AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
CAIRO – EGYPT
Computer and Systems Engineering Department

On the Improvement of Neural Key Exchange

A Thesis
Submitted in partial fulfillment for the requirements of the degree of
Master of Science in Electrical Engineering

Submitted by

Ahmed Mohamed Allam Mohamed
Computer and Systems Engineering Dept.
Faculty of Engineering - Ain Shams University

Supervised by

Prof. Hazem Mohammed Abbas
Professor. Computer and Systems Engineering Dept.
Faculty of Engineering - Ain Shams University

Prof. Mohamed Watheq El-Kharashi
Professor Computer and Systems Eng. Dept.
Faculty of Engineering - Ain Shams University

Feb 2014

AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
CAIRO - EGYPT

Examiners Committee

Name : **Ahmed Mohamed Allam Mohamed**
Thesis : **On the Improvement of Neural Key Exchange**
Degree: **Master of Science in Electrical Engineering (Computer and Systems Engineering)**

Name, Title and Affiliation — Signature

1. Hussein Ismail Shahin **……**

Professor, Computer and systems department, Faculty of Engineering, Ain Shams University.

2. Mohsen Rashwan **……**

Professor, Department of electronics and electrical communications, Faculty of Engineering, Cairo University.

3. Hazem Mohamed Abbas ……..

Professor, Computer and systems department, Faculty of Engineering, Ain Shams University.

4. Mohamed Watheq El-Kharashi ……...

Associate Professor, Computer and systems department, Faculty of Engineering, Ain Shams University.

Date: 15/6/2013

To My Father

To My Mother

To My Wife

I present to you this thesis

May I by this express my deep gratitude and love

Thanks

You make me reach this successful step in my life

C.V.

Name of the Researcher	Ahmed Mohamed Allam Mohamed
Date of Birth	26 January 1986
Place of Birth	Cairo, Egypt
First University Degree	B.Sc in Electrical Engineering
Department	Computer and Systems Engineering Department
University	Ain Shams University
Date of Degree	June 2008

STATEMENT

This Thesis is submitted to Ain Shams University in partial fulfillment of the degree of Master of Science in Electrical Engineering.

The work included in this thesis was carried out by the author in the department of electronics and communications engineering, Ain Shams University.

No part of this Thesis has been submitted for a degree or a qualification at any other university or institute.

Name : Ahmed Mohamed Allam Mohamed
Signature: Ahmed Mohamed Allam Mohamed
Date : 2014-02-07

Acknowledgment

First of all, I would like to thank Allah for his blessing and generosity that without them I will not do anything in this research. I believe that ideas are not only generated from the mechanistic mind but also are gifts from Allah.

Second, I would like to thank prof. Hazem Abbas and Prof. Mohamed Watheq El-Kharashi very much for their appreciation and guiding me through this research as he actually proved that they are real professors as they listened to me and encouraged me all time. Their efforts in teaching me how to write a good paper has a significant impact in my thesis.

I would like also to thank Dr. Andreas Ruttor for his invaluable discussions about his work in neural cryptography. Dr. Andreas was very cooperative and gentle. He was never bored from my questions in the preparation phase for the subject as he is one of the major contributors in the field of neural cryptography.

Special thanks to Dr. Hatem El Refaai who was the first kind of support and encouragement from the first year in electrical engineering department when he taught me quantum mechanics , he listened to my ideas and discussed me though he had no time for that. Dr. Hatem was and still my mentor in science and many scientific skills from out of the box thinking to critical thinking and philosophy of science was originally amplified from

Abstract

Key exchange is one of the major concerns in cryptography. Many protocols are proposed since the seminal paper of Diffie-Hellman which introduced the concept of the public key. While many of the protocols are proven to be secure, one of the major drawback is it depends on a computationally intensive mathematical problems like modular exponentiation and discrete logarithm. While these algorithms are systematic, dealing with long keys is not an easy task. The long key used in public key cryptography is a must in order to prevent exhaustive search and force the attacker to attempt solving the hard mathematical problem.

If these algorithms are required to be implemented as software programs, the developer should create an algorithm to deal with slice of the key or plaintext with the maximum data length that the processor supports but this is very time consuming. It can also be developed on FPGAs or ASIC chips to exploit the parallel nature of these devices. However, the cryptographic keys are really very long and there is no FPGA or ASIC that can support doing mathematical computations on it and even this requires dealing with slices of key but with larger size than that is supported by processors.

Most of the two previous directions focus on classical cryptography to achieve fast secure key exchange. In this thesis, we aim to explore non classical approaches for key exchange and see whether it can provide an alternative mechanism for fast secure key exchange.

Neural cryptography is found to be a recent non classical approach for achieving key exchange between two parties. It is based on a physical phenomenon called synchronization and a learning approach called mutual learning that achieves the synchronization by training the networks using identical input patterns and exchanging the output values

Neural cryptography is a simple protocol which has several advantages in terms of implementation and execution such as simple arithmetic, scalability and parallel implementation. However, the security of the neural cryptography is still under arguments. The classical key exchange protocols outperform neural cryptography in terms of mathematical formulation and security proof. Relying on well defined hard mathematical problems, it is easy to judge the security strength of a classical cryptographic protocol. However, neural cryptography is still a new area in the field of cryptography and its security is based on probabilistic analysis. The bidirectional learning between the two communicating parties has an advantage over the unidirectional learning that the attacker uses in terms of synchronization

time.

This thesis aims to explore the neural cryptography as an alternative strategy for key exchange. In order to reach this goal, we focus on three main directions. First, we target improving the security of neural cryptography. Second, the neural key exchange protocol is analyzed from security perspective. Third, we extend the neural cryptography so that it provides more cryptographic services.

In order to achieve the first goal, an algorithm is proposed to improve the security of neural cryptography by injecting controlled noise over the communication channel where only the two parties can detect and remove. The algorithm comes in two forms. One injects the noise on the input channel which is called *Synchronization with Common Secret Feedback*(SCSFB) and one injects the noise on the output channel which we call (Dont Trust My Partner)(DTMP). The two algorithms are combined together to achieve higher security. An attacker listening to the communication will not be able to cancel the noise and hence will not be able to learn so that it cannot obtain the final session key. Moreover, the mutual learning algorithm that is the core of the neural cryptography is modified in order to make the neural key exchange authenticated so that only two specific parties can obtain the final key.

The second goal is accomplished by investigating the neural cryptography parameters to uncover its contribution to neural dynamics and hence its impact on the security of the algorithm. Some results are obtained from our analysis. The parameter N which represents the number of weights per network is analyzed and found that it contributes to the protocol security significantly and its impact appears especially when the attacker starts with initial weight configurations close to that of any of the two parties. It is found that this parameter is responsible for increasing the uncertainty of the network output and reducing the probability that the attacker has a frequent output matching with any of the two parties. Also, the input pattern generation mechanism is investigated. The *Linear Feedback Shift Register* (LFSR) was proposed previously to be an input vector generator that leads to fast synchronization. This mechanism is investigated and found to reduce the security of the protocol significantly. Also, an attack strategy is proposed that works on analyzing the difference between the successive input patterns and estimating the hidden perceptrons outputs.

Another part achieved within the second goal is investigating the robustness of neural cryptography against physical implementation attacks. The power analysis attack is applied to the neural cryptography in order to find a vulnerability to break into the protocol. After that, a countermeasure hiding technique is implemented to make the power consumption uniform

in order to prevent power analysis attacks from revealing information about the secret key. Moreover, two Trojan insertion based attacks are proposed to reveal secret information via either side channel or public channel.

In order to achieve the third goal, the neural cryptography protocol is extended to deal with multi party configuration which is termed at Neural Group Key Exchange (NGKE). Two algorithms are proposed to exchange key between multiple parties with logarithmic complexity using binary tree architecture. Moreover, a password authenticated form of the NGKE protocol is proposed so that only legal parties can learn from the information exchanged through the channel.

Contents