FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

ASSIGNMENT OF MASTER'S THESIS

Title:	Multivariate cryptography
Student:	Bc. Jan Rahm
Supervisor:	Ing. Jiří Buček, Ph.D.
Study Programme:	Informatics
Study Branch:	Computer Security
Department:	Department of Information Security
Validity:	Until the end of summer semester 2020/21

Instructions

Study the topic of multivariate cryptography as one of the approaches to post-quantum cryptography.
Select a specific algorithm based on multivariate cryptography such as Unbalanced Oil and Vinegar (UOV).
Create an educational implementation of the selected algorithm in Wolfram Mathematica.
Examine the reference implementation of the selected algorithm. Evaluate its time and memory complexity on a PC. Implement the algorithm on a chosen microcontroller such as ARM or ESP32 and evaluate its usability in an embedded environment.
Compare the time and memory complexity of the selected algorithm with a conventional algorithm such as RSA or ECDSA.

References

Will be provided by the supervisor.

prof. Ing. Róbert Lórencz, CSc.
Head of Department

doc. RNDr. Ing. Marcel Jiřina, Ph.D.
Dean

Prague February 5, 2020

FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Master's thesis

Multivariate cryptography

Bc. Jan Rahm

Department of Information Security
Supervisor: Ing. Jiří Buček, Ph.D.

February 18, 2020

Acknowledgements

I would like to thank Ing. Jiří Buček, Ph.D. for the willingness, consultation and valuable advice he gave me.

Declaration

I hereby declare that the presented thesis is my own work and that I have cited all sources of information in accordance with the Guideline for adhering to ethical principles when elaborating an academic final thesis.

I acknowledge that my thesis is subject to the rights and obligations stipulated by the Act No. 121/2000 Coll., the Copyright Act, as amended, in particular that the Czech Technical University in Prague has the right to conclude a license agreement on the utilization of this thesis as a school work under the provisions of Article 60 (1) of the Act.

In Prague on February 18, 2020 . . . . . .

Czech Technical University in Prague
Faculty of Information Technology

Citation of this thesis

Rahm, Jan. *Multivariate cryptography.* Master's thesis. Czech Technical University in Prague, Faculty of Information Technology, 2020.

Abstrakt

V několika větách shrňte obsah a přínos této práce v českém jazyce.

Klíčová slova Replace with comma-separated list of keywords in Czech.

Abstract

Summarize the contents and contribution of your work in a few sentences in English language.

Keywords Replace with comma-separated list of keywords in English.

Contents

List of Figures

Introduction

Chapter 1

Basic terms and definitions

Description; How it works

Chapter 2

Realisation

Mathematica; Specific implementation + difference on IoT; (presentation for teaching)

Chapter 3

Testing and discussion

On what was tested (PC and EPS32/ARM); Comparasition with RSA,ECDSA; Time and memory complexity; Usability in an embedded enviroment;

Conclusion

How good I was...

Appendix A

Acronyms

GUI Graphical user interface

XML Extensible markup language

Appendix B

Contents of enclosed CD

- `readme.txt` ..... the file with CD contents description
- `exe` ..... the directory with executables
- `src` ..... the directory of source codes
  - `mathematica` ..... implementation in Mathematica
  - `thesis` ..... the directory of LaTeX source codes of the thesis
- `text` ..... the thesis text directory
  - `thesis.pdf` ..... the thesis text in PDF format