Special Issue on Cryptography and Its Applications in Information Security

Safwan El Assad, René Lozi, William Puech

applied sciences

MDPI

Editorial

Special Issue on Cryptography and Its Applications in Information Security

Safwan El Assad [1,*], René Lozi [2] and William Puech [3]

[1] Institut d'Electronique et des Technologies du NumériQue (IETR), UMR CNRS 6164, Nantes Université-Polytech Nantes, 44306 Nantes, France
[2] Department of Mathematics, Laboratoire J. A. Dieudonné, Côte d'Azur University, CEDEX 2, 06108 Nice, France; rene.lozi@univ-cotedazur.fr
[3] Department of Computer Science, Laboratoire d'Informatique, de Robotique et de Micro Electronique de Montpellier (LIRMM), University of Montpellier, UMR CNRS 5506, CEDEX 05, 34392 Montpellier, France; william.puech@lirmm.fr
* Correspondence: safwan.elassad@univ-nantes.fr

1. Introduction

Nowadays, mankind is living in a cyber world. Modern technologies involve fast communication links between potentially billions of devices through complex networks (satellite, mobile phone, Internet, Internet of Things (IoT), etc.). The main concern posed by these entangled complex networks is their protection against passive and active attacks that could compromise public security (sabotage, espionage, cyber-terrorism) and privacy.

To face it, most of the world web traffic (digital multimedia contents such as images, speech signal, videos, and emails) is protected against security threats, occurring among different societies and within several societal levels. Even governments (rogue or not) and some of their official agencies are suspected of promoting and actively participating in the hacking of other government officials, democratic processes, industrial secrets, and the citizens.

Thousands of private or official hackers target the sensitive information of citizens, industries, and governments. The threat is actual, and it is escalating year after year.

The aim of this Special Issue on "Cryptography and its Applications in Information Security" was to address the range of problems related to the security of information in networks and multimedia communications and to bring together researchers, practitioners, and industrials interested by such questions. Papers both from theoretical and practical aspects were welcome, including ongoing research projects, experimental results, and recent developments related to, but not limited to, the following topics: cryptography; chaos-based cryptography; block and stream ciphers; hash functions; steganography; watermarking; selective encryption; multimedia data hiding and security; secure FPGA implementation for cryptographic primitives; security methods for communications; Wireless Network Security (Internet, WSNs, UMTS, WiFi, WiMAX, WiMedia, and others); sensor and mobile ad hoc network security; security and privacy in mobile systems, secure cloud computing; security and privacy in social networks, vehicular networks, Web services; database security and privacy; intellectual property protection, lightweight cryptography for green computing; personal data protection for information systems; protocols for security; cryptanalysis, side channel attack; fault injection attack; and physical layer security for communications.

2. The Papers

In this Special Issue, we received a total of 24 submissions and, after the peer review, accepted and published 8 outstanding papers that span across several interesting topics on security, relationship between chaos pseudo-random numbers and stream ciphers, and blockchain technologies.

check for updates

Citation: El Assad, S.; Lozi, R.; Puech, W. Special Issue on Cryptography and Its Applications in Information Security. *Appl. Sci.* **2022**, *12*, 2588. https://doi.org/10.3390/app12052588

Received: 21 February 2022
Accepted: 25 February 2022
Published: 2 March 2022

In the field of security, four papers are presented. The first one suggests employing a homomorphic encryption (HE) scheme that can directly perform arithmetic operations on ciphertexts without decryption to protect the model parameters. Using the HE scheme, the proposed privacy-preserving federated learning (PPFL) algorithm enables a centralized server to aggregate encrypted local model parameters without decryption. Furthermore, the proposed algorithm allows each node to use a different HE private key in the same FL-based system using a distributed cryptosystem [1].

A second paper in this field proposes a new anomaly detection algorithm for the Intrusion Detection System (IDS), where a machine learning algorithm is applied to detect deviations from legitimate traffic, which may indicate an intrusion. It involves a novel approach based on the transformation of the network flow statistics to gray images on which the Gray-Level Co-occurrence Matrix (GLCM) is applied together with an entropy measure recently proposed in the literature—2D Dispersion Entropy. This approach is assessed using the recently public IDS data set CIC-IDS2017. The results show that it is competitive in comparison to other approaches proposed in the literature on the same data set [2].

The main objective of the third paper is the classification of the Strongly Asymmetric Public Key Agreement (SAPKA) algorithms. SAPKA is a class of key exchanges between Alice and Bob that was introduced in 2011. The greatest difference from the standard PKA algorithms is that Bob constructs multiple public keys and Alice uses one of these to calculate her public key and her secret shared key. Therefore, the number of public keys and calculation rules for each key differ for each user. Although algorithms with high security and computational efficiency exist in this class, the relation between the parameters of SAPKA and its security and computational efficiency has not yet been fully clarified. By attempting algorithm attacks, the authors found that certain parameters are more strongly related to security. On this basis, they construct concrete algorithms and a new subclass of SAPKA, in which the responsibility of maintaining security is significantly more associated with the secret parameters of Bob than those of Alice [3].

The last paper in security designs a secure chaos-based stream cipher (SCbSC) and evaluates its hardware implementation performance in terms of computational complexity and its security. The fundamental element of this system is the proposed secure pseudo-chaotic number generator (SPCNG). The architecture of the proposed SPCNG includes three first-order recursive filters, each containing a discrete chaotic map and a mixing technique using an internal pseudo-random number (PRN). The three discrete chaotic maps, namely, the 3D Chebyshev map (3D Ch), the 1D logistic map (L), and the 1D skew-tent map (S), are weakly coupled by a predefined coupling matrix M. The mixing technique combined with the weak coupling technique of the three chaotic maps allows the system to be protected against side-channel attacks (SCAs) [4].

Linked to the topic of this paper, two other papers analyze the performances of stream ciphers. In [5], the bit independence criterion, which was proposed to evaluate the security of the S-boxes used in block ciphers, is assessed and improved. This paper proposes an algorithm that extends this criterion to evaluate the degree of independence between the bits of inputs and outputs of the stream ciphers. The effectiveness of the algorithm is experimentally confirmed in two scenarios: random outputs independent of the input, in which it does not detect dependence; and in the RC4 ciphers, where it detects significant dependencies related to some known weaknesses. The complexity of the algorithm is estimated based on the number of inputs l, and the dimensions, n and m, of the inputs and outputs, respectively.

Alternatively, in [6], a novel intermittent jumping CML system based on multiple chaotic maps is proposed. The intermittent jumping mechanism seeks to incorporate the multi-chaos, and to dynamically switch coupling states and coupling relations, varying with spatiotemporal indices. Extensive numerical simulations and comparative studies demonstrate that, compared with the existing CML-based systems, the proposed system has a larger parameter space, better chaotic behavior, and comparable computational

complexity. These results highlight the potential of the proposal for deployment into an image cryptosystem.

The third topic highlighted in this Special Issue is the blockchain theory, either for digital cash or "digital authorization" for museums. Digital cash is a form of money that is stored digitally. Its main advantage when compared to traditional credit or debit cards is the possibility of carrying out anonymous transactions. Diverse digital cash paradigms have been proposed during recent decades, providing different approaches to avoid the double-spending fraud, or features such as divisibility or transferability. In [7], a new digital cash paradigm that includes the so-called no-valued e-coins, which are e-coins that can be generated free of charge by customers, is proposed. This new paradigm has also proven its validity in the scope of privacy-preserving pay-by-phone parking systems, and the authors believe it can become a very versatile building block in the design of privacy-preserving protocols in other areas of research.

The American Alliance of Museums (AAM) recently stated that nearly a third of the museums in the United States may be permanently closed since museum operations are facing "extreme financial difficulties", especially since the outbreak of COVID-19 at the beginning of this year (2020). The research published in [8] aimed at museums using the business model of "digital authorization". It proposes an authorization mechanism based on blockchain technology protecting the museums' digital rights in the business model and the application of cryptography. The signature and time stamp mechanism achieve non-repudiation and a timeless mechanism, which combines blockchain and smart contracts to achieve verifiability, non-forgery, decentralization, and traceability, as well as the non-repudiation of the issue of cash flow with signatures and digital certificates, for the digital rights of museums in business.

Author Contributions: All the editors have contributed equally. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: This issue would not be possible without the contributions of the authors who submitted their valuable papers. We would like to thank all reviewers and the editorial team of Applied Sciences for their great work.

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

References

1. Park, J.; Lim, H. Privacy-Preserving Federated Learning Using Homomorphic Encryption. *Appl. Sci.* **2022**, *12*, 734. [CrossRef]
2. Baldini, G.; Ramos, J.L. Intrusion Detection Based on Gray-Level Co-Occurrence Matrix and 2D Dispersion Entropy. *Appl. Sci.* **2021**, *11*, 5567. [CrossRef]
3. Satoshi Iriyama, S.; Jimbo, K.; Regoli, M. New Subclass Framework and Concrete Examples of Strongly Asymmetric Public Key Agreement. *Appl. Sci.* **2021**, *11*, 5540. [CrossRef]
4. Dridi, F.; El Assad, S.; Youssef, W.E.H.; Machhout, M.; Lozi, R. The Design and FPGA-Based Implementation of a Stream Cipher Based on a Secure Chaotic Generator. *Appl. Sci.* **2021**, *11*, 625. [CrossRef]
5. Madarro-Capó, E.J.; Legón-Pérez, C.M.; Rojas, O.; Sosa-Gómez, G.; Socorro-Llanes, R. Bit Independence Criterion Extended to Stream Ciphers. *Appl. Sci.* **2020**, *10*, 7668. [CrossRef]
6. Huang, R.; Han, F.; Liao, X.; Wang, Z.; Dong, A. A Novel Intermittent Jumping Coupled Map Lattice Based on Multiple Chaotic Maps. *Appl. Sci.* **2021**, *11*, 3797. [CrossRef]
7. Ricard Borges, R.; Sebé, F. A Digital Cash Paradigm with Valued and No-Valued e-Coins. *Appl. Sci.* **2021**, *11*, 9892. [CrossRef]
8. Wang, Y.-C.; Chen, C.-L.; Deng, Y.-Y. Authorization Mechanism Based on Blockchain Technology for Protecting Museum-Digital Property Rights. *Appl. Sci.* **2021**, *11*, 1085. [CrossRef]