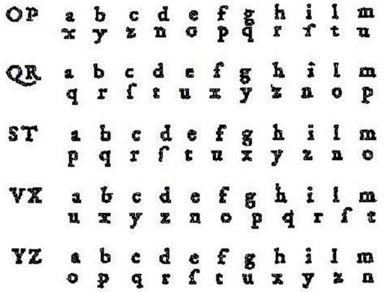
COLLECTIO CIPHRARUM

Book Series

1

COLLECTIO CIPHRARUM
Book Series



OP	a	b	c	d	e	f	g	h	i	l	m
	x	y	z	n	o	p	q	r	ſ	t	u
QR	a	b	c	d	e	f	g	h	î	l	m
	q	r	ſ	t	u	x	y	z	n	o	p
ST	a	b	c	d	e	f	g	h	i	l	m
	p	q	r	ſ	t	u	x	y	z	n	o
VX	a	b	c	d	e	f	g	h	i	l	m
	u	x	y	z	n	o	p	q	r	ſ	t
YZ	a	b	c	d	e	f	g	h	i	l	m
	o	p	q	r	ſ	t	u	x	y	z	n

> 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 may 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.

ALGEBRA FOR CRYPTOGRAPHY

edited by

RICCARDO ARAGONA, NORBERTO GAVIOLI, FILIPPO MIGNOSI

preface by

MASSIMILIANO SALA

Contributions of

MARTINO BORELLO, MARCO CALDERINI, ROBERTO CIVINO
ILARIA COLAZZO, FRANCESCA DALLA VOLTA, LUCIANO MAINO
ALESSIO MENEGHETTI, NADIR MURRU, FEDERICO PINTORE
MARIA TOTA, GIOVANNI ZINI

aracne

aracne

©

ISBN
979–12–5994–328–6

FIRST EDITION
ROMA 29 NOVEMBER 2021

Index

Part I
Introduction

11 Preface
Massimiliano Sala

13 Algebra arm-in-arm with Cryptography
Riccardo Aragona, Norberto Gavioli, Filippo Mignosi

Part II
Extended Abstracts

19 The Pell conic in cryptography
Nadir Murru

23 A new isogeny-based lossy identification protocol for a tightly secure digital signature
Federico Pintore

27 Primitivity of PRESENT and other lightweight ciphers
Maria Tota

31 Differential cryptanalysis: study of a variation on a theme
Roberto Civino

35 Braces: between regular subgroups and solutions of the Yang-Baxter equation
Ilaria Colazzo

39 The Möbius function for finite groups and some related topics
Martino Borello, Francesca Dalla Volta, Giovanni Zini

45 A formula for the weight distribution of codes
Alessio Meneghetti

49 On vectorial Boolean functions with good cryptographic properties
Marco Calderini

55 Mathematical and Computational Aspects of CSIDH-based Algorithms
Luciano Maino, Federico Pintore

Part I

INTRODUCTION

Algebra for Cryptography
ISBN 979-12-5994-328-6
DOI 10.53136/97912599432861
pp. 11-11 (November 2021)

Preface

Massimiliano Sala

The initiative "De Componendis Cifris" aims at fostering the teaching and the research of cryptography in Italy, including its applicative aspects. Under the guidance of the late Michele Elia, we have started several publishing projects. This book in your hands is the first volume of our new book series *Collectio Ciphrarum*, which is devoted to proceedings. This book, titled "Algebra for Cryptography" by its editors, is the perfect match for the following reasons. First, the talks reported here cover a wide range of algebraic methods of cryptographic interest, such as group theory, elliptic curves and Boolean functions. Second, many authors are young and Italian, which is a clear sign of the growing national community. The third and final reason is the high scientific quality of all contributions, including the invited survey.

I am entirely satisfied by the work done by the book's editors: our L'Aquila colleagues Riccardo Aragona, Norberto Gavioli, and Filippo Mignosi. Of this book, you will appreciate both the skimming, which will give you a general idea of current research, and the careful reading, which will show you the depth of the related mathematics.

Algebra for Cryptography
ISBN 979-12-5994-328-6
DOI 10.53136/97912599432862
pp. 13-15 (November 2021)

Algebra arm-in-arm with Cryptography

Riccardo Aragona   Norberto Gavioli   Filippo Mignosi

Over the last decades, many different sectors of society have become increasingly reliant on the digitalization of information and its communication. This induced a parallel increase in the importance of their security. Our society experienced this in the citizens' privacy for their e-mails, in the reliability and security of e-payment transactions, and lately even at a national security level, in defence from massive cyber attacks. Science responds to these requests with several disciplines that investigate technological and theoretical aspects of security. In this direction, mathematical cryptography is playing a central role with several fields, ranging from algebra to geometry, number theory and algorithm theory, involving also their computational aspects.

For all these reasons, some years ago, the Department of Information Engineering, Computer Science and Mathematics (DISIM) at University of L'Aquila has identified cryptography as a strategic sector with a considerable investment on several research fellowships and with the creation of a network of national and international contacts and a laboratory dedicated to this activity. As a consequence, algebraists, computer scientists and engineers of DISIM started a collaboration for a research program focused on these topics and their applications.

In these years we have often carried out our research in algebraic cryptography during the cycle of seminars "Gruppi al Centro" organized at the headquarter of the Istituto Nazionale di Alta Matematica "Fracesco Severi" (INdAM) in Rome. During these research seminars we have conceived the organization of the "1$^{\text{st}}$ workshop in Algebra for Cryptography (A4C2019)", funded by INdAM and held at DISIM between 10 and 11 October 2019, aiming at emphasizing the close link between abstraction and applications, which is proper of cryptography.

Cryptographic systems are frequently built using abstract algebraic objects, e.g. such as Boolean permutations in the case of block ciphers or pairing functions on elliptic curves in the case of post quantum pairing-based ciphers. Consequently, the evaluation of the security and the study of possible weaknesses of a cryptosystem is linked to the study of sophisticated algebraic properties which are often also of interest in abstract research. In other words, as well as cryptographers exploit abstract algebra concepts to build secure encryption systems, algebraists can also use cryptography as a rich source of new open problems arising from technological applications.

All the invited speakers have kindly contributed to the drafting of these proceedings. The volume consists of eight extended abstracts, relating to all the talks held during the workshop, and ends with a summary. The first three extended abstracts describe cryptographic systems and protocols exploiting some algebraic and geometric objects. Nadir Murru (University of Trento, Italy) presents a joint work with Emanuele Bellini (DarkMatter LLC, United Arab Emirates), where they construct a novel RSA-like scheme based on the Pell conic, whose decryption procedure turns to be two times faster than RSA. Federico Pintore (University of Oxford, England) describes a joint work with Ali El Kaafarani (University of Oxford, England) and Shuichi Katsumata (National Institute of Advanced Industrial Science and Technology, Japan), where they introduce a variant of CSI-FiSh, named Lossy CSI-FiSh, providing a tight security proof both in the classical and quantum setting. In the contribution of Maria Tota (University of Salerno, Italy), regarding a joint work with Riccardo Aragona (University of L'Aquila, Italy), Marco Calderini (University of Bergen, Norway) and Antonio Tortora (University of Campania, Italy), some conditions to guarantee that the round functions of a translation based lightweight cipher generate a primitive group are provided; it is also proved that, under certain hypotheses, such a group is the alternating group.

The following four extended abstracts deal with theoretical aspects of algebra which have application to cryptography and cryptanalysis. Roberto Civino (University of L'Aquila, Italy) presents a joint paper with Riccardo Aragona, Norberto Gavioli and Carlo Maria Scoppola (University of L'Aquila, Italy), studying the relationship between the elementary abelian regular subgroups and the Sylow 2-subgroups of their normalisers in the symmetric group $\mathrm{Sym}(2^n)$. The contribution of Ilaria Colazzo (Vrije Universiteit Brussel, Belgium), joint work with Francesco Catino and Paola Stefanelli (University of Salento, Italy), regards the connection between braces, algebraic structures generalizing radical rings, and regular subgroups, and contains special constructions of braces that lead to describing particular classes of regular subgroups. The application of two previous works to cryptography is given by some recent results which show that a cryptanalyst can exploit conjugates of the translation group on the message space of a block cipher, which are elementary abelian regular groups, to perform algebraic and statistical attacks. The abstract of Francesca Dalla Volta (University of Milano-Bicocca, Italy), joint work with Martino Borello (Laboratoire Analyse, Géométrie et Applications, France) and Giovanni Zini (University of Campania, Italy), mainly describes some computational aspects related to the Möbius function of the subgroup poset of the group $\mathrm{PSL}(3; 2^p)$, with p a prime number. This contribution also contains a possible application of the theory of Möbius functions to the study of the group of units of the finite monoid of all cellular automata over the configuration space A^G, for a given finite set A and a group G. Cellular automata represent indeed an interesting approach to the design of non-linear Boolean functions with good cryptographic properties and low implementation costs. Alessio Meneghetti (University of Trento, Italy), a researcher working on the application of coding theory to post-quantum cryptography, presents a formula for the weight distribution computation, based on the classification of some submatrices of the code's parity-check matrix.

The last extended abstract is a brief survey, where Marco Calderini (University of Bergen, Norway) presents an overview of vectorial Boolean functions with good cryptographic properties. These functions play a crucial role in the design of block ciphers and they need to satisfy several algebraic properties in order to resists to the known attacks. Among these, low differential and boomerang uniformity are useful to avoid differential and boomerang attacks.

Finally, the volume ends with the extended abstract of an invited survey by Luciano Maino (University of Bristol, UK) and Federico Pintore (University of Oxford, UK) on isogeny based cryptography. In 2018, Castryck et al. designed a key-exchange protocol, called CSIDH, which requires the computation of chains of isogenies between elliptic curves defined over a given prime field $\mathbb{F}_p$. Since then, many speed-ups for the computation of the isogenies and several strategies to make the computation in constant-time have been proposed. In this volume, Maino and Pintore review these different contributions. First, they consider the case of generic parameters. Then, they focus on the CSIDH-512 parameters, for which Beullens et al. made a record class-group computation, exploited to construct CSI-FiSh, the first practical isogeny-based signature scheme.

Part II

EXTENDED ABSTRACTS

Algebra for Cryptography
ISBN 979-12-5994-328-6
DOI 10.53136/97912599432863
pp. 19-22 (November 2021)

The Pell conic in cryptography

Nadir Murru

The Pell equation is one of the most famous and studied Diophantine equation, it is

$$x^2 - Dy^2 = 1$$

for D a non–square integer and we want to find integer solutions (x, y). It arises from the Archimede's cattle problem:

> "*Compute, O friend, the number of the cattle of the sun which once grazed upon the plains of Sicily, divided according to color into four herds, one milk-white, one black, one dappled and one yellow. The number of bulls is greater than the number of cows, and the relations between them are as follows: etc...*"

The first mathematician who found a method for solving the Pell equation was the Indian Brahmagupta. If you know two solutions (x_1, y_1) and (x_2, y_2) of the Pell equation, their Brahmagupta product

$$(x_1, y_1) \otimes (x_2, y_2) = (x_1x_2 + Dy_1y_2, x_1y_2 + y_1x_2)$$

is also a solution. Moreover, all the solutions of the Pell equation can be found by some convergents of the continued fraction expansion of $\sqrt{D}$. For details about the Pell equation see [1]. It is natural to give a geometric intepretation of the Pell equation, considering the Pell conic

$$\mathcal{H} = \{(x, y) \in \mathbb{F} \times \mathbb{F} : x^2 - Dy^2 = 1\}$$

over a general field $\mathbb{F}$, which is a group equipped with the Brahamagupta product. It is interesting to observe that $\otimes$ can be introduced in a geometrical way similar to the sum over elliptic curves [4]. This similarity with elliptic curves shows possible applications of the Pell conic in cryptography. In particular, it can be used for defining RSA–like cryptosystems. It is well–known that RSA scheme can be attacked when either the private exponent or the public exponent is small; RSA leaks additional vulnerabilities in broadcast applications. RSA–like schemes have been proposed in order to avoid some of these attacks; some of these schemes turn to have also a faster decryption procedure. They are based on isomorphisms between two groups, one of which is the set of points over a curve, usually a cubic or a conic. In [5, 6], the authors exploited in this context the Pell conic. In particular this cryptographic scheme is based on a specific parametrization of $\mathcal{H}$ given by the line $y = (x+1)/m$ that yields to the set of parameters $P = \mathbb{F} \cup \alpha$ (α the point at infinity not in $\mathbb{F}$) equipped with a non–standard product

$$m_1 \odot m_2 = \frac{D + m_1 m_2}{m_1 + m_2}$$

when $m_1 + m_2 \neq 0$. The following properties are exploited for the cryptographic application:

— If $\mathbb{F} = \mathbb{Z}_p$ and D is not a quadratic residue modulo p, then $\mathbb{A} = GF(p^2)$ and $P = \mathbb{A}^*/\mathbb{F}^*$ has order $p+1$. Thus, an analogous of the Fermat's little theorem holds in P: $z^{\odot(p+2)} \equiv z \pmod{p}, \quad \forall z \in P$, [2].

— The powers in P can be efficiently computed by means of the Rédei rational functions. They arise from the development of $(z + \sqrt{D})^n = A_n(D, z) + B_n(D, z)\sqrt{D}$, for any integer $z \neq 0$, D non–square integer. The Rédei rational functions are defined as $Q_n(D, z) = \dfrac{A_n(D, z)}{B_n(D, z)}, \quad \forall n \geq 1$, see [8]. We have $Q_{n+m}(D, z) = Q_n(D, z) \odot Q_m(D, z)$ and consequently $z^{\odot n} = Q_n(D, z)$, see [3].

— The Rédei rational functions can be evaluated by means of an algorithm of complexity $O(\log_2(n))$ with respect to addition, subtraction and multiplication over rings [7].

In this way, we can introduce an efficient RSA–like cryptosystem over the Pell conic.

Key generation.

— choose two prime numbers p, q and compute $N = pq$;

— choose an integer e such that $gcd(e, lcm(p+1)(q+1)) = 1$. The pair (N, e) is the *public* or *encryption key*;

— evaluate $d = e^{-1} \pmod{lcm(p+1)(q+1)}$.
The triple (p, q, d) is the *secret* or *decryption key.*

Encryption.
We can encrypt pair of messages $(M_x, M_y) \in \mathbb{Z}_N^* \times \mathbb{Z}_N^*$, such that