ENIGMA – Brazilian Journal of Information Security and Cryptography
Volume 1 Issue 1 September 2014

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 1 of ENIGMA – Brazilian Journal of Information Security and Cryptography. Papers submissions were accepted in English, Portuguese and Spanish. In this first issue, 10 papers are published, of which 4 were peer-reviewed while the other 6 were invited and reviwed by the editorial board of the journal. In addition, 2 of the 6 invited papers are Best Papers from conferences CIBSI'2013 and TIBETS'2013 respectively.**

***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 scientist in the history of computing. The world as we all know today would probably be very different it were not Turing's scientific contributions to humanity.

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.

E. T. Ueda, Senac University Center of São Paulo, edutakeo@gmail.com
M. S. M. A. Notare, IEEE Latin America Transactions Editor in Chief, IEEE South Brazil, mirela@ieee.org
R. T. de Sousa Júnior, University of Brasilia, desousa@unb.br

II. ABOUT VOLUME 1, ISSUE 1 OF ENIGMA

In this first issue of Volume 1 of ENIGMA – Brazilian Journal of Information Security and Cryptography – 10 papers were published, and in this section we briefly describe the contribution of each of these papers.

The first paper entitled "*Unconditionally Secure Quantum Communications via Decoherence-Free Subspaces*" by E. B. Guedes and F. M. de Assis, shows how to use decoherence-free subspaces over collective-noise quantum channels to convey classical information in perfect secrecy. The results obtained show how secure communication protocols can be simplified while reducing significantly the communication overhead.

The second paper entitled "*Revocation of User Certificates in a Military Ad Hoc Network*" by J. Jormakka and H. Jormakka, presents a scheme for revoking certificates in a medium-small size semi ad-hoc military network. Note that the solution can also be used in the civilian applications, such as police and crisis management, among others. It describes the functionalities of a protocol to handle certificates, a set of policy rules in a node for handling certificates and an analysis how the proposed mechanisms can mitigate attacks on the certificate revocation solution.

The paper "*Synthetic Steganographic Series and Finance*" by P. C. Ritchey and V. J. Rego, provide a comprehensive methodology that enables an agent to embed secret messages in public data that is sent or broadcasted to a receiving agent. The experiments have shown that one can develop a relatively sophisticated and practical secret-key stego-systems for a variety of applications including financial market based applications.

The paper "*Securing Automation Systems against Malware Intrusion*" by R. Fitz and W. A. Halang, focuses on the fact that computers employed for automation and control purposes are today more and more connected to networks, and thereby could be endangered by malware. As such, new architectures for their hardware and software as presented in this paper and proven to be necessary to solve the security problem due to their intrinsic properties.

The paper entitled "*Isomorphism Theorem and Cryptology*" by R. L. de Carvalho and F. L. de Mello, presents a theory of computational study based on recursive functions computability and presents innovative parallel mechanism relevant to enhance the performance of cryptography schemes. The main issue, as discussed in this paper, is closley related to the Isomorphism Theorem which supports the Church-Turing

thesis and provides a connection between cryptology and linguistics.

The paper entitled "*Harnessing Nature's Randomness: Physical Random Number Generator*" by G. A. Barbosa, presents some guidelines for construction of a fast (telecommunication speed) Physical Random Number Generator. It discusses the fundamental physical elements involved, technicalities of signal recording, its limitations, and the final bit extraction The need for randomness tests is emphasized and the impossibility of guaranteeing true randomness of a finite sequence is discussed.

The paper "*QC-MDPC McEliece: an Optimized Implementation of a New McEliece Variant*" by H. O. Martins and A. C. A. Nascimento, presents the implementation of an optimized version of a McEliece variant. The McEliece cryptosystem is an example of code-based cryptography which is an alternative to the most popular and commercial cryptosystems nowadays as it is believed to be immune to quantum computing. It has simple and uses fast algorithms. Its main drawback is the size of the keys it has to deal with. By substituting the Goppa codes of the McEliece original proposalby LDPC and MDPC codes it's possible to achieve much smaller keys.

The paper "*Securing Web Applications: Techniques and Challenges*" by M. Vieira, discusses key techniques for security testing and assessment, providing the basis for understanding existing research challenges on developing and deploying secure web applications. The paper highlighted several research challenges in an attempt to motivate further research in these topics. The paper did not intend to provide a comprehensive survey. However, it does focus on key promising aspects in which research is need, and can be applied in the context of large-scale software based industry.

The ninth paper entitled "*Design of a Set of Software Tools for Side-Channel Attacks*" by A. F. Rodrígues et al, is the Best Paper of CIBSI'2013 (Congreso Iberoamericano de Seguridad Informática). In this paper, the authors present the first experimental results of a set of software tools for side channels attacks on cryptographic devices. The authors discuss the main types of attack, with an emphasis on attack called for an analysis of power consumption.

The last paper entitled "*Content related to Computing Security on Computer Engineering Degree according to International Professional Certificates*" by D. G. Rosado et al, is an extension of the best selectd papers of TIBETS'2013 (Taller Iberoamericano de Enseñanza e Innovación Educativa en Seguridad de la Información). This paper establishes a transverse guide for implementing information security content for courses and modules in the area of informatics or computer. The authors argue that basic knowledge of information security should be taught to students from the beginning of their training at university or college. In addition, the integrated content in the curriculum of the institutions should be based on professional certifications to prepare students for the industry.

III. CONCLUSION

ENIGMA – Brazilian Journal of Information Security and Cryptography – is a young publication but the beginning follow the best practices adopted by IEEE Transactions publications. It is hoped that soon this journal will become an icon of reference among the leading international publication dedicated to information security and cryptography.

With the creation of this journal the Brazil a considerable step toward the future, because 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, threats to security and privacy of information are the enemy of any nation, which justifies this creation of this ENIGMA journal, indeed a unique initiatives for Brazil.

ACKNOWLEDGEMENTS

Initially, we would like to thank all the authors who contributed with their papers for the first 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 of papers. We are grateful to National Network of Information Security and Cryptography (RENASIC) and the Cyber Defense Center (CDCiber) of the Defense Minister 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. Moreover, we wish to thank Coronel Luiz Carlos Rodrigues Pereira and Major Luciano de Oliveira for their support and in believing in this journal as well as their continuous help to get the printed version of this first issue. Last but not least, thanks to Itamar Annoni Notare for his hard work and for his assistance in the revision process as well as on the formatting this journal.

Eduardo Takeo Ueda received the Ph.D. degree in Electrical Engineering in 2012, and MSc degree in Computer Science in 2007, both from University of São Paulo (USP). He also holds a Mathematics degree 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 member in conferences and reviewer of scientifics journals. Currently, he is Professor in Senac University Center of São Paulo, Master's Thesis Advisor in Institute for Technological Research of São Paulo, member of the Brazilian Computer Society (SBC), member of 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. Her main research of interest focuses on the proposition of security management solutions for Wireless, Mobile, Sensor and Ad-Hoc Networks. 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 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 (19 years) of IEEE, and member of SBrT and SBC societies. http://lattes.cnpq.br/8224632340074096.

Rafael Timóteo de Sousa Júnior, was born in Campina Grande – PB, Brazil, on June 24, 1961. He 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. 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. From 2006 to 2007, supported by the Brazilian R&D Agency CNPq, on leave from the University of Brasília, He took a sabbatical year in the Group for the Security of Information Systems and Networks, at Ecole Superiéure d´Electricité, Rennes, France. He is a member of the Post-Graduate Program on Electrical Engineering (PPGEE) and supervises the Decision Technologies Laboratory (LATITUDE) of the University of Brasília. His field of study is distributed systems and network management and security. http://lattes.cnpq.br/3196088341529197