An Innovative HSS Algebra for Designing a Secure Like-NTRU Encryption

Hiba Shakir Salman*[1], Hassan Rashed Yassein[2]

[1]Department of Mathematics, Faculty of Education for Girls, University of Kufa, Iraq

[2]Department of mathematics, College of Education, University of Al-Qadisiyah, Iraq

e-mail: shakerhaba396@gmail.com ; hassan.yaseen@qu.edu.iq

Article Info

Page Number: 6098 - 6113

Publication Issue:

Vol 71 No. 4 (2022)

Article History

***Article Received**: 25 March 2022*

***Revised**: 30 April 2022*

***Accepted**: 15 June 2022*

***Publication**: 19 August 2022*

Abstract

This paper aims to improve NTRU by creating a multi-dimensional public key cryptosystem called NTRSHH by replacing the algebra $Z[x]\backslash (x^N - 1$used in NTRU with a new algebra called HSS. This cryptosystem provides high security and speed compared to some cryptosystems similar to NTRU as HXDTRU and TOTRU by increasing the number of private keys in the public keys and the cipher text. The property of the multi-dimensionality of this cryptosystem gives it an advantage in the possibility of its application in many scopes.

Keywords: NTRU, HXDTRU,TOTRU, Security of key, and security of message.

Introduction

In 1996, Hoffstein et al. proposed the NTRU public key cryptosystem in 1996, which works with the ring of truncated polynomials $Z[x]\backslash (x^N - 1)$ [1]. It's the first system that doesn't rely on discrete logarithm problem or factorization integer numbers. One of the notable characteristics of NTRU is its speed, its much faster than RSA and ECC and has a much smaller key. Since it was proposed, many studies have improved NTRU performance.

In 2002, Gaborit et al. introduced analog of NTRU called CTRUdepending on $F_2[x]\backslash (x^N - 1)$[2]. In 2005, Coglianese and Goi proposed MaTRU an like-NTRU, this system depends on a ring of $k \times k$matrices of polynomials in $Z[x]\backslash (x^N - 1)$ [3]. In 2009, Malekian et al. introduced QTRU, a four-dimensional cryptosystem based on quaternion algebra [4]. In 2010, Malekian et al. proposed OTRU, a multi-dimensional cryptosystem based on alternative octonion algebra [5]. In 2011, Jarvis proposed ETRU based on the Eisenstein integer ring [6].In 2016, Yassein and Al-Saidi introducedHXDTRU and BITRU, defined by the hexadecnion and binary algebras as analog to NTRU cryptosystem [7–10]. In 2018, Yassein and Al-Saidi created BCTRU, a multidimensional NTRU-like cryptosystem that depends on Bi-cartesian algebra [11, 12]. Atani et al. [13] presented a new NETRU cryptosystem that operates over the ring of $k \times k$ matrices of polynomials in $Z[x]\backslash (x^N - 1)$. Yassein et al. [14] suggested a novel NTRU-analogue based on carternion algebra in 2020, dubbed QOBTRU. Yassein et al. [15] introduced NTRTE, a new multi-dimensional public key cryptosystem based on a commutative quaternion algebra with a novel structure.

In 2021, Yassein et al. designed a new mathematical structure to offer an analog QTRU cryptosystem, termed QMNTR [16]. In the same year, Yassein et al. introduced BOTRU, a new public key cryptosystem based on the bi-octonion subalgebra with a novel mathematical structure. Also, Yassein et al. designed NTRS and TRTSH cryptosystems like-NTRU depend on tripternion algebra, also, QOTRU depends on qu-octonion algebra [18-20]. In 2022, Yassein et al. improved NTRU through the design of NTRTRN and TOTRU which depend on tripternion algebra and octonion algebra respectively [21, 22].

In this paper, we have created a new public key cryptosystem, known as NTRHSS like-NTRU based on a new algebra called HSS and a new mathematical structure that gives it higher security and speed. Also, we compared its performance with NTRU, HXDTRU, and TOTRU.

ASS Algebra

Let F be a field with $Char(F) \neq 2$, then the algebra HSS defined over Fas follows:
$HSS = \{(a_1, a_2, a_3)(1,1,1) + (a_4, a_5, a_6)(x, x, x) + (a_7, a_8, a_9)\ (y, y\ , y) \backslash\ a_i \in F,$ for all i=1,2,…,9}, where $\{(1,1,1), (x, x, x), (y, y, y)\ \}$ form the basis of this algebra. Now,if have three truncated polynomial rings

$K = Z[x] \setminus (x^N - 1)$, $K_p = Z_p[x] \setminus (x^N - 1)$, and$K_q = Z_q[x] \setminus (x^N - 1)$.

We show three algebraß , $ß_p$and $ß_q$as follows:

ß $=\{(f_1, f_2, f_3)(1,1,1) + (f_4, f_5, f_6)(x, x, x) + (f_7, f_8, f_9)(y, y\ , y) \backslash\ f_1,\ldots,f_9 \in K\}$

$ß_p$ $=\{(f_1, f_2, f_3)(1,1,1) + (f_4, f_5, f_6)(x, x, x) + (f_7, f_8, f_9)\ (y, y\ , y) \backslash\ f_1,\ldots,f_9 \in K_p\}$

$ß_q$ $=\{(f_1, f_2, f_3)(1,1,1) + (f_4, f_5, f_6)(x, x, x) + (f_7, f_8, f_9)\ (y, y\ , y) \backslash\ f_1,\ldots,f_9 \in K_q\}$

Let μ_1,μ_2 ∈ $ß_p$ or$ß_q$ such that
μ_1=$(f_1, f_2, f_3)(1,1,1) + (f_4, f_5, f_6)(x, x, x) + (f_7, f_8, f_9)(y, y, y)$ and
μ_2=$(g_1, g_2, g_3)(1,1,1) + (g_4, g_5, g_6)(x, x, x) + (g_7, g_8, g_9)(y, y, y)$. The addition $\mu_1 + \mu_2$is performed by adding corresponding coefficients. The multiplication $\mu_1 * \mu_2$can be determined by
$\mu_1 * \mu_2$=$(f_1g_1 + f_4g_7 + f_7g_4, f_2g_2 + f_5g_8+f_8g_5, f_3g_3 + f_6g_9 + f_9g_6)$ (1,1,1) + $(f_4g_4 + f_1g_7 +$ *f7g1,f5g5+f2g8+f8g2, f6g6+f3g9+f9g3x,x,x+(f7g7+f1g4+f4g1,f8g8+f5g2+f2g5,* $f_9g_9 + f_3g_6 + f_6g_3)$ (y, y, y).

This multiplication is not associative, but it is commutative and alternative. Then the identity multiplication is

$$\varrho = (1,,1,1)(1,1,1) + (0,0,0)(x, x, x) + (0,0,0)\ (y, y, y).$$

Inverse multiplication of $\mu_1$is defined by
$\mu_1{}^{-1} = (e_1, e_2, e_3)(1,1,1) + (e_4, e_5, e_5)(x, x, x) + (e_7, e_8, e_9)\ (y, y, y)$where

$$e_1 = \frac{f_4f_7-(f_1)^2}{3f_1f_4f_7-(f_1)^2-(f_4)^2-(f_7)^2},\ e_2 = \frac{f_5f_8-(f_2)^2}{3f_2f_5f_8-(f_2)^2-(f_5)^2-(f_8)^2},\ e_3 = \frac{f_6f_9-(f_3)^2}{3f_3f_6f_9-(f_3)^2-(f_6)^2-(f_9)^2},$$

$$e_4 = \frac{f_1f_4-(f_7)^2}{3f_1f_4f_7-(f_1)^2-(f_4)^2-(f_7)^2},\ e_5 = \frac{f_2f_5-(f_8)^2}{3f_2f_5f_8-(f_2)^2-(f_5)^2-(f_8)^2},\ e_6 = \frac{f_3f_6-(f_9)^2}{3f_3f_6f_9-(f_3)^2-(f_6)^2-(f_9)^2},$$

$$e_7 = \frac{f_1f_7-(f_4)^2}{3f_1f_4f_7-(f_1)^2-(f_4)^2-(f_7)^2},\ e_8 = \frac{f_2f_8-(f_5)^2}{3f_2f_5f_8-(f_2)^2-(f_5)^2-(f_8)^2},\ e_9 = \frac{f_3f_9-(f_6)^2}{3f_3f_6f_9-(f_3)^2-(f_6)^2-(f_9)^2}.$$

NTRHSS Cryptosystem

Public Parameters

The public parameters in NTRHSS are similar to NTRU and subsetsT_F, T_V, T_Z, T_G, T_θ, $T_R$and$T_M \subset ß$ as defined in Table 1.

Table 1: subsets of NTRHSS

Notation	Definition
T_F	$F = \{(f_1, f_2, f_3)(1,1,1) + (f_4, f_5, f_6)(x, x, x) + (f_7, f_8, f_9)(y, y, y) \in ß \mid f_i \in K,$ $i = 1,2, \ldots, 9$ satisfy$\ell\ (d_f, d_f - 1)\}$
T_V	$V = \{(v_1, v_2, v_3)(1,1,1) + (v_4, v_5, v_6)(x, x, x) + (v_7, v_8, v_9)(y, y, y) \in ß \mid v_i \in K,$ $i = 1,2, \ldots, 9$ satisfy$\ell\ (d_v, d_v - 1)\}$

T_Z	Z= $\{(z_1, z_2, z_3)(1,1,1) + (z_4, z_5, z_6)(x, x, x) + (z_7, z_8, z_9)(y, y, y) \in$ ß $\|z_i \in K$, $i = 1,2, \dots, 9$ satisfy $\ell\ (d_z, d_z - 1)\}$
T_G	G=$\{(g_1, g_2, g_3)(1,1,1) + (g_4, g_5, g_6)(x, x, x) + (g_7, g_8, g_9)(y, y, y) \in$ ß$\|g_i \in K$, $i = 1,2, \dots, 9$ satisfy $\ell\ (d_g, d_g)\}$
T_θ	θ=$\{(\theta_1, \theta_2, \theta_3)(1,1,1) + (\theta_4, \theta_5, \theta_6)(x, x, x) + (\theta_7, \theta_8, \theta_9)(y, y, y) \in$ ß$\|\theta_i \in K$, $i = 1,2, \dots, 9$ satisfy $\ell\ (d_\theta, d_\theta)\}$
T_R	$R = \{(r_1, r_2, r_3)(1,1,1) + (r_4, r_5, r_6)(x, x, x) + (r_7, r_8, r_9)(y, y, y) \in$ ß$\|r_i \in K$, $i = 1,2, \dots, 9$ satisfy $\ell\ (d_r, d_r)\}$
T_M	$M = \{(m_1, m_2, m_3)(1,1,1) + (m_4, m_5, m_6)(x, x, x) + (m_7, m_8, m_9)(y, y, y) \in$ ß$\|m_i \in K$,coefficients $i = 1,2, \dots, 9$ are the chosen modulo between $-p/2$ and $p/2$ }

Where $\ell\ (d_1,\ d_2)$ = $\{f \in K | f$ has d_1 coefficients equal 1, d_2 coefficientsequal -1, the remaining equal 0$\}$.The constants $d_f, d_v, d_z, d_g, d_\theta$, d_r and d_m are defined in a similar role as in NTRU.

NTRHSS Phases

The NTRHSS cryptosystem can be denoted through the following three phases

I. Key Creation

The recipient generates the public keys H and K by choosing invertible element $F \in T_F$ mod p and q denoted by F_p^{-1} and F_q^{-1} respectively,invertible element $V \in T_V$ mod p denoted by V_p^{-1}, invertible element $Z \in T_Z$ mod q denoted by Z_q^{-1} and $G \in T_G$ and are calculated as follows:

$H = F_q^{-1} * G(modq)$; $K = V * Z_q^{-1}(modq)$

II. Encryption

To obtain the cipher text E of the plaintext M, the sender chooses $\theta \in T_\theta$ and $R \in T_R$ and converts the plaintext into an element in HSS and uses the following formula

$$E\ =\ p(H * \theta + R) + M * K(modq).$$

III. Decryption

To find the plaintext of the cipher text, the recipient performs the following steps:

$B = F * E * Z\ (modq)$

$$= F * (p\,(H * \theta + R) + M * K) * Z\,(modq)$$
$$= p(F * H * \theta * Z) + p(F * R * Z) + F * (M * K) * Z\,(modq)$$
$$= p\big(F * \big(F_q^{-1} * G\big) * \theta * Z\big) + p(F * R * Z) + F * (M * (V * Z_q^{-1}) * Z)\,(modq)$$
$$= \big(F * F_q^{-1}\big) * (G * \theta * F\big) + p(F * R * Z) + F * \Big((M * V) * (Z_q^{-1} * Z)\Big)\,(modq)$$
$$= p(G * \theta * F) + p(F * R * F) + F * M * V(modq),$$

Such that the coefficient of $p(G * \theta * V) + p(F * R * V) + F * (M * V)$lie inthe interval $(-q/2, q/2]$.

Convert $B = p(G * \theta * V) + p(F * R * V) + F * (M * V)(modq)$ to $modp$

$$B(modp) = p(G * \theta * V) + p(F * R * V) + F * (M * V)(modp)$$
$$= F * M * V(modp).$$

$F_p^{-1} * B * V_p^{-1}(modp) = M(modp)$ and the resulting coefficients are adjusted to lie in the interval$(-p/2, p/2]$.

Security Analysis

In a brute force attack, any attacker that obtains the public parameters and public keys $H = F_q^{-1} * G(modq)$and $K = V * Z_q^{-1}(modq)$of NTRHSS can access the plaintext by finding ($F \in T_F$ or $G \in T_G$) and ($V \in T_V$ or $Z \in T_Z$). The size of the subsets $T_F, T_G,\ T_V$and$T_Z$are calculated as follows:

$|T_F| = \left(\frac{N!}{(d_{f}!)^2 (N-2d_f)!}\right)^9$,$|T_G| = \left(\frac{N!}{(d_{g}!)^2 (N-2d_g)!}\right)^9$,$|T_V| = \left(\frac{N!}{(d_{v}!)^2 (N-2d_v)!}\right)^9$, and $|T_z| = \left(\frac{N!}{(d_{z}!)^2 (N-2d_z)!}\right)^9$

Therefore, the security of key is equal to the following:

$$\left(\frac{(N!)^{18}}{\big(d_g!\ d_v!\big)^{18}\Big(\big(N-2d_g\big)!\,(N-2d_v)!\Big)^9}\right)^{\frac{1}{2}}$$

Similarly, to find the original message, an attacker must search in $T_\theta$andT_R.The size of the subsets $T_\theta$and$T_R$are calculated as follows:

$$|T_\theta| = \left(\frac{N!}{(d_{\theta}!)^2 (N-2d_\theta)!}\right)^9 \text{ and} |T_r| = \left(\frac{N!}{(d_{r}!)^2 (N-2d_r)!}\right)^9$$

Therefore, the security of message is equal to the following:

$$\left(\frac{(N!)^{18}}{(d_\theta!\,d_r!\ )^{18}\big((N-2d_\theta)!\,(N-2d_r)!\big)^{9}}\right)^{\frac{1}{2}}$$

Table 2 show security of key and security of message for NTRHSS according to generic parameters $d_v, d_g, d_\theta\ , d_r, N$.

Table 2: NTRHSS 's security of key and security of message

N	d_v	d_g	d_θ	d_r	Security of Key	Security of Message
107	12	12	5	5	$1.5387{\times}10^{271}$	$3.3459{\times}10^{143}$
107	20	20	10	10	$1.9512{\times}10^{360}$	$6.4256{\times}10^{239}$
149	12	12	10	10	$1.1609{\times}10^{299}$	$7.5988{\times}10^{267}$
149	25	25	20	20	$1.1628{\times}10^{488}$	$6.9376{\times}10^{428}$
167	18	18	18	18	$1.6919{\times}10^{414}$	$5.3505{\times}10^{419}$
167	27	27	22	22	$6.1899{\times}10^{537}$	$8.3259{\times}10^{476}$
211	20	20	18	18	$2.2155{\times}10^{489}$	$1.4695{\times}10^{456}$
211	34	34	22	22	$2.5306{\times}10^{682}$	$4.2822{\times}10^{522}$
257	20	20	18	18	$1.3088{\times}10^{522}$	$1.7715{\times}10^{486}$
257	24	24	24	24	$3.1457{\times}10^{594}$	$3.1457{\times}10^{594}$

Comparison of NTRU, TOTRU, HXDTRU, and NTRHSS

Relying on the values in Table 1, Tables 3 and 4 show the comparison between key security and message security between NTRU, TOTRU, HXDTRU, and NTRHSS cryptosystem respectively. Accordingly, the security of the key and the message ofNTRHSS is more secure than NTRU, TOTRU, and HXDTRU.

Table 3: Security key of the NTRU and its Improvements

Security Key of NTRU	Security Key of TOTRU	Security Key of HXDTRU	Security Key of NTRHSS
1.1640×10^{15}	1.135×10^{241}	1.135×10^{241}	1.5387×10^{271}
2.3836×10^{20}	1.0859×10^{326}	1.0859×10^{326}	1.9512×10^{360}
9.3902×10^{16}	3.6545×10^{271}	3.6545×10^{271}	1.1609×10^{299}
1.3024×10^{27}	6.8558×10^{433}	6.8558×10^{433}	1.1628×10^{488}

2.0808×10^{23}	1.2357×10^{478}	1.2357×10^{478}	1.6919×10^{414}
7.5390×10^{29}	1.0891×10^{478}	1.0891×10^{478}	6.1899×10^{537}
1.7433×10^{27}	7.2895×10^{435}	7.2895×10^{435}	2.2155×10^{490}
8.1525×10^{29}	3.8075×10^{606}	3.8075×10^{606}	2.5306×10^{682}
1.3088×10^{29}	7.4107×10^{465}	7.4107×10^{465}	1.3088×10^{522}
1.0657×10^{33}	1.2915×10^{432}	1.2915×10^{432}	3.1457×10^{594}

Table 4: Security message of the NTRU and its Improvements

Message security of NTRU	Message security of TOTRU	Message security of HXDTRU	Message security of NTRHSS
2.9757×10^{8}	3.7788×10^{127}	3.7788×10^{127}	3.3459×10^{143}
2.1021×10^{13}	1.4541×10^{213}	1.4541×10^{213}	6.4256×10^{239}
2.4114×10^{15}	1.3068×10^{238}	1.3068×10^{238}	7.5988×10^{267}
2.1111×10^{24}	1.5568×10^{381}	1.5568×10^{381}	6.9376×10^{428}
2.0809×10^{23}	1.2357×10^{373}	1.2357×10^{373}	5.3505×10^{419}
3.13036×10^{26}	8.4972×10^{423}	8.4972×10^{423}	8.3259×10^{476}
2.2009×10^{25}	3.0335×10^{405}	3.0335×10^{405}	1.4695×10^{456}
1.0842×10^{29}	3.6438×10^{464}	3.6438×10^{464}	4.2822×10^{522}
1.0323×10^{27}	1.6621×10^{432}	1.6621×10^{432}	1.7715×10^{486}
1.0656×10^{33}	2.7825×10^{528}	2.7825×10^{528}	3.1457×10^{594}

Table 5 shows the number of mathematical operations from addition (α) and convolution multiplication (λ) in the three phasesof NTRU ,HXDTRU,TOTRU and NTRHSS. Therefore, the speed of key creation, encryption, and decryption ofNTRHSS are faster than those of HXDTRU and TOTRU.

Table 5: Arithmetic operations of NTRU,TOTRU, HXDTRU and NTRSAA.

	NTRU	TOTRU	HXDTRU	NTRHSS
Key Generation	1 λ	128λ	265 λ	54 λ
Encryption	1λ and 1 α	128 λ and 16 α	265λ and 16 α	54 λ and18α

Decryption	2λ and 1 α	1536λ and 16 α	4096λand 16 α	486λand 18α

Table 6 shows the speed NTRU, TOTRU, HXDTRU, and NTRHSS based on Table 5 such that$\tau$is the time of convolution multiplication and τ_1 is the time of polynomial addition. Therefore, NTRHSS is faster than TOTRU and HXDTRU and slower than NTRU.

Table 6: Speed of NTRU and its Improvements

	NTRU	HXDTRU	TOTRU	NTRHSS
speed	$4\tau+ 2\tau_1$	$4608\tau + 32\tau_1$	$1792\tau + 32\tau_1$	$594\tau + 36\tau_1$

Conclusion

NTRHSS is multi-dimensional public key cryptosystem based on a new commutative and alternative algebra HSS with high security and acceptable speedwhen compared to some of NTRU improvements. It can encrypt nine different messages from one source or from multiple sources, this feature can be very useful in designing protocols or similar applications.

References

[1] J. Hoffstein, J. Pipher, J. Silverman, NTRU: A ring based public key cryptosystem. Proceeding of ANTS III, LNCS, Springer Verlag, 1998,pp. 267–288.

[2] P. Gaborit, J. Ohler, P. Soli,CTRU, A polynomial analogue of NTRU,INRIA, Rapport de recherch´e, no. 4621, 2002.

[3] M. Coglianese, B. Goi, MaTRU: A new NTRU based cryptosystem,SpringerVerlag Berlin Heidelberg, 2005, pp. 232–243.

[4] E. Malekian, A. Zakerolhsooeini, A. Mashatan, QTRU: A lattice attack resistant version of NTRU PCKS based on quaternion algebra,The ISC Int'l Journal of Information Security, vol. 3, no. 1, 2011, pp. 29–42.

[5] E. Malekian, A. Zakerolhsooeini, OTRU: A non-associative and high speed public key cryptosystem. IEEE Computer Society, (2010), 83–90.

[6] K. Jarvis, NTRU over the Eisenstein Integers, M. Sc. thesis, Universityof Ottawa, 2011.

[7] H. R. Yassein, N. M. Al-Saidi, HXDTRU Cryptosystem Based on Hexadecnion Algebra. In proceeding of 5th international cryptology and information security conference, 2016.

[8] N. M. Al-Saidi, H. R. Yassein, A new alternative to NTRU cryptosystem based on highly dimensional algebra with dense lattice structure,Malaysian Journal of Mathematical Sciences, vol. 11, no. s, 2017, pp. 29–43.

[9] H. R. Yassein, N. M. Al-Saidi, BITRU: Binary Version of the NTRU Public Key Cryptosystem via Binary Algebra, International Journalof Advanced Computer Science and Applications, vol. 7, no.11,2016, pp. 1–6.

[10] H. R. Yassein, N. M. G. Al-Saidi, A Comparative Performance Analysisof NTRU and Its Variant Cryptosystems, Proceeding of InternationalConferenceon Current Research in Computer Science and Information Technology, 2017, pp. 115–120.

[11] H. R. Yassein, N.M. Al-Saidi, BCTRU: A New Secure NTRUCrypt Public Key System Based on a Newly Multidimensional Algebra. In proceeding of 6th international cryptology and information security conference,(2018).

[12]H. R. Yassein, N. M. Al-Saidi, An Innovative Bi-Cartesian Algebra for Designing of Highly Performed NTRU Like Cryptosystem, MalaysianJournal of Mathematical Sciences, vol. 13, no. s, 2019, pp. 29–43.

[13] R. E. Atani, S. E. Atani, A. H. Karbasi, NETRU: A Non-commutative and Secure Variant of CTRU Cryptosystem, The ISC International Journal of Information Security, vol. 10, no. 1, 2018, pp. 45–53.

[14] H. R. Yassein, N. M. Al-Saidi, A. K. Farhan A New NTRU Cryptosystem Outperforms Three Highly Secured NTRU-Analog Systems through an Innovation Algebraic Structure, Journal of Discrete Mathematical Sciences and Cryptography, vol. 23, no. 2,2020, pp. 1–20.

[15] H. R.Yassein,N. M. Al-Saidi,A. K. Jabber, A MultidimensionalAlgebra for Designing an Improved NTRU Cryptosystem,Eurasian Journal of Mathematical and Computer Applications, vol. 8, no.4, 2020, pp. 97–107.

[16] H. R. Yassein, A. A. Abidalzahra, N. M. G. Al-Saidi, A New Designof NTRU Encryption with High Security and Performance Level, AIP Conference Proceedings, vol. 2334,2021, pp. 080005-1 - 080005-4.

[17] H. R. Yassein, H. H. Abo-Alsood, A new Designof an Alternative NTRU Encryption with High Secure,Efficient International Journal of Mathematics and Computer Science, vol. 16, no. 4, 2021,pp. 1469–1477.

[18] H. R. Yassein, S. H. Shahhadi, A New Design of NTRUEncrypt-analog Cryptosystem with High Security and Performance Level via Tripternion Algebra, International Journal of Mathematics and Computer Science, vol.16, no. 4, 2021,pp. 1515-1522.

[19] H. H. Abo-Alsood and H. R. Yassein, QOTRU: A New Design of NTRU Public Key Encryption Via Qu-Octonion Subalgebra, Journal of Physics: Conference Series, vol. 1999, pp. 1-7, 2021

[20] S. H. shahhadi and H. R. Yassein, NTRsh: A New Secure Variant of NTRUEncrypt Based on Tripternion Algebra, Journal of Physics: Conference Series, vol. 1999,2021, pp. 1-6.

[21] S. H. shahhadi and H. R. Yassein, An Innovative Tripternion Algebra for Designing NTRU - Like Cryptosystem with High security, AIP Conference Proceedings, vol. 2386, 2022, pp.060009-1 - 060009-6.

[22] H. H. Abo-Alsood and H. R. Yassein, Analogue to NTRU Public Key Cryptosystem by Multi-Dimensional Algebra with High Security, AIP Conference Proceedings, vol. 2386, 2022, pp. 060009-1 - 060009-6.

This template provides authors with most of the formatting specifications needed for preparing electronic versions of their papers. All standard paper components have been specified for three reasons: (1) ease of use when formatting individual papers, (2) automatic compliance to electronic requirements that facilitate the concurrent or later production of electronic products, and (3) conformity of style throughout a conference proceedings. Margins, column widths, line spacing, and type styles are built-in; examples of the type styles are provided throughout this document and are identified in italic type, within parentheses, following the example. PLEASE DO NOT RE-ADJUST THESE MARGINS. Some components, such as multi-leveled equations, graphics, and tables are not prescribed, although the various table text styles are provided. The formatter will need to create these components, incorporating the applicable criteria that follow.

Type Style and Fonts

Wherever Times is specified, Times Roman or Times New Roman may be used. If neither is available on your word processor, please use the font closest in appearance to Times. Avoid using bit-mapped fonts if possible. True-Type 1 or Open Type fonts are preferred. Please embed symbol fonts, as well, for math, etc.

Ease of Use

Selecting a Template (Heading 2)

First, confirm that you have the correct template for your paper size. This template has been tailored for output on the US-letter paper size. If you are using A4-sized paper, please close this template and download the file for A4 paper format called "CPS_A4_format".

Maintaining the Integrity of the Specifications

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

Prepare Your Paper Before Styling

Before you begin to format your paper, first write and save the content as a separate text file. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar:

Abbreviations and Acronyms

Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

Units

- Use either SI (MKS) or CGS as primary units. (SI units are encouraged.) English units may be used as secondary units (in parentheses). An exception would be the use of English units as identifiers in trade, such as "3.5-inch disk drive".
- Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersteds. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity that you use in an equation.

- Do not mix complete spellings and abbreviations of units: “Wb/m2” or “webers per square meter”, not “webers/m2”. Spell out units when they appear in text: “. . . a few henries”, not “. . . a few H”.
- Use a zero before decimal points: “0.25”, not “.25”.

Equations

The equations are an exception to the prescribed specifications of this template. You will need to determine whether or not your equation should be typed using either the Times New Roman or the Symbol font (please no other font). To create multileveled equations, it may be necessary to treat the equation as a graphic and insert it into the text after your paper is styled.

Number equations consecutively. Equation numbers, within parentheses, are to position flush right, as in (1), using a right tab stop. To make your equations more compact, you may use the solidus (/), the exp function, or appropriate exponents. Italicize Roman symbols for quantities and variables, but not Greek symbols. Use a long dash rather than a hyphen for a minus sign. Punctuate equations with commas or periods when they are part of a sentence, as in

Note that the equation is centered using a center tab stop. Be sure that the symbols in your equation have been defined before or immediately following the equation. Use “(1)”, not “Eq. (1)” or “equation (1)”, except at the beginning of a sentence: “Equation (1) is . . .”

Some Common Mistakes

- The word “data” is plural, not singular.
- The subscript for the permeability of vacuum $\square_0$, and other common scientific constants, is zero with subscript formatting, not a lowercase letter “o”.
- In American English, commas, semi-/colons, periods, question and exclamation marks are located within quotation marks only when a complete thought or name is cited, such as a title or full quotation. When quotation marks are used, instead of a bold or italic typeface, to highlight a word or phrase, punctuation should appear outside of the quotation marks. A parenthetical phrase or statement at the end of a sentence is punctuated outside of the closing parenthesis (like this). (A parenthetical sentence is punctuated within the parentheses.)
- A graph within a graph is an “inset”, not an “insert”. The word alternatively is preferred to the word “alternately” (unless you really mean something that alternates).
- Do not use the word “essentially” to mean “approximately” or “effectively”.
- In your paper title, if the words “that uses” can accurately replace the word “using”, capitalize the “u”; if not, keep using lower-cased.

- Be aware of the different meanings of the homophones “affect” and “effect”, “complement” and “compliment”, “discreet” and “discrete”, “principal” and “principle”.
- Do not confuse “imply” and “infer”.
- The prefix “non” is not a word; it should be joined to the word it modifies, usually without a hyphen.
- There is no period after the “et” in the Latin abbreviation “et al.”.
- The abbreviation “i.e.” means “that is”, and the abbreviation “e.g.” means “for example”.

An excellent style manual for science writers is [7].

Using the Template

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper.

Authors and Affiliations

The template is designed so that author affiliations are not repeated each time for multiple authors of the same affiliation. Please keep your affiliations as succinct as possible (for example, do not differentiate among departments of the same organization). This template was designed for two affiliations.

For author/s of only one affiliation (Heading 3): To change the default, adjust the template as follows.

Selection (Heading 4): Highlight all author and affiliation lines.

Change number of columns: Select Format >

Columns >Presets > One Column.

Deletion: Delete the author and affiliation lines for the second affiliation.

For author/s of more than two affiliations: To change the default, adjust the template as follows.

Selection: Highlight all author and affiliation lines.

Change number of columns: Select Format >

Columns > Presets > One Column.

Highlight author and affiliation lines of affiliation 1 and copy this selection.

Formatting: Insert one hard return immediately after the last character of the last affiliation line. Then paste the copy of affiliation 1. Repeat as necessary for each additional affiliation.

Reassign number of columns: Place your cursor to the right of the last character of the last affiliation line of an even numbered affiliation (e.g., if there are five affiliations, place your cursor at end of fourth affiliation). Drag the cursor up to highlight all of the above author and affiliation lines. Go to Format > Columns and select "2 Columns". If you have an odd number of affiliations, the final affiliation will be centered on the page; all previous will be in two columns.

Identify the Headings

Headings, or heads, are organizational devices that guide the reader through your paper. There are two types: component heads and text heads.

Component heads identify the different components of your paper and are not topically subordinate to each other. Examples include Acknowledgments and References and, for these, the correct style to use is "Heading 5". Use "figure caption" for your Figure captions, and "table head" for your table title. Run-in heads, such as "Abstract", will require you to apply a style (in this case, italic) in addition to the style provided by the drop down menu to differentiate the head from the text.

Text heads organize the topics on a relational, hierarchical basis. For example, the paper title is the primary text head because all subsequent material relates and elaborates on this one topic. If there are two or more sub-topics, the next level head (uppercase Roman numerals) should be used and, conversely, if there are not at least two sub-topics, then no subheads should be introduced. Styles named "Heading 1", "Heading 2", "Heading 3", and "Heading 4" are prescribed.

Figures and Tables

Positioning Figures and Tables: Place figures and tables at the top and bottom of columns. Avoid placing them in the middle of columns. Large figures and tables may span across both columns. Figure captions should be below the figures; table heads should appear above the tables. Insert figures and tables after they are cited in the text. Use the abbreviation "Fig. 1", even at the beginning of a sentence.

Figure Labels: Use 8 point Times New Roman for Figure labels. Use words rather than symbols or abbreviations when writing Figure axis labels to avoid confusing the reader. As an example, write the quantity "Magnetization", or "Magnetization, M", not just "M". If including units in the label, present them within parentheses. Do not label axes only with units. In the example, write "Magnetization (A/m)" or "Magnetization {A[m(1)]}", not just "A/m". Do not label axes with a ratio of quantities and units. For example, write "Temperature (K)", not "Temperature/K".

Footnotes

Use footnotes sparingly (or not at all) and place them at the bottom of the column on the page on which they are referenced. Use Times 8-point type, single-spaced. To help your readers, avoid using footnotes altogether and include necessary peripheral observations in the text (within parentheses, if you prefer, as in this sentence).

Copyright Forms and Reprint Orders

You must submit the Copyright Form per Step 7 of the CPS author kit's web page. THIS FORM MUST BE SUBMITTED IN ORDER TO PUBLISH YOUR PAPER.

Please see Step 9 for ordering reprints of your paper. Reprints may be ordered using the form provided as <reprint.doc> or <reprint.pdf>.

Acknowledgment

The preferred spelling of the word "acknowledgment" in America is without an "e" after the "g". Avoid the stilted expression, "One of us (R.B.G.) thanks . . ." Instead, try "R.B.G. thanks". Put applicable sponsor acknowledgments here; DO NOT place them on the first page of your paper or as a footnote.

References

List and number all bibliographical references in 9-point Times, single-spaced, at the end of your paper. When referenced in the text, enclose the citation number in square brackets, for example [1]. Where appropriate, include the name(s) of editors of referenced books. The template will number citations consecutively within brackets [1]. The sentence punctuation follows the bracket [2]. Refer simply to the reference number, as in [3]—do not use "Ref. [3]" or "reference [3]" except at the beginning of a sentence: "Reference [3] was the first . . ."

Number footnotes separately in superscripts. Place the actual footnote at the bottom of the column in which it was cited. Do not put footnotes in the reference list. Use letters for table footnotes.

Unless there are six authors or more give all authors' names; do not use "et al.". Papers that have not been published, even if they have been submitted for publication, should be cited as "unpublished" [4]. Papers that have been accepted for publication should be cited as "in press" [5]. Capitalize only the first word in a paper title, except for proper nouns and element symbols.

For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [6].

[1] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] K. Elissa, “Title of paper if known,” unpublished.

[5] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

[8] Electronic Publication: Digital Object Identifiers (DOIs):

[9] D. Kornack and P. Rakic, “Cell Proliferation without Neurogenesis in Adult Primate Neocortex,” Science, vol. 294, Dec. 2001, pp. 2127-2130, doi:10.1126/science.1065467.

[10] H. Goto, Y. Hasegawa, and M. Tanaka, “Efficient Scheduling Focusing on the Duality of MPL Representatives,” Proc. IEEE Symp. Computational Intelligence in Scheduling (SCIS 07), IEEE Press, Dec. 2007, pp. 57-64, doi:10.1109/SCIS.2007.357670.