ENIGMA – Brazilian Journal of Information Security and Cryptography Volume 3 Issue 1 September 2016

E. T. Ueda, *Editor in Chief*, M. S. M. A. Notare, *Associate Editor in Chief*, and R. T. de Sousa Júnior, *Associate Editor in Chief*

Abstract—**This is the first issue of Volume 3 of ENIGMA – Brazilian Journal of Information Security and Cryptography. Submissions were accepted in English, Portuguese and Spanish. In this issue, 4 papers are published, of which 3 were peer-reviewed while another was invited and reviewed by the editorial board of the Journal. In addition, the invited paper was the Best Paper of the conference SBSeg'2015.**

Keywords—**Brazilian Journal, Cryptography, Information Security.**

I. Introduction

ENIGMA – Brazilian Journal of Information Security and Cryptography – is a technical-scientific publication that aims at discussing theoretical aspect contributions and practical applications results in information security, cryptography and cyber defense as well as fundamental subjects in support of those issues.

The choice of the name ENIGMA for this publication is related to the ENIGMA cryptography machine. However, the main reason for this choice is to pay tribute to the mathematician and computer scientist Alan Mathison Turing (1912-1954), considered one of the leading scientists in the history of computing.

This journal is directed to academia researchers, industry professionals, members of government and military organizations, and all people that have interest in the area of information security and cryptography in order to disseminate and share their new technologies, scientific discoveries and research contributions.

The creation of this periodical is due the necessity to solve a gap represented by the lack of a technical-scientific brazilian journal that emphasizes information security and cryptography. In this manner, ENIGMA – Brazilian Journal of Information Security and Cryptography – must provide this demand, publishing papers of high quality within the international state-of-the-art. Therefore, ENIGMA – Brazilian Journal of Information Security and Cryptography – will fulfill this demand, and will publish state-of-art and original research papers and timely review articles on the theory, design, and evaluation of all aspects of information, network and system security.

II. About Volume 3, Issue 1 of Enigma

In this first issue of Volume 3 of ENIGMA – Brazilian Journal of Information Security and Cryptography – 4 papers are published, and in this section we briefly describe the contribution of each of these papers.

The first selected paper, entitled "Machine Learning for Cryptographic Algorithm Identification", studies classical cryptographic algorithms identification with the support of machine learning. It shows the viability of classifying cryptograms, according to their encryption algorithm, by using data mining techniques. In this paper experiment, the random probability for guessing those algorithms is 25%. However, the mean value of correctness obtained reaches 97,23%. In addition, it seems that it is possible to increase this value.

The selected paper "A Wireless Physically Secure Key Distribution System" presents how to achieve wireless secure communication at fast speeds with bit-to-bit symmetric encryption. A fast and secure key distribution system is shown that operates in classical channels but with a dynamic protection given by the low noise of the light signal. The binary signals in transit in the channel are protected by coding with random bases and by the addition of physical noise that is recorded and added bit by bit to the signals. The hardware requirements is described as well as how to calculate the security level associated with the communication. A correct implemented system would offer privacy at a top-secret level for the users. Furthermore, the correct choice of parameters creates post-quantum security privacy.

In the next selected paper, "Future Internet and Reconfigurable Computing: Considerations on Flexibility and Security", the authors argue that it is necessary to approximate the areas of computer architecture and computer networks, or more specifically bridge the gap between research in Reconfigurable Computing and in the Future Internet Architectures. A brief survey with plainly successful examples indicates how some of the needs and future internet objectives can be met through reconfigurable computing, especially with respect to flexibility and security requirements.

The last paper in this ENIGMA issue, the invited paper "A Secure Protocol for Exchanging Cards in P2P Trading Card Games Based on Transferable e-Cash", which was considered the best paper of SBSeg´2015, presents a set of requirements for allowing secure trades in P2P TCGs, defining the cheating types that need to be detected. A transferable e-cash protocol

E. T. Ueda, Institute for Technological Research of the State of São Paulo, edutakeo@usp.br

M. S. M. A. Notare, IEEE Latin America Transactions Editor in Chief, FAERO Technology University in Fly Transportation, mirela@ieee.org

R. T. de Sousa Júnior, University of Brasilia, desousa@unb.br

is adapted for creating a concrete scheme that fulfills those requirements. The proposed scheme is based on P-signatures, allowing a vector of messages to be signed, which is combined with a compact blind signature scheme in the asymmetric pairing setting to allow a more memory-efficient representation. According to preliminary analysis, the scheme is quite efficient to be used in practice.

III. Conclusion

ENIGMA – Brazilian Journal of Information Security and Cryptography – is now in its third year. By adopting since its creation the best practices from IEEE Transactions publications, we hope that soon this journal will become a reference among the leading international publications dedicated to information security and cryptography.

With the publication of this journal issue, Brazil is taking another step towards the future, because the ENIGMA Journal is an important tool for communication and integration of knowledge between universities, research centers, industries, government or military institutions around the world. Moreover, as threats to information security and privacy are risks for any nation, the ENIGMA journal can envision the international community.

Acknowledgments

We would like to thank all the authors who contributed with their papers for this issue of the ENIGMA journal; this publication would not exist if not for the dedication to their research. We must also thank all reviewers who worked very hard and in a timely fashion, so that we could select high quality papers. We are grateful to National Network of Information Security and Cryptography (RENASIC) and the Cyber Defense Center (CDCiber) of the Defense Ministry of Brazil for their support in the creation of this journal, and the University of Brasilia (UnB) for providing space on one of their servers to host the official website of this journal.

Eduardo Takeo Ueda received the Ph.D. degree in Electrical Engineering in 2012, MSc degree in Computer Science in 2007, both from University of São Paulo (USP), and Specialist degree in Health Informatics in 2014 by Federal University of São Paulo (UNIFESP). He also holds a Mathematics BSc by the São Paulo State University (UNESP), year 2000. His research interest includes topics of Cryptographic Algorithms and Protocols, Models of Access Control, and Computational Trust and Reputation. He has been committee Professor in Senac University Center of São Paulo, Master's Thesis Advisor in Institute for Technological Research of the State of São Paulo, member in conferences program commitees and reviewer of scientific journals. Currently, he is member of the National Network of Information Security and Cryptography (RENASIC), and Editor in Chief of ENIGMA – Brazilian Journal of Information Security and Cryptography.
http://lattes.cnpq.br/8367973725203446.

Mirela Sechi Moretti Annoni Notare received her Ph.D. and MSc degrees from the Federal University of Santa Catarina (UFSC) and a BSc degree from Passo Fundo University – all the three degrees in Computer Science. She is Professor at FAERO Tecnology University in Fly Transportation. Her main research of interest focuses on the proposition of security management solutions for Wireless, Mobile, Sensor Ad- Hoc Networks, Intelligent Vehicular Networks and Fly Transportation. Dra. Mirela Notare published widely in these areas. She also received several awards and citations, such as National Award for Telecommunication Software, British Library, TV Globo, INRIA and Elsevier Science. She served as General Co-chair for the I2TS (International Information and Telecommunication Technologies Symposium) and Program Co-Chair for the IEEE MobiWac (Mobility and Wireless Access Workshop) and IEEE ISCC. She has been a committee member in several scientific conferences, including ACM MSWiM, IEEE/ACM ANSS, IEEE ICC, IEEE IPDPS/WMAN IEEE/SBC SSI, and IEEE Globecom/Ad-Hoc, Sensor and Mesh Networking Symposium. She has been Guest Editor for several international journals, such as JOIN (The International Journal of Interconnection Networks), IJWMC (Journal of Wireless and Mobile Computing), JBCS (Journal of Brazilian Computer Society), Elsevier ScienceJPDC (The International Journal of Parallel and Distributed Computing), Wiley & Sons Journal of Wireless Communications & Mobile Computing, and Wiley InterScience Journal Concurrency & Computation: Practice & Experience. She has some Books and Chapters – Protocol Engineering with LOTOS/ISO (UFSC) and Solutions to Parallel and Distributed Computing Problems (Wiley Inter Science), for instance. She is the current Regional Committees Chair of IEEE NoticIEEEro, Editorial Advisory Board of IEEE Spectrum/The Institute newsletter, Editor in Chief of IEEE Latin America Transactions magazine and Associate Editor in Chief of ENIGMA – Brazilian Journal of Information Security and Cryptography. She is the founding and president of STS Co, a senior member (22 years) of IEEE, and member of SBrT and SBC societies.
http://lattes.cnpq.br/8224632340074096.

Rafael Timóteo de Sousa Júnior graduated in Electrical Engineering, from the Federal University of Paraíba – UFPB, Campina Grande-PB, Brazil, 1984, and got his Doctorate Degree in Telecommunications, from the University of Rennes 1, Rennes, France, 1988. From 2006 to 2007, supported by the Brazilian R&D Agency CNPq, He took a sabbatical year in the Group for the Security of Information Systems and Networks, at Ecole Superiéure d´Electricité, Rennes, France. He worked as a software and network engineer in the private sector from 1989 to 1996. Since 1996, he is a Network Engineering Professor in the Electrical Engineering Department, at the University of Brasília, Brazil, where he is a member of the Post-Graduate Program on Electrical Engineering (PPGEE) and supervises the Decision Technologies Laboratory (LATITUDE). He is a member of the Brazilian Computer Society (SBC), member of the National Network of Information Security and Cryptography (RENASIC) and coordinates the Unit 6 of the Brazilian National Science and Technology Institute (INCT) on Cyber Defense. He has developed research in information and network security, distributed data services and knowledge discovery for intrusion and fraud detection, as well as signal processing, energy harvesting and security at the physical layer.
http://lattes.cnpq.br/3196088341529197.