Ntrū-like Public Key Cryptosystems beyond Dedekind Domain Up to Alternative Algebra

Ehsan Malekian, Ali Zakerolhosseini[*]
Faculty of Electrical & Computer Engineering
Shahid Beheshti University, Tehran, Iran

August 14, 2009

Abstract

In this paper, we show that the fundamental concepts behind the Ntrū cryptosystem can be extended to a broader algebra than Dedekind domains. Also, we present an abstract and generalized algorithm for constructing a Ntrū-like cryptosystem such that the underlying algebra can be non-commutative or even non-associative.

To prove the main claim, we show that it is possible to generalize Ntrū over non-commutative Quaternions (algebra in the sense of Cayley-Dikson, of dimension four over an arbitrary principal ideal domain) as well as non-associative Octonions (a power-associative and alternative algebra of dimension eight over a principal ideal domain).

Given the serious challenges ahead of non-commutative/non-associative algebra in quaternionic or octonionic lattices, the proposed cryptosystems are more resistant to lattice-based attacks when compared to Ntrū.

Concisely, this paper is making an abstract image of the mathematical base of Ntrū in such a way that one can make a similar cryptosystem based on various algebraic structures with the goal of better security against lattice attack and/or more capability for protocol design.

Keywords: Public Key Cryptography, Ntrū, Alternative algebra, lattice based cryptography, non-associative cryptosystem, Gtru

1 Introduction

Ntrū is a probabilistic public key cryptosystem that was first proposed by Jeffrey Hoffstein, Jill Pipher and Joseph H. Silverman in the rump session of Crypto 96 and its precise and operational description was officially published in 1998 [HPS98]. Ntrū is classified as a lattice-based cryptosystem since its security is based on intractability of hard-problems in certain types of lattices, contrary to RSA or ECC. On the other hand, Ntrū is also classified as a probabilistic cryptosystem as each encryption process involves a random vector (ephemeral key) and, hence, corresponding to a single message there are many possible encrypted forms.

[*] Corresponding author.

Compared to other well-known cryptosystems such as RSA, ECC or ElGamal, the greatest advantage of Ntrū is that it is based on convolution polynomial ring with coefficients in $\mathbb{Z}$ whose inherent complexity is rather low, amounting to $\mathcal{O}(N^2)$ in worst-case. Computational efficiency along with low cost of implementation have turned Ntrū into a very suitable choice for a large number of applications such as embedded systems, mobile phones, RFID tags, portable devices and resource constrained devices [BCE+01, Kap06].

During the past ten years, Ntrū has been scrutinized by numerous researchers and despite some minor flaws, its main core is still assumed to be safe. Most sophisticated attacks against Ntrū are based on lattice reduction techniques. Although two famous lattice problems, Shortest Vector Problem (SVP) and Closest Vector Problem (CVP), have shown to be among NP-hard problems [Ajt98, Mic01a, Mic01b, MG02], however, the lattice problem arising in Ntrū is classified as a Convolution Modular Lattice (CML) and it is not determined, yet, whether or not the cyclic structure of CML is going to help reducing the complexity of CVP or SVP. This issue and other minor flaws have been considered in new versions of Ntrū [MS01, HgHP+05] and recently, IEEE has completed the development of a standard specification for NtrūEncrypt.

After recognition of Ntrū as a secure and safe core, several researches were carried out on generalization of Ntrū algebraic structure to different Euclidean rings from $\mathbb{Z}$ including $GF(2^k)[x]$ and generally Dedekind domain like $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\zeta_3]$ and $\mathbb{Z}[\zeta_5]$ [Kou06, Kar07, GOS02]. Although generalization of Ntrū to $GF(2^k)[x]$ in [GOS02] never had a desirable result and was broken soon after [Kou06], however, it resulted in a better understanding of the Ntrū cryptosystem and suggested the idea of replacing Ntrū algebraic structure with other rings, free modules and algebras.

Ntrū relies on two fundamental concepts: according to the first concept, this cryptosystem has acquired its inherent security from intractability of the Shortest Vector Problem (SVP) in a certain type of lattice which is assumed to be a NP-Hard problem. From this aspect, Ntrū is different from all known cryptosystems like RSA or ECC. According to the second concept that has not been considered in the sense of algebraic generalization, is the possibility of decryption failure, which may lead to the concept of *provable security* (though this feature has not been proven yet). In Ntrū, decryption failure arises from the fact that there is no well-defined and non-trivial homomorphism between two rings $\mathbb{Z}_p$ and $\mathbb{Z}_q$ as well as the polynomial rings $\mathbb{Z}_p[x]$ and $\mathbb{Z}_q[x]$ (assuming $gcd(p, q) = 1$). Despite this fact, one may impose some restrictions on the coset representatives and switch over $\mathbb{Z}_p[x]$ and $\mathbb{Z}_q[x]$.

In this paper we show that fundamental concepts of Ntrū can be extended to a broader algebra than of $\mathbb{Z}$. As a matter of fact, this paper presents an abstract model for extending Ntrū core to an *algebra* (in the sense of Cayley-Dikson construction method) beyond Dedekind domain along with sufficient conditions for correctness of the cryptosystem core. To make our claim more concrete, two functional cryptosystems are presented. Those two examples are public key cryptosystems with non-associative and non-commutative algebraic structure which can be implemented in software or hardware in addition to crossing borders of Dedekind domain.

This paper is organized as follows: Section 2 summarizes the Ntrū cryptosystem over any arbitrary Dedekind domain including $\mathbb{Z}$. In section 3, we present our claim regarding possibility of building a cryptosystem over an algebra up to some constraints. In section 4, a brief description of two cryptosystems on the basis of our claim will be provided and correctness of the proposed cryptosystems will be shown.

2 Ntrū Cryptosystem over a Dedekind Domain

This section briefly introduces the Ntrū cryptosystem over a Dedekind domain including $\mathbb{Z}$. It is presumed that the reader is familiar with precise details of this cryptosystem as well as concepts of abstract algebra. Otherwise, references [HPS08] and [Rot02] are recommended for comprehensive introduction to Ntrū and abstract algebra concepts, respectively.

Suppose $\mathcal{D}$ is a Dedekind domain and consider the convolution polynomial ring $\mathcal{R} = \mathcal{D}[x]/(x^N - 1)$ with multiplication denoted by the symbol $\star$, where N is a fixed prime number. Let a be an arbitrary element in $\mathcal{D}$ and $< a >$ be the ideal generated by a. Let $\mathcal{R}_a$ denote $(\mathcal{D}/ < a >)[x]/(x^N - 1)$ which is evidently isomorphic to $\mathcal{R}/ < a >$. Let p and q be two elements in $\mathcal{D}$ such that $< p > \cap < q >= \{1\}$. Also let $\mathcal{L}_f$, $\mathcal{L}_g$, $\mathcal{L}_m$ and $\mathcal{L}_\phi$, be *suitable* subsets of $\mathcal{R}$. By *suitable* we mean a subset of relatively sparse polynomials with coefficients of small norm. Note that the process of key generation, encryption and decryption are exactly the same as Ntrū standard version but with two differences: (i) $\mathbb{Z}$ has been replaced with an arbitrary Dedekind domain $\mathcal{D}$, (ii) Modular arithmetic is generalized to its abstract equivalent, i.e., modular arithmetic modulo an ideal generated by $a \in \mathcal{D}$. Having set the above notations, the Ntrū cryptosystem over a Dedekind domain can now be described as follows.

Public Parameters. The following parameters in (Generalized) Ntrū are assumed to be fixed and public and must be agreed upon by both the sender and the receiver: N is a prime number which determines the structure of the ring $\mathcal{D}[x]/(x^N - 1)$ and p and q are two elements in $\mathcal{D}$ such that $< p > \cap < q >= \{1\}$ and $\|q\|$ is much greater than $\|p\|$, where $\|.\|$ denotes Euclidean function or ordinary norm function. d_f, d_g, d_m, and d_ϕ are constant integers less than N which determine the distribution of the coefficients of the polynomials in the subsets $\mathcal{L}_f$, $\mathcal{L}_g$, $\mathcal{L}_m$ and $\mathcal{L}_\phi$.

Key Generation. In the key generation process, two *small* polynomials f and g are randomly chosen from $\mathcal{L}_f$ and $\mathcal{L}_g$, respectively. The polynomial f must be invertible in $\mathcal{R}_p$ and $\mathcal{R}_q$ ($\mathcal{R}_a = (\mathcal{D}/ < a >)[x]/(x^N - 1)$). Upon suitable selection of public parameters, when f is randomly selected from the subset $\mathcal{L}_f$, the probability for this polynomial to be invertible in $\mathcal{R}_p$ and $\mathcal{R}_q$ is very high. However, in rare event that f is not invertible, a new polynomial f can be easily generated. The inverse of f over $\mathcal{R}_p$ and $\mathcal{R}_q$ are computed using the generalized extended Euclid algorithm. As is pointed out in [Kar07, NKM09], when p and q are prime elements (or power of a prime) in a Dedekind domain $\mathcal{D}$, there exist a polynomial time algorithm for computing the inverse of a unit element in $\mathcal{R}_p$ and $\mathcal{R}_q$. We call those two inverses f_p^{-1} and f_q^{-1}, respectively. Hence, we have $f_p^{-1} \star f \equiv 1 \,(\text{mod } < p >)$ and $f_q^{-1} \star f \equiv 1 \,(\text{mod } < q >)$.

While f, g, f_p^{-1}, and f_q^{-1} are kept private, the public key h is computed as follows

$$h = f_q^{-1} \star g \,(\text{mod } < q >).$$

Encryption. The system generates a random polynomial $\phi \in \mathcal{L}_\phi$, called the blinding polynomial (or ephemeral key), and converts the input message to a polynomial $m \in \mathcal{L}_m$. The ciphertext is computed as follows

$$e = p.(h \star \phi) + m \ (\text{mod } < q >).$$

Reduction modulo the ideal $< q >$ is performed based on a predefined mapping which assigns a member of $\mathcal{D}$ as a representative to each equivalence class $\mathcal{D}/ < q >$. Let denote the set of all representatives for each equivalence class modulo the ideal $< q >$ as S.

Decryption. The first step of decryption process starts by multiplying (convolving) the received polynomial e by the private key f

$$\begin{aligned} a := f \star e \ (\text{mod } < q >) &= f \star (p.h \star \phi + m) \quad (\text{mod } < q >) \\ &= \ p.f \star h \star \phi + f \star m \quad (\text{mod } < q >) \\ &= p.f \star f_q^{-1} \star g \star \phi + f \star m \quad (\text{mod } < q >) \\ &= p.g \star \phi + f \star m \quad (\text{mod } < q >). \end{aligned}$$

In the second step, the coefficients of $a \in \mathcal{R}_q$ are identified with the equivalent representatives in S. Assuming that the public parameters have been chosen properly, the resulting polynomial is exactly equal to $p.g \star \phi + f \star m$ in $\mathcal{R}$. With this assumption, when we reduce the coefficients of a modulo $< p >$, the term $p.g \star \phi$ vanishes and $f \star m$ (mod $< p >$) remains. In order to extract the message m, it is enough to multiply $f \star m$ (mod $< p >$) by f_p^{-1}.

Successful Decryption. In order to ensure that the decryption process never fails or has a very high probability of succeeding, we have to impose some constraints on the cryptosystem constants and derive conditions under which the coefficients of $p.g \star \phi + f \star m$ in $\mathcal{R}$ lie in S almost always. For example, in standard Ntrū if the public parameters (N, p, q, d) are chosen to satisfy $q > (6d + 1).p$ then decryption process will never fail. However, to have a better performance and also to reduce the size of the public key, smaller value of q may be chosen for q such that the probability of decryption failure be very small of order 2^{-80} [HPS08, p. 395].

Security of Generalized Ntrū over Dedekind Domains. When one selects an arbitrary Dedekind domain as $\mathcal{D}$, an efficient and functional cryptosystem will emerge, but the security and efficiency of the cryptosystem have no connection to its abstract definition and must be studied precisely and independently. In [Kou06, Kar07], it has been proven that besides $\mathbb{Z}$, if we choose $\mathcal{D}$ to be one of the Dedekind domains: $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\zeta_3]$ and $\mathbb{Z}[\zeta_5]$, a Ntrū-like cryptosystem will emerge that works well and enjoys high security. On the other hand, in CTRU where the ring of integers is replaced by the finite field $GF(2^k)$, the emerged cryptosystem is totally insecure [Kou06].

3 From Dedekind domain towards a broader algebra

In this section, we present our claim regarding the possibility for replacing Dedekind domains by a broader algebra and generalizing Ntrū cryptosystem based on $\mathcal{R}$-Algebra; we call this extension *Gtru*. The main difference between Gtru and those proposed in [NKM09, Kou06] is that the underlying algebra can be non-commutative or even non-associative. In this paper we focus on normed division/split algebras but the proposed extension can also be adapted to some other type of algebras.

Dedekind domains has been chosen as Ntrū base ring in order to achieve an efficient algorithm for finding the inverse of an invertible polynomial in $\mathcal{R}_a = (\mathcal{D}/<a>)[x]/(x^N - 1)$. For normed division or split algebra finding the inverse of an element depends on finding the inverse of the norm of the element over the ground ring/field on which the algebra is defined.

First, we show that extension and generalization of Ntrū over an *algebra* is possible and may be useful for increasing security of the cryptosystem and also protocol design. By *algebra* it means a vector space V over a field $\mathbb{F}$ (or generally a R-module over any ring $\mathcal{R}$ denoted by $\mathcal{R} - algebra$) that is equipped with a bilinear map.

Let $\mathbb{A}$ and $\mathbb{A}'$ be two algebras of dimension n over the commutative rings $\mathcal{R}$ and $\mathcal{R}'$ respectively, equipped with a same bilinear multiplication (denoted by $\circ : \mathbb{A} \times \mathbb{A} \to \mathbb{A}$). Assume there exists a homomorphism ρ from the ring $\mathcal{R}$ into $\mathcal{R}'$. Evidently, there exists a homomorphism ϕ between two algebras $\mathbb{A}$ and $\mathbb{A}'$ defined as follows

$$\phi : \mathbb{A} \to \mathbb{A}'$$

$$\forall \underset{\sim}{x} \in \mathbb{A}, \quad \underset{\sim}{x} := \sum_{i=1}^{n} x_i \mathbf{b}_i, \quad \phi(\underset{\sim}{x}) = \sum_{i=1}^{n} \rho(x_i)\mathbf{b}_i$$

where $\mathbf{b}_i$'s form the basis of the $\mathcal{R}$-module and x_i's are scalars in $\mathcal{R}$. The multiplication in $\mathbb{A}$ can be determined by mean of *structure coefficients* via the following rule

$$\mathbf{b}_i\mathbf{b}_j = \sum_{k=1}^{n} c_{i,j,k}\mathbf{b}_k$$

where $c_{i,j,k}$ are scalars (called structure coefficients or multiplication constants) in $\mathcal{R}$ and must be specified such that the resulting multiplication satisfies the algebra laws. (For more comprehensive details see [Sch96].)

Now, assume we have an algebra $\mathbb{A}$ which satisfies the following five conditions

1. the algebra must have an explicit rule for finding the inverse of a unit element in $\mathbb{A}$. For example, for quaternions ($\mathbb{H}$) or octonions ($\mathbb{O}$), the inverse of a unit element $\underset{\sim}{x}$ is computed

by the explicit rule $\underset{\sim}{x}^{-1} = \frac{\underset{\sim}{x}^*}{N(\underset{\sim}{x})}$, provided that it has a nonzero norm, i.e., $N(\underset{\sim}{x}) \neq 0$ [CS03]. The symbol $*$ denotes conjugate of $\underset{\sim}{x}$ and $N(.) : \mathbb{A} \to \mathcal{R}$ is a multiplicative norm function that assigns to every elements in $\mathbb{A}$ a scalar in the ground ring $\mathcal{R}$, as we will see in the following section.

2. the ring $\mathcal{R}$ should be at least a Dedekind domain; since every prime ideal is maximal and it would allow us to use the polynomial time extended Euclidean algorithm to find the inverse of a scalar in $\mathcal{R}$.

3. the algebras should be alternative, i.e., a non-associative algebra in which the subalgebra generated by any two elements is associative. [Sch96, p. 17]

4. two non-trivial homomorphisms ϕ_1 and ϕ_2 should exist from algebra $\mathbb{A}$ into finite split algebras $\mathbb{A}_1$ and $\mathbb{A}_2$ respectively, such that $\phi(\underset{\sim}{x}) = \sum_{i=1}^{n} \rho(x_i)\mathbf{b}_i$, where ρ is a homomorphism from ground ring of $\mathbb{A}$ into ground ring of $\mathbb{A}_1$ (or $\mathbb{A}_2$). Also, a non-trivial homomorphism between the ground rings of $\mathbb{A}_1$ and $\mathbb{A}_2$ should not exist.

5. every element in the finite split algebras $\mathbb{A}_1$ and $\mathbb{A}_2$ should be represented by a coset representative in $\mathbb{A}$.

Based on above assumptions and definitions, we can now abstractly describe Gtru, a Ntrū-like cryptosystem beyond Dedekind domain up to alternative algebra, as follows.

Public Parameters and System Setup.

- Choose a Dedekind domain $\mathcal{D}$ and algebra $\mathbb{A}$ based on the aforementioned conditions with the ground ring $\mathcal{R} := \mathcal{D}[x]/(x^n - 1)$. The convolution polynomial ring $\mathcal{R}$ enjoys high implementation efficiency.

- Fix a prime integer N and two elements $p, q \in \mathcal{D}$ such that $< p > \cap < q >= \{1\}$ and $\|p\| \gg \|q\|$.

- Define two rings $\mathcal{R}_p = (\mathcal{D}/ < p >)[x]/(x^N - 1)$ and $\mathcal{R}_q = (\mathcal{D}/ < q >)[x]/(x^N - 1)$.

- Let $\mathbb{A}_p$ and $\mathbb{A}_q$ be the algebras over $\mathcal{R}_p = (\mathcal{D}/ < p >)[x]/(x^N - 1)$ and $\mathcal{R}_q = (\mathcal{D}/ < q >)[x]/(x^N - 1)$ respectively with the same structure coefficients (i.e. algebras of same dimension and bilinear function but different underlying rings).

- Fix a set Ω of coset representatives in a way that every elements in $\mathbb{A}_q$ could be identified with a unique coset representative in $\mathbb{A}$. Also, let Λ be the set of representatives for every elements of $\mathbb{A}_q$ in $\mathbb{A}$.

- Let the sets $\mathcal{L}_f$, $\mathcal{L}_g$, $\mathcal{L}_m$ and $\mathcal{L}_\phi$ be subsets of $\mathbb{A}$. Assuming that every element $\underset{\sim}{x}$ in $\mathbb{A}$ is represented by $\underset{\sim}{x} := \sum_{i=1}^{n} x_i\mathbf{b}_i$, these subsets impose some constraints on the values that x_i's can take on. The constraints should be determined based on the set Λ, the probability of successful decryption and maximum bound for short vectors.

Key Generation. In order to generate the private key, two elements $\underset{\sim}{F}$ and $\underset{\sim}{G}$ are randomly chosen from $\mathcal{L}_f$ and $\mathcal{L}_g$ respectively. $\underset{\sim}{F}$ must be invertible over both algebras $\mathbb{A}_p$ and $\mathbb{A}_q$. In case $\underset{\sim}{F}$ is non-invertible, another element can be easily generated. We call those two inverses $\underset{\sim}{F}_p^{-1}$ and $\underset{\sim}{F}_q^{-1}$, respectively. Hence, we have $\underset{\sim}{F}_p^{-1} \circ f = 1$ (over algebra $\mathbb{A}_p$) and $\underset{\sim}{F}_q^{-1} \circ f = 1$ (over algebra $\mathbb{A}_q$). $\underset{\sim}{F}$, $\underset{\sim}{F}_p^{-1}$ and $\underset{\sim}{F}_q^{-1}$ will be kept secret in order to be used in the decryption process and the public key $\underset{\sim}{H}$ is computed and made public as $\underset{\sim}{H} := \underset{\sim}{F}_q^{-1} \circ \underset{\sim}{G} \in \mathbb{A}_q$ (or $\underset{\sim}{H} := \underset{\sim}{G} \circ \underset{\sim}{H}_q^{-1}$).

Encryption. In the encryption process, the cryptosystem first converts the incoming message into an element $\underset{\sim}{M} \in \mathcal{L}_m$ and generates a random element $\underset{\sim}{\Phi} \in \mathcal{L}_\phi$. The ciphertext will be computed as

$$\underset{\sim}{E} := p.\underset{\sim}{H} \circ \underset{\sim}{\Phi} + \underset{\sim}{M} \in \mathbb{A}_q \quad (or \quad \underset{\sim}{E} := p.\underset{\sim}{\Phi} \circ \underset{\sim}{H} + \underset{\sim}{M} \in \mathbb{A}_q)$$

Decryption, in case the algebra $\mathbb{A}$ is associative.

- The ciphertext $\underset{\sim}{E}$ is first multiplied by the private key $\underset{\sim}{F}$ on the left (right)

$$\begin{aligned}
\underset{\sim}{A} :&= \underset{\sim}{F} \circ \underset{\sim}{E} \in \mathbb{A}_q \\
&= p.\underset{\sim}{F} \circ (\underset{\sim}{H} \circ \underset{\sim}{\Phi} + \underset{\sim}{M}) \in \mathbb{A}_q \\
&= p.\underset{\sim}{F} \circ \underset{\sim}{F}_q^{-1} \circ \underset{\sim}{G} \circ \underset{\sim}{\Phi} + \underset{\sim}{F} \circ \underset{\sim}{M} \in \mathbb{A}_q \\
&= p.\underset{\sim}{G} \circ \underset{\sim}{\Phi} + \underset{\sim}{F} \circ \underset{\sim}{M} \in \mathbb{A}_q.
\end{aligned}$$

- In the second step, $\underset{\sim}{A} \in \mathbb{A}_q$ are identified with its equivalent representative in Ω and all the coefficients of the scalars in $\underset{\sim}{A} := \sum_{i=1}^{n} x_i \mathbf{b}_i \in \mathbb{A}$ are reduced mod $< p >$

$$\underset{\sim}{A} \text{ mod } < p >= \underset{\sim}{F} \circ \underset{\sim}{M} \in \mathbb{A}_p.$$

  In order to recover the original message $\underset{\sim}{M}$, first multiply $\underset{\sim}{F} \circ \underset{\sim}{M} \in \mathbb{A}_p$ on the left by $\underset{\sim}{F}_p^{-1}$ and adjust the resulting based on the representative set Λ.

  Successful decryption depends on whether $p.\underset{\sim}{G} \circ \underset{\sim}{\Phi} + \underset{\sim}{F} \circ \underset{\sim}{M} \in \mathbb{A}$ lie in Λ or not. Thus, the public parameters must be chosen such that the condition holds with extremely high probability.

Decryption, in case the algebra $\mathbb{A}$ is non-associative but alternative.

- The ciphertext $\underset{\sim}{E}$ is first multiplied by the private key $\underset{\sim}{F}$ on the left and then on right as follows

$$\begin{aligned}\underset{\sim}{A} :&= (\underset{\sim}{F} \circ \underset{\sim}{E}) \circ \underset{\sim}{F} \in \mathbb{A}_q \\ &= (p.\underset{\sim}{F} \circ (\underset{\sim}{H} \circ \underset{\sim}{\Phi} + \underset{\sim}{M})) \circ \underset{\sim}{F} \in \mathbb{A}_q \\ &= p.(\underset{\sim}{F} \circ (\underset{\sim}{H} \circ \underset{\sim}{\Phi})) \circ \underset{\sim}{F} + (\underset{\sim}{F} \circ \underset{\sim}{M}) \circ \underset{\sim}{F} \in \mathbb{A}_q\end{aligned}$$

Now, based on the Moufang Identity [Sch96] we can rearrange parentheses as follows

$$\begin{aligned}&= p.(\underset{\sim}{F} \circ \underset{\sim}{H}) \circ (\underset{\sim}{\Phi} \circ \underset{\sim}{F}) + (\underset{\sim}{F} \circ \underset{\sim}{M}) \circ \underset{\sim}{F} \in \mathbb{A}_q \\ &= p.(\underset{\sim}{F} \circ (\underset{\sim}{F}_q^{-1} \circ \underset{\sim}{G})) \circ (\underset{\sim}{\Phi} \circ \underset{\sim}{F}) + (\underset{\sim}{F} \circ \underset{\sim}{M}) \circ \underset{\sim}{F} \in \mathbb{A}_q \\ &= p.\underset{\sim}{G} \circ (\underset{\sim}{\Phi} \circ \underset{\sim}{F}) + (\underset{\sim}{F} \circ \underset{\sim}{M}) \circ \underset{\sim}{F} \in \mathbb{A}_q.\end{aligned}$$

- In the second step, all the scalars in $\underset{\sim}{A} \in \mathbb{A}_q$ should be identified with its equivalent representative in Ω and reduced mod $< p >$

  $$\underset{\sim}{A} \text{ mod} < p >= (\underset{\sim}{F} \circ \underset{\sim}{M}) \circ \underset{\sim}{F} \in \mathbb{A}_p.$$

  In order to recover the original message $\underset{\sim}{M}$, first multiply $(\underset{\sim}{F} \circ \underset{\sim}{M}) \circ \underset{\sim}{F} \in \mathbb{A}_p$ on the right by $\underset{\sim}{F}_p^{-1}$ and then on the left and finally adjust the result based on the representative set Λ. Similarly, successful decryption depends on conditions under which $p.\underset{\sim}{G} \circ (\underset{\sim}{\Phi} \circ \underset{\sim}{F}) + (\underset{\sim}{F} \circ \underset{\sim}{M}) \circ \underset{\sim}{F}$ lie in Λ with extremely high probability.

This algebraic generalization may not reveal its power at first glance, however, when we turn our attention from Dedekind domains to other algebraic structures (e.g. free modules, vector spaces, algebra and sub-algebra defined over convolution polynomial ring given that they are equipped with norm function), we may construct a new multi-dimensional public key cryptosystem with higher level of security. In the next section, this concept will be made concrete through introducing two practical examples.

4 Description of two cryptosystems based on $\mathcal{R}$-Algebra

In this section, we will show that if algebra $\mathbb{A}$ be a non-commutative (like Quaternions) or non-associative (like Octonions) algebra, then a new multi-dimensional public key cryptosystem will be emerged that is more secure against lattice attack and also provides more capability for protocol design. To the best of the our knowledge, no practical public key cryptosystem based on non-associative algebra has ever been proposed in the literature.

4.1 A Ntrū-like cryptosystem based on Quaternions algebra

In this cryptosystem, the algebra $\mathbb{A}$ in the abstract algorithm described in the previous section is assumed to be quaternions non-commutative algebra. Let us call the proposed cryptosystem QTRU. Due to non-commutativity of this algebra, none of the known lattice reduction algorithms work on the QTRU lattice and naturally, the cryptosystem security increases considerably. Detailed and analytical description of the proposed cryptosystem are beyond the scope of this paper; see our report [MZM09] for further details. Similar to Ntrū we fix an integer prime N and two co-prime moduli p and q and we define algebras $\mathbb{A}$, $\mathbb{A}_p$ and $\mathbb{A}_q$ as follows

$$\begin{aligned}\mathbb{A} :=\{&f_0(x) + f_1(x).i + f_2(x).j + f_3(x).k \mid \\ &f_0, f_1, f_2, f_3 \in \mathbb{Z}[x]/(x^N - 1), \\ &i^2 = -1, j^2 = -1, ij = -ji = k.\}.\end{aligned}$$

$$\begin{aligned}\mathbb{A}_p :=\{&f_0(x) + f_1(x).i + f_2(x).j + f_3(x).k \mid \\ &f_0, f_1, f_2, f_3 \in \mathbb{Z}_p[x]/(x^N - 1), \\ &i^2 = -1, j^2 = -1, ij = -ji = k.\}.\end{aligned}$$

$$\begin{aligned}\mathbb{A}_q :=\{&f_0(x) + f_1(x).i + f_2(x).j + f_3(x).k \mid \\ &f_0, f_1, f_2, f_3 \in \mathbb{Z}_q[x]/(x^N - 1), \\ &i^2 = -1, j^2 = -1, ij = -ji = k.\}.\end{aligned}$$

One can easily conclude that $\mathbb{A}$, $\mathbb{A}_0$ and $\mathbb{A}_1$ are split algebras. In other words, $\mathbb{A}$, $\mathbb{A}_0$ and $\mathbb{A}_1$ algebras possess all characteristics of quaternion algebra, except that there are some nonzero elements whose norm is zero and naturally such elements do not have a multiplicative inverse. (See references [CS03] and [Sha08] for an introduction to quaternion algebra.)

Since encryption and decryption are taking place in a vector space of dimension four, in order to describe QTRU the following notations and symbols are required

$$\begin{gathered}\underset{\sim}{F} = f_0 + f_1.i + f_2.j + f_3.k \in \mathbb{A} \\ f_0 \triangleq f_0(x),\ f_1 \triangleq f_1(x), f_2\ \triangleq f_2(x),\ f_3 \triangleq f_3(x) \in \mathbb{Z}[x]/(x^N - 1).\end{gathered}$$

The symbol $\circ$ denotes the quaternionic multiplication and is defined as follows

$$\begin{aligned}\underset{\sim}{F} \circ \underset{\sim}{G} =&(f_0 + f_1.i + f_2.j + f_3.k) \circ (g_0 + g_1.i + g_2.j + g_3.k) \\ =\ \ &(f_0 \star g_0 - f_1 \star g_1 - f_3 \star g_3 - f_2 \star g_2) \\ &+ (f_0 \star g_1 + f_1 \star g_0 - f_3 \star g_2 + f_2 \star g_3).i \\ &+ (f_3 \star g_1 + f_2 \star g_0 + f_0 \star g_2 - f_1 \star g_3).j \\ &+ (f_1 \star g_2 + f_0 \star g_3 - f_2 \star g_1 + f_3 \star g_0).k,\end{aligned}$$

where $\star$ denotes the convolution product. We denote the conjugate of a quaternion $\underset{\sim}{F} = (f_0 + f_1.i + f_2.j + f_3.k)$ by $\underset{\sim}{F}^* = (f_0 - f_1.i - f_2.j - f_3.k)$. Let the subsets $\mathcal{L}_f$, $\mathcal{L}_g$, $\mathcal{L}_m$ and $\mathcal{L}_\phi$ have the same definitions as defined in Ntrū (i.e. the subsets of binary or ternary polynomials with some degree of sparseness determined by the public constant d). The QTRU cryptosystem can now be described as follows.

Key Generation. In order to generate a pair of public and private keys, two small quaternion (i.e., quaternions with small norm) $\underset{\sim}{F}$ and $\underset{\sim}{G}$ are randomly generated.

$$\begin{aligned}\underset{\sim}{F} &= f_0 + f_1.i + f_2.j + f_3.k, \quad \text{such that} \quad f_0, f_1, f_2, f_3 \in \mathcal{L}_f \subset \mathbb{A},\\ \underset{\sim}{G} &= g_0 + g_1.i + g_2.j + g_3.k, \quad \text{such that} \quad g_0, g_1, g_2, g_3 \in \mathcal{L}_g \subset \mathbb{A}.\end{aligned}$$

The quaternion $\underset{\sim}{F}$ must be invertible over $\mathbb{A}_p$ and $\mathbb{A}_q$. The necessary and sufficient condition for $\underset{\sim}{F}$ to be invertible over $\mathbb{A}_p$ and $\mathbb{A}_q$ is that the polynomial $\left\|\underset{\sim}{F}\right\| = (f_0^2 + f_1^2 + f_2^2 + f_3^2)$ be invertible over the rings $\mathbb{Z}_p[x]/(x^N - 1)$ and $\mathbb{Z}_q[x]/(x^N - 1)$. The inverses (denoted by $\underset{\sim}{F}_p$ and $\underset{\sim}{F}_q$) will be computed as follows.

$$\begin{aligned}\underset{\sim}{F}_p \quad &:= (f_0^2 + f_1^2 + f_2^2 + f_3^2)^{-1} \cdot \underset{\sim}{F}^* \triangleq \mu_0 + \mu_1.i + \mu_2.j + \mu_3.k,\\ &\mu_0 \triangleq (f_0^2 + f_1^2 + f_2^2 + f_3^2)^{-1}.f_0 \in \mathbb{Z}_p[x]/(x^N - 1)\\ &\mu_1 \triangleq -(f_0^2 + f_1^2 + f_2^2 + f_3^2)^{-1}.f_1 \in \mathbb{Z}_p[x]/(x^N - 1)\\ &\mu_2 \triangleq -(f_0^2 + f_1^2 + f_2^2 + f_3^2)^{-1}.f_2 \in \mathbb{Z}_p[x]/(x^N - 1)\\ &\mu_3 \triangleq -(f_0^2 + f_1^2 + f_2^2 + f_3^2)^{-1}.f_3 \in \mathbb{Z}_p[x]/(x^N - 1)\\ \underset{\sim}{F}_q \quad &:= (f_0^2 + f_1^2 + f_2^2 + f_3^2)^{-1} \cdot \underset{\sim}{F}^* \triangleq \eta_0 + \eta_1.i + \eta_2.j + \eta_3.k\\ &\eta_0 \triangleq (f_0^2 + f_1^2 + f_2^2 + f_3^2)^{-1}.f_0 \in \mathbb{Z}_q[x]/(x^N - 1)\\ &\eta_1 \triangleq -(f_0^2 + f_1^2 + f_2^2 + f_3^2)^{-1}.f_1 \in \mathbb{Z}_q[x]/(x^N - 1)\\ &\eta_2 \triangleq -(f_0^2 + f_1^2 + f_2^2 + f_3^2)^{-1}.f_2 \in \mathbb{Z}_q[x]/(x^N - 1)\\ &\eta_3 \triangleq -(f_0^2 + f_1^2 + f_2^2 + f_3^2)^{-1}.f_3 \in \mathbb{Z}_q[x]/(x^N - 1).\end{aligned}$$

Now, the public key, which is a quaternion, is computed as follows

$$\begin{aligned}\underset{\sim}{H} = \underset{\sim}{F}_q \circ \underset{\sim}{G} = \quad &(\eta_0 \star g_0 - \eta_1 \star g_1 - \eta_3 \star g_3 - \eta_2 \star g_2) +\\ &(\eta_0 \star g_1 + \eta_1 \star g_0 - \eta_3 \star g_2 + \eta_2 \star g_3).i +\\ &(\eta_3 \star g_1 + \eta_2 \star g_0 + \eta_0 \star g_2 - \eta_1 \star g_3).j +\\ &(\eta_1 \star g_2 + \eta_0 \star g_3 - \eta_2 \star g_1 + \eta_3 \star g_0).k.\end{aligned}$$

The quaternions $\underset{\sim}{F}$, $\underset{\sim}{F}_p$ and $\underset{\sim}{F}_q$ will be kept secret in order to be used in the decryption phase.

Encryption. In the encryption process, the system first generates a random quaternion $\utilde{\Phi}$. The plaintext must be converted into a quaternion $\utilde{M} \in \mathcal{L}_m$ including four small polynomials. The messages could be generated from the same or four different sources but transformed into one quaternion based on a simple and pre-determined encoding scheme. The ciphertext will be computed as follows

$$\utilde{E} = p.\utilde{H} \circ \utilde{\Phi} + \utilde{M} \in \mathbb{A}_q.$$

Decryption. In the first step, the received ciphertext $\utilde{E}$ is first multiplied by the private key $\utilde{F}$ on the left

$$\begin{aligned} \utilde{B} := \utilde{F} \circ \utilde{E} &= \utilde{F} \circ (p.\utilde{H} \circ \utilde{\Phi} + \utilde{M}) \mod q \\ &= (\utilde{F} \circ p.\utilde{H} \circ \utilde{\Phi} + \utilde{F} \circ \utilde{M}) \mod q \\ &= (p.\utilde{F} \circ \utilde{F}_q \circ \utilde{G} \circ \utilde{\Phi} + \utilde{F} \circ \utilde{M}) \mod q \\ &= (p.\utilde{G} \circ \utilde{\Phi} + \utilde{F} \circ \utilde{M}) \in \mathbb{Z}_q[x]/(x^N - 1). \end{aligned}$$

The coefficients of the four polynomials in the resulting quaternion must be reduced mod q into the interval $(-q/2, +q/2]$, i.e., $\Omega = \{-q/2+1, \cdots, +q/2\}$ is regarded as the set of representatives. Assuming that $\utilde{B} \in \mathbb{Z}_q[x]/(x^N - 1)$ is exactly equal to $p.\utilde{G} \circ \utilde{\Phi} + \utilde{F} \circ \utilde{M}$ in $\mathbb{A}$, when $\utilde{B}$ is reduced mod p, the term $p.\utilde{G} \circ \utilde{\Phi}$ vanishes and $\utilde{F} \circ \utilde{M}$ (mod p) remains. In order to extract the original message $\utilde{M}$, it will suffice to multiply $\utilde{F} \circ \utilde{M}$ (mod$p$) by $\utilde{F}_p$ on the left and adjust the resulting coefficients within the interval $\Lambda = [-p/2, +p/2]$.

It is apparent that in QTRU, the variance of the coefficients $p.\utilde{G} \circ \utilde{\Phi} + \utilde{F} \circ \utilde{M}$ increases by a factor of 4 and, hence, the probability for decryption failure increases. In return, constant parameters of the system, including d_ϕ , d_g, d_f, q, and N, can be chosen in such a way that the decryption failure rate in QTRU remains equal to that of Ntrū.

Given the fact that quaternion algebra is a non-commutative algebraic structure, it implies that lattice-based attacks against QTRU are generally more difficult. This is because lattice theory inherently relies on the commutativity in the commutative rings while quaternionic matrices or lattices inherently possess certain complexities which do not seem to be solvable [JO05]. Quaternionic matrices have been analyzed by many researches and it seems that these matrices lack many properties that matrices over an arbitrary field (commutative ring) $\mathbb{F}$ ($\mathcal{R}$) possess. In particular, the determinant function of quaternionic matrices is not generally well-defined. They also have different left and right eigenvalues and eigenvectors. On the other hand, the existence of inverse for a quaternionic matrix has been proven and can be calculated by a method similar to Gaussian elimination (see references [Zha97, Asl96]). Consequently, the lack of such properties makes QTRU more resistant against lattice attacks using well-known algorithms. In our report [MZM09] we have shown that lattice attack on QTRU may be applied using two methods *Partial Lattice Attack* and *Full Quaternionic Lattice Attack* and both of the methods will not succeed in finding a short quaternion for full or partial recovery of the plaintext.

Although in totally equal circumstances (i.e., choosing the same parameters for both Ntrū and QTRU cryptosystems), QTRU seems to be about four times slower than Ntrū, one can partially compensate for the speed by reducing N and still obtain the same level of security. In addition, it can be optimized for efficiency based on the various methods proposed in [HS00].

4.2 A Ntrū-like cryptosystem based on non-associative Octonions algebra

In this cryptosystem, called OTRU, the algebra $\mathbb{A}$ in the abstract algorithm described in Section 3 has been replaced by octonions non-associative algebra. Although this cryptosystem resembles to QTRU and Ntrū with regard to key generation and encryption algorithm, however, the non-associativity of the cryptosystem algebraic structure highly improves the security.

The octonions may be regarded as a vector space of dimension 8 with the basis $\{1, e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$ over a field or commutative ring with a multiplication defined using the following rules

$$\begin{aligned}
&e_i^2 = -1,\\
&e_i.e_j = -e_i.e_j \quad i \neq j,\ i = 1, \cdots, 7\\
&e_i.e_j = e_k \to e_{i+1}.e_{j+1} = e_{k+1}, \quad i \neq j,\ i = 1, \cdots, 7\\
&e_i.e_j = e_k \to e_{2i}.e_{2j} = e_{2k}, \quad i \neq j,\ i = 1, \cdots, 7
\end{aligned}$$

where the indices greater than 7 should be reduced mod 7.

We begin by assuming that the reader is fully familiar with the theoretical background of non-associative algebra and octonions. (See [Bae02, CS03] for comprehensive introduction to the octonions.) Consider three public parameters (N, p, q) as well as four subsets $\mathcal{L}_f$, $\mathcal{L}_g$, $\mathcal{L}_m$ and $\mathcal{L}_\phi$ with definitions similar to QTRU. Let us define the required algebras $\mathbb{A}$, $\mathbb{A}_p$ and $\mathbb{A}_q$ as follows.

$$\begin{aligned}
\mathbb{A} &:= \{f_0(x) + \sum_{i=1}^{7} f_i(x).e_i \mid f_0(x), \cdots, f_7(x) \in \mathbb{Z}[x]/(x^N - 1)\}\\
\mathbb{A}_p &:= \{f_0(x) + \sum_{i=1}^{7} f_i(x).e_i \mid f_0(x), \cdots, f_7(x) \in \mathbb{Z}_p[x]/(x^N - 1)\}\\
\mathbb{A}_q &:= \{f_0(x) + \sum_{i=1}^{7} f_i(x).e_i \mid f_0(x), \cdots, f_7(x) \in \mathbb{Z}_q[x]/(x^N - 1)\}
\end{aligned}$$

Consider two elements $\underset{\sim}{F}$ and $\underset{\sim}{G}$ in $\mathbb{A}$, the multiplication operation is defined in the following way

$$\underset{\sim}{F} = f_0(x) + f_1(x)e_1 + f_2(x)e_2 + f_3(x)e_3 + f_4(x)e_4 + f_5(x)e_5 + f_6(x)e_6 + f_7(x)e_7$$

$$\underset{\sim}{G} = g_0(x) + g_1(x)e_1 + g_2(x)e_2 + g_3(x)e_3 + g_4(x)e_4 + g_5(x)e_5 + g_6(x)e_6 + g_7(x)e_7$$

For ease of notation, the argument (x) is dropped in what follows.

$$\begin{aligned}
\underset{\sim}{F} \circ \underset{\sim}{G} = {} & (f_0.g_0 - f_1.g_1 - f_2.g_2 - f_3.g_3 - f_4.g_4 - f_5.g_5 - f_6.g_6 - f_7.g_7) \\
& + (f_0.g_1 + f_1.g_0 + f_2.g_4 + f_3.g_7 - f_4.g_2 + f_5.g_6 - f_6.g_5 - f_7.g_3).e_1 \\
& + (f_0.g_2 - f_1.g_4 + f_2.g_0 + f_3.g_5 + f_4.g_1 - f_5.g_3 + f_6.g_7 - f_7.g_6).e_2 \\
& + (f_0.g_3 - f_1.g_7 - f_2.g_5 + f_3.g_0 + f_4.g_6 + f_5.g_2 - f_6.g_4 + f_7.g_1).e_3 \\
& + (f_0.g_4 + f_1.g_2 - f_2.g_1 - f_3.g_6 + f_4.g_0 + f_5.g_7 + f_6.g_3 - f_7.g_5).e_4 \\
& + (f_0.g_5 - f_1.g_6 + f_2.g_3 - f_3.g_2 - f_4.g_7 + f_5.g_0 + f_6.g_1 + f_7.g_4).e_5 \\
& + (f_0.g_6 + f_1.g_5 - f_2.g_7 + f_3.g_4 - f_4.g_3 - f_5.g_1 + f_6.g_0 + f_7.g_2).e_6 \\
& + (f_0.g_7 + f_1.g_3 + f_2.g_6 - f_3.g_1 + f_4.g_5 - f_5.g_4 - f_6.g_2 + f_7.g_0).e_7
\end{aligned}$$

Note that in the algebras $\mathbb{A}$, $\mathbb{A}_p$ and $\mathbb{A}_q$, scalars are polynomials in the convolution polynomial rings $\mathbb{Z}[x]/(x^N - 1)$, $\mathbb{Z}_p[x]/(x^N - 1)$ and $\mathbb{Z}_q[x]/(x^N - 1)$ respectively, and the operations of addition, subtraction and multiplication will be performed over the underlying ring. Let denote the conjugate and inverse of an octonion $\underset{\sim}{F} = f_0 + \sum_{i=1}^{7} f_i(x).e_i$ by $\underset{\sim}{F}^* = f_0 - \sum_{i=1}^{7} f_i(x).e_i$ and $\underset{\sim}{F}^{-1} = (\sum_{i=0}^{7} f_i^2(x))^{-1}.\underset{\sim}{F}^*$, respectively. OTRU operates as described below.

Key Generation. Similar to QTRU, two small octonions $\underset{\sim}{F}$ and $\underset{\sim}{G}$ are randomly generated.

$$\underset{\sim}{F} := f_0 + f_1.e_1 + \cdots + f_7.e_7 \in \mathbb{A}, \qquad f_0, \cdots, f_7 \in \mathcal{L}_f \subset \mathbb{A}$$

$$\underset{\sim}{G} := g_0 + g_1.e_1 + \cdots + g_7.e_7 \in \mathbb{A}, \qquad g_0, \cdots, g_7 \in \mathcal{L}_g \subset \mathbb{A}$$

The octonion $\underset{\sim}{F}$ must be invertible over $\mathbb{A}_p$ and $\mathbb{A}_q$. If such an inverse does not exist (i.e., when $\sum_{i=0}^{7} f_i^2(x)$ is not a unit element in $\mathbb{Z}_p[x]/(x^N - 1)$ or $\mathbb{Z}_q[x]/(x^N - 1)$), a new octonion $\underset{\sim}{F}$ will be generated. The inverses of $\underset{\sim}{F}$ over the algebras $\mathbb{A}_p$ and $\mathbb{A}_q$ are denoted by $\underset{\sim}{F}_p^{-1}$ and $\underset{\sim}{F}_q^{-1}$. The public key, which is an octonion, is computed as follows

$$\underset{\sim}{H} = \underset{\sim}{F}_q^{-1} \circ \underset{\sim}{G} \in \mathbb{A}_q.$$

Encryption. Initially, a random octonion $\underset{\sim}{\Phi}$ is generated. The incoming data must be converted into an octonion including eight polynomial in $\mathcal{L}_\phi$. This is done according to a simple and predetermined convention. The ciphertext $\underset{\sim}{E}$ is then calculated as follows

$$\underset{\sim}{E} = p.\underset{\sim}{H} \circ \underset{\sim}{\Phi} + \underset{\sim}{M} \in \mathbb{A}_q.$$

OTRU works eight times slower than Ntrū and the data are encrypted simultaneously as eight vectors.

Decryption. Since the octonions algebra is non-associative, not only the terms of $(\utilde{F}_q^{-1} \circ \utilde{G}) \circ \utilde{\Phi}$ do not commute, but also the parentheses order can not be changed, and this will reveal some problem during decryption, because one cannot simply remove the term $\utilde{F}_q^{-1}$ from $((\utilde{F}_q^{-1} \circ \utilde{G}) \circ \utilde{\Phi})$ by multiplying $\utilde{F}$ on the left. Thus, in order to decrypt, first of all, the received octonion $\utilde{E}$ is multiplied on the left by the private key $\utilde{F}$ and then on the right as follows

$$\begin{aligned}
\utilde{B} := ((\utilde{F} \circ \utilde{E}) \circ \utilde{F}) &= p.(\utilde{F} \circ (\utilde{H} \circ \utilde{\Phi})) \circ \utilde{F} + (\utilde{F} \circ \utilde{M}) \circ \utilde{F} \in \mathbb{A}_q \\
&= p.(\utilde{F} \circ \utilde{H}) \circ (\utilde{\Phi} \circ \utilde{F}) + (\utilde{F} \circ \utilde{M}) \circ \utilde{F} \in \mathbb{A}_q \quad \text{(Moufang Identity)} \\
&= p.(\utilde{F} \circ (\utilde{F}_q^{-1} \circ \utilde{G})) \circ (\utilde{\Phi} \circ \utilde{F}) + (\utilde{F} \circ \utilde{M}) \circ \utilde{F} \in \mathbb{A}_q \\
&= p.\utilde{G} \circ (\utilde{\Phi} \circ \utilde{F}) + (\utilde{F} \circ \utilde{M}) \circ \utilde{F} \in \mathbb{A}_q.
\end{aligned}$$

In the second step, $\utilde{B} \in \mathbb{A}_q$ should be identified with its equivalent representative in Ω and all the coefficients in the eight polynomials should be reduced mod p. Thus we have $(\utilde{B} \bmod p) = (\utilde{F} \circ \utilde{M}) \circ \utilde{F} \in \mathbb{A}_p$. In order to extract message $\utilde{M}$, simply multiply $\utilde{B}$ on the right by $\utilde{F}_p^{-1}$ and then repeat the same operation on the left and adjust the resulting coefficients in $[-p/2, +p/2]$.

Note that the octonions algebra (contrary to that of quaternions) does not have any matrix isomorphic representation and normally lattice attack against this cryptosystem, according to the well-known methods described in [CS97] or [May99] is impossible. OTRU may be attacked merely by the Partial Lattice Attack method that was proposed by authors of this article in [MZM09] and it seems that this type of attack has no chance to succeed. A more detailed and analytical description of the OTRU cryptosystem, including the probability of successful decryption, message and key security, message expansion, optimization methods, suggested public parameters, and the system security against lattice attack will be released soon.

5 Conclusion

In this paper we have focused on the fact that the algebraic concepts upon which Ntrū public key cryptosystem is based are abstract concepts not limited to Dedekind domain or commutative rings. Those concepts can be applied to broader algebras like quaternions non-commutative algebra as well as octanions non-associative algebra in order to create a new Ntrū-like cryptosystem.

In order to prove the claims proposed in this paper, first of all, we have shown that the fundamental concepts behind Ntrū could be extended and generalized in a way that would work in an algebra broader than Dedekind domains. Then an abstract construction method have been proposed, on the basis of which, a Ntrū-like cryptosystem can be correctly implemented with an algebraic structure broader and more complex than the polynomial rings over Dedekind domains.

In order to justify our claim, we have introduced two cryptosystems which have been implemented by the authors of the article. The first cryptosystem, QTRU, works based on quaternions algebra and due to its non-commutative nature, it can hardly be attacked by the existing lattice attack algorithms. The second cryptosystem, OTRU, is constructed based on the octonions algebra which is a non-associative but alternative algebraic structure and possesses a very complex and secure core.

References

[Ajt98] Miklós Ajtai. The shortest vector problem in L2 is NP-hard for randomized reductions. In *STOC '98: Proceedings of the thirtieth annual ACM symposium on Theory of computing*, pages 10–19, New York, NY, USA, 1998. ACM.

[Asl96] Helmer Aslaksen. Quaternionic determinants. *The Mathematical Intelligencer*, 18(3):57–65, 1996.

[Bae02] John C. Baez. The octonions. *Bulletin of the American Mathematical Society*, 39:145, 2002.

[BCE$^+$01] Daniel V. Bailey, Daniel Coffin, Adam Elbirt, Joseph H. Silverman, and Adam D. Woodbury. NTRU in constrained devices. In *CHES '01: Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems*, pages 262–272, London, UK, 2001. Springer-Verlag.

[CS97] Don Coppersmith and Adi Shamir. Lattice attacks on NTRU. In *EUROCRYPT*, pages 52–61, 1997.

[CS03] John H. Conway and Derek A. Smith. *On Quaternions and Octonions: Their Geometry, Arithmetic, and Symmetry.* A. K. Peters, Ltd., 2003.

[GOS02] Philippe Gaborit, Julien Ohler, and Patrick Solé. Ctru, a polynomial analogue of ntru. Technical report, INRIA, 2002.

[HgHP$^+$05] Nick Howgrave-graham, Jeff Hoffstein, Jill Pipher, William Whyte, and Ntru Cryptosystems. On estimating the lattice security of NTRU, 2005.

[HPS98] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In *Lecture Notes in Computer Science*, pages 267–288. Springer-Verlag, 1998.

[HPS08] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. *An Introduction to Mathematical Cryptography.* Science+Business Media, LLC. Springer, 2008.

[HS00] Jeffrey Hoffstein and Joseph Silverman. Optimizations for ntru. In *In Public Key Cryptography and Computational Number Theory.*, pages 11–15, 2000.

[JO05] D. Janovska and G. Opfer. Linear equations in quaternions. *Numerical Mathematics and Advanced Applications, Proceedings of ENUMATH*, 2005.

[Kap06] Jens-Peter Kaps. *Cryptography for Ultra-Low Power Devices.* Ph.d. dissertation, ECE Department, Worcester Polytechnic Institute, Worcester, Massachusetts, USA, May 2006.

[Kar07] Camelia Karimianpour. Lattice-based cryptosystems. Master's thesis, Ottawa, Canada, 2007.

[Kou06] R. Kouzmenko. Generalizations of the NTRU cryptosystem. Master's thesis, Polytechnique, Montreal, Canada, 2006.

[May99] Alexander May. Cryptanalysis of NTRU, unpublished paper, 1999.

[MG02] Daniele Micciancio and Shafi Goldwasser. *Complexity of Lattice Problems: a cryptographic perspective*, volume 671 of *The Kluwer International Series in Engineering and Computer Science.* Kluwer Academic Publishers, Boston, Massachusetts, 2002.

[Mic01a] Daniele Micciancio. The hardness of the closest vector problem with preprocessing. *IEEE Transactions on Information Theory*, 47(3):1212–1215, 2001.

[Mic01b] Daniele Micciancio. The shortest vector problem is NP-hard to approximate to within some constant. *SIAM Journal on Computing*, 30(6):2008–2035, 2001. Preliminary version in FOCS 1998.

[MS01] Alexander May and Joseph H. Silverman. Dimension reduction methods for convolution modular lattices. In *CaLC '01: Revised Papers from the International Conference on Cryptography and Lattices*, pages 110–125, London, UK, 2001. Springer-Verlag.

[MZM09] Ehsan Malekian, Ali Zakerolhosseini, and Atefeh Mashatan. Qtru: A lattice attack resistant version of ntru pkcs. Cryptology ePrint Archive, Report 2009/330, 2009. http://eprint.iacr.org/, submitted for publication.

[NKM09] Monica Nevins, Camelia Karimianpour, and Ali Miri. Ntru over rings beyond z. *accepted to Designs, Codes and Cryptography*, May 2009.

[Rot02] Joseph J. Rotman. *Advanced Modern Algebra.* Prentice Hall, 2002.

[Sch96] Richard D. Schafer. *An introduction to non-associative algebras.* Dover Publications Inc., New York, 1996. Corrected reprint of the 1966 original.

[Sha08] Zi Yang Sham. Quaternion algebras and quadratic forms. Master's thesis, Waterloo, Ontario, Canada, 2008.

[Zha97] Fuzhen Zhang. Quaternions and matrices of quaternions. *Linear Algebra and its Applications*, 251:21–57, 1997.