UNIVERSIDADE FEDERAL DE SANTA CATARINA
Centro Tecnológico
Departamento de Informática e Estatística
Programa de Pós-Graduação em Ciência da Computação

COURSE PROGRAM

1) Identification

Course: INE410134 - Post Quantum Cryptography and Computation
Credits: 45 hours/class (3 credits)
Professors: Ricardo Felipe Custódio e Jean Everson Martina
Courses: Master and Doctorate
Semester: 2018/2 until the present date.

2) Prerequisites

There are no prerequisites for this course. Some prior familiarity with cryptography or formal methods may be helpful, but all necessary background will be covered in class.

3) Aim

Post-quantum cryptography. Quantum computing. Hash based Digital Signature Schemes. Code based cryptography. Lattice-based cryptography. Multivariate public key cryptography.

4) Objectives

General Objectives: Understand the concepts of pos-quantum cryptography e their main algorithms.

Specific Objectives:

- Comparison tradicional to pos-quantum cryptography
- Definition of quantum computacional model

5) Course Outline

- Post-quantum cryptography.
  - Motivation, Challenges [1 hour]
  - Comparison cryptography to pos-quantum cryptography [1 hour]
- Quantum computing.
  - Classical and quantum computing [2 hours]
  - Computational model [1 hours]
  - Search algorithms [2 hours]
- Hash based Digital Signature Schemes.
  - One time signatures [2 hours]
  - Merkle tree authentication [1 hour]
  - Cryptography key generation [1 hours]
  - Authentication path [1 hour]
  - Tree chaining [1 hour]
  - Security analysis [2 hours]

- Code based cryptography.
    - Introduction to coding theory [4 hours]
    - Codes and structures available [2 hours]
    - Practical aspects [2 hours]
- Lattice-based cryptography.
    - Introduction to Lattices [2 hours]
    - Finding Short Vectors [2 hours]
    - Cryptographic keys [1 hours]
    - Digital signature schemes [2 hours]
- Multivariate public key cryptography.
    - Introduction to multivariate public key cryptography [2 hours]
    - Basic constructions [1 hours]
- Implementing Post-quantum cryptography [12 hours]

6) Methodology

The course will consist of lectures and presentation of scientific papers on each topic planned. There will also be discussion about the difficulties in managing the life cycle of cryptographic keys and the new cryptographic services that emerge from post-quantum cryptography. Particular attention will be given to complexity and security analysis. As for the complexity, attention will be paid to a) memory consumption for storing the cryptographic keys and the internal state of the schemas that so require; b) number of cryptographic operations required, either for digitally signing or encrypting and for verifying signatures or deciphering ciphertext.

7) Bibliography

[1] BERNSTEIN, Daniel J. et. al. Post-quantum cryptography. In: Post-quantum cryptography. Springer, Berlin, Heidelberg, 2009. 249p.

[2] BUCHMANN, Johannes; DING, Jintai. Post-quantum cryptography. In: second international workshop, PQCrypto. 2008. p. 17-19.

[3] FINIASZ, Matthieu; SENDRIER, Nicolas. Security bounds for the design of code-based cryptosystems. In: International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2009. p. 88-105.

[4] OVERBECK, Raphael; SENDRIER, Nicolas. Code-based cryptography. In: **Post-quantum cryptography**. Springer, Berlin, Heidelberg, 2009. p. 95-145.

[5] MICCIANCIO, Daniele; REGEV, Oded. Lattice-based cryptography. In: **Post-quantum cryptography**. Springer Berlin Heidelberg, 2009. p. 147-191.

[6] DING, Jintai; YANG, Bo-Yin. Multivariate public key cryptography. In: **Post-quantum cryptography**. Springer, Berlin, Heidelberg, 2009. p. 193-241.

[7] MERKLE, Ralph C. A digital signature based on a conventional encryption function. In: **Conference on the Theory and Application of Cryptographic Techniques**. Springer, Berlin, Heidelberg, 1987. p. 369-378.

[8] DODS, Chris; SMART, Nigel P.; STAM, Martijn. Hash based digital signature schemes. In: **IMA International Conference on Cryptography and Coding**. Springer, Berlin, Heidelberg, 2005. p. 96-115.

[9] BUCHMANN, Johannes et al. On the security of the Winternitz one-time signature scheme. In: **International Conference on Cryptology in Africa**. Springer, Berlin, Heidelberg, 2011. p. 363-378.

[10] BUCHMANN, Johannes; DAHMEN, Erik; HÜLSING, Andreas. XMSS-a practical forward secure signature scheme based on minimal security assumptions. In: **International Workshop on Post-Quantum Cryptography**. Springer, Berlin, Heidelberg, 2011. p. 117-129.