A New Non-Associative Cryptosystem Based on NTOW Public Key Cryptosystem and Octonions Algebra

Kadijeh Bagheri, Mohammad-Reza Sadeghi
Amirkabir University of Technology (Iran)

msadeghi@aut.ac.ir

Extended abstract

In this work, we present a public key cryptosystem, called OTWO, based on octonions algebra and NTWO cryptosystem [1] which is a multivariate version of NTRU [2]. Inherent security of this system relies on the difficulty of the shortest vector problem (SVP) in a certain type of lattices with a hybrid norm. Since the octonions are non-associative (power-associative) and alternative algebra, they do not have a matrix isomorphic representation. So, normally lattice attacks [3] against this cryptosystem are impossible. The only way to cryptanalysis and to find the private key for decryption in this cryptosystem is to expand the equation of public key as a linear system of equations and form a non-circular lattice. However, this type of attack seems to has no chance to succeed.

We change the underlying algebraic structure of NTWO and use a different lattice for key generation and decryption that it increases complexity of decryption. Furthermore, the non-associativity of underlying algebraic structure and existence of different lattice for key generation and decryption improve the security of cryptosystem markedly.

Method: The octonion algebra can be consider over a field or any arbitrary commutative ring R [4]. In our work, we use the bivariate convolution polynomial ring $R' = \mathbb{Z}[X]/(X^N - 1) = \mathbb{Z}[x, y]/(x^n - 1, y^n - 1)$ which n is a fixed prime number. Hence, we define $\mathbb{A}$, $\mathbb{A}_p$ and $\mathbb{A}_q$ as the three octonion algebras over the rings $R', R'_p = \mathbb{Z}_p[X]/(X^N - 1)$ and $R'_q = \mathbb{Z}_q[X]/(X^N - 1)$, respectively with bilinear multiplication (denoted by the symbol $\circ$), as follows

$$\begin{aligned}
\mathbb{A} &:= \left\{ f_0(x, y) + \textstyle\sum_{i=1}^{7} f_i(x, y) \cdot e_i \;\middle|\; f_0(x, y), \dots, f_7(x, y) \in R' \right\},\\
\mathbb{A}_p &:= \left\{ f_0(x, y) + \textstyle\sum_{i=1}^{7} f_i(x, y) \cdot e_i \;\middle|\; f_0(x, y), \dots, f_7(x, y) \in R'_p \right\},\\
\mathbb{A}_q &:= \left\{ f_0(x, y) + \textstyle\sum_{i=1}^{7} f_i(x, y) \cdot e_i \;\middle|\; f_0(x, y), \dots, f_7(x, y) \in R'_q \right\}.
\end{aligned}$$

where $\{1, e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$ are the basis of the algebras and they have the following rules

$$\begin{aligned}
&e_i^2 = -1, i = 1, \dots, 7\\
&e_i \cdot e_j = -e_j \cdot e_i \quad i \neq j, \, i, \, j = 1, \dots, 7\\
&e_i \cdot e_j = e_k \;\rightarrow\; e_{i+1} \cdot e_{j+1} = e_{k+1} \quad i \neq j, \, i, \, j = 1, \dots, 7\\
&e_i \cdot e_j = e_k \;\rightarrow\; e_{2i} \cdot e_{2j} = e_{2k} \quad i \neq j, \, i, \, j = 1, \dots, 7
\end{aligned}$$

and the indices greater than 7 should be reduced mod 7. For simplification we use the notation $f_i \triangleq f_i(x, y)$, for $i = 0, 1, 2, 3$.

We denote the conjugate and inverse of the octonion F by $F^\star = f_0 - \sum_{i=1}^{7} f_i \cdot e_i$ and $F^{-1} = (\sum_{i=1}^{7} {f_i}^2)^{-1} \cdot F^\star$, respectively.

In OTWO, the public parameters (n, p, q, d) play the same role as the alternative parameters do in NTWO, i.e., n is an integer number such that $n|(q - 1)$, p and q are two different prime numbers such that $gcd(p, q) = gcd(n, q) = 1$ and $q \gg p$. The subsets L_f, L_g, L_ϕ and L_m of R' contain small polynomials which are polynomials with coefficients with small Euclidian norm and small Hamming norm (defined as the number of nonzero coefficient of a polynomial).

Let $J_q = Q_q + \sum_{i=1}^{7} Q_q \cdot e_i$, where $Q_q = \langle \sigma = \sum_{(a,b) \in T} \lambda_{(a,b)} \rangle$ is an ideal generated by σ and $\lambda_{(a,b)}$'s are Lagrange interpolators as follows

$$\lambda_{(a,b)} = \frac{ab(x^n - 1)(y^n - 1)}{n^2(x - a)(y - b)}.$$

T is a small subset of L, the set of pairs of n-th roots of unity. We define Q_q similar to NTWO. Clearly, J_q is an ideal of $\mathbb{A}_q = R'_q + \sum_{i=1}^{7} R'_q \cdot e_i$ and it contains the ideal $\langle x^n - 1, y^n - 1\rangle$ of $\mathbb{A}$. It can be shown that $J = \langle J_q, q\rangle$ is an ideal of $\mathbb{A} = R' + \sum_{i=1}^{7} R' \cdot e_i$. Indeed, once can prove $J = Q + \sum_{i=1}^{7} Q \cdot e_i$ where $Q = \langle \sigma, q\rangle$. We call J *private ideal and use it for key generation and decryption.*

0.1 Key generation

For creating public and private keys, we randomly choose two quaternion polynomials F and G in $\mathbb{A}$ with small coefficients

$$\begin{array}{ll} F = f_0 + \sum_{i=1}^{7} f_i \cdot e_i, & f_0, \dots, f_7 \in L_f \\ G = g_0 + \sum_{i=1}^{7} g_i \cdot e_i, & g_0, \dots, g_7 \in L_g \end{array}$$

where F and G both are invertible over $\mathbb{A}/J$ and also F must be invertible over $\mathbb{A}_p$ (i.e., the polynomials $\sum_{i=1}^{7} {f_i}^2$ and $\sum_{i=1}^{7} {g_i}^2$ should be nonzero and invertible over its underlying ring R'/Q and R'_p ($\mathbb{A}/J$ is a octonion algebra over the ring R'/Q).

The inverses of the quaternion F over $\mathbb{A}/J$ and $\mathbb{A}_p$ are denoted by F_J^{-1} and F_p^{-1} respectively. If one of the above inverses does not exist, we generate a new quaternion F such that $\sum_{i=1}^{7} {f_i}^2 \neq 0$.

To generate the public key, compute $\tilde{H} = F_J^{-1} \circ G \ (mod\ J)$. Thus we have $\tilde{H} = F_J^{-1} \circ G + \vartheta \ (mod\ q)$ where $\vartheta \in J_q$ and it is unknown to attacker. Then

$$\tilde{H} \quad = \quad F_J^{-1} \circ G + \vartheta \ (mod\ q)$$

is published as the public key which satisfies $F \circ \tilde{H} + \xi \equiv G \ (mod\ q)$, where $\xi \in J_q$. Subsequently, the private key consists (G, F, ξ).

With the same public parameters (n, p, q, d), the key generation in OTWO is 64 times slower than that of NTWO because public key is multiplied by 64 convolutional products. This means we can choose a smaller dimension n in OTWO without reducing its security.

0.2 Encryption

To encrypt a binary message m, it is mapped to an octonion $M = m_0 + \sum_{i=1}^{7} m_i \cdot e_i \ \in \mathbb{A}$ where $m_i \in L_m$ for $i = 0, \dots, 7$ are eight small polynomials. Then a random octonion $\Phi = \phi_0 + \sum_{i=1}^{7} \phi_i \cdot e_i$ is generated such that $\phi_i \in L_\phi$ for $i = 0, \dots, 7$. Now, the encrypted message is as follows

$$C = p.\tilde{H} \circ \Phi + M \ \in \mathbb{A}/J.$$

In this cryptosystem, eight messages set up once as one octonion and they are encrypted simultaneously. So, in the same dimension, the encryption process in OTWO is eight times slower than NTWO.

0.3 Decryption

According to the non-associativity of octonions algebra for removing the term F_J^{-1} from $(F_J^{-1} \circ G)) \circ \Phi$, the receiver multiply C by the private key F on the left and then on the right. Since octonions algebra are alternative, using Moufang identities we have:

$$\begin{aligned} E &= ((F \circ C) \circ F = p.(F \circ (\tilde{H} \circ \Phi) \circ F) + (F \circ M) \circ F \ \in \mathbb{A}/J \\ &= p.(F \circ \tilde{H}) \circ (\Phi \circ F) + (F \circ M) \circ F \ \in \mathbb{A}/J \\ &= p.(F \circ (F_J^{-1} \circ G)) \circ (\Phi \circ F) + (F \circ M) \circ F \ \in \mathbb{A}/J \\ &= p.G \circ (\Phi \circ F) + (F \circ M) \circ F \ \in \mathbb{A}/J. \end{aligned}$$

In this way, the octonion F_J^{-1} with very large norm is removed and the polynomials with small norm remain in E. On the other hand, E is equivalent to

$$E' = p.G \circ (\Phi \circ F) + (F \circ M) \circ F + B \in \mathbb{A}_q,$$

where $B \in J$ is unknown to the receiver. In order to perform a feasible decryption the receiver must have $p.G \circ (\Phi \circ F) + (F \circ M) \circ F \in \mathbb{A}_q$. For this purpose, the octonion B is found and is subtracted from E'.

When we consider and fixe a basis for $\mathbb{A}$ (for example monomial basis) then $\mathbb{A}$ is isomorphic to $\mathbb{Z}^{n^2} + \sum_{i=1}^{7} \mathbb{Z}^{n^2} \cdot e_i \cong \mathbb{Z}^{8n^2}$ as an additive group. Thus, we have $J \subset \mathbb{A} \cong \mathbb{Z}^{8n^2}$ and J will be a lattice in $\mathbb{A}$. Indeed, B is the closest vector of this lattice to E with a high probability. Upon finding the closest vector in private lattice J and subtracting it from E', the octonion $p.G \circ (\Phi \circ F) + (F \circ M) \circ F \in \mathbb{A}_q$ would be available to the receiver and decryption process can be continued easily.

If the public parameters in the cryptosystem are chosen suitably, the coefficients of eight polynomials in $p.G \circ (\Phi \circ F) + (F \circ M) \circ F$ will lie in the interval $[-\frac{q-1}{2}, \frac{q-1}{2}]$ and the decryption will not fail so the reduction modulo q will superfluous. Then, the receiver can reduce $p.G \circ (\Phi \circ F) + (F \circ M) \circ F$ modulo p and obtain the term $(F \circ M) \circ F \in \mathbb{A}_p$. Finally, message recovery $(F \circ M) \circ F \in \mathbb{A}_p$ is multiplied on the right and then on the left by F_p^{-1}.

Furthermore, it can be estimated that the decryption process of OTWO is 16 times slower than NTWO, whereas its encryption process is almost 8 times slower. So, decryption speed is at least half of the encryption speed that is one of advantages of OTWO. Moreover, we can compensate the speed decrease of OTWO by considering a lower dimension n. In addition, if one can undertake more cost for parallelization, OTWO can be implemented in higher speed than NTWO and achieve a higher security.

0.4 The OTWO Lattice

We said only way for cryptanalysis and finding the private key (G, F, ξ) for decryption is to expand the octonion equation $F \circ \tilde{H} + \xi \equiv G \ (mod\ q)$ for a given octonion $\tilde{H}$ as the following

$$\begin{cases}
(f_0 * h_0 - f_1 * h_1 - f_2 * h_2 - f_3 * h_3 - f_4 * h_4 - f_5 * h_5 - f_6 * h_6 - f_7 * h_7) + \xi_0 = g_0 + qu_0 \\
(f_0 * h_1 + f_1 * h_0 + f_2 * h_4 + f_3 * h_7 - f_4 * h_2 + f_5 * h_6 - f_6 * h_5 - f_7 * h_3) + \xi_1 = g_1 + qu_1 \\
(f_0 * h_2 - f_1 * h_4 + f_2 * h_0 + f_3 * h_5 + f_4 * h_1 - f_5 * h_3 + f_6 * h_7 - f_7 * h_6) + \xi_2 = g_2 + qu_2 \\
(f_0 * h_3 - f_1 * h_7 - f_2 * h_5 + f_3 * h_0 + f_4 * h_6 + f_5 * h_2 - f_6 * h_4 + f_7 * h_1) + \xi_3 = g_3 + qu_3 \\
(f_0 * h_4 + f_1 * h_2 - f_2 * h_1 - f_3 * h_6 + f_4 * h_0 + f_5 * h_7 + f_6 * h_3 - f_7 * h_5) + \xi_4 = g_4 + qu_4 \\
(f_0 * h_5 - f_1 * h_6 + f_2 * h_3 - f_3 * h_2 - f_4 * h_7 + f_5 * h_0 + f_6 * h_1 + f_7 * h_4) + \xi_5 = g_5 + qu_5 \\
(f_0 * h_6 + f_1 * h_5 - f_2 * h_7 + f_3 * h_4 - f_4 * h_3 - f_5 * h_1 + f_6 * h_0 + f_7 * h_2) + \xi_6 = g_6 + qu_6 \\
(f_0 * h_7 + f_1 * h_3 + f_2 * h_6 - f_3 * h_1 + f_4 * h_5 - f_5 * h_4 - f_6 * h_2 + f_7 * h_0) + \xi_7 = g_7 + qu_7,
\end{cases}$$

where $*$ is the convolution product.

Let us denote the ordered monomials of the form $x^i y^j$, $0 \leq i, j \leq n$, by X^α for $0 \leq \alpha \leq n^2$. Then for two polynomials k and h in R' we have

$$k * h = (k_0, \cdots k_{n^2-1})\mathcal{H} = (k_0, \cdots k_{n^2-1}) \left[\begin{array}{c} \overline{h} \\ \overline{X \circ h} \\ \vdots \\ \overline{X^{N^2} \circ h} \end{array} \right]. \tag{1}$$

Note that the matrix $\mathcal{H}$ is no longer a circulant matrix. Indeed, each row of $\mathcal{H}$ is a permutation of first row and these permutations are related to the monomial order that we have used. Upon the above notations, we can set up the lattice, denoted by Λ_{OTWO}, that is generated by the rows of the matrix

$$\left[\begin{array}{ccc} qI_{8n^2} & 0 & 0 \\ \mathfrak{H} & I_{8n^2} & 0 \\ \mathfrak{D} & 0 & I_{8n^2} \end{array} \right],$$

where

$$\mathfrak{H} = \left[\begin{array}{cccccccc}
+\mathcal{H}_0 & +\mathcal{H}_1 & +\mathcal{H}_2 & +\mathcal{H}_3 & +\mathcal{H}_4 & +\mathcal{H}_5 & +\mathcal{H}_6 & +\mathcal{H}_7 \\
-\mathcal{H}_1 & +\mathcal{H}_0 & -\mathcal{H}_4 & -\mathcal{H}_7 & +\mathcal{H}_2 & -\mathcal{H}_6 & +\mathcal{H}_5 & +\mathcal{H}_3 \\
-\mathcal{H}_2 & +\mathcal{H}_4 & +\mathcal{H}_0 & -\mathcal{H}_5 & -\mathcal{H}_1 & +\mathcal{H}_3 & -\mathcal{H}_7 & +\mathcal{H}_6 \\
-\mathcal{H}_3 & +\mathcal{H}_7 & +\mathcal{H}_5 & +\mathcal{H}_0 & -\mathcal{H}_6 & -\mathcal{H}_2 & +\mathcal{H}_4 & -\mathcal{H}_1 \\
-\mathcal{H}_4 & -\mathcal{H}_2 & +\mathcal{H}_1 & +\mathcal{H}_6 & +\mathcal{H}_0 & -\mathcal{H}_7 & -\mathcal{H}_3 & +\mathcal{H}_5 \\
-\mathcal{H}_5 & +\mathcal{H}_6 & -\mathcal{H}_3 & +\mathcal{H}_2 & +\mathcal{H}_7 & +\mathcal{H}_0 & -\mathcal{H}_1 & -\mathcal{H}_4 \\
-\mathcal{H}_6 & -\mathcal{H}_5 & +\mathcal{H}_7 & -\mathcal{H}_4 & +\mathcal{H}_3 & +\mathcal{H}_1 & +\mathcal{H}_0 & -\mathcal{H}_2 \\
-\mathcal{H}_7 & -\mathcal{H}_3 & -\mathcal{H}_6 & +\mathcal{H}_1 & -\mathcal{H}_5 & +\mathcal{H}_4 & +\mathcal{H}_2 & +\mathcal{H}_0
\end{array} \right], \mathfrak{D} = \left[\begin{array}{cccc} D & 0 & \cdots & 0 \\ 0 & D & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & D \end{array} \right].$$

Eeach $D_{n^2\times n^2}$ consist of all Lagrange *interpolators $\lambda_{(a,b)}$, where $(a,b)\in L$ and each $\mathcal{H}_i$ for $i=0,\dots,7$ has the form of matrix $\mathcal{H}$ in Equation (1). Clearly, the vector (G,F,ξ) belongs to Λ_{OTWO}. Moreover, if we consider a hybrid metric on $\mathbb{A}^3$ which is Euclidean on the first two components and Hamming on the third component, the private key (G,F,ξ) will be the smallest vector in the lattice with high probability. Thus, the security of this cryptosystem relies on the difficulty of the shortest vector problem in the hybrid lattice of dimension $24n^2$. To the best of our knowledge, lattice basis reduction algorithms such as LLL [5] and BKZ [6] or BKZ 2.0 [7] have not been developed to solve SVP with this hybrid metric. Consequently, this cryptosystem is capable of having a high security.*

One can estimate that for any selection of public parameters (n,p,q,d), OTWO has a security equal to that of NTWO with $(8n,p,q,d)$. But NTWO with dimension $8n$ is 64 times slower than NTWO with dimension n while QTWO acts approximately four times slower, compared to NTWO. As a result, OTWO with dimension n has a security equal to NTWO with dimension $8n$ but OTWO with dimension n is 8 times faster than NTWO with dimension $8n$. Consequently, the main advantage of applying non-associative algebra in OTWO is that it can present a higher security than NTWO with smaller dimensions.

References

[1] M. Caboara, F. Caruso and C. Traverso, "Grobner Bases for Public Key Cryptography", Symbolic and algebraic computation Proc. ISSAC '08, ACM, pp. 315-323, 2008.

[2] J. Hoffstein, J. Pipher and J.H. Silverman, "NTRU, a ring-based public-key cryptosystem", Algorithmic number theory, Portland, OR, Springer, vol. 1423, pp. 267288, 1996.

[3] D. Coppersmith and A. Shamir, "Lattice attacks on NTRU", In Lecture Notes in Computer Science, Berlin / Heidelberg, Springer, vol. 1233, pp. 52-61, 1997.

[4] J. H. Conway and D. A. Smith and A K Peters "On Quaternions and Octonions: their geometry, arithmetic, and symmetry, A K", 2003.

[5] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovasz, "Factoring Polynomials with Rational Coefficients", Mathematische Annalen, vol. 261, pp. 513534, 1982.

[6] C. P. Schnorr and M. Euchner, "Lattice basis reduction: improved practical algorithms and solving subset sum problems", Math. Programming, pp.181199, 1993.

[7] Y. Chen and P.Q. Nguyen "BKZ 2.0: better lattice security estimates", In Advances in Cryptology ASIACRYPT 2011, Lecture Notes in Computer Science, Springer, Heidelberg, vol. 7073, pp. 120, 2011.