Neural Synchronization and Light-weight Cryptography in Embedded Systems

Vom Promotionsausschuss der

Technischen Universität Hamburg-Harburg

zur Erlangung des akademischen Grades
Doktor Ingenieur
genehmigte Dissertation

von

Oscar Mauricio Reyes Torres

aus

Bucaramanga

2012

1. Gutachter: Prof. Dr. Karl-Heinz Zimmermann,
   Institut für Rechnertechnologie, Technische Universität Hamburg-Harburg

2. Gutachter: Prof. Dr. Klaus Obermayer,
   Institut für Softwaretechnik und Theoretische Informatik, Technische Universität Berlin

3. Gutachter: Dr. Andreas Ruttor,
   Institut für Softwaretechnik und Theoretische Informatik, Technische Universität Berlin

Tag der mündlichen Prüfung: 23.05.2012

Vorsitzender des Prüfungsausschusses: Prof. Dr. Sven-Ole Voigt,
Institut für Zuverlässiges Rechnen, Technische Universität Hamburg-Harburg

Gedruckt mit Unterstützung des Deutschen Akademischen Austauschdienstes

Berichte aus der Informatik

Oscar Mauricio Reyes Torres

Neural Synchronization and Light-weight Cryptography in Embedded Systems

Gedruckt mit Unterstützung des Deutschen Akademischen Austauschdienstes

Shaker Verlag
Aachen 2012

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Zugl.: Hamburg-Harburg, Techn. Univ., Diss., 2012

Printed in Germany.

ISBN 978-3-8440-1233-0
ISSN 0945-0807

Shaker Verlag GmbH • P.O. BOX 101818 • D-52018 Aachen
Phone: 0049/2407/9596-0 • Telefax: 0049/2407/9596-9
Internet: www.shaker.de • e-mail: info@shaker.de

To my beloved wife and children: Ivonne, Andrés and Alejandra

Abstract

Synchronization is a phenomenon that is widely studied in different fields. In the case of artificial neural networks, two feed-forward networks can eventually synchronize by exchanging their outputs and applying a suitable learning rule. The dynamics of this process has been studied for the so-called permutation parity machine. This is a binary variant of the well-known tree parity machine in which the weights are small integers that are not adjusted, but completely replaced during each learning step. In the permutation parity machine, a new set of weights is pseudo-randomly drawn from a pool of binary data after the outputs have been exchanged. Synchronization is a result of competing stochastic forces given by a sequence of increasing and decreasing overlaps. This sequence constitutes a random process endowed with the Markov property. More concretely, the mutual learning process can be described by a first-order Markov chain where synchronization amounts to the stationarity of the chain.

Nowadays, cryptography plays an ever more important role in information security given the countless scenarios in which information exchange requires different levels of privacy, secrecy or reliability. To this end, cryptographic algorithms based on neural synchronization can be used, since mutual learning leads to synchronization much faster than learning by examples.

In this work, a key exchange protocol based on permutation parity machines has been studied. It has been proved that even though the weights used during each learning step are not strongly correlated, synchronization still occurs. Moreover, the lack of correlation among the weights during the synchronization process makes the key exchange protocol robust not only against common attacks, e.g. simple or geometric attacks, but also against attacks based on non-standard schemes, such as majority, genetic or probabilistic attacks.

Permutation parity machines make use of a more complex learning rule than the tree parity machines, especially due to the process of weight assignment. Nevertheless, the simplicity of the network compensates for the complexity of the learning rule in terms of hardware implementation. Additionally, the use of a permutation network based on a linear feedback shift register helps to reduce considerably the complexity in the assignment of the weights during the learning step.

The key exchange protocol based on permutation parity machines does not require lengthy mathematical calculations and so is suitable for implementation by embedded systems where hardware constraints are decisive. Various alternatives of hardware implementations have been considered, including FPGA, RISC MCU, RFID tags and NFC devices.

Acknowledgements

There are many people who, in different ways, have collaborated to make this work come a reality. My special thanks go to:

- My supervisor, Prof. Dr. Karl-Heinz Zimmermann, for giving me the opportunity of being his student and for his invaluable support and guidance during every single step of the research.
- My examiners, Prof. Dr. Klaus Obermayer and Dr. Andreas Ruttor for their contribution during the last part of this journey.
- Dipl. Ing. Ingo Kopitzke for having taken a step forward in the fascinating field of neural cryptography.
- The German Academic Exchange Service (DAAD), Industrial University of Santander (UIS) and the Administrative Department of Science, Technology and Innovation (COLCIENCIAS) for the financial support. In particular, I wish to express my gratitude to Mrs. Patricia Guzman, Mrs. Elke Massa and Mrs. Silke Hamacher for their willingness to help me with all the fellowship issues.
- The technical staff of the Institute of Computer Technology: Stefan Just, Egon Kirsch and Wolfgang Brand, for their friendship and support during the course of this work.
- Svetlana Torgasin, Cem Bassoy, Fabian May and Karsten Becker who have helped me during my work in one way or another.
- Kashif, Mahwish, Srinivasa, Cristina, Nico and Esteban for their friendship, the enjoyable conversations and their positive feedback.
- My parents and brothers, Jorge H. and Gustavo A., and their families, for their constant support and love during this journey.

Finally, my most heartfelt thank to Ivonne Andrea, my beloved wife, for her unconditional love and constant words of encouragement and faith. And a special dedication deserve my children, Andrés Mauricio and Alejandra, who are light and motivation in my life.

List of Abbreviations

ANN	Artificial neural network
APDU	Application data unit
API	Application programming interface
ASIC	Application-specific integrated circuit
BSGD	Baby steps gradient descent
FPGA	Field-programmable gate array
FSM	Finite state machine
HF	High frequency
HSM	Hierarchical state machine
IP core	Intellectual property core
ISO	International Organization for Standardization
LF	Low frequency
LFSR	Linear feedback shift register
LUT	Lookup table
MITM	Man-in-the-middle attack
NDEF	NFC data exchange format
NFC	Near field communication
NPP	NDEF push protocol
P2P	Peer-to-peer
PCD	Proximity coupling device
PICC	Proximity integrated circuit card
PPM	Permutation parity machine
PRNG	Pseudorandom number generator
QMC	Quine-McCluskey minimization algorithm
RAM	Random access memory
RF	Radio frequency
RFID	Radio frequency identification
SNEP	Simple NDEF exchange protocol
TPM	Tree parity machine
TPMRA	Tree parity machine rekeying architecture
UHF	Ultra high frequency
WLAN	Wireless local area network

Contents

1 Introduction **1**
- 1.1 Frame of Reference and Background . . . 1
- 1.2 Contribution of this Work . . . 2
- 1.3 Organization . . . 3

2 Fundamentals **5**
- 2.1 Neural Synchronization . . . 5
  - 2.1.1 Tree Parity Machines . . . 5
  - 2.1.2 Learning Process . . . 7
  - 2.1.3 Synchronization Process . . . 7
- 2.2 Neural Cryptography . . . 8
- 2.3 Security in Embedded Systems . . . 9
  - 2.3.1 Radio Frequency Identification . . . 10
  - 2.3.2 Near Field Communication . . . 11

3 Permutation Parity Machines **13**
- 3.1 Structure . . . 13
- 3.2 Learning Rule . . . 15
  - 3.2.1 Inner Rounds . . . 16
  - 3.2.2 Outer Rounds . . . 17
- 3.3 Order Parameters . . . 18

4 Dynamics of the Mutual Learning Process **23**
- 4.1 Effects of the Learning Rule during Inner Rounds . . . 23
  - 4.1.1 Stochastic Forces . . . 23
  - 4.1.2 Synchronization Steps . . . 24
  - 4.1.3 Increasing and Decreasing Steps . . . 27
  - 4.1.4 Distribution of the State Vector . . . 29
- 4.2 Synchronization . . . 30
  - 4.2.1 Completion of an Outer Round . . . 31
  - 4.2.2 Evolution of the Overlap . . . 32
  - 4.2.3 Synchronization Time . . . 36
- 4.3 Finite-size Effects . . . 40
- 4.4 Outlook . . . 41

5 Key Exchange Protocol Based on PPMs **43**
5.1 Description . . . 43
5.2 Cryptanalysis Based on Unidirectional Learning . . . 44
5.2.1 Simple Attack . . . 45
5.2.2 Geometric Attack . . . 45
5.2.3 Probability of Success . . . 48
5.3 Attacks Using an Ensemble of Networks . . . 51
5.3.1 Majority Attack . . . 52
5.3.2 Genetic Attack . . . 52
5.4 Other Cryptanalytic Techniques . . . 55
5.4.1 Algebraic Attack . . . 55
5.4.2 Probabilistic Attack . . . 59
5.5 Outlook . . . 63

6 Implementation **67**
6.1 Design of a PPM Core . . . 67
6.1.1 General Conditions . . . 67
6.1.2 Neural Network Unit . . . 69
6.1.3 Input and Weight Generation . . . 69
6.1.4 State Vector Unit . . . 72
6.1.5 Bit-Packaging . . . 74
6.2 Hierarchical State Machine . . . 75
6.3 Communications Protocols . . . 78
6.3.1 RFID System Based on ISO/IEC 14443-4 . . . 78
6.3.2 NFC in Peer-to-Peer Mode . . . 79
6.4 Outlook . . . 82

7 Conclusions and Outlook **85**

A General Boolean Equations to Describe a PPM **89**
A.1 Boolean algebra . . . 89
A.2 Output of a PPM as a Sum of Products . . . 89

B RFID Transmission Protocol: ISO/IEC 14443-4 **93**

Bibliography **97**

List of Figures

2.1 General structure of a tree parity machine. 6

3.1 General structure of a permutation parity machine. 14
3.2 Some possible output layer configurations for permutation parity machines 15
3.3 Average number of bits exchanged to achieved synchronization . . 16
3.4 Inner and outer rounds during the mutual learning process of permutation parity machines. 17
3.5 Error probabilities between two perceptrons in dependence of normalized overlap 21

4.1 Error probability of corresponding hidden units in two permutation parity machines 25
4.2 Effect of the parameters G and N on the probability of synchronization steps for mutual learning 26
4.3 Effect of the parameters G and N on the probability of increasing steps for mutual learning 29
4.4 Probability distribution of the state vectors 31
4.5 Expected value of the outer round duration 32
4.6 Time evolution of the Markov chain 35
4.7 Effect of the number of inputs on the expected value of the number of outer rounds 37
4.8 Effect of the number of inputs on the expected value of synchronization time 37
4.9 Cumulative distribution of the synchronization time between two permutation parity machines 39
4.10 Probability of increasing the overlap during the outer rounds depending on normalized overlap 40

5.1 Key exchange protocol between two permutation parity machines. 44
5.2 Probability of increasing steps in the case of simple attack 46
5.3 Probability of increasing steps in the case of geometric attack . . 49
5.4 Probability of increasing steps and different types of interaction . 49
5.5 Probability of success of the simple attack 50
5.6 Probability of success of the geometric attack 51
5.7 Evolution of normalized overlap for a variant of the majority attack 53
5.8 Probability of success of the genetic attack 54

5.9 Representation of an outer round as a block cipher 56
5.10 Cost function of exclusive-or gate 62

6.1 Block diagram of a system implementing a PPM core to perform symmetric cryptography. 68
6.2 Block diagram of the PPM core 68
6.3 Neural network unit. 70
6.4 Mapping process to select one single weight 71
6.5 Relative frequency of occurrence of the n-element subsets of weights used more than once during the same outer round. 73
6.6 Hardware implementation of the state vector unit 73
6.7 HSM of the permutation parity machine. 77
6.8 Resource usage in an FPGA-based PPM core 78
6.9 Sequence diagram of the key exchange protocol for an RFID system. 80
6.10 FSM of an Android application using NFC to implement the key exchange protocol based on PPMs. 81

B.1 ISO/OSI layer model in a smart card. 93
B.2 Sequence diagram of the transmission between PCD and PICC . . 94
B.3 Block format of a frame in ISO/IEC 14443-4 95
B.4 Application data unit 95

List of Tables

2.1 RFID Standards 10

5.1 Results of an algebraic attack using QMC for $N = 2$ 58
5.2 Simulation time of an algebraic attack using QMC 59
5.3 Probability of success of a probabilistic attack using BSGD 63
5.4 Simulation time of a probabilistic attack using BSGD 63

6.1 Efficiency of bit packaging for different packet sizes compared with the dynamical assignment 75
6.2 Resource usage of implementations of different key exchange protocols 79