic PUFs.

3.3.3. Hybrid Attacks

In addition to ML and DL attacks, the literature outlined some hybrid attacks against PUFs. For example, the authors of [68] proposed a hybrid side channel/ML attack to break the resistance of PUFs against ML attacks. Another hybrid attack was reported in [69], wherein attacks based on CNNs were boosted by side channel attacks. In this proposal, the input challenges of XOR APUFs were utilized by the side channel attack to improve the correlation of CNNs.

4. AIRC

This stage attempts to ensure resilience in cryptosystems against AI-based attacks. In this stage, protective provisions are added to cryptographic systems and mechanisms in the design phase. Figure 4 illustrates this stage and its properties.

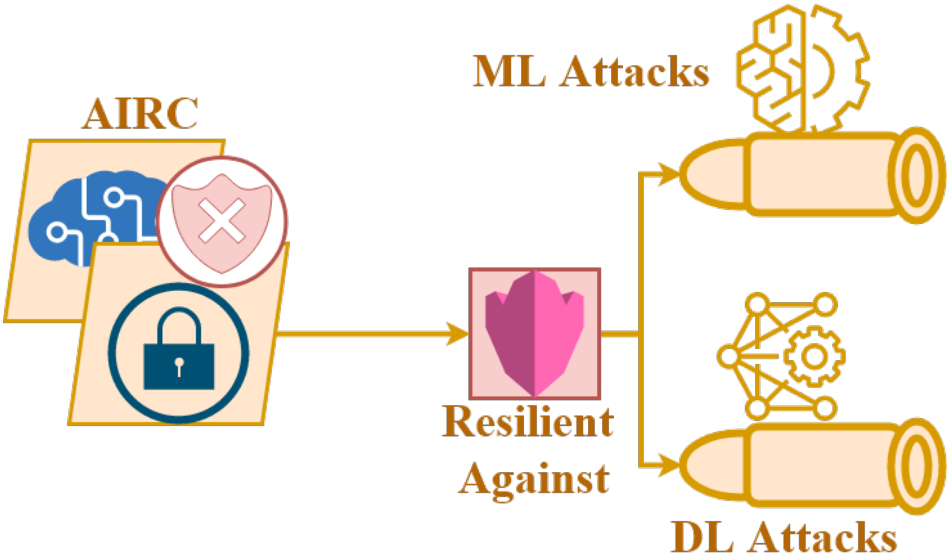

Figure 4. AIRC: Resilient Against ML and DL Attacks.

In the rest of this section, we focus on ML-Resilient PUFs because of the attention they received from the research community.

PUFs Resilient against ML Attacks

In the previous section, we discussed the many ways PUFs can be targeted by ML attacks. This motivated several research works aiming to improve the resilience of PUFs against these attacks.

The authors of [70] proposed a PUF that utilizes the strong nonlinearity of the convergence time of Bistable Rings (BRs) with respect to variations in the threshold voltage. Their simulations returned a prediction accuracy of 50% for SVM in the responses of the proposed PUF. This indicated that SVM cannot perform better than a random guessing algorithm. Another PUF was proposed in [71,72] with the goal of reducing the accuracy of ML attacks to 50%.

The authors of [73] presented a practical smooth-routing PUF authentication procedure in the settings where the server authenticated the device and when the authentication number was limited during the manufacturer's lifetime. The CRPs would not be available for ML attacks in the same way as other PUFs. They would instead be encrypted using protocols to limit their availability.

AN ML-resistant PUF was designed using Linear Feedback Shift Registers (LFSRs) in [74]. The PUF takes n as the challenge from the input and clocks the LFSR n times with no output. In this way, the state of the LFSR is kept unknown to the attacker. At the n-th stage, it would send all the output bits to the APUF.

A Configurable Tristate PUF (CTPUF), proposed in [75], is also resilient to ML attacks. It contains structures from APUF, Configurable RO PUF, BR PUF, to dual-mode PUF. It uses n stages inverters and multiplexers at the front of the design to determine the signal transmission path. According to the path or the position of the response bit, different types of PUF would be used to generate the challenge and response bit. It uses a bitwise XOR obfuscation mechanism to prevent matching between challenging and response pairs for further protection. The complexity of this design makes it more secure than other PUFs. However, it requires more computing power as a tradeoff.

Furthermore, the short function proposed in [76] provides a subtramentive intention-between backed by the relentlessly powerful PUF. The PUF derives its uniqueness from the random mismatch of the threshold voltage with the inverted gate and drain drains and checking in the underground region. The nonlinear current relations in the underground tunnel region of the proposed PUF are also supported by ML resistance (ML) attacks. The prediction accuracy of the PUF response with logistic regression SVM and MLP is close to 51%. The PUF prototype fabricated at 65 nm consumes only 0.3 pJ/bit and achieves the optimum combination of energy efficiency and ML impact resistance.

An Ising-PUF is a PUF that imitates the Ising model originating from the field of physics. A PUF of this type was designed in [77] to be robust against ML attacks. The authors used some small PUFs as spins in the Ising model. Each PUF would send its value as a challenge signal to its adjacent PUFs. The value of the PUFs would be random since they interact with each other. The results demonstrated that it possessed ML resistance due to its chaotic property.

The authors of [71] argued that there is a tradeoff between AM-resistance and error rate. They employed a two-stage non-linear cascaded structure to manage this tradeoff.

Additionally, a stability-aware challenge pruning technique was used in [78] to keep the temperature steady. Similar to two-staged PUFs, the proposed Two-Round SRAM PUF (2SPUF) uses two rounds of implementations for PUFs to reduce the correlation between CRPs. The correlation is key for ML attacks to learn the pattern. Furthermore, SRAM cells would invert the challenge bit to provide more secure and random states.

In another research study reported in [79], responses were generated by the PUF which were then mapped to a polynomial equation for reconstruction. The mapping of CRPs would be random due to these procedures. It can be used to prevent attacks from ML. The error-tolerant variation would be used when performing authentication to increase the stability of the PUF. The result shows that the ML attack only has an accuracy of 60% for the proposed PUF.

Time variables were used in [80] for ML resistance. This research presented a dynamic domain design with an efficient algorithm, namely the Optimal Time Delay Algorithmic (OTPA), to balance the ROPUF CRPs (interval CRPs). CRPs generated using this interval algorithm exhibited a high level of PUF performance in terms of uniqueness and consistency. A similar idea was shown in the proposed algorithm [70], which introduced a new unrelenting Coin FlippingPUF (CF-PUF) that significantly improved resistance against ML attacks. The proposed function utilizes a non-explosive physically strong nonlinearity of ring BRs with respect to threshold voltage variations.

In [81], multiple PUFs were used to form a more complex PUF with more robustness against ML attacks. A current mirror PUF and an APUF were combined to form a PUF that was unpredictable for ML algorithms. The output of the current mirror PUF would be placed into the APUF as an input. The result from this PUF would have Configurable Tristate PUF (CTPUF) $(1616)^{16}$ possible outcomes, which depend on delays and voltage.

This provides more randomness for the PUF circuit. A similar study was reported in [82]. An APUF combined with Ring Oscillators can provide randomness to prevent ML attacks. Responses generated from the APUF would select ring oscillators. Ring oscillators would be compared through frequencies to form final response bits. The result revealed its higher prediction error when using modern ML algorithms as opposed to regular PUF. Furthermore, the authors of [83] proposed a new design for PUF that improved the existing weak PUF to a strong PUF. The goal for the PUF is to have better resistance against ML attacks. It used a 1-bits MPUF design that contained multiple PicoPUFs with one APUF. The output response bit of PicoPUFs would be used as a challenging bit for APUF to increase security. Hamming distance was used again for randomness measurements.

Moreover, a strong subthreshold current counter PUF resilient to ML attacks was proposed in [84]. Similarly, the algorithm proposed in [85] used an output voltages subthreshold array to provide randomness. The array here consisted of unit cells with switch transistors in every one of them. These transistors can have a large variation with respect to voltages. Hamming distance was used to analyze the stability of this PUF. The average BER (temporal stability) in the worst case was only 9%. A similar framework was developed in [86]. In the latter research, a Strong PUF was proposed that uses three subthreshold voltage divider arrays to provide randomness that can resist ML attacks. It uses biases from PUF cells for MOS transistors to generate threshold voltages in a variety of ways. It also allows the PUFs to turn off if there is no work for them to save power. Even with 15,000 training data of CPRs, modern ML techniques such as ANNs can only reach 60% of accuracy.

Furthermore, it was reported that a Novel PUF that simulates a double-layer RRAM array structure can be used to resist ML attacks [87]. The read instability of RRAM cells is the key to maintaining RRAM PUF's stability. The proposed algorithm used the 1-RESET-multi-SET method for the continuous current distribution of the RRAM array. As a result, it would have stable reads but many states. A high-temperature environment was used during the testing process, and it revealed high stability compared to a one-layered RRAM PUF. PUFs can be enhanced with inputs from other systems. In [88], the randomness of intrinsic process-induced variations and the memory turning process were used to construct PUF. It also used time as a variable to expand CRPs size. The results revealed that it can have a pair size of 10^{211} with a 50.3% average uniformity and low energy consumption. It also possessed good resistance to ML attacks.

5. AIB

In this stage, AI models support cryptosystems to improve them in terms of performance, reliability or other design objectives, but not security. Additionally, in this stage of evolution, AI models can be used along with cryptographic mechanisms as auxiliary tools (not as internal components) in security-related scenarios such as authentication and privacy. This stage is demonstrated in Figure 5.

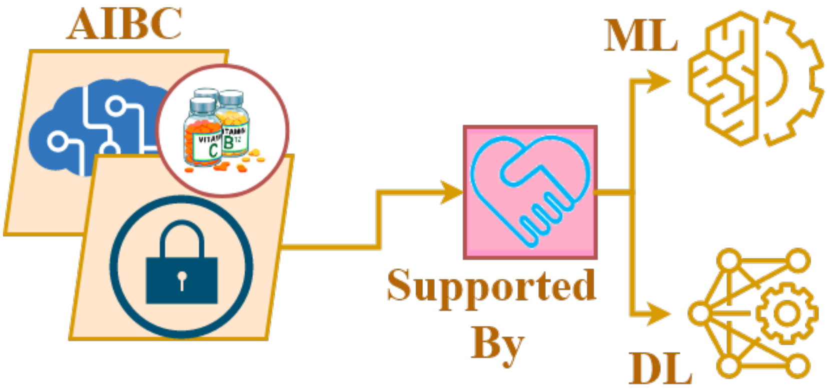

Figure 5. AIBC: Supported by ML and DL.

In the rest of this section, we first discuss the design objectives improved by AI (Section 5.1), and then study the security-related scenarios where cryptosystems have been used along with AI models (Section 5.2).

5.1. Improved Design Objectives

In this subsection, we briefly overview some design objectives in cryptosystems that have been improved with the support of AI.

5.1.1. Performance

In [89], logistic maps were used for text randomization before applying the secret key. This approach along with replacing the encryption process with NN-based chaotic attractors provided an encryption scheme with a performance higher than that of traditional cryptosystems.

5.1.2. Reliability

The authors of [90] improved PUFs in terms of reliability in device authentication and key generation under noisy conditions. A two-step methodology was employed in this research. The acquisition of the parameters of PUF models and utilization of the obtained parameters by ML algorithms as well as CRPs were the main ideas behind the methodology. The experiments demonstrated a notable improvement in reliability.

5.1.3. Signal Quality and Noise Resistance

Some researchers focused on improving signal quality in the output of cryptosystems. For example, in [91], the authors used chaotic NNs to improve the signal quality in the output of signal encryption systems.

Noise immunity is another design objective considered by researchers focusing on AIBC. As an example, the authors of [92] used CNNs to improve the noise resistance of digital signals encrypted using the Rivest–Shamir–Adleman (RSA) cipher. As another example, in [93], Cohen–Grossberg NNs were coupled with the Arnold chaotic map in order to achieve improved noise resistance in colored image encryption. In the method proposed in this research, the image was represented using the Red–Green–Blue (RGB) standard when used as an input to the NN. The pixel matrix for the image is hidden, and the NN is able to store the hidden message as a stable representation. This provides noise cancellation and a secure image encryption mechanism.

5.2. Security-Related Scenarios

AI models have supported cryptosystems in different security-related scenarios. Some of these scenarios are detailed below.

5.2.1. Authentication

In [94], the authors examined improving security in IoT environments through the authentication of wireless nodes using a PUF supported by in situ Machine Learning. The high prediction precision provided by ML algorithms was utilized in this research to mitigate the error issue key generation for authentications.

Furthermore, a novel Multimodal Deep Hashing Neural Decoder (MDHND) architecture was used in multibiometric, error-correcting codes and authentication by the authors of [95]. The MDHND framework is trained via three-stage joint optimization. The first stage is learning to generate a shared multimodal latent code, the second one is using a traditional error-correcting code decoder to obtain data for training a Neural Network Decoder (NND), and the third stage is using data from stage two to train the NND decoder and for the joint optimization of the MDH and NND.

It was previously shown that existing WiMax technology has key security flaws when it comes to wireless functionality. A solution to this problem was proposed in [96] using NNs to generate a pair of secret keys for authentication via neural synchronization.

A study reported in [97] presented PUF signatures to identify a speaker based on a high-level NN structure, which performed wireless node authentication using inherent effects. In this study, the variation in the voice processing properties of wireless broadcasts was detected using in situ ML on the receiver side.

5.2.2. Privacy

TPMs were used by the authors of [98] to achieve privacy-preserving ubiquitous computing with Radio Frequency IDentification (RFID). TPMs are a sort of NNs. In [99], the authors combined NNs with homomorphic encryption schemes aiming at improved privacy.

Moreover, in [100], the authors conducted a Ciphertext Only Attack (COA) to evaluate the privacy of a pixel-based image encryption scheme that utilizes DNNs. They showed that the use of identical encryption keys for different images reduces privacy. These researchers proposed a method for generating different keys for different images. A similar study was reported in [101].

5.2.3. Trust

Reinforcement learning was used in [102] to support decision making for multiple trusted third Parties. PUF-cash mainly functions by leveraging the random and unique statistics properties.

5.2.4. Information Hiding

The application of AIBC in information hiding has been of interest to some researchers. For example, the authors of [103] proposed an NN-based steganography method that is more resistant against steganalysis. In their method, the secret data were encrypted before being embedded in the cover image. Neural networks are used in order to identify the best locations in the cover image to embed the secret data to improve the image quality. In a similar study, steganography methods were combined with Elliptic Curve Cryptography (ECC), and this combination was supported by neural networks.

5.2.5. Visual Cryptography

As an example of research works focusing on AI-boosted visual cryptography, one may refer to [104]. This research proposes an NN-based approach for visual authorization, which is an application of visual cryptography. In the proposed method, the system can visually recognize the authority assigned to a particular user by checking the information carried by the superposed image. A similar study was reported in [105].

6. AIAC

A cryptosystem typically consists of an encryption/decryption engine along with some cryptographic mechanisms and modules such as Random Number Generators (RNGs) and hashing modules. In the AIAC stage, AI is used to support one or more of the cryptographic modules, but not in the encryption/decryption engine. This stage is shown in Figure 6.

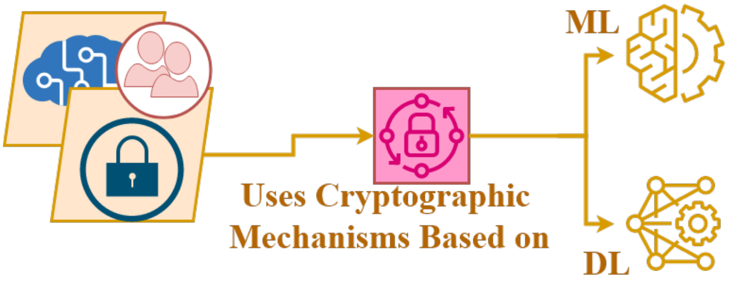

Figure 6. AIRC: Uses Cryptographic Mechanisms Based on ML and DL.

In the following, we discuss the state-of-the-art in AIRC.

6.1. AI-Assisted Key Management

In research reported in [106], NNs were used as part of a key exchange protocol for application in RFID systems. The authors of [107] used key-controlled NNs to enlarge the available key space of a chaotic encryption scheme and add to the protection provided to the chaotic function. It was shown in [108] that the need for a secret key can be eliminated using an NN-technique based on mutual Learning. In the method proposed in this research, the two parties did not have to exchange keys through a public network. Instead, they used neural weights as a secret key when encrypting and decrypting messages. Encryption was performed through the recursive modulo-2 substitution technique.

A challenge with mutual learning is presented in the case of a group key exchange using NNs. This challenge can be resolved using a recursive algorithm that orders the communicating parties in binary trees and uses NNs to communicate the key among them. This was demonstrated in [109]. One can also use reflecting boundaries with mutual learning through NNs as a way to exchange key information over a public channel. Similarly, it was shown in [110] that delays in PUFs can be used to predict response bits with given challenge bits. After training these delays, the third party was able to produce different challenge bits for both users with the same response bit used as a key for them to share messages.

6.2. Neural Hashing

Recurrent Neural Networks (RNNs) [111], Cell Neural Network [112].

In an article [111], the hash value—a fixed-size value— was returned by the cryptographic Hash function. RNN as a possible approach was validated by a software implementation of RNN. The principles of RNN and possibilities of RNN as well as experiment-tested RNNs with three layers on the basis of several examples of general texts were presented. An efficient one-way hash function is a crucial part of modern cryptography research.

A hash function construction based on a cell neural network was proposed with the chaotic sequence generated by a cell neural network using the Runge–Kutta algorithm [112]. Through the transformation of the latter chaos sequence, the hash code was obtained and could be generated from the former hash result.

Previous generations of Hashing algorithms were often deployed in combination with chaotic functions to avoid prediction. However, they revealed vulnerabilities because of the involvement of AI. Combining AI with chaotic functions could introduce more secure hashes and offer resistance to ML attacks.

The most commonly used method is to combine ANNs with hash techniques to ensure greater security. Secure Hash Algorithms (SHA), as the standard of cryptography Hash Functions, helps to provide message integrity, authentication and digital signature. Due to the properties of Chaos and NNs, a new technology based on chaotic NNs was used [113]. By conducting a comparison of these two methods, a new structure of Hash function was presented.

There are also studies that focus on the efficiency of the hashing algorithm. The NNs that were used aimed to speed up the program. The effective generation of the Hash function is a transformation that takes an input and returns a fixed-size value representing the achievement of security in today's networks. The ANN was used for the hash function generation and provided network configuration [114]. Moreover, due to the compact and efficient binary codes of image Hashing, it is often applied to large-scale content-based visual retrieval.

Neural Networks can also be combined with the chaotic function to produce secure hashes. The chaotic function and NNs were used in data encryption due to their cipher-suitable properties, and a hash function based on them was constructed which made use of their advantageous properties. The proposed function [115] encodes the plaintext of arbitrary length into the fixed length, improving security against statistical attacks, birthday attacks, and meet-in-the-middle attacks. Furthermore, the implemented Hash function demonstrated good statistical properties, strong Collision Resistance and High Message

Sensitivity. Furthermore, this proposed algorithm [116] can be used in cryptography, which includes the following two major operations: generation of NN parameters using fast and efficient Chaotic Generator and the iteration of the message through the Chaotic NN. Effective hash functions are the cornerstone of security in today's communication networks. A similar idea was presented in [117], which focused on a theoretical analysis of the possibility of using ANNs and chaotic maps for hashing. ANN could be used to generate a one way hash function. This paper used several testing sets to show the validity of the presented proposal. Similar uses of chaotic maps were apparent in [118]. It proposed a new structure named Keyed Sponge Chaotic Neural Network (KSCNN hash function) based on chaotic maps, NN and sponge construction. The security of the proposed hash function improved after KSCNN. The theoretical analysis and experimental simulations showed that the proposed hash function KSCNN has good statistical properties and strong collision resistance.

6.3. AI-Assisted Random Number Generation

RNGs are of essential importance in cryptography. They can be used for many cryptographic functions. RNGs play an important role in cryptography as random keys and many other types of random objects are of critical use in cryptosystems [119]. RNGs can be divided into two main categories. Pseudo-Random Number Generators (PRNGs) try to generate deterministic sequences of numbers using computer algorithms. In contrast, True Random Number Generators (TRNGs) use uncertainties in electronic circuits or physical phenomena such as waves or noises to create random numbers. The following section discusses how AI assists in the design and evaluation of RNGs.

Design

Designing a PRNG with cryptographic properties is a challenging tasks. Several enabling technologies including AI [120] were used for this purpose.

In order to overcome the shortcomings of SP 800-22 with regard to pseudo random number generation, a pseudo-random binary sequence generator was designed by employing a chaotic NN. This form of PRNG outperforms a PRNG based on Linear Feedback Shift Registers (LFSRs) in terms of randomness and statistical complexity [121].

The chaotic NN based on a Pseudo-Random Sequence Generator (PRSG) leverages a chaotic map coupled with the non-linear complexity of a four-layer NN [122].

Cellular NNs have properties which can be used to create psuedo-random number generation using random properties. A special type of cellular automata can be considered for the generation of random numbers at high speeds (greater than 1000 bits key space) [123]. The current NIST SP 800-22 is a framework that allows for the evaluation of a PRNG but it overlooks statistical biases.

One kind of NN that is used in this area is the Hopfield Neural Network (HNN). These networks networks were used to improve the security of the RNG system. Ref. [124] presents a model for PRNG using HNNs that produced unpredictable outputs under specific circumstances.

A similar idea was shown in [125]; a new pseudo-random number generator was used in the field of secure communications in the proposed article. The novel pseudo-random number generator was based on HNN technology with the output function as the generator of the pseudo-random number.

The quality of the random numbers it generates can meet the requirements of secure communication. Since the HNN is nonlinear, it can be used to improve the traditional random number generator. The study in [126] also proposed a new PRNG model using a non-converging HNN. The results of the study show that the new model was effective because the model passed the National Institute of Standards and Technology (NIST) statistical test and ENT test and was evaluated using random numbers generated by HNN.

Other research also focused on specific objectives. The Elman Neutral Network (ENN) was used in the proposed pseudorandom number generator in [127]. This pseudorandom number generator could generate pseudorandom numbers from the weight matrices obtained from the layer weights of the Elman network. The proposed pseudo random number generator is easy to implement for varying bit sequences, while not computationally demanding. Furthermore, the study [128] focused on demonstrating a new random number generator with adjustable adaptability. It was shown that the standard deviation of the resistance state had a negative correlation with the Compliance Current (CC); an Adaptive RNG (ARNG) can be implemented by controlling CC during the RRAM setup. Additionally, the RRAM-based ARNG can achieve the same performance as the software ARNG. Moreover, the proposed study [129] analyzed the effect of noise sources using error calibration and quantum tomography experiments. An ML model was proposed to predict the optimal quantum gate parameters based on the quantum bit error norm. It can correct up to 88.57% of the deviation in any worst-case quantum bit in real quantum hardware.

There are also studies that focus on the comprehensive view of the RNG algorithm. In [130], a novel and secure RNG architecture was proposed, which is a backward propagation neural network based on the SHA-2 (512) hash function. The SHA-2 (512) hash function guarantees the unpredictability of the generated random numbers. The results revealed that the quality of random numbers generated by the new RNG architecture were able to meet the security of cryptosystems and improve the performance of power, flexibility, cost, and area in network security.

6.4. Attack, Test and Cryptanalysis

AI can be used in not only the design of RNGs, but also in the analysis of the output of RNG and to provide predictions. Moreover, AI can be used to cryaptanalyze RNGs and conduct attacks against them. These applications are discussed below.

6.4.1. Test and Analysis

Testing and analysis of PRNGs is of critical importance, especially in the design of stream ciphers [131]. The authors of [132] compared three ML methods with the goal of identifying the most suitable one for PRNG testing. They used the results of their comparisons to design a testing tool for PRNGs. They showed that their tool can reveal the weaknesses of PRNGs that are wrongly considered as Cryptographically-Secure PRNGs (CSPRNGs).

6.4.2. Cryptanalysis

There are only a few works focusing on the AI-assisted cryptanalysis of PRNGs. Among these works, one may refer to the one published in [131]. In this research, NNs have been leveraged to identify statistical biases in the output of a PRNG through the use of supervised learning. Statistical bias analysis is the very first step in cryptanalysis.

6.4.3. Attack

DL was used in [133] for testing RNGs such as regular ML algorithms. The first deep DL-based side channel attack on an FPGA-implemented TRNG hawas reported in this research. The reported attack successfully leveraged offline statistical tests, online health tests, and countermeasures to monitor the quality of entropy sources at runtime.

6.5. AI-Assisted Cryptographic Arithmetic Module

In [134], the authors introduced a One-Time Pad (OTP) cipher scheme, where the encryption and decryption were asynchronous through the use of NNs. This is achieved through the chaotic series produced by Laguerre chaotic NNs. It is seen to be a strong asynchronous encryption algorithm that overcomes the pitfalls of its synchronous counterparts such as parameter matching and noise interference.

6.6. AI-Assisted Substitution Boxes

Substitution boxes (S-boxes) play critical roles in many cryptosystems [135]. A few researchers investigated the use of AI in the design of S-boxes. For example, the authors of [136] employed a chaotic NN to design a cryptographic S-box.

6.7. AI-Assisted PUF

Several researchers have focused on the design and implementation of AI-assisted PUFs. For example, in [137], the authors used ML in the design of a PUF and demonstrated how the resulting PUF can eliminate IoT requirements. Another AI-assisted PUF was proposed in [138]. The latter PUF makes use of the capabilities of an Extreme Learning Machine (ELMs) to achieve higher levels of configurability.

7. AIEC

This stage incorporated AI capabilities directly in the encryption/decryption engine as illustrated in Figure 7.

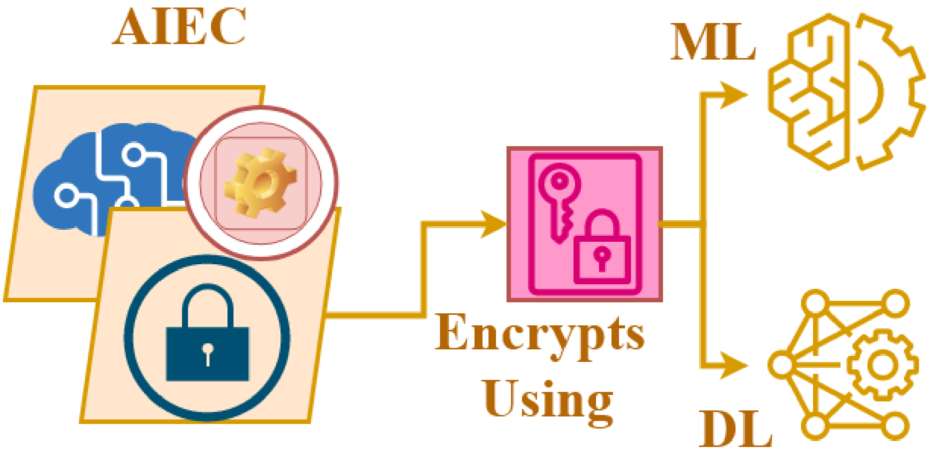

Figure 7. AIRC: Adopts ML and DL for Encryption.

AIEC has received attention in research over recent years [139,140]. AIEC has found its applications in a variety of technological environments [141,142]. In this section, we focus on neural cryptography, especially homomorphic neural cryptography because of its importance.

7.1. Neural Cryptography

Neural cryptography is a cutting-edge cryptographic paradigm, wherein key exchange depends on mutual learning between two different NNs fed by identical input patterns, which update their weights according to predefined rules [143]. It is the most significant trend in the realm of AIEC [144–147]. It has converged with other emerging trends such as chaotic cryptography [148] and DNA cryptography [149]. Neural cryptography has been successfully applied to different content types such as text [149,150] or binary messages [151,152]. In this subsection, we study the current state of neural cryptography.

Neural Encryption can also be used on multimedia applications such as Image Encryption with applications ranging from medicine through to encrypting satellite imaging [153]. This is seen in the Chaos Sequence generated by Cellular NNs and it's application in Encrypting Images.

One such application of this uses block encryption on an image and then strengthens it with a 'radius basis chaotic neural network' [154]. A wavelet based Chaotic Neural Network can be leveraged for image encryption. Specifically, WCNN provides two key security features along with data compression. The first one is the encryption of the image itself and the second is the comparison properties between the scrambled images. WCNN based encryption is strong because similar keys encrypted with different keys have little to no correlation with each other [155].

Furthermore, Cellular NN's chaotic properties can be combined with compressive sensing (which can achieve synchronous compression and encryption) in order to create an encryption algorithm. The measurement matrix for this algorithm is implemented through Lissajous map and is controlled by the index sequence of the CNN. This encryption scheme has a large key space, high key sensitivity and a strong compression system [156].

Image encryption can be accomplished by the Chaotic Dynamics present in the HNNs. The cryptosystem uses chaotic signals generated by the human body which are developed and implemented as FPGA hardware. During testing it was found that the correlation co-efficient for encrypted images with this method was close to zero. thereby proving that it is quite robust [157].

Rather than relying on key exchange, another approach to encrypt digital media using NNs is to use random substitutes and impurity additions onto the image. Once the image is received, ANNs will decrypt the image and extract the original image [158].

The Hermite chaotic NN has impressive application in the area of image encryption—specifically medical imaging [159]. First, the chaotic sequences are created using logistic mapping which is used to train a Hermite chaotic NN. The image is encrypted using two streams of keys generated by the NN. Experiments with this encryption system show a strong algorithm which is resistant to statistical analysis, and has a large key space and good sensitivity [160].

Another way NNs can be used for image encryption is through Memristive bidirectional associative memory neural networks. The model relies on leakage delays and time varying delays; it is used to develop a color image encryption algorithm. This algorithm has a large key space and resists attacks such as brute force and differential attacks [161]. It can also be applied by using an RBG plane where the first stage of this process involves Logistic mapping on all three planes of the image. Then, by using the chaotic functions in NNs present in the Newton–Leipbik chaotic system, the weights for the pixels can be changed and the output of the previous stage is used as the input of this step. This creates a strong encryption system which is resistant to attacks [162].

Image encryption can be accomplished by the Chaotic Dynamics present in HNNs. The cryptosystem uses chaotic signals generated by the human body which are developed and implemented as FPGA hardware. During testing, it was found that the correlation coefficent for encrypted images with this method was close to zero, thereby proving that it is quite robust [157].

Fractional-Order Quantum Neural Networks (QNNs) provide another source for image encryption. This system uses a technique known as the anamorphic fractional Fourier Transformation which increases the leeway offered by the optical cryptosystem. The chaos order/sequence generated from the QCNN is used to provide a complex key space which can be used to encrypt the image and provides robust protection against attacks such as noise and occlusion [163].

Furthermore, combining Hyper Chaotic systems from cellular NNs along with encryption schemes that use Latin squares was shown to provide better security than traditional encryption methods for Grayscale image encryption [164].

Even though synchronization can be archived through the NN synchronization protocol, its performance can still be affected by delays. Asymptotical synchronization of the unbounded delayed inertial NNs model can be used to solve problem of unbounded delay within the synchronization system [165]. The encryption algorithm based on these NNs provides relatively more secure communication since it requires a hybrid input from the response system. Furthermore, NN can be leveraged for image encryption and compression. The middle layer in the NNs can be represented as the compressed image [166]. The compressing process occurs during the transformation from the input layer to the middle layer, and the decompressing process occurs from the middle layer to the output layer. Then, it can XOR with some chaotic functions to enhance security in encryption. There are many types of lag in the synchronization system. It is known that NNs can be applied to perform synchronization for communication. They can also be used to perform lag synchronization [167]. The reason for lag synchronization is because complete synchronization is hard to achieve due to transmission delay. As a result, lag synchronization may be preferred. Switched NNs can be used to solve globally exponential lag synchronization problems by adding an additional controller based on the neuron activation function. These NNs can perform encryptions in the same way as other NNs for synchronization systems. The traditional scrambling–diffusion structure for image encryption separates scrambling and diffusion into two processes and makes them available for hackers to decrypt simultaneously. Strong encryption must exist for both processes to resist decryption from attackers. Neural networks can be applied here with the chaotic function to provide robust and secure encryption for the diffusion process [168].

Another application of NNs in encryption comes with looking at ANNs and key distributions for symmetric encryption. The application of TPM which is a special type of ANN was used to establish a secret key exchange protocol. An interesting point which is to be noted is much of the TPM learning derived from changing the weights of TPM and not changing the inputs. This implies that the key exchange protocol is difficult to decipher [169].

The implementation of chaotic NNs extends to the public key cryptosystem, especially the Diffie–Hellman PKI. There exists a one way function between the chaotic sequence of NNs and the Overstored Hopfield Neural Network (OHNN). The Diffie–Helman public key cryptosystem can be implemented with changes in the synaptic matrix and changes of OHNN with the private key being the permutation operation of the synaptic matrix and the public key being the neural synaptic matrix after the permutation [170].

Another way NNs can be used as an encryption system is through the time delays between different neurons in the original data. This form of encryption has a wide array of applications ranging from using it as a one way function to generate a public key from a private one to using it as an encryption mechanism for communication between two entities [171].

Clipped Hopfield Neural Network (CHNN) and multivariate cryptography can also be used for a public key cryptography system [172].

Symmetric key cryptography can use genetic algorithms and an Error back propogration neural network to encrypt and decrypt data. The encryption process uses the GA while the decryption process uses EP-NN which is a commonly used for supervised learning NNs. The time complexity for this algorithm is significantly less than that of Advanced Encryption Standard (AES), Data Encryption Standard (DES) and RSA [173].

The chaos property of ANNs can also be used to encrypt digital video transmission. One encryption algorithm from chaotic NN uses MPEG-2 video codec standard to change the audio–visual video data into an encrypted form [174,175]. The encrypted data are then transmitted to the destination using the OFDM modulation technique. The creation of a cipher based on the chaotic NN property reveals an interesting characteristic where the control parameter must be close to 4 [174]. Otherwise, the cipher system does not possess sufficient chaotic properties which can lead to crypt-analytic vulnerability. Another way this can be achieved is through the binary sequence that is generated via the chaotic system along with the biases and weights that are set. This, in combination with the VLSI architecture, can create an encryption method which has the following characteristics: high security, limited distortion and suitability for digital integration.

The noise-like chaotic properties of ANN can also be used for signal encryption using time-series generation and hash-value generation. These can be fused with the ANN and the chaotic sequences to create a signal digital envelope which has a secret key and a hash value associated with it [176,177].

Delayed NNs can be applied in the master–slave synchronisation field. Specifically, they can be deployed where network and controller modes are asynchronous and a memory asynchronous control allows for a solution to the outer synchronization problem. The verifiability of this is seen through chaotic-like NNs and their application to encryption [178].

Memristor-Based BAM Neural Networks are widely used in synchronization system. They can also be applied to encryption processes because of their chaotic property [179].

With the efficiency of key generation and high development ability of NNs, many communication systems use NNs to achieve secure communication networks. An NN can provide system synchronization and the encryption process [180]. Furthermore, it can be made more secure by combining a hyper-chaotic function with the NN. A hyper-chaotic system would require at least 4Di chaotic functions, which the NN can quickly obtain. The encryption process from the hyper-chaotic NN would provide even more secure communication. Impulsive synchronization can be achieved using two reaction–diffusion NNs [181]. The networks can be combined with the Lyapunov function to ensure less conservative criteria compared to the regular impulsive synchronization system. Similarly to other NNs in synchronization, reaction–diffusion NNs can also provide encryption and decryption while synchronizing computers. We mentioned the Memristor-Based Neural Networks above, which can be used for synchronization systems. Now, they can become be more powerful as they can be improved for finite-time synchronization [182]. They can perform synchronization with time-varying delays and distributed delays to guarantee the synchronization time in a finite time. The delays algorithm would be integrated into the NN to perform synchronization and encryption. Traditional time-triggered communication systems with data-sampled control would send additional sampled data that are unnecessary. The event-triggered communication system can prevent the problem of wasting limited bandwidth due to its properties [183]. It only transmits data when the event condition is met. Inertial Neural Networks(INNs) can be used to construct this communication system with an additional Markovian function and reaction–diffusion terms.

Information security has three basic tenets to protect the following: confidentiality, integrity and availability. The current state of cryptography looks at how to protect confidentiality through the use of crypto-graphic systems. One of the newest fields of study is cellular NNs/Cellular Automata and how to use them in cryptography [184–186].

With the significant amount of work being produced in this field, there are two main types of NNs at play, namely Feed Forward Neural Networks (FFNNs) and RNNs. The techniques employed in cryptography for NNs include using sequential machines and employing a chaotic NN [187–189].

Artificial neural networks can be trained to decrypt ciphertext that is created by random encryption algorithms. The pseudorandom mapper is used in conjunction with garbage values at random positions to encrypt the image. The ANN is then able to identify the garbage values and decrypt the messages [190].

An interesting proposition is combining the AES encryption algorithm with NNs. This encryption scheme is based on looking at the weights of synaptic connections in NNs as the bases for input images. This approach provides a constant key rotation which increases the cryptography complexity required to break the encryption [191].

Chaotic properties of NNs can further be used to generate S-boxes which are cryptographically strong and secure NNs can be leveraged to detect ciphers which use the same key. RNNs were shown to have reduced learning abilities when the confusion and diffusion parameters of the cryptographic system were strong [192].

With a comparison having been performed between AES and chaotic NNs, it was found that chaotic NNs were more suitable for encrypting shorter plaintexts while AES was more efficient at encrypting larger plaintexts [193].

A symmetric cryptography system was created through the use of CNNs and was compared with AES symmetric cryptography. The CNN cryptosystem has potential for encrypting small file sizes but its susceptibility to attacks has not yet been confirmed [194].

The cryptosystem can be improved by adding noise/random bits into the ciphertext which can only be caught and decrypted by the end user. This foils many of the attacks where the attacker can feed the ciphertext into the NN to try and extract the key [195].

While chaotic NNs use binary inputs for the training of their models, using Auto Associative neural networks can create a strong encryption algorithm by using a bipolar input instead [196]. The input pattern is deemed known if and only if there is an output that is the same as the input for this pattern. The auto associative NNs are used to encrypt plaintext into ciphertext where the relation between different ciphertexts is independent.

Another way NNs can be used as an encryption system is through the time delays between different neurons in the original data [171]. This form of encryption has a wide array of applications ranging from using it as a one way function to generate a public key from a private one to using it as an encryption mechanism for communication between two entities. Moreover, a Generalized Synchronization Network is a kind of NN that can be thought of as a discrete time array. The GSDTAE can design a encryption scheme with an OTP. Through this, we were successfully able to encrypt and decrypt the original information with a large key space [197].

The resilience of ANNs can be measured when sensitive Intellectual Properties are stored in the system [198]. It is known that the weight in NNs is unpredictable without knowledge about the training data. As a result, it could be a valid key for encryption and decryption. RNNs can be used to produce keys and to provide Cipher Block-Chaining (CBC) mode encryption [199]. It takes the first output (ciphertext) of the NN and places it back as part of the input for the second plaintext. The same implementation was also shown in [200].

Furthermore, NNs consume a large amount of energy under the current von-neumman architecture due to the presence of a memory wall. In order to rectify this, Non-Volatile Memory (NVM) systems are seen as an alternative but they are susceptible to confidentiality attacks where the attacker can steal the NN model. With little performance overhead, a Sparse Fast Gradient Encryption (SFGE) method coupled with Runtime Encryption Scheduling (RES) can be used to secure the confidentiality of NNs. This can help mitigate the AI hardware-based attacks with a strong encryption scheme [201].

One method to leverage NNs in order to encrypt and decrypt text messages is the use of Auto Encoder Neural Networks (AENNs). An AENN is an FFNN which can be used for unsupervised learning where the input can also be the output. By leveraging the encryption scheme, key generation becomes extremely secure because for every training set it produces a different key. Therefore, for the same plaintext a different ciphertext is produced [56]. Real-time RNN-based ciphers can be employed to secure the transfer of mobile ad hoc networks through the use of a Multi-Path Routing Scheme. The steps involved in this process include message encryption through the use of RRNN symmetric cipher, message routing through multi-path DSR and message decryption with the RRNN-SC. This system helps address many of the underlying issues of confidentiality, integrity and access control currently experienced with Mobile Adhoc NETworks (MANETs). Looking at the Fast Handover protocol, which is usually in effect when a mobile router from a previous access point connects to a new one, it can be seen that it is susceptible to DOS and Masquerading attacks. In order to combat this, NNs can be used by leveraging their property of mutual learning. The Two parties communicating with each other use a TPM and the key generated is the synchronized weights of the two entities. This provides a better communication system than the proposed solutions of using PKI or Diffie–Helman because of their slowness and lack of efficiency [202].

An HNN encryption scheme can be used to encrypt text-messages. Then, in order to bolster security, a DNA cryptography model can be used [149].

Security of Neural Cryptography

Interestingly, side channel attacks can be curbed through the use of Tree Parity Machine Public Key Exchanges (TPMPKE) [203]. Neural Synchronization looks at the communication of two TPMs to establish a secret key via an open channel. Once this is successfully established, it is highly resistant to the majority flipping attack by a cooperating attacker.

The security of neural cryptography can be compromised if there are multiple cooperators that work together to decrypt the exchange key using their own NNs [185].

Symmetric ciphers based on real-time RNNs can be subject to Chosen Plaintext Attacks (CPA). If the adversary has access to arbitrary amounts of plaintext and can generate the ciphertext for them: the resulting input and output can be fed into an NN and the key can be discovered [204].

Neural Cryptography protocols can be attacked using a technique known as 'power analysis'. This protocol is weak against this attack where the power can trace the information which is exploited [205]. A counter measure is sending Erroneous information which can be transmitted in order to deceive the attacker listening to the communication about the content of the information.

7.2. Homomorphic Neural Cryptography

Homomorphic encryption is a recent trend in cryptography [206–208]. Homomorphic encryption allows trusted third parties to process encrypted data without knowledge of the data. Data can be encrypted before transmission. A Fully Homomorphic Encryption (FHE) scheme would allow people to perform any arbitrary manipulation on encrypted data such as addition or multiplication at the same time. This section studies how AI-based techniques, specifically NNs, could be used to enhance homomorphic encryption.

The authors of [209] argued that homomorphic encryption is susceptible to errors because of the calculations performed by the algorithm in each step. They attempted to solve this problem by separating the computational operations while encrypting and decrypting the data at each stage. Combining this with NNs provides a robust encryption algorithm that minimizes the errors and offers a strong encryption system.

Further, the authors of [210] firstly argued that the complexity caused by a modification in encrypted data increases the difficulty of the implementation of FHE. In their method, noises would be added to the plaintext at the time of encryption using NNs. It would be hard to predict/evaluate when the modification procedures also modify the noise. Secondly, they argued that it takes a lot of time and computing power to perform decryption through bootstrapping. One possible solution is to limit the time of modification for the encrypted data.

While FHE is still in progress, Partial Homomorphic Encryption (PHE) can be implemented in real-world applications. The Paillier encryption algorithm, as a PHE algorithm, was used in [211] with the support of DNNs for face recognition.

8. Future Roadmap: The Promise of Secure AI

We anticipate that research on AIIC will move towards quantum-inspired AIIC in the near future. Our reason for this belief is the existence of trends in quantum-inspired AI and its use in cryptography, which are discussed in Sections 8.1 and 8.2, respectively.

8.1. Quantum-Inspired AI

In this section, we provide insights into quantum-inspired AI. The capacities of quantum computing can be adopted by AI to perform learning techniques. We analyze how the capabilities of quantum computing would improve the learning performance of AI.

A study reported in [212] presented a Quantum-inspired Reinforcement Learning (QiRL) solution to the problem of Unmanned Aerial Vehicle (UAV) trajectory planning. This QiRL used a novel collapse behavior selection strategy inspired by quantum mechanics, which provided a natural balancing approach for exploration and development by ranking the collapse probabilities of different behaviours. The proposed QiRL method was proven to be effective, and the proposed method was shown to be capable of balancing convergence speed and learning quality better than the traditional Q-learning method.

Moreover, an algorithm for navigation control of autonomous mobile robots was presented in [213] using QiRL. In quantum information retrieval, probabilistic behavior selection and probabilistic enhancement strategies were applied, which were influenced by the amplitude amplification and collapse phenomenon of quantum measurements and computation. Several simulation experiments on the Markov state transfer revealed that QiRL was more robust in terms of learning rate and the initial state than traditional reinforcement learning. Simulations and experimental results demonstrated the effectiveness of the QiRL-based navigation control method when applied to a real mobile robot.

Another study proposed a Quantum Fuzzy Neural Network (Q-FNN) classifier that was able to solve the overlapping sample classification problem [214]. According to empirical results, Q-FNN outperforms existing classifiers in terms of classification accuracy. The model used a tenfold cross-verification scheme, and generated accurate results. In a second experiment, the classification model proposed was applied to 11 of 15 state-of-the-art datasets. Another study also aimed to develop a framework for Deep Reinforcement Learning (DRL) supported by quantum computation based on the results of an empirical replay [215].

Furthermore, self-convergent iterative learning model algorithms were notably improved using quantum computing in [216]. Quantum-inspired Hopfield Associative Memory (QHAM) demonstrated quantum information processing in neural structures. In this study, a new Quantum-inspired Multidirectional Association Model was introduced (QMAM), combining one-off learning and self-convergent iterative learning methods. The simulation results show that the proposed model was of acceptable stability, memory capacity and recall reliability.

8.2. (Quantum-AI)-Supported Cryptography

Recently, neural cryptography and quantum cryptography were combined by some researchers [217]. We refer to this combination as *(quantum-AI)-supported cryptography*. Quantum-supported AI was used for image encryption in [163]. Furthermore, ML was used for the cryptanalysis of Quantum Random Number Generators (QRNGs) [218]. Moreover, the authors of [219] showed how ANNs can be leveraged to assist error correction within quantum cryptography. This can be performed using partially-synchronized NNs and TPMs that work with weights randomly generated for the NN. In [220], another cryptosystem was devised that caused two NNs to exchange the ciphertexts (in qubits) with the key being synchronized by both parties. This system relies on multilayer qubits combined with a back-propagation algorithm.

Figure 8 illustrates our predictions for the future of AIIC.

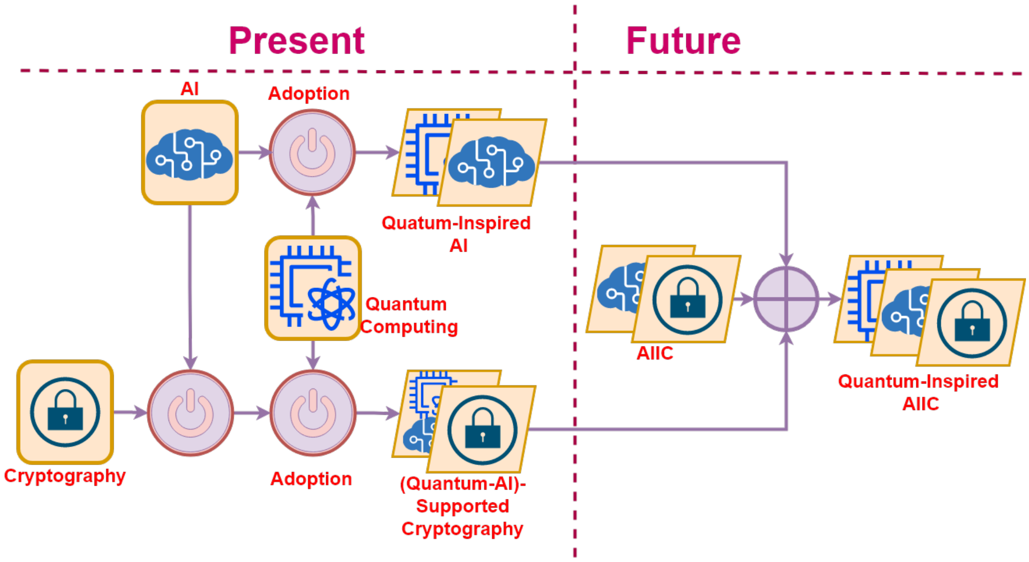

Figure 8. The Future of AIIC.

9. Conclusions and Further Works

The recent literature revealed strong crossimpact between AI and cryptography, indicating great promise for both. Crossimpact creates a dichotomy in the context of which, the two technologies coevolve. The evolution of AI under the impact of cryptography was studied in previous research works. This research was an attempt to provide a comprehensive perspective on the evolution of cryptography under the impact of AI. We identified five stages on the evolutionary path of AI-Influenced Cryptography (AIIC), namely AI-Unaware Cryptography (AIUC), AI-Resilient Cryptography (AIRC), AI-Boosted Cryptography (AIBC), AI-Assisted Cryptography (AIAC) and AI-Embedded Cryptography (AIEC). We observed that going through these stages, cryptosystems not only learn to protect themselves against AI-based attacks, but also use the capabilities of AI to improve security, performance, etc. Moreover, they learn to take advantage of AI's capabilities in different security-related scenarios and different internal modules. We also took a look at what the future may hold for AIIC given the role of quantum computing in current trends of research on AI.

Our work presented in this paper can be built upon in the following ways:

- Investigating challenges and applications of AIIC;
- Developing a taxonomy, an ecosystem or a life cycle for AIIC;
- Studying the impact of bio computing on the future of AIIC given its impact on current trends in AI as well as cryptography;
- Providing a look-ahead at the future of Crypto-Influenced AI (CIAI) with a focus on the role of bio computing;
- Anticipating the role of information theory in future AI, and consequently on the future of both AIIC and CIAI;
- Investigating the coevolution of AI and blockchain.

Author Contributions: T.K. has contributed to the review. B.Z. has contributed in review, writing and preparation. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

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

References

1. Yu, M.; Yao, H.; Qin, C.; Zhang, X. A Comprehensive Analysis Method for Reversible Data Hiding in Stream-Cipher-Encrypted Images. *IEEE Trans. Circuits Syst. Video Technol. Early Access Artic.* **2022**, 1. [CrossRef]
2. Teranishi, K.; Sadamoto, T.; Chakrabortty, A.; Kogiso, K. Designing Optimal Key Lengths and Control Laws for Encrypted Control Systems based on Sample Identifying Complexity and Deciphering Time. *IEEE Trans. Autom. Control. Early Access Artic.* **2022**, 1. [CrossRef]
3. Vo, V.; Yuan, X.; Sun, S.; Liu, J.K.; Nepal, S.; Wang, C. ShieldDB: An Encrypted Document Database with Padding Countermeasures. *IEEE Trans. Knowl. Data Eng. Early Access Artic.* **2021**, 1. [CrossRef]
4. Parida, P.; Pradhan, C.; Gao, X.Z.; Roy, D.S.; Barik, R.K. Image Encryption and Authentication With Elliptic Curve Cryptography and Multidimensional Chaotic Maps. *IEEE Access* **2021**, *9*, 76191–76204. [CrossRef]
5. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Khalil, A.; Hasbullah, I.H. Security and Privacy Schemes in Vehicular Ad-Hoc Network With Identity-Based Cryptography Approach: A Survey. *IEEE Access* **2021**, *9*, 121522–121531. [CrossRef]
6. Xiong, L.; Han, X.; Yang, C.N.; Shi, Y.Q. Robust Reversible Watermarking in Encrypted Image with Secure Multi-party based on Lightweight Cryptography. *IEEE Trans. Circuits Syst. Video Technol. Early Access Artic.* **2021**, *32*, 75–91. [CrossRef]
7. Li, F.; Liu, K.; Zhang, L.; Huang, S.; Wu, Q. EHRChain: A Blockchain-based EHR System Using Attribute-Based and Homomorphic Cryptosystem. *IEEE Trans. Serv. Comput. Early Access Artic.* **2021**, 1. [CrossRef]
8. Chen, D.; Wang, H.; Zhang, N.; Nie, X.; Dai, H.N.; Zhang, K.; Choo, K.R. Privacy-Preserving Encrypted Traffic Inspection with Symmetric Cryptographic Techniques in IoT. *IEEE Internet Things J. Early Access Artic.* **2021**, 1. [CrossRef]
9. Zhou, Y.; Hu, Z.; Li, F. Searchable Public-Key Encryption with Cryptographic Reverse Firewalls for Cloud Storage. *IEEE Trans. Cloud Comput. Early Access Artic.* **2021**, 1. [CrossRef]

10. Zolfaghari, B.; Koshiba, T. Chaotic Image Encryption: State-of-the-Art, Ecosystem, and Future Roadmap. *Appl. Syst. Innov.* **2022**, *5*, 1–38. [CrossRef]
11. Zolfaghari, B.; Bibak, K.; Koshiba, T. The Odyssey of Entropy: Cryptography. *Entropy* **2022**, *24*, 266. [CrossRef]
12. Zolfaghari, B.; Singh, V.; Rai, B.K.; Bibak, K.; Koshiba, T. Cryptography in Hierarchical Coded Caching: System Model and Cost Analysis. *Entropy* **2021**, *23*, 1459. [CrossRef]
13. 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]
14. Zolfaghari, B.; Bibak, K.; Nemati, H.R.; Koshiba, T.; Mitra, P. *Statistical Trend Analysis on Physically Unclonable Functions: An Approach via Text Mining*; CRC Press: Boca Raton, FL, USA, 2021.
15. Sun, Y.; Lo, F.P.W.; Lo, B. Light-weight Internet-of-Things Device Authentication, Encryption and Key Distribution using End-to-End Neural Cryptosystems. *IEEE Internet Things J. Early Access Artic.* **2021**, 1. [CrossRef]
16. Ding, Y.; Tan, F.; Qin, Z.; Cao, M.; Choo, K.K.R.; Qin, Z. DeepKeyGen: A Deep Learning-Based Stream Cipher Generator for Medical Image Encryption and Decryption. *IEEE Trans. Neural Netw. Learn. Syst. Early Access Artic.* **2021**, 1. [CrossRef]
17. Dai, S. Quantum Cryptanalysis on a Multivariate Cryptosystem Based on Clipped Hopfield Neural Network. *IEEE Trans. Neural Netw. Learn. Syst. Early Access Artic.* **2021**, 1–5. [CrossRef]
18. Olaniyan, R.; Maheswaran, M. A Fast Edge-Based Synchronizer for Tasks in Real-Time Artificial Intelligence Applications. *IEEE Internet Things J. Early Access Artic.* **2021**, *9*, 3825–3837. [CrossRef]
19. Wen, S.; Rios, A.; Ge, Y.; Itti, L. Beneficial Perturbation Network for Designing General Adaptive Artificial Intelligence Systems. *IEEE Trans. Neural Netw. Learn. Syst. Early Access Artic.* **2021**, 1–14. [CrossRef]
20. Mühlroth, C.; Grottke, M. Artificial Intelligence in Innovation: How to Spot Emerging Trends and Technologies. *IEEE Trans. Eng. Manag. Early Access Artic.* **2020**, *69*, 493–510. [CrossRef]
21. Lai, H.; Lee, S. The Application of Artificial Intelligence and VR Technology in Clothing Store Display Design. *IEEE Access Early Access Artic.* **2020**, 1. [CrossRef]
22. Stock, S.; Babazadeh, D.; Becker, C. Applications of Artificial Intelligence in Distribution Power System Operation. *IEEE Access Early Access Artic.* **2021**, *9*, 150098–150119. [CrossRef]
23. Letaief, K.B.; Shi, Y.; Lu, J.; Lu, J. Edge Artificial Intelligence for 6G: Vision, Enabling Technologies, and Applications. *IEEE J. Sel. Areas Commun. Early Access Artic.* **2021**, *40*, 5–36. [CrossRef]
24. Zolfaghari, B.; Koshiba, T. The Dichotomy of Neural Networks and Cryptography: War and Peace. *Appl. Syst. Innov.* **2022**, *5*, 1–28. [CrossRef]
25. Zolfaghari, B.; Rabieinejad, E.; Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A. Crypto Makes AI Evolve. *arXiv* **2022**, arXiv:2206.12669.
26. Zhang, C.; Yu, Y.; Wang, Y.; Han, Z.; Zhou, M. Chaotic Neural Network-Based Hysteresis Modeling With Dynamic Operator for Magnetic Shape Memory Alloy Actuator. *IEEE Trans. Magn.* **2021**, *57*, 1–4. [CrossRef]
27. Cui, Z.; Chen, Z.H.; Zhang, Q.; Gribova, V.V.; Filaretov, V.F.; Huang, D.S. RMSCNN: A Random Multi-Scale Convolutional Neural Network for Marine Microbial Bacteriocins Identification. *IEEE/ACM Trans. Comput. Biol. Bioinform. Early Access Artic.* **2021**, 1. [CrossRef] [PubMed]
28. Cho, K.; Miyano, T. Chaotic Cryptography Using Augmented Lorenz Equations Aided by Quantum Key Distribution. *IEEE Trans. Circuits Syst. Regul. Pap.* **2015**, *62*, 478–487. [CrossRef]
29. Feng, Y.; Wu, J.; Zhan, X.; Liu, J.; Sun, Z.; Zhang, J.; Kobayashi, M.; Chen, J. A Novel Encrypted Computing-in-Memory (eCIM) by Implementing Random Telegraph Noise (RTN) as Keys Based on 55 nm NOR Flash Technology. *IEEE Electron Device Lett. Early Access Artic.* **2022**, *69*, 1698–1705.
30. Buczak, A.L.; Guven, E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Commun. Surv. Tutorials* **2016**, *18*, 1153–1176. [CrossRef]
31. Boulgouris, N.V.; Plataniotis, K.N.; Micheli-Tzanakou, E. A Comparative Survey on Biometric Identity Authentication Techniques Based on Neural Networks. In *Biometrics: Theory, Methods, and Applications*; Boulgouris, N.V., Plataniotis, K.N., Micheli-Tzanakou, E., Eds.; Wiley-IEEE Press: Hoboken, NJ, USA, 2010; Chapter 3, pp. 47–79.
32. Vinayakvitthal, L.; Charniya, N.N. Review of advances in Neural Network based biometric authentication. In Proceedings of the International Conference on Communications and Signal Processing (ICCSP), Melmaruvathur, India, 2–4 April 2015.
33. Dibaei, M.; Zheng, X.; Xia, Y.; Xu, X.; Jolfaei, A.; Bashir, A.K.; Tariq, U.; Yu, D.; Vasilakos, A.V. Investigating the Prospect of Leveraging Blockchain and Machine Learning to Secure Vehicular Networks: A Survey. *IEEE Trans. Intell. Transp. Syst. Early Access Artic.* **2021**, *23*, 683–700. [CrossRef]
34. Alimi, O.A.; Ouahada, K.; Abu-Mahfouz, A.M. A Review of Machine Learning Approaches to Power System Security and Stability. *IEEE Access* **2020**, *8*, 113512–113531. [CrossRef]
35. Hossain, E.; Khan, I.; Un-Noor, F.; Sikander, S.S.; Sunny, M.S.H. Application of Big Data and Machine Learning in Smart Grid, and Associated Security Concerns: A Review. *IEEE Access* **2019**, *7*, 13960–13988. [CrossRef]
36. Singh, S.; Sulthana, R.; Shewale, T.; Chamola, V.; Benslimane, A.; Sikdar, B. Machine Learning Assisted Security and Privacy Provisioning for Edge Computing: A Survey. *IEEE Internet Things J. Early Access Artic.* **2021**, *9*, 236–260. [CrossRef]

37. Zaman, S.; Alhazmi, K.; Aseeri, M.A.; Ahmed, M.R.; Khan, R.T.; Kaiser, M.S.; Mahmud, M. Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey. *IEEE Access* **2021**, *9*, 94668–94690. [CrossRef]
38. Wu, H.; Han, H.; Wang, X.; Sun, S. Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey. *IEEE Access* **2020**, *8*, 153826–153848. [CrossRef]
39. Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.K.; Du, X.; Ali, I.; Guizani, M. A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. *IEEE Commun. Surv. Tutorials* **2020**, *22*, 1646–1685. [CrossRef]
40. Uprety, A.; Rawat, D.B. Reinforcement Learning for IoT Security: A Comprehensive Survey. *IEEE Internet Things J.* **2021**, *8*, 8693–8706. [CrossRef]
41. Shaukat, K.; Luo, S.; Varadharajan, V.; Hameed, I.A.; Xu, M. A Survey on Machine Learning Techniques for Cyber Security in the Last Decade. *IEEE Access* **2020**, *8*, 222310–222354. [CrossRef]
42. Hadke, P.P.; Kale, S.G. Use of Neural Networks in cryptography: A review. In Proceedings of the World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), Coimbatore, India, 29 February–1 March 2016.
43. Meraouche, I.; Dutta, S.; Tan, H.; Sakurai, K. Neural Networks-Based Cryptography: A Survey. *IEEE Access* **2021**, *9*, 124727–124740. [CrossRef]
44. Blackledge, J.; Mosola, N. Applications of Artificial Intelligence to Cryptography. *Trans. Mach. Learn. Artif. Intell.* **2020**, *8*, 21–60. [CrossRef]
45. Su, J.; Kankani, A.; Zajko, G.; Elchouemi, A.; Kurniawan, H. Review of Image encryption techniques using neural network for optical security in the healthcare sector—PNO System. In Proceedings of the 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA), Sydney, Australia, 25–27 November 2020.
46. Alani, M. Applications of Machine Learning in Cryptography: A Survey. *arXiv* **2019**, arXiv:1902.04109v1.
47. Sooksatra, K.; Rivas, P. A Review of Machine Learning and Cryptography Applications. In Proceedings of the International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 16–18 December 2020.
48. ÖzÇakmak, B.; ÖzbIlen, A.; YavanoGlu, U.; CIn, K. Neural and Quantum Cryptography in Big Data: A Review. In Proceedings of the IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 9–12 December 2019.
49. Nassif, A.B.; Talib, M.A.; Nasir, Q.; Albadani, H.; Dakalbab, F.M. Machine Learning for Cloud Security: A Systematic Review. *IEEE Access* **2021**, *9*, 20717–20735. [CrossRef]
50. Wright, J.L.; Manic, M. Neural network approach to Locating Cryptography in object code. In Proceedings of the IEEE Conference on Emerging Technologies & Factory Automation, Palma de Mallorca, Spain, 22–25 September 2009.
51. Jia, L.; Zhou, A.; Jia, P.; Liu, L.; Wang, Y.; Liu, L. A Neural Network-Based Approach for Cryptographic Function Detection in Malware. *IEEE Access* **2020**, *8*, 23506–23521. [CrossRef]
52. Pastor, A.; Mozo, A.; Vakaruk, S.; Canavese, D.; López, D.R.; Regano, L.; Gómez-Canaval, S.; Lioy, A. Detection of Encrypted Cryptomining Malware Connections With Machine and Deep Learning. *IEEE Access* **2020**, *8*, 158036–158055. [CrossRef]
53. Yu, W. Convolutional neural network attack on cryptographic circuits. *Electron. Lett.* **2019**, *55*, 246–248. [CrossRef]
54. Albassal, A.; Wahdan, A.M. Neural network based cryptanalysis of a feistel type block cipher. In Proceedings of the International Conference on Electrical, Electronic and Computer Engineering, Cairo, Egypt, 5–7 September 2004.
55. Apolinario, J.; Mendonca, P.; Chaves, R.; Caloba, L. Cryptanalysis of speech signals ciphered by TSP using annealed Hopfield neural network and genetic algorithms. In Proceedings of the the 39th Midwest Symposium on Circuits and Systems, Ames, IA, USA, 18–21 August 1996.
56. Kumar, S.; Niamat, M. Machine Learning based Modeling Attacks on a Configurable PUF. In Proceedings of the IEEE National Aerospace and Electronics Conference, Dayton, OH, USA, 23–26 July 2018.
57. Aseeri, A.O.; Zhuang, Y.; Alkatheiri, M.S. A Subspace Pre-learning Approach to Fast High-Accuracy Machine Learning of Large XOR PUFs with Component-Differential Challenges. In Proceedings of the IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 10–13 December 2018.
58. Hospodar, G.; Maes, R.; Verbauwhede, I. Machine learning attacks on 65 nm Arbiter PUFs: Accurate modeling poses strict bounds on usability. In Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS), Costa Adeje, Spain, 2–5 December 2012.
59. Alamro, M.A.; Zhuang, Y.; Aseeri, A.O.; Alkatheiri, M.S. Examination of Double Arbiter PUFs on Security against Machine Learning Attacks. In Proceedings of the IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 9–12 December 2019.
60. Sahoo, D.P.; Nguyen, P.H.; Mukhopadhyay, D.; Chakraborty, R.S. A Case of Lightweight PUF Constructions: Cryptanalysis and Machine Learning Attacks. *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **2015**, *34*, 1334–1343. [CrossRef]
61. Aseeri, A.O.; Zhuang, Y.; Alkatheiri, M.S. A Machine Learning-Based Security Vulnerability Study on XOR PUFs for Resource-Constraint Internet of Things. In Proceedings of the IEEE International Congress on Internet of Things (ICIOT), San Francisco, CA, USA, 2–7 July 2018.
62. Alkatheiri, M.S.; Zhuang, Y. Towards fast and accurate machine learning attacks of feed-forward arbiter PUFs. In Proceedings of the IEEE Conference on Dependable and Secure Computing, Taipei, Taiwan, 7–10 August 2017.

63. Che, W.; Martinez-Ramon, M.; Saqib, F.; Plusquellic, J. Delay model and machine learning exploration of a hardware-embedded delay PUF. In Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington, DC, USA, 30 April–4 May 2018.
64. Ganji, F.; Forte, D.; Seifert, J.P. PUFmeter a Property Testing Tool for Assessing the Robustness of Physically Unclonable Functions to Machine Learning Attacks. *IEEE Access* **2019**, *7*, 122513–122521. [CrossRef]
65. Ikezaki, Y.; Nozaki, Y.; Yoshikawa, M. Deep learning attack for physical unclonable function. In Proceedings of the IEEE 5th Global Conference on Consumer Electronics, Kyoto, Japan, 11–14 October 2016.
66. Khalafalla, M.; Gebotys, C. PUFs Deep Attacks: Enhanced modeling attacks using deep learning techniques to break the security of double arbiter PUFs. In Proceedings of the Design, Automation & Test in Europe Conference & Exhibition (DATE), Florence, Italy, 25–29 March 2019.
67. Atakhodjaev, I.; Bosworth, B.T.; Grubel, B.C.; Kossey, M.R.; Villalba, J.; Cooper, A.B.; Dehak, N.; Foster, A.C.; Foster, M.A. Investigation of Deep Learning Attacks on Nonlinear Silicon Photonic PUFs. In Proceedings of the Conference on Lasers and Electro-Optics (CLEO), San Jose, CA, USA, 13–18 May 2018.
68. Xu, X.; Burleson, W. Hybrid side-channel/machine-learning attacks on PUFs: A new threat? In Proceedings of the Design, Automation & Test in Europe Conference & Exhibition (DATE), Dresden, Germany, 24–28 March 2014.
69. Yu, W.; Wen, Y. Efficient hybrid side-channel/machine learning attack on XOR PUFs. *Electron. Lett.* **2019**, *55*, 1080–1082. [CrossRef]
70. Tanaka, Y.; Bian, S.; Hiromoto, M.; Sato, T. Coin Flipping PUF: A Novel PUF With Improved Resistance Against Machine Learning Attacks. *IEEE Trans. Circuits Syst. II Express Briefs* **2018**, *65*, 602–606. [CrossRef]
71. Suresh, V.; Kumar, R.; Anders, M.; Kaul, H.; De, V.; Mathew, S. A 0.26% BER, 1028 Challenge-Response Machine-Learning Resistant Strong-PUF in 14 nm CMOS Featuring Stability-Aware Adversarial Challenge Selection. In Proceedings of the IEEE Symposium on VLSI Circuits, Honolulu, HI, USA, 16–19 June 2020.
72. Suresh, V.B.; Kumar, R.; Mathew, S. INVITED: A 0.26% BER, Machine-Learning Resistant 1028 Challenge-Response PUF in 14nm CMOS Featuring Stability-Aware Adversarial Challenge Selection. In Proceedings of the 57th ACM/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, 20–24 July 2020.
73. Yu, M.D.; Hiller, M.; Delvaux, J.; Sowell, R.; Devadas, S.; Verbauwhede, I. A Lockdown Technique to Prevent Machine Learning on PUFs for Lightweight Authentication. *IEEE Trans. -Multi-Scale Comput. Syst.* **2016**, *2*, 146–159. [CrossRef]
74. Dubrova, E.; Näslund, O.; Degen, B.; Gawell, A.; Yu, Y. CRC-PUF: A Machine Learning Attack Resistant Lightweight PUF Construction. In Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Stockholm, Sweden, 17–19 June 2019.
75. Wu, Q.; Zhang, J. CT PUF: Configurable Tristate PUF against Machine Learning Attacks. In Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS), Seville, Spain, 12–14 October 2020.
76. Venkatesh, A.; Venkatasubramaniyan, A.B.; Xi, X.; Sanyal, A. 0.3 pJ/Bit Machine Learning Resistant Strong PUF Using Subthreshold Voltage Divider Array. *IEEE Trans. Circuits Syst. II Express Briefs* **2020**, *67*, 1394–1398. [CrossRef]
77. Awano, H.; Sato, T. Ising-PUF: A machine learning attack resistant PUF featuring lattice-like arrangement of Arbiter-PUFs. In Proceedings of the Design, Automation & Test in Europe Conference & Exhibition (DATE), Dresden, Germany, 19–23 March 2018.
78. Rai, V.K.; Tripathy, S.; Mathew, J. 2SPUF: Machine Learning Attack Resistant SRAM PUF. In Proceedings of the Third ISEA Conference on Security and Privacy (ISEA-ISAP), Guwahati, India, 27 February–1 March 2020.
79. Chen, S.; Li, B.; Dan, F.; Chen, J. A machine learning resistant Arbiter PUFs scheme based on polynomial reconstruction. In Proceedings of the IEEE 2nd International Conference on Signal and Image Processing (ICSIP), Singapore, 4–6 August 2017.
80. Amsaad, F.; Choudhury, M.; Chaudhuri, C.R.; Niamat, M. An innovative delay based algorithm to boost PUF security against machine learning attacks. In Proceedings of the Annual Connecticut Conference on Industrial Electronics, Technology & Automation (CT-IETA), Bridgeport, CT, USA, 14–15 October 2016.
81. Su, H.; Zwolinski, M.; Halak, B. A Machine Learning Attacks Resistant Two Stage Physical Unclonable Functions Design. In Proceedings of the IEEE 3rd International Verification and Security Workshop (IVSW), Costa Brava, Spain, 2–4 July 2018.
82. Pundir, N.; Hazari, N.A.; Amsaad, F.; Niamat, M. A novel hybrid delay based physical unclonable function immune to machine learning attacks. In Proceedings of the IEEE National Aerospace and Electronics Conference (NAECON), Dayton, OH, USA, 27–30 June 2017.
83. Ma, Q.; Gu, C.; Hanley, N.; Wang, C.; Liu, W.; O'Neill, M. A machine learning attack resistant multi-PUF design on FPGA. In Proceedings of the 23rd Asia and South Pacific Design Automation Conference (ASP-DAC), Jeju, Korea, 22–25 January 2018.
84. Zhuang, H.; Xi, X.; Sun, N.; Orshansky, M. A Strong Subthreshold Current Array PUF Resilient to Machine Learning Attacks. *IEEE Trans. Circuits Syst. Regul. Pap.* **2020**, *67*, 135–144. [CrossRef]
85. Xi, X.; Zhuang, H.; Sun, N.; Orshansky, M. Strong subthreshold current array PUF with 265 challenge-response pairs resilient to machine learning attacks in 130 nm CMOS. In Proceedings of the Symposium on VLSI Circuits, Kyoto, Japan, 5–8 June 2017.
86. Venkatesh, A.; Sanyal, A. A Machine Learning Resistant Strong PUF using Subthreshold Voltage Divider Array in 65 nm CMOS. In Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS), Sapporo, Japan, 26–29 May 2019.
87. Pang, Y.; Wu, H.; Gao, B.; Wu, D.; Chen, A.; Qian, H. A novel PUF against machine learning attack: Implementation on a 16 Mb RRAM chip. In Proceedings of the IEEE International Electron Devices Meeting (IEDM), San Francisco, CA, USA, 2–6 December 2017.

88. Mahmoodi, M.; Nili, H.; Larimian, S.; Guo, X.; Strukov, D. ChipSecure: A Reconfigurable Analog eFlash-Based PUF with Machine Learning Attack Resiliency in 55 nm CMOS. In Proceedings of the 56th ACM/IEEE Design Automation Conference (DAC), Las Vegas, NV, USA, 2–6 June 2019.
89. Zhang, Y.; Xue, T.; Zhai, Z.; Ma, C.; Cai, X. The Improvement of Public Key Cryptography Based on Chaotic Neural Networks. In Proceedings of the Eighth International Conference on Intelligent Systems Design and Applications, Kaohsuing, Taiwan, 26–28 November 2008.
90. Wen, Y.; Lao, Y. Enhancing PUF reliability by machine learning. In Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS), Baltimore, MD, USA, 28–31 May 2017.
91. Dogaru, R.; Murgan, A.; Ioan, D. Chains of discrete-time chaotic neural networks for generation of broadband signals with applications in improved ciphering systems. In Proceedings of the 8th Mediterranean Electrotechnical Conference on Industrial Applications in Power Systems, Computer Science and Telecommunications, Bari, Italy, 16 May 1996.
92. Hu, G.; Kou, W.; Dong, J.; Peng, J. A Novel Image Encryption Algorithm Based on Cellular Neural Networks Hyper Chaotic System. In Proceedings of the IEEE 4th International Conference on Computer and Communications (ICCC), Chengdu, China, 7–10 December 2018.
93. Liu, Y.; Zhang, J.; Tang, W. Noise removal using Cohen-Grossberg neural network for improving the quality of the decrypted image in color encryption. In Proceedings of the IEEE 3rd International Conference on Communication Software and Networks, Xi'an, China, 27–29 May 2011.
94. Chatterjee, B.; Das, D.; Maity, S.; Sen, S. RF-PUF: Enhancing IoT Security Through Authentication of Wireless Nodes Using In-Situ Machine Learning. *IEEE Internet Things J.* **2019**, *6*, 388–398. [CrossRef]
95. Talreja, V.; Soleymani, S.; Valenti, M.C.; Nasrabadi, N.M. Learning to Authenticate with Deep Multibiometric Hashing and Neural Network Decoding. In Proceedings of the IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019.
96. Hu, D.; Wang, Y. Secure Authentication on WiMAX with Neural Cryptography. In Proceedings of the International Conference on Information Security and Assurance, Busan, Korea, 24–26 April 2008.
97. Chatterjee, B.; Das, D.; Sen, S. RF-PUF: IoT security enhancement through authentication of wireless nodes using in-situ machine learning. In Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington, DC, USA, 30 April–4 May 2018.
98. Hu, D.; Lao, H. Privacy Research on Ubicomp Computing with Neural Cryptography. In Proceedings of the The 3rd International Conference on Grid and Pervasive Computing—Workshops, Kunming, China, 25–28 May 2008.
99. Navghare, N.; Kulkarni, D.B. Data Privacy and Prediction Using Neural Network and Homomorphic Encryption. In Proceedings of the Second International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 14–15 June 2018.
100. Sirichotedumrong, W.; Kinoshita, Y.; Kiya, H. On the Security of Pixel-Based Image Encryption for Privacy-Preserving Deep Neural Networks. In Proceedings of the IEEE 8th Global Conference on Consumer Electronics (GCCE), Osaka, Japan, 15–18 October 2019.
101. Sirichotedumrong, W.; Maekawa, T.; Kinoshita, Y.; Kiya, H. Privacy-Preserving Deep Neural Networks with Pixel-Based Image Encryption Considering Data Augmentation in the Encrypted Domain. In Proceedings of the IEEE International Conference on Image Processing (ICIP), Taipei, Taiwan, 22–25 September 2019.
102. Fragkos, G.; Minwalla, C.; Plusquellic, J.; Tsiropoulou, E.E. Reinforcement Learning Toward Decision-Making for Multiple Trusted-Third-Parties in PUF-Cash. In Proceedings of the IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2–16 June 2020.
103. Seethalakshmi, K.; A, U.B.; N, S.K. Security enhancement in image steganography using neural networks and visual cryptography. In Proceedings of the International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), Bengaluru, India, 6–8 October 2016.
104. Yue, T.W.; Chiang, S. A neural network approach for visual cryptography. In Proceedings of the the IEEE-INNS-ENNS International Joint Conference on Neural Networks, Como, Italy, 27 July 2000.
105. Ge, S.; Changgen, P.; Xuelan, M. Visual Cryptography Scheme Using Pi-sigma Neural Networks. In Proceedings of the International Symposium on Information Science and Engineering, Shanghai, China, 20–22 December 2008.
106. Firmino, M.; Brandão, G.B.; Guerreiro, A.M.G.; de M. Valentim, R.A. Neural cryptography applied to key management protocol with mutual authentication in RFID systems. In Proceedings of the International Conference for Internet Technology and Secured Transactions, (ICITST), London, UK, 9–12 November 2009.
107. Thoms, G.R.W.; Muresan, R.; Al-Dweik, A. Chaotic Encryption Algorithm With Key Controlled Neural Networks for Intelligent Transportation Systems. *IEEE Access* **2019**, *7*, 158697–158709. [CrossRef]
108. Allam, A.M.; Abbas, H.M. Group key exchange using neural cryptography with binary trees. In Proceedings of the 24th Canadian Conference on Electrical and Computer Engineering(CCECE), Niagara Falls, ON, Canada, 8–11 May 2011.
109. Kinzel, W.; Kanter, I. Neural cryptography. In Proceedings of the the 9th International Conference on Neural Information Processing, Singapore, 18–22 November 2002.
110. Zhang, J.; Qu, G. Physical Unclonable Function-Based Key Sharing via Machine Learning for IoT Security. *IEEE Trans. Ind. Electron.* **2020**, *67*, 7025–7033. [CrossRef]

111. Turcaník, M. Using recurrent neural network for hash function generation. In Proceedings of the International Conference on Applied Electronics (AE), Pilsen, Czech Republic, 5–6 September 2017.
112. Yang, Q.T.; Gao, T.G.; Fan, L.; Gu, Q.L. Analysis of One-way Alterable Length Hash Function Based on Cell Neural Network. In Proceedings of the Fifth International Conference on Information Assurance and Security, Xi'an, China, 18–20 August 2009.
113. Abdoun, N.; Assad, S.E.; Taha, M.A.; Assaf, R.; Deforges, O.; Khalil, M. Secure Hash Algorithm based on Efficient Chaotic Neural Network. In Proceedings of the International Conference on Communications (COMM), Bucharest, Romania, 9–10 June 2016.
114. Turcaník, M.; Javurek, M. Hash function generation by neural network. In Proceedings of the New Trends in Signal Processing (NTSP), Demanovska dolina, Slovakia, 12–14 October 2016.
115. Lian, S.; Liu, Z.; Ren, Z.; Wang, H. Hash function based on chaotic neural networks. In Proceedings of the IEEE International Symposium on Circuits and Systems, Island of Kos, 21–24 May 2006.
116. Abdoun, N.; Assad, S.E.; Taha, M.A.; Assaf, R.; Deforges, O.; Khalil, M. Hash function based on efficient Chaotic Neural Network. In Proceedings of the 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 14–16 December 2015.
117. Turcaník, M. Hash function generation based on neural networks and chaotic maps. In Proceedings of the Communication and Information Technologies (KIT), Vysoke Tatry, Slovakia, 4–6 October 2017.
118. Abdoun, N.; Assad, S.E.; Hammoud, K.; Assaf, R.; Khalil, M.; Deforges, O. New keyed chaotic neural network hash function based on sponge construction. In Proceedings of the 12th International Conference for Internet Technology and Secured Transactions (ICITST), Cambridge, UK, 11–14 December 2017.
119. Zolfaghari, B.; Bibak, K.; Koshiba, T. From Random Numbers to Random Objects. *Entropy* **2022**, *24*, 928. [CrossRef]
120. Yayık, A.; Kutlu, Y. Improving Pseudo random number generator using artificial neural networks. In Proceedings of the 21st Signal Processing and Communications Applications Conference (SIU), Haspolat, Turkey, 24–26 April 2013.
121. Singla, P.; Sachdeva, P.; Ahmad, M. A Chaotic Neural Network Based Cryptographic Pseudo-Random Sequence Design. In Proceedings of the Fourth International Conference on Advanced Computing & Communication Technologies, Rohtak, India, 8–9 February 2014.
122. Lokesh, S.; Kounte, M.R. Chaotic neural network based pseudo-random sequence generator for cryptographic applications. In Proceedings of the International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Davangere, India, 29–31 October 2015.
123. Crounse, K.; Yang, T.; Chua, L. Pseudo-random sequence generation using the CNN universal machine with applications to cryptography. In Proceedings of the Fourth IEEE International Workshop on Cellular Neural Networks and Their Applications Proceedings (CNNA-96), Seville, Spain, 24–26 June 1996.
124. Hameed, S.M.; Ali, L.M.M. Utilizing Hopfield Neural Network for Pseudo-Random Number Generator. In Proceedings of the IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA), Aqaba, Jordan, 28 October–1 November 2018.
125. Wang, Y.H.; Shen, Z.D.; Zhang, H.G. Pseudo Random Number Generator Based on Hopfield Neural Network. In Proceedings of the International Conference on Machine Learning and Cybernetics, Dalian, China, 13–16 August 2006.
126. Tirdad, K.; Sadeghian, A. Hopfield neural networks as pseudo random number generators. In Proceedings of the Annual Meeting of the North American Fuzzy Information Processing Society, Toronto, ON, Canada, 12–14 July 2010.
127. Desai, V.; Deshmukh, V.; Rao, D.H. Pseudo random number generator using Elman neural network. In Proceedings of the IEEE Recent Advances in Intelligent Computational Systems, Trivandrum, India, 22–24 September 2011.
128. Bao, L.; Wang, Z.; Yu, Z.; Fang, Y.; Yang, Y.; Cai, Y.; Huang, R. Adaptive Random Number Generator Based on RRAM Intrinsic Fluctuation for Reinforcement Learning. In Proceedings of the International Symposium on VLSI Technology, Systems and Applications (VLSI-TSA), Hsinchu, Taiwan, 10–13 August 2020.
129. Ash-Saki, A.; Alam, M.; Ghosh, S. Improving Reliability of Quantum True Random Number Generator using Machine Learning. In Proceedings of the 21st International Symposium on Quality Electronic Design (ISQED), Santa Clara, CA, USA, 25–26 March 2020.
130. Wang, B.J.; Cao, H.J.; Wang, Y.H.; Zhang, H.G. Random Number Generator of BP Neural Network Based on SHA-2 (512). In Proceedings of the International Conference on Machine Learning and Cybernetics, Hong Kong, China, 19–22 August 2007.
131. Kimura, H.; Isobe, T.; Ohigashi, T. Neural-Network-Based Pseudo-Random Number Generator Evaluation Tool for Stream Ciphers. In Proceedings of the Seventh International Symposium on Computing and Networking Workshops (CANDARW), Nagasaki, Japan, 26–29 November 2019.
132. Fischer, T. Testing Cryptographically Secure Pseudo Random Number Generators with Artificial Neural Networks. 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.
133. Yu, Y.; Moraitis, M.; Dubrova, E. Can Deep Learning Break a True Random Number Generator? *IEEE Trans. Circuits Syst. II Express Briefs* **2021**, *68*, 1710–1714. [CrossRef]
134. Zou, A.; Xiao, X. An Asynchronous Encryption Arithmetic Based on Laguerre Chaotic Neural Networks. In Proceedings of the WRI Global Congress on Intelligent Systems, Xiamen, China, 19–21 May 2009.
135. Chung, D.; Lee, S.; Choi, D.; Lee, J. Alternative Tower Field Construction for Quantum Implementation of the AES S-box. *IEEE Trans. Comput. Early Access Artic.* **2021**, 1. [CrossRef]

136. Ahmad, M.; Malik, M. Design of chaotic neural network based method for cryptographic substitution box. In Proceedings of the International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, India, 3–5 March 2016.
137. Chen, Y.; Wang, Z.; Patil, A.; Basu, A. A 2.86-TOPS/W Current Mirror Cross-Bar-Based Machine-Learning and Physical Unclonable Function Engine For Internet-of-Things Applications. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2019**, *66*, 2240–2252. [CrossRef]
138. Wang, Z.; Chen, Y.; Patil, A.; Jayabalan, J.; Zhang, X.; Chang, C.H.; Basu, A. Current Mirror Array: A Novel Circuit Topology for Combining Physical Unclonable Function and Machine Learning. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2018**, *65*, 1314–1326. [CrossRef]
139. Wassermann, S.; Seufert, M.; Casas, P.; Gang, L.; Li, K. ViCrypt to the Rescue: Real-time, Machine-Learning-driven Video-QoE Monitoring for Encrypted Streaming Traffic. *IEEE Trans. Netw. Serv. Manag. Early Access Artic.* **2020**, *17*, 2007–2023. [CrossRef]
140. Ghouse, M.; Nene, M.J.; Vembuselvi, C. Data Leakage Prevention for Data in Transit using Artificial Intelligence and Encryption Techniques. In Proceedings of the International Conference on Advances in Computing, Communication and Control (ICAC3), Mumbai, India, 20–21 December 2019.
141. Jain, N.; Naik, O.; Yalagoud, A.; Bhuyan, P.; K, M. Face-Crypt Messenger: Enhancing Security of Messaging Systems using AI based Facial Recognition and Encryption. In Proceedings of the 6th International Conference on Computing Methodologies and Communication (ICCMC), Tamil Nadu, India, 29–31 March 2022.
142. Sahoo, A.K.; Rudra, S.; Mohanty, A.S. Artificial intelligence based electric grid operation enabled with data encryption. In Proceedings of the International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, India, 3–5 March 2016.
143. Allam, A.M.; Abbas, H.M.; El-Kharashi, M.W. Authenticated key exchange protocol using neural cryptography with secret boundaries. In Proceedings of the 2013 International Joint Conference on Neural Networks (IJCNN), Amman, Jordan, 14–15 July 2013.
144. Hu, D. A New Service-Based Computing Security Model with Neural Cryptography. In Proceedings of the Second Pacific-Asia Conference on Web Mining and Web-based Application, Wuhan, China, 6–7 June 2009.
145. Godhavari, T.; Alamelu, N.; Soundararajan, R. Cryptography Using Neural Network. In Proceedings of the Annual IEEE India Conference—Indicon, Chennai, India, 11–13 December 2005.
146. Dong, T.; Huang, T. Neural Cryptography Based on Complex-Valued Neural Network. *IEEE Trans. Neural Netw. Learn. Syst. (Early Access Artic.)* **2019**, *31*, 4999–5004. [CrossRef] [PubMed]
147. Tenorio, R.H.V.; Sham, C.W.; Vargas, D.V. Preliminary study of applied binary neural networks for neural cryptography. In Proceedings of the the 2020 Genetic and Evolutionary Computation Conference Companion, Cancún, Mexico, 8–12 July 2020.
148. Fei, X.; Liu, G.; Zheng, B. A chaotic encryption system using PCA neural networks. In Proceedings of the IEEE Conference on Cybernetics and Intelligent Systems, Chengdu, China, 21–24 September 2008.
149. Roy, S.S.; Shahriyar, S.A.; Asaf-Uddowla, M.; Alam, K.M.R.; Morimoto, Y. A novel encryption model for text messages using delayed chaotic neural network and DNA cryptography. In Proceedings of the 20th International Conference of Computer and Information Technology (ICCIT), Dhaka, Bangladesh, 22–24 December 2017.
150. Gaffar, A.F.O.; Putra, A.B.W.; Malani, R. The Multi Layer Auto Encoder Neural Network (ML-AENN) for Encryption and Decryption of Text Message. In Proceedings of the 5th International Conference on Science in Information Technology (ICSITech), Yogyakarta, Indonesia, 23–24 October 2019.
151. Liu, C.Y.; Woungang, I.; Chao, H.C.; Dhurandher, S.K.; Chi, T.Y.; Obaidat, M.S. Message Security in Multi-Path Ad Hoc Networks Using a Neural Network-Based Cipher. In Proceedings of the IEEE Global Telecommunications Conference, Houston, TX, USA, 5–9 December 2011.
152. Hu, D.; Wang, Y. Security Research on WiMAX with Neural Cryptography. In Proceedings of the International Conference on Information Security and Assurance, Busan, Korea, 24–26 April 2008.
153. Ismail, I.A.; Galal-Edeen, G.H.; Khattab, S.; Bahtity, M.A.E.M.E. Satellite image encryption using neural networks backpropagation. In Proceedings of the 22nd International Conference on Computer Theory and Applications (ICCTA), Alexandria, Egypt, 13–15 October 2012.
154. Zhou, S. Image Encryption Technology Research Based on Neural Network. In Proceedings of the International Conference on Intelligent Transportation, Big Data and Smart City, Halong Bay, Vietnam, 19–20 December 2015.
155. Kumar, S.; Aid, R. Image encryption using wavelet based chaotic neural network. In Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI), Jaipur, India, 21–24 September 2016.
156. Lin, J.; Luo, Y.; Liu, J.; Bi, J.; Qiu, S.; Cen, M.; Liao, Z. An Image Compression-Encryption Algorithm Based on Cellular Neural Network and Compressive Sensing. In Proceedings of the IEEE 3rd International Conference on Image, Vision and Computing (ICIVC), Chongqing, China, 27–29 June 2018.
157. de Almeida Ramos, E.; Filho, J.C.B.; Reis, R. Cryptography by Synchronization of Hopfield Neural Networks that Simulate Chaotic Signals Generated by the Human Body. In Proceedings of the 17th IEEE International New Circuits and Systems Conference (NEWCAS), Munich, Germany, 23–26 June 2019.
158. Joshi, S.D.; Udupi, V.R.; Joshi, D.R. A novel neural network approach for digital image data encryption/decryption. In Proceedings of the International Conference on Power, Signals, Controls and Computation, Thrissur, India, 3–6 January 2012.

159. Dridi, M.; Hajjaji, M.A.; Bouallegue, B.; Mtibaa, A. Cryptography of medical images based on a combination between chaotic and neural network. *IET Image Process.* **2016**, *10*, 830–839. [CrossRef]
160. Han, B.; Jia, Y.; Huang, G.; Cai, L. A Medical Image Encryption Algorithm Based on Hermite Chaotic Neural Network. In Proceedings of the IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chongqing, China, 12–14 June 2020.
161. Xiao, J.; Wang, W.; Wang, M. Image Encryption Algorithm Based on Memristive BAM Neural Networks. In Proceedings of the IEEE Third International Conference on Data Science in Cyberspace (DSC), Guangzhou, China, 18–21 June 2018.
162. Bharadwaj, G.V.S.E.; Vijaya, K.; Balaga, S.K.; Thanikaiselvan, V. Image Encryption Based on Neural Network Architecture and Chaotic Systems. In Proceedings of the Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 29–31 March 2018.
163. Liu, X.; Jin, X.; Zhao, Y. Optical Image Encryption Using Fractional-Order Quantum Cellular Neural Networks in a Fractional Fourier Domain. In Proceedings of the 14th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), Huangshan, China, 28–30 July 2018.
164. Lin, M.; Long, F.; Guo, L. Grayscale image encryption based on Latin square and cellular neural network. In Proceedings of the Chinese Control and Decision Conference (CCDC), Yinchuan, China, 28–30 May 2016.
165. Li, H.; Li, C.; Ouyang, D.; Nguang, S.K. Impulsive Synchronization of Unbounded Delayed Inertial Neural Networks With Actuator Saturation and Sampled-Data Control and Its Application to Image Encryption. *IEEE Trans. Neural Netw. Learn. Syst. (Early Access Artic.)* **2020**, *32*, 1460–1473. [CrossRef] [PubMed]
166. Yang, F.; Mou, J.; Cao, Y.; Chu, R. An image encryption algorithm based on BP neural network and hyperchaotic system. *China Commun.* **2020**, *17*, 21–28. [CrossRef]
167. Wen, S.; Zeng, Z.; Huang, T.; Meng, Q.; Yao, W. Lag Synchronization of Switched Neural Networks via Neural Activation Function and Applications in Image Encryption. *IEEE Trans. Neural Netw. Learn. Syst.* **2015**, *26*, 1493–1502. [CrossRef]
168. Liu, L.; Zhang, L.; Jiang, D.; Guan, Y.; Zhang, Z. A Simultaneous Scrambling and Diffusion Color Image Encryption Algorithm Based on Hopfield Chaotic Neural Network. *IEEE Access* **2019**, *7*, 185796–185810. [CrossRef]
169. Anikin, I.V.; Makhmutova, A.Z.; Gadelshin, O.E. Symmetric encryption with key distribution based on neural networks. In Proceedings of the 2nd International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), Chelyabinsk, Russia, 19–20 May 2016.
170. Liu, N.; Guo, D. Security Analysis of Public-key Encryption Scheme Based on Neural Networks and Its Implementing. In Proceedings of the International Conference on Computational Intelligence and Security, Guangzhou, China, 3–6 November 2006.
171. Ohira, T. Neural network model with delay toward encryption. In Proceedings of the the IEEE-INNS-ENNS International Joint Conference on Neural Networks, Como, Italy, 27 July 2000.
172. Wang, J.; Cheng, L.M.; Su, T. Multivariate Cryptography Based on Clipped Hopfield Neural Network. *IEEE Trans. Neural Netw. Learn. Syst.* **2018**, *29*, 353–363. [CrossRef]
173. Sagar, V.; Kumar, K. A symmetric key cryptography using genetic algorithm and error back propagation neural network. In Proceedings of the 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 11–13 March 2015.
174. Fadil, T.A.; Yaakob, S.N.; Ahmad, B. A hybrid chaos and neural network cipher encryption algorithm for compressed video signal transmission over wireless channel. In Proceedings of the 2nd International Conference on Electronic Design (ICED), Penang, Malaysia, 19–21 August 2014.
175. Su, S.; Lin, A.; Yen, J.C. Design and realization of a new chaotic neural encryption/decryption network. In Proceedings of the IEEE Asia-Pacific Conference on Circuits and Systems. Electronic Communication Systems. (Cat. No.00EX394), Tianjin, China, 4–6 December 2000.
176. Chatzidakis, S.; Forsberg, P.; Tsoukalas, L.H. Chaotic neural networks for intelligent signal encryption. In Proceedings of the The 5th International Conference on Information, Intelligence, Systems and Applications, Chania, Greece, 7–9 July 2014.
177. Kanter, I. The theory of neural networks: Learning from examples, time-series and cryptography. In Proceedings of the IEEE International Workshop on VLSI Design and Video Technology, Suzhou, China, 28–30 May 2005.
178. Zhang, X.; Sheng, S.; Lu, G.; Zheng, Y. Synchronization for arrays of coupled jumping delayed neural networks and its application to image encryption. In Proceedings of the IEEE 56th Annual Conference on Decision and Control (CDC), Melbourne, VIC, Australia, 12–15 December 2017.
179. Wang, W.; Wang, X.; Luo, X.; Yuan, M. Finite-Time Projective Synchronization of Memristor-Based BAM Neural Networks and Applications in Image Encryption. *IEEE Access* **2018**, *6*, 56457–56476. [CrossRef]
180. Bi, M.; Zhuo, X.; Fu, X.; Yang, X.; Hu, W. Cellular Neural Network Encryption Scheme for Time Synchronization and CPAs Resistance in OFDM-PON. *IEEE Access* **2019**, *7*, 57129–57137. [CrossRef]
181. Chen, W.H.; Luo, S.; Zheng, W.X. Impulsive Synchronization of Reaction–Diffusion Neural Networks With Mixed Delays and Its Application to Image Encryption. *IEEE Trans. Neural Netw. Learn. Syst.* **2016**, *27*, 2696–2710. [CrossRef] [PubMed]
182. Wang, W.; Yu, X.; Luo, X.; Kurths, J. Finite-Time Synchronization of Chaotic Memristive Multidirectional Associative Memory Neural Networks and Applications in Image Encryption. *IEEE Access* **2018**, *6*, 35764–35779. [CrossRef]
183. Song, X.; Man, J.; Song, S.; Ning, Z. Event-triggered synchronisation of Markovian reaction–diffusion inertial neural networks and its application in image encryption. *IET Control. Theory Appl.* **2020**, *14*, 2726–2740. [CrossRef]

184. Vandewalle, J.; Preneel, B.; Csapodi, M. Data security issues, cryptographic protection methods, and the use of cellular neural networks and cellular automata. In Proceedings of the Fifth IEEE International Workshop on Cellular Neural Networks and their Applications. Proceedings (Cat. No.98TH8359), London, UK, 14–17 April 1998.
185. Mislovaty, R.; Klein, E.; Kanter, I.; Kinzel, W. Security of neural cryptography. In Proceedings of the the 2004 11th IEEE International Conference on Electronics, Circuits and Systems, Tel Aviv, Israel, 15 December 2004.
186. Choi, Y.; Sim, J.; Kim, L.S. CREMON: Cryptography Embedded on the Convolutional Neural Network Accelerator. *IEEE Trans. Circuits Syst. II Express Briefs Early Access Artic.* **2020**, *67*, 3337–3341. [CrossRef]
187. Arora, B.; Srishti, K.; Khatri, N.; Niranjan, V. Application of Artificial Neural Network in Cryptography. In Proceedings of the 2nd International Conference on Power Energy, Environment and Intelligent Control (PEEIC), Greater Noida, India, 18–19 October 2019.
188. Zhu, Y.; Vargas, D.V.; Sakurai, K. Neural Cryptography Based on the Topology Evolving Neural Networks. In Proceedings of the Sixth International Symposium on Computing and Networking Workshops (CANDARW), Takayama, Japan, 27–30 November 2018.
189. Wright, J.L.; Manic, M. Neural network architecture selection analysis with application to cryptography location. In Proceedings of the International Joint Conference on Neural Networks (IJCNN), Barcelona, Spain, 18–23 July 2010.
190. Munukur, R.K.; Gnanam, V. Neural network based decryption for random encryption algorithms. In Proceedings of the 3rd International Conference on Anti-Counterfeiting, Security, and Identification in Communication, Hong Kong, China, 20–22 August 2009.
191. Lytvyn, V.; Peleshchak, I.; Peleshchak, R.; Vysotska, V. Information Encryption Based on the Synthesis of a Neural Network and AES Algorithm. In Proceedings of the 3rd International Conference on Advanced Information and Communications Technologies (AICT), Lviv, Ukraine, 2–6 July 2019.
192. Srivastava, S.; Bhatia, A. On the Learning Capabilities of Recurrent Neural Networks: A Cryptographic Perspective. In Proceedings of the IEEE International Conference on Big Knowledge (ICBK), Singapore, 17–18 November 2018.
193. Skovajsová, L. Comparison of Cryptography by Chaotic Neural Network and by AES. In Proceedings of the IEEE 19th International Symposium on Computational Intelligence and Informatics and 7th IEEE International Conference on Recent Achievements in Mechatronics, Automation, Computer Sciences and Robotics (CINTI-MACRo), Szeged, Hungary, 14–16 November 2019.
194. Forgác, R.; Ockay, M. Contribution to Symmetric Cryptography by Convolutional Neural Networks. In Proceedings of the Communication and Information Technologies (KIT), Vysoke Tatry, Slovakia, 9–11 October 2019.
195. Allam, A.M.; Abbas, H.M. Improved security of neural cryptography using don't-trust-my-partner and error prediction. In Proceedings of the International Joint Conference on Neural Networks, Atlanta, GA, USA, 14–19 June 2009.
196. Saraswat, P.; Garg, K.; Tripathi, R.; Agarwal, A. Encryption Algorithm Based on Neural Network. In Proceedings of the 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 18–19 April 2019.
197. Zang, H.; Min, L. Generalized synchronization theorems for a kind of Neural Network with application in data encryption. In Proceedings of the 3rd IEEE Conference on Industrial Electronics and Applications, Singapore, 3–5 June 2008.
198. Cantoro, R.; Deligiannis, N.I.; Reorda, M.S.; Traiola, M.; Valea, E. Evaluating Data Encryption Effects on the Resilience of an Artificial Neural Network. In Proceedings of the IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), Frascati, Italy, 19–21 October 2020.
199. Arvandi, M.; Wu, S.; Sadeghian, A. On the use of recurrent neural networks to design symmetric ciphers. *IEEE Comput. Intell. Mag.* **2008**, *3*, 42–53. [CrossRef]
200. Arvandi, M.; Wu, S.; Sadeghian, A.; Melek, W.; Woungang, I. Symmetric Cipher Design Using Recurrent Neural Networks. In Proceedings of the IEEE International Joint Conference on Neural Network, Vancouver, BC, Canada, 16–21 July 2006.
201. Cai, Y.; Chen, X.; Tian, L.; Wang, Y.; Yang, H. Enabling Secure in-Memory Neural Network Computing by Sparse Fast Gradient Encryption. In Proceedings of the IEEE/ACM International Conference on Computer-Aided Design (ICCAD), Westminster, CO, USA, 4–7 November 2019.
202. Hu, D. Secure mobile network handover with neural cryptography. In Proceedings of the International Symposium on Communications and Information Technologies, Sydney, Australia, 16–19 October 2007.
203. Stöttinger, M.; Huss, S.A.; Mühlbach, S.; Koch, A. Side-Channel Resistance Evaluation of a Neural Network Based Lightweight Cryptography Scheme. In Proceedings of the IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, Hong Kong, China, 11–13 December 2010.
204. Arvandi, M.; Sadeghian, A. Chosen Plaintext Attack against Neural Network-Based Symmetric Cipher. In Proceedings of the International Joint Conference on Neural Networks, Orlando, FL, USA, 12–17 August 2007.
205. Allam, A.M.; Abbas, H.M.; El-Kharashi, M.W. Security analysis of neural cryptography implementation. In Proceedings of the IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM), Victoria, BC, Canada, 27–29 August 2013.
206. Ganjavi, R.; Sharafat, A.R. Edge-Assisted Public Key Homomorphic Encryption for Preserving Privacy in Mobile Crowdsensing. *IEEE Trans. Serv. Comput. Early Access Artic.* **2022**, 1. [CrossRef]

207. Zhang, P.; Huang, T.; Sun, X.; Zhao, W.; Liu, H.; Lai, S.; Liu, J.K. Privacy-Preserving and Outsourced Multi-Party K-Means Clustering Based on Multi-Key Fully Homomorphic Encryption. *IEEE Trans. Dependable Secur. Comput. (Early Access Artic.)* **2022**, 1–12. [CrossRef]
208. Zhang, L.; Xu, J.; Vijayakumar, P.; Sharma, P.K.; Ghosh, U. Homomorphic Encryption-based Privacy-preserving Federated Learning in IoT-enabled Healthcare System. *IEEE Trans. Netw. Sci. Eng. (Early Access Artic.)* **2022**, 1–17. [CrossRef]
209. Yelina, T.N.; Bezzateev, S.V.; Mylnikov, V.A. The Homomorphic Encryption in Pipelines Accident Prediction by Using Cloud-based Neural Network. In Proceedings of the Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), St. Petersburg, Russia, 3–7 June 2019.
210. Ghimes, A.M.; Vladuta, V.A.; Patriciu, V.V.; Ionita, A. Applying Neural Network Approach to Homomorphic Encrypted Data. In Proceedings of the 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Iasi, Romania, 28–30 June 2018.
211. Li, X.; Han, Q.; Jin, X. A Secure and Efficient Face-Recognition Scheme Based on Deep Neural Network and Homomorphic Encryption. In Proceedings of the International Conference on Virtual Reality and Visualization (ICVRV), Qingdao, China, 22–24 October 2018.
212. Li, Y.; Aghvami, A.H.; Dong, D. Intelligent Trajectory Planning in UAV-Mounted Wireless Networks: A Quantum-Inspired Reinforcement Learning Perspective. *IEEE Wirel. Commun. Lett. Early Access Artic.* **2021**, *10*, 1994–1998. [CrossRef]
213. Dong, D.; Chen, C.; Chu, J.; Tarn, T.J. Robust Quantum-Inspired Reinforcement Learning for Robot Navigation. *IEEE/ASME Trans. Mechatron.* **2012**, *17*, 86–97. [CrossRef]
214. Patel, O.P.; Bharill, N.; Tiwari, A.; Prasad, M. A Novel Quantum-Inspired Fuzzy Based Neural Network for Data Classification. *IEEE Trans. Emerg. Top. Comput.* **2021**, *9*, 1031–1044. [CrossRef]
215. Wei, Q.; Ma, H.; Chen, C.; Dong, D. Deep Reinforcement Learning With Quantum-Inspired Experience Replay. *IEEE Trans. Cybern. Early Access Artic.* **2021**, 1–13. [CrossRef] [PubMed]
216. Masuyama, N.; Loo, C.K.; Seera, M.; Kubota, N. Quantum-Inspired Multidirectional Associative Memory With a Self-Convergent Iterative Learning. *IEEE Trans. Neural Netw. Learn. Syst.* **2018**, *29*, 1058–1068. [CrossRef] [PubMed]
217. Forgác, R.; Ockay, M. Big data protection via neural and quantum cryptography. In Proceedings of the 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 16–18 March 2016.
218. Truong, N.D.; Haw, J.Y.; Assad, S.M.; Lam, P.K.; Kavehei, O. Machine Learning Cryptanalysis of a Quantum Random Number Generator. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 403–414. [CrossRef]
219. Niemiec, M.; Mehic, M.; Voznak, M. Security Verification of Artificial Neural Networks Used to Error Correction in Quantum Cryptography. In Proceedings of the 26th Telecommunications Forum (TELFOR), Belgrade, Serbia, 20–21 November 2018.
220. Anh, T.T.; Thanh, N.V.; Luong, T.D. A construction of cryptography system based on quantum neural network. In Proceedings of the Eighth International Conference on Knowledge and Systems Engineering (KSE), Hanoi, Vietnam, 6–8 October 2016.