Int. J. Communications, Network and System Sciences, **2011, 4, 197-204**
doi:10.4236/ijcns.2011.44024 Published Online April 2011 (http://www.SciRP.org/journal/ijcns)

Cubic Root Extractors of Gaussian Integers and Their Application in Fast Encryption for Time-Constrained Secure Communication

Boris Verkhovsky
Computer Science Department, *New Jersey Institute of Technology*, *Newark*, *USA*
E-mail: *verb73@gmail.com*
Received March 2, 2011; *revised April* 12, 2011; *accepted April* 15, 2011

Abstract

There are settings where encryption must be performed by a sender under a time constraint. This paper describes an encryption/decryption algorithm based on modular arithmetic of complex integers called Gaussians. It is shown how cubic extractors operate and how to find all cubic roots of the Gaussian. All validations (proofs) are provided in the Appendix. Detailed numeric illustrations explain how to use the method of digital isotopes to avoid ambiguity in recovery of the original plaintext by the receiver.

Keywords: Cryptographic Protocol, Secure Communication, Time-Constrained Encryption, Cubic Root Extractor, Gaussian Integers, Modular Arithmetic, Prefix/Suffix Positioning, Digital Isotope, Quadratic Residue, Jacoby Symbol

1. Introduction

This paper describes a cryptographic algorithm based on the extraction of cubic roots from complex numbers $a + bi$ with integer components a and b. Such complex integers are called Gaussian integers (Gaussians, for short) [1]. Let's denote $(a, b) := a + bi$ and $N := a^2 + b^2$, where N is called a norm of (a, b). In modular arithmetic based on Gaussians, if p is a prime and $N \bmod p \neq 0$, then for every integer a and b holds an equivalent of the Fermat identity [2]:

$$(a,b)^{p^2-1} \bmod p = (1,0) = 1. \tag{1}$$

This means that the cycles in Gaussian modular arithmetic have order $O(p^2)$, while the cycles in modular arithmetic based on real integers have order $O(p)$. Application of Gaussians for ElGamal cryptosystem is considered in [3]; and the RSA digital signature is described in [4]. Public key cryptography based on cubic roots of real integers is provided in [5] and in [6].

Definition1: A Gaussian integer (x, y) is called the cubic root of (a, b) modulo integer n, and defined as $\sqrt[3]{(a,b)} \bmod n$, if

$$(x,y)^3 = (a,b) \bmod n. \tag{2}$$

Proposition1: If p is a prime, $p \bmod 12 = 1$ and

$$V := (a,b)^{(p-1)/3} \bmod p = (1,0) = 1, \tag{3}$$

then there exists a cubic root of (a, b) modulo p.

Proposition2: If $p \bmod 12 = 5$, then for *every* integer a and b there exists an unique cubic root of (a, b) modulo p.

Proposition3: If $p^2 \bmod 9 \neq 1$ and

$$W := V^{p+1} \bmod p = (1,0) = 1, \tag{4}$$

then there exists a cubic root of (a, b) modulo prime p.

***Remark*1**: Here are examples, where $p^2 \bmod 9 = 1$: p = 17, 19, 53, 71, 89, 107, 109, 179, 197, 199, 269, 271.

The following two algorithms are constructive proofs of these propositions.

2. Algorithm-1

Step 1.1: Compute

$$W := (a,b)^{(p^2-1)/3} \bmod p; \tag{5}$$

Step 2.1: if $W \neq (1,0)$, **then** cubic root of (a, b) modulo p does not exist;

Step 3.1: Compute

$$s := p \bmod 9; \tag{6}$$

{there are six possibilities $s = \pm 1; \pm 2; \pm 4$};

Step 4.1: if $s \neq \pm 1$, then

$$m := 4/|s|, \tag{7}$$

otherwise apply Algorithm-2;

Step 5.1: Compute

$$E_p := \left[m\left(p^2 - 1\right) + 3 \right] / 9, \tag{8}$$

{where m = 1 or 2, see **Table 1**};

Step 6.1: Compute

$$(x, y) := (a, b)^{E_p} \bmod p. \tag{9}$$

***Example* 1**: Let $p = 23$; $(a,b) = (19,4)$;

$W := (19,4)^{(23^2-1)/3} = (19,4)^{176} \bmod 23 = (1,0)$; hence (19,4) is a cubic residue. $E_p := 59$;

$(x, y) := \sqrt[3]{(19,4)} = (19,4)^{59} \bmod 23 = (16,16)$. Indeed, $(16,16)^3 \bmod 23 = (19,4)$. It is easy to verify that (5, 2) and (2, 5) are also cubic roots of (19, 4). Hence, algorithm (5)-(9) computes only one of three cubic roots of (a, b). How to compute the two other cubic roots is discussed in sections 5 and A3.

3. Algorithm-2

If q mod 12 = 5, then a cubic root exists for every (a, b); and each Gaussian has a unique cubic root. The following algorithm computes such a cubic root (1).

Step 1.2: Compute cubic extractor

$$E_q := (2q - 1)/3;$$

Step 2.2: Compute $R := (a,b)^{E_q} \bmod q$ (10)

Step 3.2: Output (x, y):=R.

Three examples are provided in **Table 2**.

4. Multiplicity of Cubic Roots

Proposition 4: Suppose C_1, C_2 and C_3 are three cubic roots of L:= (a, b) modulo p, each satisfying the equation

$$\left(C^3 - L\right) \bmod p = 0; \tag{11}$$

then for every i = 1, 2, 3 the following identities hold:

$$C_i^3 \equiv L \bmod p. \tag{12}$$

$$\left(C_1 + C_2 + C_3\right) \bmod p = 0;$$

$$C_1 C_2 C_3 \bmod p = L \quad [7];$$

$$\left(C_1 C_2 + C_1 C_3 + C_2 C_3\right) \bmod p = 0. \tag{13}$$

$$\left(C_i C_j - C_k^2\right) \bmod p = 0, \tag{14}$$

where $\{i, j, k\}$ is every permutation of {1, 2, 3}.

$$\left[\left(C_i + C_j\right)^2 - C_i C_j\right] \bmod p = 0. \tag{15}$$

Table 1.Cubic extractors E_p and m.

p	7	11	13	23
E_p ; m	5; 2	27; 2	19; 1	59; 1
p	29	31	41	43
E_p ; m	187; 2	107; 1	187; 1	411; 2

Table 2. Illustrations of cubic root extraction; q mod 12 = 5.

q; (a, b)	53; (19, 13)	89; (17, 77)	269; (19, 73)
E_q	35	59	179
(x, y)	(45, 28)	(6, 85)	(112, 124)

5. Cubic Roots of (1, 0) and Gaussians

In order to find two other roots of (a, b), consider cubic roots of unity:

$$(u, w) := \sqrt[3]{(1,0)} \bmod n. \tag{16}$$

If (x, y) is a cubic root of (a, b), then $(u,w)(x,y)$ and $(u,w)^2 (x,y) \bmod p$ are also its cubic roots modulo n.

Proposition 5: If p is a Blum prime, then either $\sqrt{3}$ or $\sqrt{-3}$ modulo p exists, but not both; if $\sqrt{3} \bmod p$ exists, then

$$\begin{aligned} &u = \left[(p-1)/2\right] \bmod p; \\ &\text{and} \quad w = \left[(p \pm 1)\sqrt{3}/2\right] \bmod p. \end{aligned} \tag{17}$$

If $\sqrt{-3} \bmod p$ exists, then

$$u = \left(1 \pm \sqrt{-3}\right) \bmod p. \tag{18}$$

Proof is provided in the Appendix.

6. Existence of $\sqrt{3} \bmod p$ or $\sqrt{-3} \bmod p$

Jacoby symbols [8,9] analyze whether a specified integer is quadratic residue (QR). If p is a Blum prime, then

$$\begin{aligned} &\left(\frac{3}{p}\right) = -\left(\frac{p \bmod 3}{3}\right) = \left\{-\left(\frac{1}{3}\right) = -1\right\} \\ &\text{or} \qquad = \left\{-\left(\frac{2}{3}\right) = -(-1)^{(3^2-1)/8} = 1\right\}. \end{aligned} \tag{19}$$

Therefore, if p mod 12 = 11, then 3 is QR. Seven examples are listed in **Table 3**.

Table 3. $\sqrt{3} \bmod p$ if p mod 12 = 11.

p	11	23	47	59	71	83	107
$\sqrt{3}$	5	16	12	48	43	70	89

Yet, if $p \bmod 12 = 7$, then –3 is *QR*. (20)

7. Properties of Gaussian Cubes

Consider

$$(t,v) := (u,w)^3 = \left(u\left(u^2 - 3w^2\right), w\left(3u^2 - w^2\right)\right) \bmod p \quad (21)$$

Property 1:

$$\left(\pm u, \pm w\right)^3 = \left(\pm u\left(u^2 - 3w^2\right), \pm w\left(3u^2 - w^2\right)\right) = \left(\pm t, \pm v\right); \quad (22)$$

Property 2:

$$\left(w,u\right)^3 = \left(w\left(w^2 - 3u^2\right), u\left(3w^2 - u^2\right)\right) = -(v,t) \bmod p; \quad (23)$$

Property 3: If $u + w = p$, then

$$\left(u,w\right)^3 = \left(w,u\right)^3 = u^3\left(1,1\right) \bmod p\,. \quad (24)$$

8. Cryptographic Protocol

System design (each user's actions):

Step 1.3: Selects two large distinct primes *p* and *q*, where $p \bmod 12 = 11$; $p^2 \bmod 9 \neq 1$; and $q \bmod 12 = 5$;

Step 2.3: Computes $n = pq$; {*n* is user's public key; *p* and *q* are his private keys};

Step 3.3: Finds cubic root (*u*, *w*) of (1, 0) modulo *p*:

$$u = \left(p-1\right)/2 \left(\bmod p\right); w = \left(u\sqrt{3}\right) \bmod p.$$

Step 4.3: Pre-computes

$$P := q\left(q^{-1} \bmod p\right); Q := p\left(p^{-1} \bmod q\right)\left(\bmod n\right);$$

Protocol implementation: Suppose a sender (Sam) wants to securely transmit a plaintext *G* to receiver (Regina);

Sam divides *G* into an array of blocks $\left\{\left(g_1,h_1\right);\ \left(g_2,h_2\right);\cdots;\ \left(g_k,\ h_k\right);\cdots\right\}$ in such a way that every $g_k < n$ and $h_k < n$;

Encryption {Sam's actions}:

Step 5.3: He gets Regina's public key *n*; computes ciphertext

$$\left(a,b\right) := \left(g,h\right)^3 \bmod n\,;$$

and sends (*a, b*) to her;

Decryption {Regina's actions}:

Step 6.3: She, using her private keys *p* and *q*, extracts cubic roots

$$M_1 := \sqrt[3]{\left(a,b\right)} \bmod p; \text{ and } R := \sqrt[3]{\left(a,b\right)} \bmod q;$$

Step 7.3: She computes

$$M_2 := M_1 \times \left(u,w\right) \bmod p; \text{ and } M_3 := M_2 \times \left(u,w\right) \bmod p;$$

Step 8.3: {Using Chinese Remainder Theorem [10], Regina computes all 3 roots of (*a, b*) $D := \sqrt[3]{\left(a,b\right)} \bmod n$ }: for $k = 1,2,3$ $D_k := \left(M_k P + RQ\right) \bmod n$;

Step 9.3: {The original plaintext is recovered via digital isotopes-see sections 10 and 11}: $D = G$.

9. Efficient Encryption of Gaussians

Squaring of a Gaussian requires two multiplications of real integers (MoRI); and multiplication of two Gaussians requires three MoRI [11]. Therefore, the cubic power of Gaussian requires five MoRI. Yet, encryption

$$\left(a,b\right) := \left(g,h\right)^3 = \left(g^3 - 3gh^2, 3g^2h - h^3\right) \bmod p$$

in **Step 5.3** requires only *four* MoRI:

$$P_1 := g^2 \bmod p; \quad P_2 := h^2 \bmod p;$$
$$S := P_1 - P_2; \quad A_3 := S - 2P_2; \quad A_4 := S + 2P_1;$$
$$P_3 := gA_3 \bmod p; \quad P_4 := hA_4 \bmod p;$$

{there are no A_1 and A_2}; where the doublings $2P_1$ and $2P_2$ are achieved by binary shifting; then $\left(a,b\right) := \left(P_3, P_4\right)$.

10. Asymmetric Tagging of Digital Isotopes

In cryptographic algorithms based on extraction of square roots of real integers [12] or Gaussians [6] there are four pairs of solutions, and only one of them is the original plaintext. To distinguish the original solution from the other three, the authors use methods of tails, which is an analogue of using isotopes to tag various chemical components.

If the digital isotopes repeat *r* rightmost digits in each component of plaintext (*g*, *h*), then the probability of erroneous recovery of the "plaintext" is of order $\mathrm{O}\left(1/10^{2r}\right)$. For instance, if the length of isotope $r = 3$, then the probability of error is *one* in *one million*.

As shown below, a more elaborate strategy must be used to avoid ambiguity in the recovery of the original plaintext.

Definition 2: If there exist Gaussians with distinct components *x* and *y* such that

$$\left(x,y\right)^3 = \left(y,x\right)^3 \left(\bmod p\right), \quad (25)$$

then such *cubic* roots are called Gaussian twins (or CT, for short).

Proposition 6: If the square root of 3 modulo prime *p* exists, then there exists the CT; {see **Table4** for examples}.

Table 4. Examples of cubic roots twins (CT) for $p = 83$.

(*a*, *b*)	(27, 56)	(31, 52)	(26, 57)	(2, 81)	(78, 5)	(53, 30)
$\sqrt[3]{\left(a,b\right)}$	(22, 76); (76, 22)	(15, 24); (24, 15)	(46, 8); (8, 46)	(77, 7); (7, 77)	(8, 5); (5, 8)	(1, 11); (11, 1)

Proof: since $(x-y) \bmod p \neq 0$, then (25) implies the following relationships:

$$\begin{aligned} &(x-y)(1,-1)\left[(x,y)^2+(x,y)(y,x)+(y,x)^2\right]=0; \\ &\left(x^2-y^2,2xy\right)+\left(0,x^2+y^2\right)+\left(y^2-x^2,2xy\right) \\ &=\left(0,2xy+(x+y)^2\right) \bmod p=0; \\ &\textit{i.e.,}\ \left[(x+y)^2+2xy\right](\bmod p)=0. \end{aligned} \tag{26}$$

Let $y := Tx \bmod p$, then $x^2\left[(1+T)^2+2T\right] \bmod p=0$, *i.e.*, $\left(T^2+4T+1\right) \bmod p=0$; which implies that $T=-2\pm\sqrt{3} \bmod p$.

For instance, if $p = 83$, then $\sqrt{3}=70$, *i.e.*, $T=-2\pm 70 \bmod 83=\{11 \text{ or } 68\}$.

If $x = 1$, then $y = \{11 \text{ or } 68\}$; hence

$(1,68)^3=(68,1)^3 (\bmod 83)=(73,10)$; and

$(1,11)^3=(11,1)^3 (\bmod 83)=(53,30)$.

It means that $\sqrt[3]{(53,30)} \bmod 83$ equals either $(1,11)$ or $(11,1)$. Yet, if in both components the rightmost digit is "1", it is not clear whether the original plaintext is (0, 1) or (1, 0). For every p mod 12 = 11 there exist $4(p-1)$ CTs that satisfy (25) {examples are provided in **Table 4**).

11. Numeric Illustration

Algorithm in a nutshell

> ***System design***: Select p, q;
> **Compute** n, P, Q, u, w, s, m, E_p, E_q;
> ***Encryption*: Create** plaintext Z with isotopes; compute ciphertext (a, b);
> ***Decryption*:** R; RQ; M_1; M_2; M_3.

System design: Let Regina's p = 227 and q = 1109, where $p^2 \bmod 9=4\neq 1$, p mod 12 = 11; and q mod 12 = 5; she computes $n = pq$ = 251,743; P and Q:

$$\begin{aligned} P &:= q\left(q^{-1} \bmod p\right)=1109\times\left(1109^{-1} \bmod 227\right) \\ &=1109\times 96=106464; \\ Q &:= p\left(p^{-1} \bmod q\right)=227\times\left(227^{-1} \bmod 1109\right) \\ &=227\times 640=145280; \end{aligned}$$

and a cubic root (u w) of (1,0) modulo p:

$u=(227-1)/2(\bmod p)=113$;

$w=u\sqrt{3}=113\times 3^{57} \bmod 227=25$;

***Remark* 2:** $(u,w)^2=(u,p-w)(\bmod p)$;

{indeed, $(113,25)^3 \bmod 227=(1,0)$;

and $(113,25)^2 \bmod 227=(113,202)$};

$s := 227 \bmod 9=2$; $m := 4/|2|=2$;

and Gaussian cubic extractor {**Step 5.1**}

$$E_p := \left[2\times\left(227^2-1\right)+3\right]/9=11451;$$

finally, Regina pre-computes another cubic extractor $E_q := (2q-1)/3=739$.

***Encryption*:** Suppose the sender (Sam) wants to securely transmit message G = (1941, 2487) to Regina with two-digit isotopes:

$$Z := 100G + G \bmod 100 = (1941\underline{\mathbf{41}}, 2487\underline{\mathbf{87}}).$$

In this case the probability of erroneous recovery of the original message will not exceed 1/10,000, *i.e.*, it equals 0.01%.

Sam computes ciphertext

$$(a,b) := Z^3 \bmod 251743=(227258,195067)$$

Decryption: Regina computes

$$\begin{aligned} M_1 &:= (227258,195067)^{11451} \bmod 227 \\ &=(31,74)^{11451} \bmod 227=(74,78) \end{aligned}$$

and two other cubic roots:

$$M_2 := M_1\times(u,w)=(74,78)\times(113,25)=(56,222);$$

$$M_3 := M_2\times(u,w)=(56,222)\times(113,25)=(97,154);$$

and then unique cubic root R modulo q

$$\begin{aligned} R &:= (a,b)^{E_q} \bmod q=(227258,195067)^{739} \\ &=(66,371)(\bmod 1109). \end{aligned}$$

Using the Chinese Remainder Theorem [10], Regina computes (28):

$$\begin{aligned} (x,y)_k &=\left[M_k\times 1109\times\left(1109^{-1} \bmod 227\right)\right. \\ &\quad \left.+R\times 227\times\left(227^{-1} \bmod 1109\right)\right] \bmod 251743 \\ &=\left(106464M_k+145280R\right) \bmod 251743; \end{aligned}$$

until she detects isotopes

$$\begin{aligned} (x,y)_1 &=106464M_1+145280\times(66,371) \\ &=\left[106464\times(74,78)+(22246,25878)\right] \bmod n \\ &=(96549,274294); \quad \text{where } n=251743 \end{aligned}$$

$$\begin{aligned} (x,y)_2 &=\left[106464M_2+(22246,25878)\right] \bmod n \\ &=\left[106464\times(56,222)+(22246,25878)\right] \bmod n \\ &=(19\mathbf{41}\underline{41}, 24\mathbf{87}\underline{87}). \end{aligned}$$

Therefore, Regina recovers the original Gaussian block of information; and it is not necessary to compute $(x,y)_3$.

12. Optimized Recovery of Information

Let $M_k=(M_{k1}, M_{k2})$; $R=(R_1, R_2)$;

then $x_k = M_{k1}P + R_1Q; y_k = M_{k2}P + R_2Q$.

$M_1 = (M_{11}, M_{12})$ is computed by cubic root extraction; if the isotopes in Z are detected, then the original information is recovered; otherwise Regina needs to compute four components of two other cubic roots of (a, b):

$$\begin{aligned} M_2 &= (M_{11}, M_{12})(u, w) \\ &= (M_{11}u - M_{12}w, M_{11}w + M_{12}u) \end{aligned}; \quad (27)$$

$$\begin{aligned} M_3 &= (M_{11}, M_{12})(u, -w) \\ &= (M_{11}u + M_{12}w, -M_{11}w + M_{12}u) \end{aligned}. \quad (28)$$

Yet, to minimize computational burden, instead of computing M_2 and M_3, she finds

$$N_1 := M_{12}wP; \quad (29)$$

and then computes

$$x_2 = (M_{11}uP + R_{11}Q) - N_1. \quad (30)$$

If the isotopes are detected, then she computes y_2, otherwise Regina computes

$$\begin{aligned} x_3 &= x_2 + 2N_1 \\ \{&= (M_{11}uP + R_{11}Q) + M_{12}wP\} \text{ and } y_3. \end{aligned} \quad (31)$$

13. Elimination of Ambiguity in Recovery of Original Information

The probability of erroneous recovery can be decreased if, instead of repeating r rightmost digits of g and h, the following procedure is applied:

1) Consider r *leftmost* digits (prefix P_r) of the first component g in plaintext (g, h) and repeat it as its digital isotope;
2) Consider r *rightmost* digits (suffix S_r) of the second component h of plaintext (g, h) and repeat it as its digital isotope.

***Example* 2:** if $(g, h) = (31415926, 27182845)$ and $r = 2$, then (**31**3**1**415926, 2718284**5**4**5**).

***NB*:** if n is t-digits long and the number of digits in g is smaller than t, then the prefix $P_r = 00\cdots0$. To avoid ambiguity, the sender must attach both digital isotopes P_r and S_r as *suffixes*. Below is a simple mnemonic/schematic rule for constructing the digital isotopes:

$$(\text{priority, cocktail}) \Rightarrow$$
$$\Rightarrow (\textit{prio}\text{rity}\mathbf{prio}, \text{cock}\textit{tail}\mathbf{tail}).$$

***Remark* 3:** Therefore, there can be two types of cubic roots with isotopes:

(*PU***P**, *VS***S**) and (*US***S,** *PV***P**). Only the former one is authentic. Hence, a receiver (Regina) searches for the cubic root with isotopes in format (*PU***P**, *VS***S**), where *P* and *S* are *prefix* and *suffix* respectively. In this case (*PU, VS*) is acceptable as the genuine plaintext.

***Example* 3:** if $t = 8$; $r = 2$;
and $(g, h) = (00415926, 07182845)$,
then

$$\begin{aligned} Z &:= \begin{pmatrix} (g - g \bmod 10^6) \times 10^8 + g, \\ (h - h \bmod 10^2) \times 10^2 + h \bmod 10^2) \end{pmatrix} \\ &= (00415926\mathbf{00}, 07182845\mathbf{45}) \end{aligned}$$

14. Second Numeric Illustration

System design: Let $p = 227$; $q = 1109$, $n = pq = 251{,}743$; $P = 106464$; $Q = 145280$; $(u, w) = (113,25)$; $s = 2$; $m = 2$; $E_p = 11451$; $E_q = 739$.

Encryption: Plaintext $G = (1756, 2011)$; plaintext with isotopes

$$Z := (175\mathbf{6}\mathbf{7}, 20\mathbf{1}\mathbf{1}\mathbf{1}\mathbf{1});$$

and ciphertext $(a,b) = (57971, 209989)$;

***Decryption*:** $R = (395, 382)$; $M := (202, 137)$;

$$QR_1 \bmod n = 239939;$$
$$N_1 := M_{12}wP = 115336;$$
$$x_2 = M_{11}uP + QR_1 - N_1 = 196688;$$

since there is no isotope in x_2, then (x_3, y_3) is the original Gaussian.

Indeed, $x_3 = x_2 + 2N_1 = 175\mathbf{6}\mathbf{1}\mathbf{7}$.

15. Algorithm Analysis

The cryptographic algorithm described above is *neither* a generalization nor a special case of the RSA protocol [13].

First of all, the following identity holds:

$$(a, b)^{(p^2-1)(q-1)} \bmod n = (1, 0) = 1. \quad (32)$$

In the RSA algorithm, if z is the length of group cycle [13], then each user selects a public key e that is co-prime with z. In the proposed algorithm the length of cycle c is equal

$$c := (p^2 - 1)(q - 1). \quad (33)$$

Therefore in the RSA extension it would have been necessary to compute a multiplicative inverse d of e modulo c. Yet, in the algorithm described above the encryption key $e = 3$. Hence, the decryption key d cannot be computed as a modular multiplicative inverse, since $\gcd(3, z) = 3$, which implies that such an inverse does not exist [14].

16. Communication Speed-Up

Suppose it is necessary to transmit an H digit-long plain-

text, where the size of each block must not exceed *sixteen* digits; in addition, suppose that we want to ensure that the probability of erroneous recovery does not exceed one in one million. There are two options:

Option 1 is to select the size of each block equal to *ten* digits and the size of each tail equal to *six* digits; Option 2 is to select the size of each block equal to *thirteen* digits and the size of each tail equal to three *digits*.

In the 1st option we will treat each block individually as a real integer; which implies that we need to transmit $H/10$ real integers. In the 2nd option we will treat a pair of blocks as a Gaussian; which implies that we need to transmit $H/26$ Gaussians, *i.e.*, $H/13$ real integers. Therefore, the first option requires $13/10 = 1.3$ times more bandwidth, than the second option. In other words, the bandwidth can be reduced by 30% if Gaussian integers are considered.

17. Possible Applications and Conclusions

The proposed cryptosystem has significant specifics: the encryption is substantially faster than the decryption. There are certain settings where the sender has limited time to transmit the message: visual images or video, and receiver does not have such restriction. For instance, the sender is a system that urgently needs to transmit information prior to either collision with a target or before it is destroyed by a hostile action [15]. Another example is if the sender (say, an interplanetary or interstellar space station) detects an impending collision with an asteroid and is programmed to report about such collision and transmit visual and other details about the asteroid.

In this case it is paramount to ensure the reliability of message delivery [15,16]. Yet another example is of a security camera that has detected an imminent explosion and is pre-designed to report the situation (audio, pictures and/or video) [17] prior to its own destruction from the explosion.

18. Acknowledgements

I express my appreciation to J. Jones, and R. Rubino for corrections, and to E. A. Verkhovsky as well as anonymous reviewers for several suggestions that improved this paper.

19. References

[1] C. F. Gauss, "Disquisitiones Arithmeticae," English translation, Yale University Press, New Haven, 1986.

[2] J. T. Cross, "The Euler's φ-Function in the Gaussian Integers," *American Mathematics*, Vol. 55, 1983, pp. 518-528. doi:10.2307/2322785

[3] A. N. El-Kassar, M. Rizk, N. Mirza and Y. Wada, "El-Gamal Public Key Cryptosystem in the Domain of Gaussian Integers," *International Journal of Applied Mathematics*, Vol. 7, No. 4, 2001, pp. 405-412.

[4] H. Elkamchouchi, K. Elshenawy and H. Shaban, "Extended RSA Cryptosystem and Digital Signature Schemes in the Domain of Gaussian Integers," *The 8th International Conference on Communication Systems*, Washington, 25-28 November 2002, pp. 91-95.

[5] S. Kak, "The Cubic Public-Key Transformation," *Circuits Systems Signal Processing*, Vol. 26, No. 3, 2007, pp. 353-359. doi:10.1007/s00034-006-0309-x

[6] B. Verkhovsky, "Accelerated Cybersecure Communication Based on Reduced Encryption/Decryption and Information Assurance Protocols," *Journal of Telecommunication Managements*, Vol. 2, No. 3, 2009, pp. 284-293.

[7] R. W. Hadden, "On the Shoulders of Merchants: Exchange and the Mathematical Conception of Nature in Early Modern Europe," State University of New York Press, New York, 1994.

[8] R. Crandall and C. Pomerance, "Prime Numbers: A Computational Perspective," Springer, New York, 2001.

[9] A. Menezes, P. van Oorschot and S. Vanstone, "Handbook of Applied Cryptography," CRC Press, Boca Raton, 1997.

[10] D. Knuth, "The Art of Computer Programming, Vol. 1: Fundamental Algorithms," 3rd Edition, Addison-Wesley, Upper Saddle River, 1998.

[11] A. Karatsuba and Y. Ofman, "Multiplication of Many-Digital Numbers by Automatic Computers," *Doklady Akademii Nauk SSSR*, Vol. 14, No. 145, 1962, pp. 293-294.

[12] M. Rabin, "Digitized Signatures and Public-Key Functions as Intractable as Factorization," Technical Report, MIT/LCS/TR-212, January 1979.

[13] R. Rivest, A. Shamir and L. Adleman, "A Method of Obtaining Digital Signature and Public-Key Cryptosystems," *Communication of ACM*, Vol. 21, No. 2, 1978, pp. 120-126. doi:10.1145/359340.359342

[14] B. Verkhovsky, "Enhanced Euclid Algorithm for Modular Multiplicative Inverse and Its Complexity," *Advances in Computer Cybernetics*, Vol. 6, 1999, pp. 51-57.

[15] B. Verkhovsky, "Selection of Entanglements in Information Assurance Protocols and Optimal Retrieval of Original Blocks," *Journal of Telecommunications Management*, Vol. 2, No. 2, 2009, pp. 186-194.

[16] B. Verkhovsky, "Information Assurance Protocols: Efficiency Analysis and Implementation for Secure Communication," *Journal of Information Assurance and Security*, Vol. 5, No. 3, 2008, pp. 263-269.

[17] Z. Xu and J. Sun, "Video Encryption Technology and Application," English translation, Nova Science Publishers Inc., New York, 2010, pp. 1-99.

Appendix

A1. Validation of Algorithm-1

If condition (5) holds; then

$$\begin{aligned}(x,y)^3 &= (a,b)^{3E_p} = (a,b)^{m\left(p^2-1\right)/3+1} \\ &= \left[(a,b)^{\left(p^2-1\right)/3}\right]^m (a,b) \bmod p\end{aligned} \quad (A1)$$

If $(a,b)^{\left(p^2-1\right)/3} \bmod p = (1,0)$, then by Definition (2) (x, y) is a cubic root of (a, b) modulo prime p. Hence, if $\left(p^2-1\right)/9$ is not an integer, then there exists an integer m such that E_p is an integer, *i.e.*, there exists an integer solution of equation

$$\left[m\left(p^2-1\right)+3\right] \bmod 9 = 0. \quad (A2)$$

Indeed, observe that

1) Every integer greater than 3 can be expressed either as p=6k+1 or as p = 6k–1;
2) $\left(p^2-1\right)/3$ is an integer for every prime greater than 3;
3) If $\left(p^2-1\right)/9$ is not an integer, then k mod 3 = 0; and $\left(p^2-1\right)/3$ is not co-prime with 3.

Therefore, (A2) can be rewritten as

$$m\left(p^2-1\right)/3 \bmod 3 = 2. \quad (A3)$$

If there is no integer solution of Equation (A3); then Algorithm-1 is not applicable for these cases. In other terms, if either $(p-1)/9$ or $(p+1)/9$ is an integer, then E_p is not an integer.

A2. Validation of Algorithm-2

Let

$$R^3 = \left[(a,b)^{(q-1)}\right]^2 \times (a,b) \bmod q. \quad (A4)$$

Since q mod 12 = 5, then $(q-1)/2$ is *even*, hence by Euler criterion of quadratic residuosity $(-1)^{(q-1)/2} \bmod q = 1$, *i.e.*,

$$i \coloneqq \sqrt{p-1} \pmod q \quad (A5)$$

is a real integer; and hence $(a, b) \bmod q$ is also a real integer. Therefore, by the Fermat identity $R^3 \bmod q = (a,b)$. Q. E. D.

A3. More on Identities for Cubic Roots

By the Vieta theorem [7], equation

$$\left(C^3 - L\right) \bmod p = 0; \quad (A6)$$

implies that

$$(C-C_1)(C-C_2)(C-C_3) \bmod p = 0. \quad (A7)$$

Hence, (A6) and (A7) imply

$$(C_1+C_2+C_3) \bmod p = 0;\ C_1C_2C_3 \bmod p = L; \quad (A8)$$

and for every permutation $\{i, j, k\}$ of

$$\{1,\ 2,\ 3\} \quad \left(C_iC_j - C_k^2\right) \bmod p = 0. \quad (A9)$$

On the other hand, (A9) implies

$$\left[\left(C_i + C_j\right)^2 - C_iC_j\right] \bmod p = 0. \quad (A10)$$

Yet, neither (A9) nor (A10) are instrumental in recovery of all cubic roots.

A4. Proof of Proposition 5

***Algebraic approach*:**

$$(u,w)^3 = \left(u^3 - 3uw^2, 3u^2w - w^3\right) \bmod p = (1,0) \quad (A11)$$

Therefore from (A6) we deduce two equations with unknown u and w:

$$u\left(u^2 - 3w^2\right) \bmod p = 1; \quad (A12)$$

and

$$w\left(3u^2 - w^2\right) \bmod p = 0. \quad (A13)$$

Since in (A13) $w \bmod p \neq 0$, then

$$3u^2 = w^2 \pmod p. \quad (A14)$$

Hence, (A12) and (A14) imply that

$$\begin{aligned}&8u^3 + 1 = 0 \pmod p;\ \text{or} \\ &(2u+1)\left(4u^2 - 2u + 1\right) \bmod p = 0.\end{aligned} \quad (A15)$$

Equation (A15) holds if either

$$u = (p-1)/2 \pmod p; \quad (A16)$$

or

$$\left(4u^2 - 2u + 1\right) \bmod p = 0. \quad (A17)$$

Thus in (A16) case, if there exists square root of 3 modulo p, then from (A14)

$$w = \pm u\sqrt{3} = \pm(p-1)\sqrt{3}/2. \quad (A18)$$

Otherwise, Equation (A17) implies that

$$u = 1 \pm \sqrt{-3} \bmod p; \quad (A19)$$

and finally from (A12) we deduce w.

***Trigonometric approach*:** Consider

$$\begin{aligned}(u,w) &= \sqrt[3]{(1,0)} = \sqrt[3]{(\cos\pi + \mathrm{i}\sin\pi)} \\ &= (\cos\pi/3 + \mathrm{i}\sin\pi/3) = \left(1, \sqrt{3}\right)/2 \pmod p\end{aligned} \quad (A20)$$

Proposition7: If (*x, y*) is a cubic root of (*a, b*) modulo *p*, then $(u,w)(x,y) \bmod p$ and $(u,w)^2(x,y) \bmod p$ are also cubic roots of (*a, b*).

Proof: From Definition1 (2) for $k = 1, 2$ $\left[(u,w)^k(x,y)\right]^3 = (a,b) \bmod p$. Q.E.D.

