East Asian Journal on Applied Mathematics
doi: 10.4208/eajam.240522.200822

Vol. **13**, No. 1, pp. 177-193
February 2023

Cryptographic Systems Based on an Algebraic Structure

Łukasz Matysiak[1,*], Monika Chrzaniuk[1,2], Maximilian Duda[1,2], Marta Hanc[1,2], Sebastian Kowalski[1,2], Zoja Skotnicka[1,2] and Martin Waldoch[1,2]

[1]*Kazimierz Wielki University, Institute of Mathematics, ul. Powstancow Wielkopolskich 2, 85-090 Bydgoszcz, Poland.*
[2]*Institute of Informatics, ul. Mikolaja Kopernika 1, 85-074 Bydgoszcz, Poland.*

Received 24 May 2022; Accepted (in revised version) 20 August 2022.

Abstract. In this paper cryptographic systems based on the Dedekind and Galois structures are considered. We supplement the created cryptosystems based on the Dedekind structure with programs written in C ++ and discuss the inner structure of Galois in cryptography. It is well-known that such a structure is based on finite fields only. Our results reveals something more internal. The final section contains additional information about square-free and radical factorizations in monoids consisting in searching for a minimal list of counterexamples. As an open problem, we leave creating a program that would generate such a list and how to use such a list to create a cryptosystem.

AMS subject classifications: 94A60, 11R32

Key words: Monoid, cryptography, Dedekind domain, Galois extension, factorization.

1. Introduction

In this paper we present developed cryptographic programs written in C ++ (see Sections 2 and 3). These cryptographic systems are based on the Dedekind structure — cf. [1,3]. This motivation is coming from the first author works [2,3].

Dedekind domains are one of the most important rings in algebra. They have many valuable properties and applications. In such rings, any nonzero proper ideal factors into primes and any non-zero fractional ideal is invertible. In Section 2, we introduce a cryptographic program, where the key is an analog to a fractional ideal. In Section 3 we present another cryptographic program, where an alphabet is analog to the fractional ideal. In Section 4 we have complementary of [2, 3]. In addition, we consider the application of

*Corresponding author. *Email addresses:* lukmat@ukw.edu.pl (Ł. Matysiak), marta.hanc@student.ukw.edu.pl (M. Hanc), monika.chrzaniuk@student.ukw.edu.pl (M. Chrzaniuk), mxdu0407@gmail.com (M. Duda), kspterna@student.ukw.edu.pl (S. Kowalski), skotnickazoja@gmail.com (Z. Skotnicka), martin.waldoch@student.ukw.edu.pl (M. Waldoch)

 ©2023 Global-Science Press

polynomial composites and monoid domains in cryptology in the form of certain cryptosystems. In this paper we present a program about this. Section 5 is devoted to a cryptosystem based on a Galois extension. Let us recall that a Galois extension is an algebraic field extension $K \subset L$ that is normal and separable. We introduce an example of such cryptosystem using $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ which is a Galois extension. This cryptosystem can be freely modified while maintaining the idea of its operation. The motivation here is the development of a cryptosystem based on the Galois theory. They do exist, of course, but there is only talk of finite fields. To the best of our knowledge, there are no cryptosystems that go deeper into this science so far.

By a monoid we mean a commutative cancellative monoid. In Section 6, we provide a minimal list of possible counterexamples to find in monoids. Note that [4, Section 4] contains 24 square-free and radical factorizations and all dependencies in general monoids and in particular monoids (GCD-, pre-Schreier-, SR-, ACCP-, atomic, factorial monoids). We recall that a monoid is called GCD-monoid, if for any two elements there exists a greatest common divisor. A monoid H is called a pre-Schreier monoid, if any element $a \in H$ is primal — i.e. for any $b, c \in H$ such that $a \mid bc$ there exist $a_1, a_2 \in H$ such that $a = a_1 a_2$, $a_1 \mid b$ and $a_2 \mid c$. A monoid H is called SR-monoid, if every square-free element is radical — cf. [4]. A monoid H is called ACCP-monoid if any ascending sequence of principal ideals of H stabilizes — i.e. for any sequence of principal ideals $I_1 \subset I_2 \subset \cdots$, there exists $n \in \mathbb{N}$ such that $I_n = I_{n+1} = \cdots$. A monoid H is called atomic, if every non-invertible element $a \in H$ is a finite product of irreducibles (atoms). A monoid H is factorial, if each non-invertible element can be written as a product of irreducible elements and this representation is unique. We also recall that any factorial monoid is ACCP-monoid, any ACCP-monoid is atomic, any factorial monoid is GCD-monoid, and any GCD-monoid is pre-Schreier. Since every pre-Schreier is AP-monoid — i.e each its irreducible element (atom) is prime, it yields that every atomic and AP-monoid is factorial.

We also note that Section 6 discusses a separate topic closely related to [4, Section 7]. More exactly, we consider a minimal list of counterexamples that we can look for (Theorem 6.1). Some of them are taken from [4, Section 7]. This list of counterexamples to be looked for concerns checking whether a given implication about whether we can obtain a different factorization from a given factorization (with respect to square-free or radical factorization) from [4, Section 7] is non-empty. Using the laws of logic, we can easily, although not quickly, generate such a list. Open search for such counterexamples is left as an open problem. It is well-known that cryptology has often used factorization of given numbers (or elements, more generally). The theory discussed in [4] and in this section can be successfully used to develop new cryptosystems.

2. First Cryptosystem with a Dedekind Structure

Consider an alphabet $A = \{a_0, a_1, \ldots, a_n\}$ such that $|A|$ is a prime number, and let $x \in \{2, 3, \ldots, |A|\}$ be the value of a letter in the alphabet, and $k \geqslant 2$ a key. Then

$$y = xk \pmod{|A|},$$