COLLECTIO CIPHRARUM

*Book Series*

4

# COLLECTIO CIPHRARUM
*Book Series*


The method is capable of dispatching with accuracy every kind of urgent messages, but in practice it requires care and exact attention.
(Polybius 150 BC)

La collana Collectio Ciphrarum pubblica atti di convegni e workshop in crittografia e argomenti affini, inclusi cicli di seminari di ampia durata. La collana ospita con preferenza non esclusiva atti di convegni in Italia o organizzati congiuntamente da sedi italiane e straniere. Di norma ogni volume ospita tra dieci e venti interventi, in formato di extended abstract ciascuno in lingua inglese, più eventuali survey tematici dietro invito degli editor. Gli abstract possono anche riassumere risultati già pubblicati in altre sedi. Tutti i contributi sono referati in maniera anonima da esperti internazionali. Gli organizzatori di un workshop sono invitati a proporre la pubblicazione degli atti nella Collectio Ciphrarum contattando il Board.

The book series Collectio Ciphrarum presents proceedings papers of talks given at workshops/conferences in Cryptography and related matters, including talks given at organized seminar series. Collectio Ciphrarum has a keen interest in workshops/conferences that are either held in Italy or co-organized by at least one Italian research institution. A book will usually contain ten to twenty extended abstracts, sketching research that June be published in another publication venue, plus invited surveys, which are meant to be published exclusively here. All papers are refereed by anonymous international experts. Any organizer of a workshop/conference, falling in the book series scope, is invited to contact the Editorial Board for proposing a new volume.

*Classificazione Decimale Dewey:*

652.8 (23.) CRITTOGRAFIA

# CRYPTORINO 2021

*edited by*

LAURA **CAPUANO**, GUGLIELMO **MORGARI**, LEA **TERRACINI**

*preface by*

MASSIMILIANO **SALA**

*Contributions of*

EMANUELE **BELLINI**, UMBERTO **CERRUTI**, NICOLA **DI CHIANO**, ANDREA **DI NENNO**
AUSTIN **DUKES**, ANDREA **GANGEMI**, IRENE **GIACOMELLI**, RICCARDO **LONGO**
ALESSIO **MENEGHETTI**, GIACOMO **MICHELI**, GUGLIELMO **MORGARI**, NADIR **MURRU**
FEDERICO **PINTORE**, GIORDANO **SANTILLI**, EDOARDO **SIGNORINI**, FRANCESCO **STOCCO**

aracne



ISBN
979-12-218-0831-5

FIRST EDITION
**ROMA** 4 AUGUST 2023

# Contents

Part I
**Introduction**

11 Preface
*Massimiliano Sala*

13 Introduction
*Laura Capuano, Guglielmo Morgari, Lea Terracini*

Part II
**Extended Abstracts**

19 DeFi 2020: the bank-less revolution
*Andrea Di Nenno*

25 An overview of blockchains' de-anonymization attacks
*Andrea Gangemi*

31 Filecoin: from Proof-of-Space blockchain to decentralized storage
*Irene Giacomelli*

35 Threshold signatures with offline parties
*Alessio Meneghetti*

39 Understanding polynomial maps over finite fields
*Austin Dukes, Giacomo Micheli*

43 A multifactor RSA-like scheme
*Emanuele Bellini, Nadir Murru*

47 Privacy-preserving signatures from isogenies
*Federico Pintore*

51 The integer factorization problem in cryptography
*Giordano Santilli*

55 On the classical authentication in Quantum Key Distribution
*Guglielmo Morgari, Edoardo Signorini, Francesco Stocco*

Part III
**Invited Surveys**

61 A survey on NIST PQ signatures
*Nicola Di Chiano, Riccardo Longo, Alessio Meneghetti, Giordano Santilli*

87 One Time Pad and the Short Key Dream
*Umberto Cerruti*

# Part I
# INTRODUCTION

*CrypTOrino 2021*
ISBN 979-12-218-0831-5
DOI 10.53136/97912218083151
pp. 11-11 (August 2023)

# Preface

Massimiliano Sala

The national initiative "De Componendis Cifris" aims at widespread study and use of cryptography and related themes. This book in your hands is the fourth volume of our book series *Collectio Ciphrarum* and it has been prepared by our (very active) team in Turin. It contains seminars presented at their annual workshop, plus some invited surveys. I am especially delighted to observe the natural blend in this book between applicative aspects (including hot topics such as blockchain technology) and theoretical research (from classic subjects such as number theory to recent trends such post-quantum cryptography). Our Turin colleagues have done a great job in organizing their workshop and even more so in organizing this nice book.

*CrypTOrino 2021*
ISBN 979-12-218-0831-5
DOI 10.53136/97912218083152
pp. 13-15 (August 2023)

# Introduction

Laura Capuano Guglielmo Morgari Lea Terracini

Nowadays cryptography plays a central role in the security of our digital world. Although normally not perceived by users, cryptography is in fact at the heart of a number of operations we routinely perform every day: withdrawals from ATM, mobile phone calls, home banking and online purchases, to name just a few examples, strongly rely on cryptographic techniques to guarantee user security rights like confidentiality and privacy. Despite its highly applicative nature, cryptography has solid theoretical foundations in different areas of mathematics, including abstract algebra, number theory, geometry, probability, complexity theory and information theory. A deep understanding of these theoretical aspects and their link with application problems is thus fundamental to use cryptography in a correct and effective way.

This volume collects some proceedings of the first CrypTo Conference, organized in May 2021 by the Cryptography and Number Theory Group of Politecnico di Torino and Università di Torino with the aim of giving an overview of the current directions in cryptography. In addition to the proceedings of the conference, two surveys are also included in the volume, authored by researchers strictly connected by scientific collaborations to the above-mentioned group. All the presented works have undergone a blind review process in order to guarantee high quality and conformance to the scope. The authors represent both academia and industry and come from numerous countries (Italy, United States, England, United Arab Emirates), thus providing different and heterogeneous views on current research trends in cryptography.

The topics addressed in the volume are many and closely interrelated, covering both theoretical and practical aspects. They concern innovative technologies of great practical interest such as blockchain and distributed ledgers; more classic but still fundamental subjects such as the integer factorization problem and related cryptosystems; the Post-Quantum world faced from different points of view; abstract

subjects like cryptographic algebraic tools and finally fundamental cryptographic primitives.

More in detail, blockchains and distributed ledgers (DLT) represent a highly topical and concrete subject, which is likely to radically and irreversibly change the operating model of many traditional and innovative businesses related to data processing. Although this technology is known above all for cryptocurrencies, it actually has countless possible applications. Examples of financial and data storage applications are presented in the volume. A somewhat controversial aspect of blockchain technology, that is the ability to (pseudo)anonymize users, is also considered with an analysis of the most promising deanonymization techniques based on Machine Learning.

Threshold Signatures, discussed in the volume, represent a very important research topic, due to their theoretical depth and possible applications. Among these, Threshold Signatures role in cryptocurrency custody services is highlighted, testifying to the close relationship between theory and application.

Although Quantum Computer is now publicly available only at a prototype level, it is generally believed that in the next few years it might be able to break the public key systems currently in use. Consequently, a topic of great importance in the world of research is the definition of quantum-resistant solutions. As is well known, two deeply distinct but complementary solutions are today considered: Post Quantum Cryptography (PQC) and Quantum Key Distribution (QKD). A survey on the ongoing process by NIST dedicated to PQC, aimed to define cryptographic standards for the next decades, is reported in the volume. Furthermore, a scheme of ring signatures is presented, based on isogenies between elliptic curves, mathematical functions arising from algebraic geometry whose computations are currently believed to be inviolable by Quantum Computer. QKD, normally studied in its aspects of quantum mechanics, is instead dealt with in the volume from the complementary and equally important point of view of information theory.

The volume also presents some more theoretical contents, enlightening the close relationship of cryptography with other branches of mathematics. Among these are considered algebraic aspects such as the study of polynomial maps over finite fields, at the base of many cryptographic techniques and relevant in many other mathematical areas as well. In addition, classical topics such as the Integer Fac-

torization Problem and the RSA cryptosystem are reconsidered and innovative contributions are provided in terms of characterization and generalization towards more efficient and safe solutions. Finally, the volume contains a survey on the One Time Pad (OTP), the only cryptographic solution that is unconditionally secure and which, for reasons of efficiency, is often approximated by more practical but necessarily imperfect solutions.

Part II

# EXTENDED ABSTRACTS

*CrypTOrino 2021*
ISBN 979-12-218-0831-5
DOI 10.53136/97912218083153
pp. 19-23 (August 2023)

# DeFi 2020: the bank-less revolution

Andrea Di Nenno

Permissionless Decentralised Financial applications have been dominating the blockchain space in 2020, from the Ethereum ecosystem later spanning across many other blockchains. Conceived, designed and implemented during the crypto winter between 2018-2019 several protocols for Stable-coins, Lending, Borrowing, Exchanging crypto and tokens were deployed on main-net and started to get traction: Total Value Locked (TVL) in those protocol, after reaching the historical milestone of 1 billion in March 2020, has exploded to 50 billion USD within the first year [1]. The revolutionary nature of this technology is twofold.

From a use-case point of view, Decentralised Finance eliminates any barrier, especially in terms of law, regulations and intermediaries, for any individual around the world to access and personally harness from a global decentralised financial system, running 24/7, where laws and mechanics are written in open source code that any user can access before interacting and at the same time providing users more control over their money through personal cryptographic wallets. DeFi products have transparency by default; as not only are they built upon open-source technology, but every transaction and interaction between users and applications is recorded in an open, immutable ledger distributed around the world. While it might be months or years before a centralised cryptocurrency exchange is discovered to have gone insolvent, DeFi's solvency and health is always subject to the collective observation and analysis of a large open-source community where anyone can point out fraud and systemic risk. This clearly is opposed to CeFi (Centralised Finance), where services are typically opaque or subject to information asymmetry, with the public being provided with much less insight than what is held by the infrastructure. This creates unknown levels of risk exposure at the same time entrusting the risk management to a small group of regulators. An example of this is from 2008: many mortgage-related financial products were considered incredibly safe

by a few big players like Moody's Investors Service, Standard and Poor's, and Fitch Ratings, until it was revealed they were insufficiently collateralized, triggering a global financial crisis.

On the tech side, given that decentralisation requires all the information to be publicly accessible in the ledger, the protocols running on it are effectively applications that store their internal state and expose APIs to the other users, being smart contracts or Externally Owned Accounts. These protocols are then composable by nature, meaning that they possibly can inter-operate between each other without requiring adapters. This allows for truly impartial and deterministic applications that run as coded and are incapable of being shut down. Ethereum composability has led to a sharp organic growth of the entire system, where basic dApps effectively enables more complex protocols and structures to be build on top of those, creating a positive feedback loop that reminds early day of Internet: as Internet grew in users, the incentive for building on it grew, while the obstacles shrank. The permission-less nature of public blockchains, where anyone can deploy its own protocol that can interact with all the existing ones, amplified the magnitude of competition which in turn led to higher quality of the systems and in some cases strong and collaborative communities.

## 1. Stable Coins

One of the most important key enablers to replicate and innovate the financial system on blockchain was the creation of stable-coins, that is crypto assets that aren't subject to volatility like other cryptocurrencies but keep their value stable. On blockchain systems this can be easily achieved via centralisation, simply via an external entity holding fiat currencies and minting blockchain native stable coins, supposedly at 1:1 ratio. While this is the most convenient way to obtain a stable-coin, it clearly introduces systemic risks with centralisation. Rather more difficult is to obtain a truly decentralised stablecoin, that is an asset that keeps its value stable through a decentralised protocol.

MakerDAO protocol [2] is so far one of the most successful projects, designed for years since 2014 and finally deployed on Ethereum mainnet by the end of 2017. Its stablecoin Dai, can be minted by anyone by simply providing collateral, in form of crypto, at a 150%