UNIVERSITÀ
POLITECNICA
DELLE MARCHE

DII Dipartimento
Ingegneria
Informazione

Workshop Announcement

Wednesday November 13, from 10 to 12

In-person attendance: Engineering building, room 160/2
On-line attendance: https://bit.ly/pqcworkshop

Code-Based Post-Quantum Cryptography

Designing, analyzing and optimizing code-based schemes are timely topics in the context of Post-Quantum Cryptography. Many schemes are currently under investigation, and many researchers have recently focused their attention on digital signatures based on difficult problems related to coding theory, such as the problems of decoding and the problem of determining whether two codes are equivalent. In this workshop we discuss recent results on the difficulty of code-based problems and on the security of schemes leveraging them. Some of these schemes are competing for NIST's selection and standardization process.

Invited Talks:

- Michele Battagliola (Università Politecnica delle Marche):
  Cutting the GRASS: Threshold GRoup Action Signature Schemes
- Giuseppe D'Alconzo (Politecnico di Torino):
  On the Sample Complexity of Code Equivalence Problems
- Alessio Meneghetti (Università di Trento):
  Information Set Decoding for Code-based Cryptography: beyond Finite Fields
- Paolo Santini (Università Politecnica delle Marche):
  Canonical Forms and Short Signatures from the Code Equivalence Problem
- Edoardo Signorini (Telsy):
  Security of Fixed-Weight Repetitions of Special-Sound Multi-Round Interactive Proofs

Finanziato dall'Unione europea
NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

Cutting the GRASS: Threshold GRoup Action Signature Schemes

Michele Battagliola (Università Politecnica delle Marche)

Abstract

Group actions are fundamental mathematical tools, with a long history of use in cryptography. In the recent NIST's call for post-quantum digital signatures, three schemes were based on group actions, namely LESS, MEDS, and ALTEQ. In this talk, we introduce the Group Action Inverse Problem (GAIP) and show that it can be viable building blocks also for threshold signature schemes. In particular, we present a full n-out-of-n threshold signature scheme, and discuss secret sharing techniques to obtain a generic t-out-of-n scheme. Lastly, we discuss the possibility of obtaining adaptive security and some recent hardness assumptions closely related to GAIP.

On the Sample Complexity of Code Equivalence Problems

Giuseppe D’Alconzo (Politecnico di Torino)

Abstract

An equivalence problem asks, given two "equivalent objects", to find the map leading to the equivalence. Recently, hard equivalence problems have gained a lot of interest since, among other applications, they are used in three proposals for NIST's call for post-quantum digital signatures, namely LESS, MEDS, and ALTEQ. In this talk, we analyze the t-sample complexity of an equivalence problem: given t pairs of objects linked by the same map, what is the complexity of retrieving the equivalence? We study the sample complexity of some problems from linear codes and tensors. Moreover, we show that some known constructions from this class of problems are insecure, as they rely on more advanced cryptographic assumptions involving a polynomial t-sample complexity.

Information Set Decoding for Code-based Cryptography: beyond Finite Fields

Alessio Meneghetti (Università di Trento)

Abstract

Information set decoding (ISD) algorithms currently offer the most powerful tool to solve the Codeword Finding Problem (CFP) and the Syndrome Decoding Problem (SDP). Traditionally, ISD has primarily been studied for classical linear codes equipped with the Hamming metric, and is the main method to study and choose the parameters in code-based schemes. Recently, other possibilities have also been explored to construct cryptographic schemes, moving away from the classical setting. In this talk we discuss new ISD algorithms specifically designed to tackle CFP and SDP for the more general case of codes over rings equipped with the Hamming, Lee or Rank metric.

Canonical Forms and Short Signatures from the Code Equivalence Problem

Paolo Santini (Università Politecnica delle Marche)

Abstract

The Code Equivalence Problem (CEP) asks to find a linear isometry (a monomial or a permutation) between two linear codes. The problem can be phrased in terms of group actions and, as such, yields a natural mean to build digital signatures (via the Fiat-Shamir transformation of a Sigma protocol). The problem has been used as the underlying assumption in LESS, one of the 14 digital signature schemes admitted to the second round of the NIST call for additional post-quantum signature schemes. In this talk we describe how, according to a recent result, the equivalence problem can be reformulated in terms of canonical forms and how this allows to significantly reduce the signature size in LESS.

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA

UNIVERSITÀ
POLITECNICA
DELLE MARCHE

DII Dipartimento
Ingegneria
Informazione

Security of Fixed-Weight Repetitions of Special-Sound Multi-Round Interactive Proofs

Edoardo Signorini (Telsy)

Abstract

Interactive proofs are a cornerstone of modern cryptography and, as such, are used in many areas, from digital signatures to multy-party computation. Often, the knowledge error of an interactive proof is not small enough and thus needs to be reduced. This is usually achieved by repeating the interactive proof in parallel. Surprisingly, it has only recently been proven that the parallel repetition of any special-sound multi-round interactive proof is still a proof of knowledge. However, in many cases, parallel repetitions lead to a significant increase in transcript size. A common technique to mitigate this drawback, which is often used in digital signatures obtained by using the Fiat-Shamir transform, is to use fixed-weight challenges, i.e., vectors of challenges having a constant number of entries (for which the last component is) equal to a fixed value. While widely used, this method has not been fully assessed from a security standpoint. In this talk, we analyze the effect of the fixed-weight technique on the knowledge error of repeated interactive proofs. In particular, we show that an explicit knowledge extractor can be built for the fixed-weight repetition of a special-sound multi-round interactive proof. Moreover, we discuss how our results can be applied to some recently proposed post-quantum digital signatures, for example, the code-based signature CROSS.

For further information please contact Prof. Marco Baldi (m.baldi@univpm.it)

Finanziato dall'Unione europea NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA