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

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.