Dispersion of Sequences for Generating a Robust Enciphering System

Tomoyuki Nagase[1], **Ryusuke Koide**[1],
Takashi Araki[1], and **Yoshiei Hasegawa**[2], Non-members

ABSTRACT

This paper introduces a new paradigm for dispersion of information into three-dimensional space to generate a strenuous crypto system. The dispersion of the information is carried out by quaternion rotation matrix which is called quadripartite public-key (QPK). We considered a private key as a unit quaternion which has an arbitrary quadruple of real numbers. The public key has three different components which are constructed using quaternion rotation matrix QRM to generate a secure key, which significantly eliminates the risk of eavesdropping. Furthermore, quaternion has capability to provide a meditative encryption system for wireless images or voice transmissions. A computer-based simulation conducted to scrutinize the capability of QPK carefully in insuring the highest level of security is reported.

Keywords: Rotation matrix, cryptography, public key

1. INTRODUCTION

Information security over vulnerable and exposed wireless networks has become a primary concern for protecting this information from piracy and malicious code attacks or even from rogue wireless access point. Therefore, many researchers have scrutinized wireless networks looking for a stronger protection system which is based on proper encryption techniques.

A quaternion is so called hyper complex number of rank 4, and has two parts; a scalar part and a vector part which is an ordinary vector in three-dimensional space R^3. Quaternion was invented by Hamilton in 1843 [1]. It has been used in computer visions and robotics for rotating objects in 3-dimension [2][3].

This paper implements a quaternion as an encryption technique by providing four encryption keys. These keys' parameters are independent coefficients that have a free rotation in a 3-D space. The rotation is used in this paper as a function to encrypt information such as data or voice. The voice application has been sampled and each group of samples is arranged in a frame that has a 3×3 miniature matrix array. All elements in the group are rotated and spread in 3-D space using mathematical model called a quaternion rotation matrix (QRM) which is often appropriate for numerous applications such as being a tool for encryption technique.

2. A BRIEF BACKGROUND OF QUATERNION

We define a quaternion as the sum of two parts; a scalar (real) part and a vector (imaginary) part, $q = (scalar\ w, vector\ V)$, or $q = (w, V)$. The basic algebraic form of quaternion q is:

$$q = w + xi + yj + zk \tag{1}$$

where w and V are a scalar and a vector, respectively. The vector part V of quaternion comprises three ordinary vectors, such as (i, j, k), which form an orthonormal basis in R^3. These vectors have the following characterstics.

$$\begin{aligned} i \times i &= j \times j = k \times k = -1 \\ i \times j &= -j \times i = k \\ j \times k &= -k \times j = i \\ k \times i &= -i \times k = j \end{aligned} \tag{2}$$

Two quaternions q_1 and q_2 are equal if they have exactly the same components:

$$\begin{aligned} q_1 &= w_1 + x_1 i + y_1 j + z_1 k \\ q_2 &= w_2 + x_2 i + y_2 j + z_2 k \end{aligned} \tag{3}$$

then $q_1 = q_2$ if and only if $a_1 = a_2$, $b_1 = b_2$, $c_1 = c_2$ and $d_1 = d_2$.

The sum of two quaternions is defined by adding the corresponding components, that is

$$\left.\begin{aligned} q_1 + q_2 &= (w_1 + w_2) + (V_1 + V_2) \\ q_2 + q_1 &= (w_1 + w_2) + (x_1 + x_2)i \\ &\quad +(y_1 + y_2)j + (z_1 + z_2)k \end{aligned}\right\} \tag{4}$$

The product of two quaternions is called quaternion product. It is different from *dot* and *cross* prod-

04PSI17: Manuscript received on December 24, 2004 ; revised on August 14, 2005.

[1] The authors are with the Department of Science and Technology, Hirosaki University, Hirosaki, 036-8561, Japan. E-mail: nagase@si.hirosaki-u.ac.jp

[2] The author is with the Micronics Japan Co., Ltd., 2-6-8 Hon-cho, Kichijoji, Musasino, Tokyo, 180-8508, Japan.

ucts, and can be written as

$$q_1q_2 = (w_1w_2 + V_1\dot{V_2}, w_1V_2 + w_2V_1 + V_1 \times V_2) \tag{5a}$$

$$q_1q_2 = \left.\begin{array}{l} (w_1w_2 + x_1x_2 + y_1y_2 + z_1z_2) \\ +(w_1x_2 + w_2x_1 + y_1z_2 - y_2z_1)i \\ +(w_1y_2 + w_2y_1 + x_2z_1 - x_1z_2)j \\ +(w_1z_2 + w_2z_1 + x_1y_2 - x_2y_1)k \end{array}\right\} \tag{5b}$$

Furthermore, we need to define other forms of quaternion $q = (w, x, y, z)$, which are the complex conjugate q^*, the norm $\|q\|$ and inverse of a quaternion q^{-1}, and are written as follows

$$\left.\begin{array}{ll} q^* & = (w, -x, -y, -z) \\ \|q\| & = \sqrt{(w^2 + x^2 + y^2 + z^2)} \\ q^{-1} & = \frac{q^*}{\|q\|^2} = \sqrt{(w^2 + x^2 + y^2 + z^2)} \end{array}\right\} \tag{6}$$

If a quaternion q has length 1, we say that q is a unit quaternion. The inverse of a unit quaternion is its conjugate $(q^{-1} = q^*)$.

3. A ROTATION OPERATOR TOOL FOR ENCRYPTING DATA

We consider in this section on how quaternion can be used to describe rotation of an object in 3-dimensional space R^3. A quaternion rotation matrix is used as a tool to rotate a group of elements which has been organized as 3×3 matrix array in 3-D space, where the elements of the group appear in a stochastic manner.

Consider two quaternions $q = (w, x, y, z)$ and $P = (0, a, b, c)$, where a vector (a, b, c) in R^3 corresponds to a pure quaternion whose real part is zero. We define the quaternion operator P_{rot} to be a rotation operator or a frame rotation in R^3 then

$$P_{rot} = q^{-1}Pq \tag{7}$$

where q^{-1} is inverse quaternion q. From equation (7) and using equation (6), P_{rot} can be written as

$$\begin{aligned} P_{rot} = \Bigg(0, & \frac{(\|q\|^2-2y^2-2z^2)a+2(xy-wz)b+2(xz+wy)c}{\|q\|^2}, \\ & \frac{2(xy+wz)a+(\|q\|^2-2x^2-2z^2)b+2(yz-wx)c}{\|q\|^2}, \\ & \frac{2(xz-wy)a+2(yz+wx)b+(\|q\|^2-2x^2-2y^2)c}{\|q\|^2}\Bigg) \end{aligned} \tag{8}$$

Suppose vector $X = (a, b, c)$ is ordinary vector in R^3, and the rotation operator of the vector X can be represented in term of the matrix and given by the following formula

$$X_{rot}=\frac{1}{\|q\|^2}\begin{pmatrix} \|q\|^2 - 2y^2 - 2z^2 & 2xy - 2wz & 2xz + 2wy \\ 2xy + 2wz & \|q\|^2 - 2z^2 - 2x^2 & 2yz - 2wz \\ 2xz - 2wy & 2yz + 2wz & \|q\|^2 - 2x^2 - 2y^2 \end{pmatrix}X \tag{9}$$

The matrix part of equation (9) is called a rotation matrix of quaternion. The rotation matrix $\Gamma(q)$ for quaternion q is given by

$$\Gamma(q) = \frac{1}{\|q\|^2}\begin{pmatrix} |q\|^2 - 2y^2 - 2z^2 & 2xy - 2wz & 2xz + 2wy \\ 2xy + 2wz & \|q\|^2 - 2z^2 - 2x^2 & 2yz - 2wz \\ 2xz - 2wy & 2yz + 2wz & \|q\|^2 - 2x^2 - 2y^2 \end{pmatrix} \tag{10}$$

Consider the quaternion $q = (w, x\mathbf{i}, y\mathbf{j}, z\mathbf{k})$, where w is a scalar and **i, j, k** are the standard orthonormal basis in R^3, the scalars x, y, z are called the components of the quaternion. Let q to be a unit quaternion or norm, the rotation matrix of the quaternion q is

$$\Gamma(q) = \begin{pmatrix} 1 - 2y^2 - 2z^2 & 2xy - 2wz & 2xz + 2wy \\ 2xy + 2wz & 1 - 2z^2 - 2x^2 & 2yz - 2wz \\ 2xz - 2wy & 2yz + 2wz & 1 - 2x^2 - 2y^2 \end{pmatrix} \tag{11}$$

Equation (11) will be used as a key element for our encryption technique, and will be considered as a public key as well.

4. CONSTRUCTION OF QUATERNION-BASED PUBLIC KEY

This section explains how the above proposed rotation matrix can be used in designing an algorithm for crypto system. Let the quaternion $q = (w, x, y, z)$ be a secret key or private key. The scalar part and components of the quaternion are considered to be any value with variable length as well. The quaternion rotation matrix in Equ.(11) will be used as pubic key for encryption system called Quaternion-based Public Key (QPK). Because the secret key components are of variable length, the QPK will be obscure and will have peculiar features to provide secure ambience for data transmissions.

Suppose that a voice signal A is to be transmitted over a communication channel. It sampled, such as a, b and c samples, and organized to frames of messages, as shown in Fig. 2(b). Each frame of the message is formed as a matrix array M which is

$$M = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ b_{11} & b_{12} & b_{13} \\ c_{11} & c_{12} & c_{13} \end{pmatrix} \tag{12}$$

The message M can be rotated using the rotation matrix $\Gamma(q)$

$$M^{'} = \Gamma(q)M \tag{13}$$

In order to revert the data B again after rotation process, the inverse rotation matrix $\Gamma(q)^{-1}$ is implemented and expressed as

$$M = \Gamma(q)^{-1}M^{'} \tag{14}$$

The quaternion representation, henceforth, provides an intrinsic means for resilient encryption system because the quaternion, as we mentioned above, implies four integrated parameters (keys) independently. These keys might be any function or any random number with a variable size. If any key is implemented incorrectly than the system will fail to disentangle its encrypted signal.

Suppose K_s is a private key which has an arbitrary quadripartite element based on a quaternion q.

$$q = \{w, x, y, z\} \tag{15}$$

As we mentioned above that w, x, y, and z are independent and variable parameters. In order to perform encryption of the data, we introduce a Quaternion Key Order (QKO) which is used as a factor that is implemented in the rotation matrix $\Gamma(q)$ in (11) to produce multiple rotations. This method is used to make the data components like a random pattern. We can generate $m = 3^n$ quaternion keys, where n is the order number. The initial order (for n=0) of quaternion key is identical to the private key and represented as

$$K_s = q_{01} = (w_{01}, x_{01}, y_{01}, z_{01}) \tag{16}$$

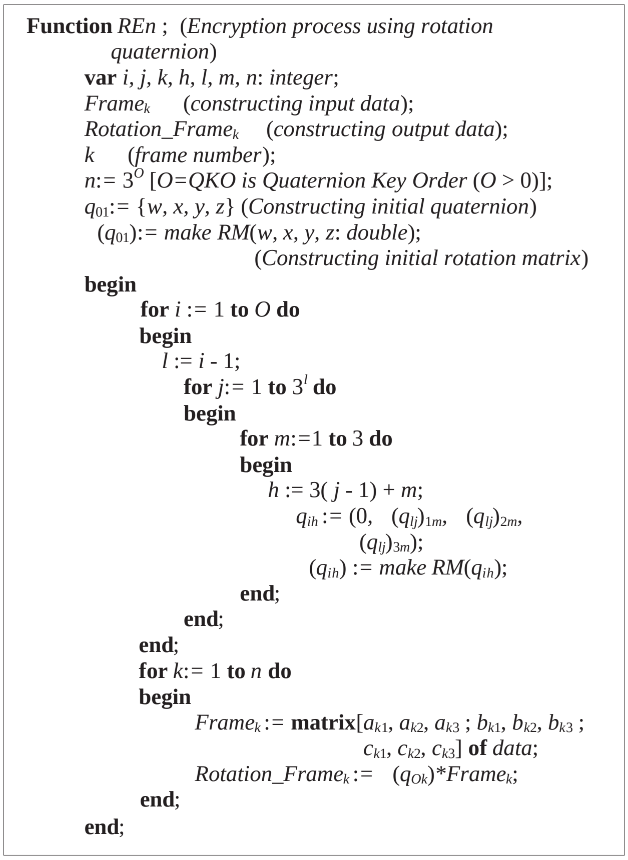
The rotation matrix of this key is identical to that as given in (11). The scalar value w_{01} in (16) is any integer number or sequence. For complexity concern here in this paper we set w_{nm} to zero for order $n \neq 0$. However, it's possible to choose any value to wnm for order $n \neq 0$. Specifically, we set

$$w_{nm} = \begin{cases} \text{Any Value} & n = 0,\ m = 1, 2, 3 \\ 0 & n = 0,\ m = 1, 2, 3 \end{cases} \tag{17}$$

Fig. 1 shows the algorithm of constructing a rotation matrix of order (i, j). As we mention above that the secret key is an initial quaternion key and is arbitrarily defined by a user, it is used to construct an initial rotation matrix, as shown in Fig. 2. Each column in the initial rotation matrix is substituted with x, y and z in the initial quaternion key, respectively, to generate first order new sub-keys q_{11}, q_{12} and q_{13}, respectively, as shown in Fig. 2(a). From the first order keys, new rotation matrices can be generated. The elements of the sub-keys (q_{11}, q_{12} and q_{13}) are vectors and the scalars elements are set to zero. The rotation process is equivalent to formula (11). If we consider a unit quaternion then the sub-keys can be expressed as

$$\begin{aligned} q_{11} &= (w_{11}, x_{11}, y_{11}, z_{11}) && (18) \\ &= (0, w^2 + x^2 - y^2 - z^2, 2(xy + wz), 2(xz - wz)) \\ q_{12} &= (w_{12}, x_{12}, y_{12}, z_{12}) && (19) \\ &= (0, 2(xy - wz), w^2 - x^2 + y^2 - z^2, 2(yz + wx)) \\ q_{13} &= (w_{13}, x_{13}, y_{13}, z_{13}) && (20) \\ &= (0, 2(xy + wz), 2(yz - wx), w^2 - x^2 - y^2 + z^2) \end{aligned}$$

Using the first order sub-keys, it's possible to generate a second order sub-keys such as $(q_{21}, q_{22}, q_{23}, \dots, q_{29})$. Obviously, we can generate myriad sub-keys and in any order such that QKO is 3(q_{3i}) or 4(q_{4i}), where $(i = 1, 2, 3, \dots, 3^3)$ and $(i = 1, 2, 3, \dots, 3^4)$, respectively. If n is the number of order then we can construct $3^n (n = 0, 1, 2, \dots)$ sub-keys. From above concept, creating innumerable sub-keys for encryption data stream strengthens the security of the system. A 3-group of sub-key is used to construct quaternion rotation matrix for the public key (QPK) of our encryption system. Fig. 2(b) illustrates an example of how encryption can be preformed using any signal such as voice or image. The signal is sampled and grouped into frames as shown in Fig.2 (b). Each group or data frame M forms a matrix. By implementing equation (12) and equation (13), the sequences of data frames are encrypted by corresponding quaternion rotation matrices or (QPK) which are constructed using sequences of sub-keys. The decryption of the data is given in equation (14).



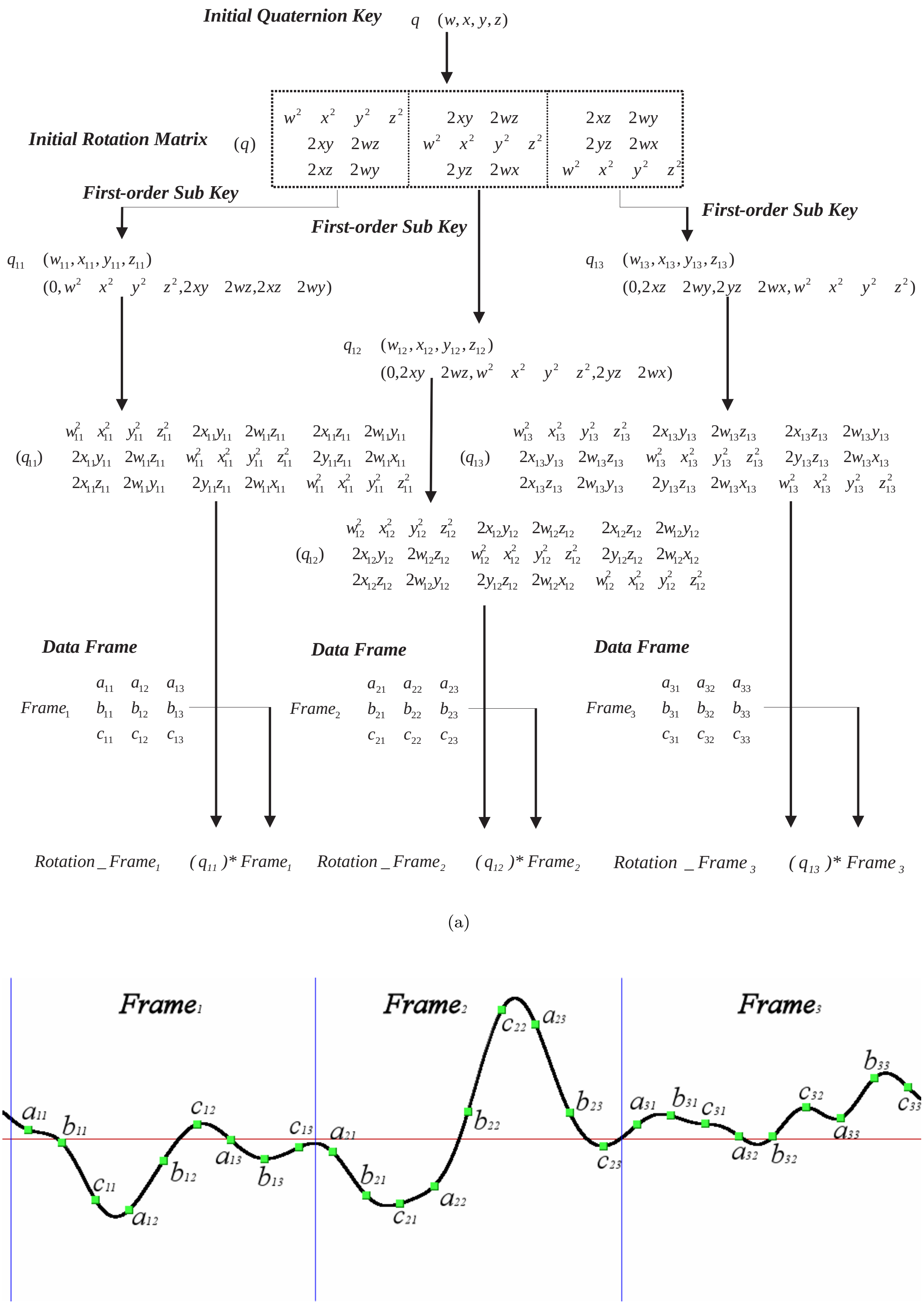
```
Function REn ; (Encryption process using rotation
      quaternion)
   var i, j, k, h, l, m, n: integer;
   Frame_k    (constructing input data);
   Rotation_Frame_k    (constructing output data);
   k    (frame number);
   n:= 3^O [O=QKO is Quaternion Key Order (O > 0)];
   q_01:= {w, x, y, z} (Constructing initial quaternion)
    (q_01):= make RM(w, x, y, z: double);
                 (Constructing initial rotation matrix)
   begin
      for i := 1 to O do
      begin
         l := i - 1;
         for j:= 1 to 3^l do
         begin
            for m:=1 to 3 do
            begin
               h := 3( j - 1) + m;
                  q_ih := (0,  (q_lj)_1m,  (q_lj)_2m,
                            (q_lj)_3m);
                  (q_ih) := make RM(q_ih);
            end;
         end;
      end;
      for k:= 1 to n do
      begin
         Frame_k:= matrix[a_k1, a_k2, a_k3 ; b_k1, b_k2, b_k3 ;
                          c_k1, c_k2, c_k3] of data;
         Rotation_Frame_k:=  (q_Ok)*Frame_k;
      end;
   end;
```

Fig.1: *Quaternion encryption algorithm*

5. SIMULATION AND EFFICIENCY ANALYSIS

In this section, simulation of the encryption technique is implemented and analyzed. A voice signal S, as shown in Fig. 3, has been sampled at sampling rate of 22 KHz and quantized with 16 bits. The message is organized as frames with 3×3 sample array/frame.

Suppose that the signal S is divided into frames, where $S = \{f_1, f_2, \dots, f_n\}$. Each frame f has a



(a)

(b)

Fig.2: *(a) Construction of the rotation matrix. (b) An example of data framing sequences*

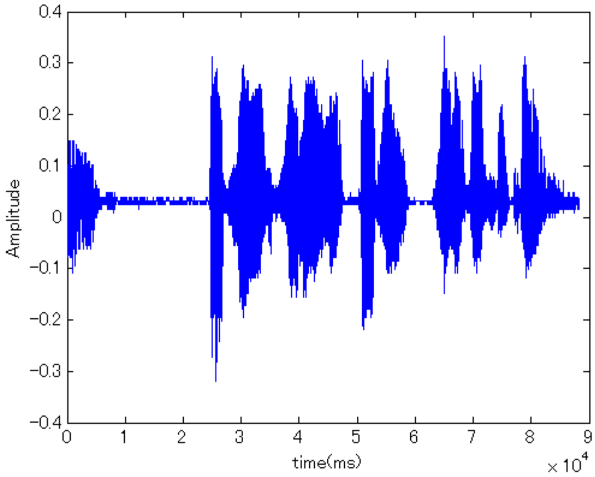


Fig.3: *An example signal*

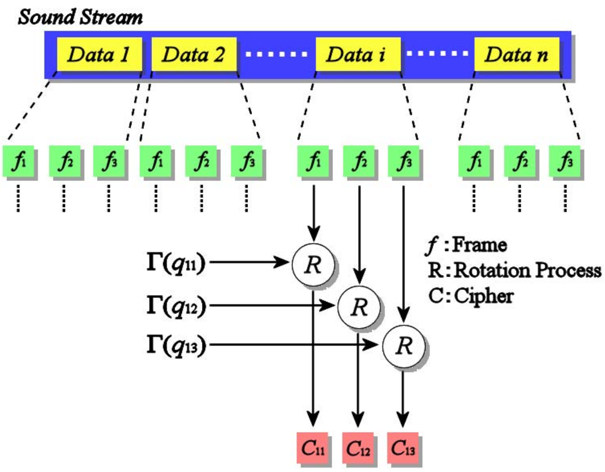


Fig.4: *Encryption processes with $n = 3$.*

set of 3 × 3 array. Suppose also that these elements are formed as 3-D vector space, as shown in Fig. 4. We assume that the number of samples per frame is limited to 3 × 3, and let $f_1 = \{(r_1, s_1, t_1), (r_2, s_2, t_2), (r_3, s_3, t_3)\}$, that is, the signal S can be written as

$$S = \{(r_1, s_1, t_1), (r_2, s_2, t_2), (r_3, s_3, t_3), \ldots, (r_n, s_n, t_n)\} \tag{21}$$

Then the frame f is represented by a triad of 3-vector matrix alignment which is equivalent to the signal data M in (12). In order to perform encryption of the signal, we implement a different Quaternion Key Order (QKO) for every frame in the rotation matrix $\Gamma(q)$ in (11). This method is used to make the signal components look like a random pattern.

Let the initial quaternion key q be an arbitrary value, for example $q = (0, 20, 40, 30)$, and be an initial quaternion key factor used to construct the rotation matrix in order 1, 2, and 3 consecutively.

Fig. 5(a) shows the encrypted signal at initial quaternion key (order = 3). The signal is extremely deformed, however, this signal will be distorted expeditiously when the quaternion order becomes large.

The decryption process is done using (14) and the obtained signal has a perfect shape. Furthermore, the signals obtained and illustrated in Fig. 3 have been examined by taking variance of the signals' power spectrum P which is given by

$$VAR(P) = \sum_{i=1}^{n} \frac{(P_i - E(P))^2}{n} \tag{22}$$

Fig. 6 shows the variance distribution of the signals. When the quaternion order increases, a good performance is achieved in view of security matter and the signal will be strenuous to attack.

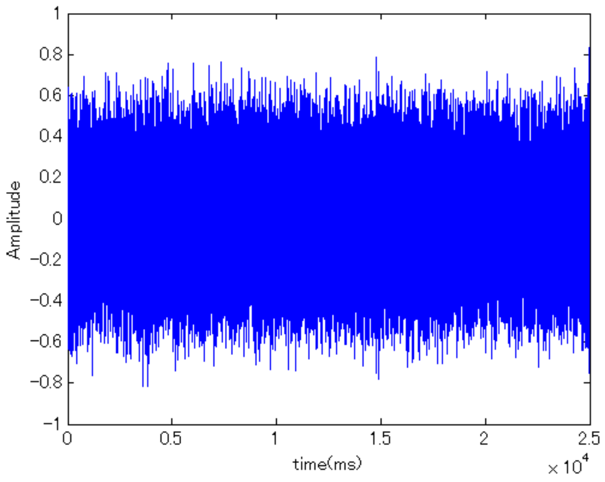


Fig.5: *Encryption process of the Data $S, n = 1$.*

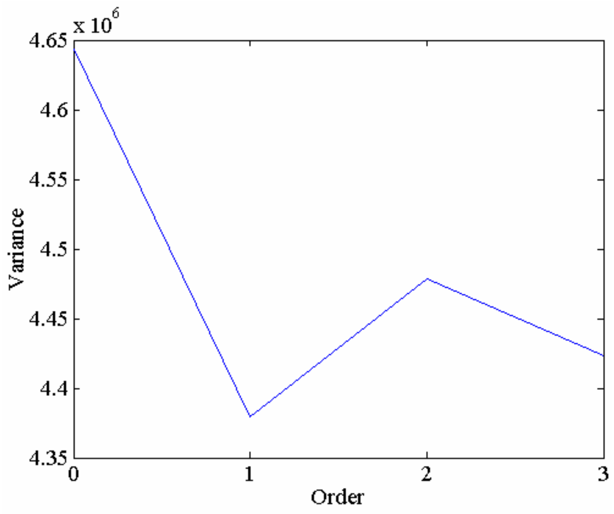


Fig.6: *The variance of the power spectrum*

6. CONCLUSION

We have presented a new concept of *quadripartite public-key* (QPK) cryptography based on a quaternion presentation. Analytical results which have been obtained demonstrate the potential of the proposed QPK scheme. According to the system model, quaternion has four optional keys. Therefore, QPK provides multiple and variable key lengths which are essential factors in determining the highest degree of security and to allowing users to maintain secure data passage over an insecure channel from eavesdroppers' attacks. Henceforth, we can construct ciphers that are effectively impossible to break.

References

[1] William Hamilton, On Quaternions, Proceedings of the Royal Irish Academy, Nov. 11, Vol. 3, pp.1-16, 1847.

[2] Kuipers, J.B., *Quaternions and Rotation Sequences*, Princeton University Press, Princeton, New Jersey 1999.

[3] João Luís Marins et al., *An Extended Kalman Filter for Quaternion-Based Orientation Estimation Using MARG Sensors*, Proceedings of the 2001 IEEE/RSJ, International Conference on Intelligent Robots and Systems, Maui, Hawaii, USA, Oct. 29 - Nov. 03, pp. 2003-2011, 2001.

Tomoyuki Nagase received a Ph.D. in Computer Science from Tohoku University, Japan. He has several years of industrial experience, primarily in Telecommunications. From 2001 to 2002, he was a Visiting Lecturer at California State University, San Diego, USA, where he taught Information theory to graduate students. He is currently Lecturer at Hirosaki University, Japan in the Faculty of Technology. His research interests include communications and Information theory with emphasis on Coding theory, Network security, ATM networks, speard-specturm communications and mobile communication systems. Dr. Nagase is a member of IEEE, Communications society and IEICE society of Japan.

Ryusuke Koide was born in Hokkaido, Japan in 1981. He received his Bachelor's degree in Information Science from Dept. of Electronic and Information System Engineering, Hirosaki University. He is now working toward his Master degree in Information Science from Hirosaki University. His present research interests involve sensors networks, fluxgates sensors and information security.

Takashi Araki received the Ph.D. Science degree in Space Physics from Tohoku University in 1973. From 1993 to 1994, he was invited Professor at New York State University of Albany. Since 1995 has been with the Department of Electronic and Information system engineering, Hirosaki University, Japan, where he is currently a Professor working in the area of Digital signal processing and intelligent sensor system, especially magnetic sensor system. He is a member of the Institute of Electrical Engineers of Japan.

Yoshiei Hasegawa was born in Aomori, Japan. He is currently President and CEO of the Micronics Japan Co., Ltd. (MJC). He led the company to develop peripheral products for the semiconductor industry and first probe cards in 1973 and 1976, respectively. He persuaded the company to develop first LCD Prober in 1985. In 2004, he served as a committee member of International Trade Partners Conference ITPC.