Int. J. Communications, Network and System Sciences, **2010, 3, 579-584**
doi:10.4236/ijcns.2010.37077 Published Online July 2010 (http://www.SciRP.org/journal/ijcns/).

Scientific Research

Hybrid Authentication Cybersystem Based on Discrete Logarithm, Factorization and Array Entanglements

Boris S. Verkhovsky
Computer Science Department, *New Jersey Institute of Technology*, *Newark*, *USA*
E-mail: *verb@njit.edu*
Received July 13, 2009; *revised February* 28, 2010; *accepted May* 10, 2010

Abstract

A hybrid cryptographic system providing digital authentication is described and analyzed in this paper. The proposed cryptosystem incorporates three features: complexity of the discrete logarithm problem, complexity of integer factorization of a product of two large primes and a combination of symmetric and asymmetric keys. In order to make the cryptosystem less vulnerable to cryptanalytic attacks a concept of digital *entanglements* is introduced. As a result, the proposed cryptographic system has four layers (entanglement-encryption-decryption-disentanglement). It is shown that in certain instances the proposed communication cryptocol is many times faster than the RSA cryptosystem. Examples provided in the paper illustrate details of the proposed authentication cryptocol.

Keywords: Crypto-Immunity, Cybersecurity, Digital Authentication, Array Entanglements, Multi-Layer Cryptographic Protection, Hybrid Cryptocol

1. Introduction and Basic Definitions

In this paper a hybrid digital signature cyber-secure communication system is described and analyzed. In order to make this cryptosystem faster and less vulnerable to cryptanalytic attacks a concept of *entanglements* is introduced [1,2]. Furthermore, in this cryptographic protocol there are *four* layers (entanglement-encryption-decryption-disentanglement). Since there is no one-to-one mapping between a plaintext block and the corresponding ciphertext block, this system of communication is less vulnerable to plaintext attacks. The overall cryptographic algorithm is a hybrid protocol that incorporates three features: discrete logarithm problem modulo large prime [3], factorization of a product of two large primes [4] and a combination of symmetric and asymmetric keys.

To describe the proposed cryptosystem, let's consider

A1. An array $m = (a_1, a_2, .., a_r)$ (1)

consisting of r blocks of a digitized plaintext that is to be transmitted from a sender (Alice) to a receiver (Bob);

B1. A square $r \times r$ non-singular matrix E with

$$|E| \neq 0 \quad \text{and} \quad h = Em. \tag{2}$$

$$\text{In the paper} \quad h = (h_1, .., h_r) \tag{3}$$

and E are respectively called a vector and matrix of *entanglements* [1].

C1. A sufficiently strong cryptographic protocol L that is used for encryption of one of the entanglements, for example, h_1, with corresponding ciphertext c_1.

In order to speed up the encryption/decryption procedure and as a result to minimize the entire communication time it is necessary to minimize the amount of computations. For that reason there is no necessity to encrypt all other entanglements $h_{j \neq i}$, where j = 1, 2,.., i – 1, i + 1,.., r and h_i is the encrypted entanglement. Indeed, if h_i is not known to a potential intruder, then he or she must solve a system of r equations, where only r – 1 components of vector h are publicly known. In the cryptosystem described below the size r of the array m is a trade-off between crypto-immunity and acceleration of the decryption: the larger the value of r, the faster the overall communication protocol. On the other hand, the larger r is, the less time is required to cryptanalyze the entire message.

To ***avoid confusions***, it is important to indicate the following distinctions:

- The matrix of entanglement E (and non-linear mappings) discussed below are not secret keys as in an affine cryptographic algorithm; all elements of matrix E are *publicly known*;
- In contrast with the RSA and Rabin algorithms, n_k

is a *private* key of the *k*-th user, not a public key.

2. Digital Signature Scheme

2.1. System Design Module (Users Establish their Private and Public Key):

A2. All users agree on a large prime p and a generator g, where

$$2 \le g \le p-2 \tag{4}$$

***Remark* 1**: selection of a generator for a large prime p is a non-deterministic procedure. However, if both p and $(p-1)/2$ are primes, then

$$g := (3p - 1)/4 \tag{5}$$

is a generator [5].

B2. Each user selects large primes p_k and q_k, such that

$$p_k \equiv q_k \equiv 2 (\mathrm{mod}\, 3), \tag{6}$$

and that their product n_k satisfies two constraints:

$$\alpha p < n_k < p \tag{7}$$

C2. Each user computes her/his public key e_k (encryption key) and private key d_k, where e_k is co-prime with z_k, *i.e.*,

$$\gcd(z_k, e_k) = 1 \tag{8}$$

D2. Every user computes a multiplicative inverse d_k of e_k modulo

$$z_k := (p_k - 1)(q_k - 1) \quad [4]$$

i.e., d_k satisfies the equation

$$d_k e_k \equiv 1 (\mathrm{mod}\, z_k) \tag{9}$$

E2. If Alice and Bob intend to secretly exchange authenticated information, they establish a secret key $w_{AB} := g^{ab} \bmod p$ by using the Diffie-Hellman key exchange [3].

2.2. Encryption/Decryption Module (Alice Sends to Bob a Plaintext Array *m*):

F2. Using an open channel Alice asks Bob to secretly send to her Bob's secret key n_B;

G2. Bob computes $x := n_B w_{AB} \bmod p$ and sends x to Alice;

she recovers $n_B := x w_{AB}^{-1} \bmod p$;

H2. Using the RSA protocol Alice encrypts h_i {see (2)}:

$$c_i := h_i^{e_B} \bmod n_B; \quad [4]; \tag{10}$$

I2. Alice transmits the array $\{h_1, .., h_{i-1}, c_i, h_{i+1}, .., h_r\}$ to Bob;

J2. Bob decrypts c_i:

$$v := c_i^{d_B} \bmod n_B; \ \{=h_i\}; \tag{11}$$

K2. Using $h = (h_1, .., h_r)$ Bob recovers all plaintext blocks $m = (a_1, a_2, .., a_r)$;

L2. If the original array m is intelligible, but the recovered text is not, then Bob realizes that it was forged by an intruder; otherwise Bob accepts authenticity of the text.

2.3. Selection of Block Size and Matrix of Entanglements

To make sure that the entanglements are smaller than every n_i, {otherwise the entire array $m = (a_1, a_2, .., a_r)$ is not recoverable}, select the matrix of entanglement E and such division of a plaintext onto blocks that the maximal value of the i-th entanglement h_i does not exceed αp, (7)}.

Example 1: Let $m := (a, b, c, d, e)$ and

$$h = (h_1, h_2, h_3, h_4, h_5), \tag{12}$$

$$\begin{aligned} \text{where } h_1 &:= d + 2e; h_2 := a - 2b; \\ h_3 &:= 2a - b + c; \\ h_4 &:= c - d + 2e; \\ h_5 &:= a + 2b + c + d. \end{aligned} \tag{13}$$

$$\begin{aligned} \text{Then } b &= h_1 + 3h_3 - (4h_2 + h_4 + 2h_5); \\ a &= h_2 + 2b; \quad c = h_3 - 2a + b; \\ d &= h_5 - a - 2b - c; e = (h_1 - d)/2. \end{aligned} \tag{14}$$

Let's specify that every block in m must satisfy a threshold $a_k < t$.

Then (13) implies that

$$\max h_i = 5t < \alpha p < n_i < p. \tag{15}$$

Therefore, for every $k = 1, \ldots, r$ must hold

$$a_k \le t \le \alpha p / 5;$$

and if $\alpha = 2/3$, then $a_k \le t \le 2p/15$.

From the recovery procedure (14) it is clear that we can compute all initial blocks *a, b, c, d* and *e* **only if** we know all numeric values h_1, h_2, h_3, h_4, h_5 from (13). Henceforth, this fact implies that it is sufficient to encrypt at least one of these entanglements to securely protect all five plaintext blocks.

Furthermore, it is necessary to notice that entanglements themselves do not provide secure protection. In the proposed cryptographic scheme instead of employing just one layer (plaintext/encryption/ciphertext) we propose **two layers** (plaintext/entanglement/encryption/ci-

phertext) between the plaintext array (a, b, c, d, e,…) and ciphertext ($c_1, h_2, h_3, h_4, h_5, \ldots$).

Remark 2: The RSA algorithm discussed below is just an example of how h_i can be encrypted. Any strong cryptocol based on the complexity of factorization of $n = pq$ can also be used. The Rabin algorithm [6] or (hyper) elliptic-curve cryptography [7-10] based on modulo composite n are other possible applications.

2.4. Essence of RSA Digital Signature Algorithm

In order to demonstrate the advantages of the proposed digital signature algorithm, let's recall the RSA digital signature algorithm [4,11]. Suppose Alice wants to send to Bob a message $m = (a_1, a_2, .., a_r)$ with a digital signature. Then for ***every*** k = 1, 2,…, r Alice signs a_k $f_k := a_k^{\,d_A} \mod n_A$ with her private key, then encrypts it with Bob's public key

$$c_k := f_k^{\,e_B} \bmod n_B; \tag{16}$$

and transmits the ciphertext c_k to Bob over an open communication channel. Bob decrypts $x := c^{d_B} \bmod n_B$ and then verifies the signature:

$$y := x^{e_A} \bmod n_A; \quad \{y = m\}; \tag{17}$$

If y is intelligible, then Bob accepts it as an authenticated message from Alice.

3. Examples of Entanglements

3.1. Linear Transformations

Example 2: Let

$$\begin{aligned} &h_0 := a_1 + \cdots + a_{r-1} + a_r;\ h_1 := -a_1 + a_2 + \cdots + a_r; \\ &h_2 := a_1 - a_2 + \cdots + a_r;\ .., h_{r-1} := a_1 + \cdots - a_{r-1} + a_r. \end{aligned} \tag{18}$$

Proposition 1: If all entanglements $h_0, h_1, h_2, .., h_{r-1}$ are known and integer, then for every k = 1,.., r – 1

$$a_k = (h_0 - h_k)/2 \tag{19}$$

$$a_r = h_0 - (a_1 + a_2 + \cdots + a_{r-1}) \tag{20}$$

and all a_k are integers as well.

Proof follows from two observations:

- for every k = 1,.., r – 1 $h_k = h_0 - 2a_k$; (21)
- all $h_0, h_1, h_2, .., h_{r-1}$ have the same parity which implies that their pair-wise differences are *even*. Therefore, every $a_1, a_2, ..$ and a_r is an integer. Q. E. D.

Complexity of recovery: It requires r – 1 subtractions and divisions by 2 (binary shifts) to recover the first r – 1 blocks in (19) and r – 1 subtractions to recover the last block in (20).

If a sender (Alice) encrypts only s of all entanglements, where $0 < s < r$, then the intruder will not be able to deduce any blocks (provided that the matrix E is properly selected and a portion of entanglements is encrypted with a sufficiently strong PKC protocol). In an extreme case, if s = 1, then the intruder must solve a system of equations $Ea = g$, where the matrix E is **known** but only $r - s$ elements of vector g are known. However, this is impossible, because to find the blocks $a_1, a_2, .., a_r$ the intruder must know all r elements of vector g.

3.2. Non-Linear Transformations

In the more general case, the entanglements can be non-linear, *i.e.* $h := E(a)$, and/or some components of the transformation $E(a)$ can be also encrypted. For example, if $h := Ea$, then we can encrypt several elements of matrix E. This approach is beyond the scope of this short paper. It is important to bear in mind that the selection of the transformation $E(a)$ affects the computational complexity of the recovery process.

The choice of the mapping E is important. If E is a matrix, then it must be non-singular and selected in such a way that the recovery will not become a computationally formidable.

Example 3: Let's consider an array of r plaintext blocks $h_1, h_2, .., h_{r-1}, h_r$ and the following r entanglements:

$$\begin{aligned} &h_1 := a_1^2 - a_2^2;\ h_2 := a_2^2 - a_3^2; \cdots \\ &h_{r-1} := a_{r-1}^2 - a_r^2;\ h_r := a_1 + a_r. \end{aligned} \tag{22}$$

It is obviously sufficient to encrypt only one of the entanglements. Then, after the decryption, we proceed as follows:

$$w := h_1 + h_2 + \cdots + h_{r-1} = a_1^2 - a_r^2. \tag{23}$$

Therefore,

$$a_1 = (h_r + w/h_r);\ a_r = (h_r - w/h_r); \tag{24}$$

and for k from 2 to r – 1

$$a_k = \sqrt{a_{k-1}^2 - h_{k-1}}. \tag{25}$$

Combined with encryption these non-linear entanglements provide secure protection and recovery for every transmitted array. Yet, they require divisions of integers and extraction of square roots, which are computationally more complicated procedures.

3.3. Improper Entanglements

Example 4: Let

$$\begin{aligned} &h_1 := 2a_1 + a_2;\ h_2 := a_1 + a_2; \\ &h_3 := a_1 + a_2 + a_3;\ .., h_r := a_1 + a_2 + \cdots + a_r. \end{aligned} \tag{26}$$

If $r > 2$, it is insufficient to encrypt only one of these entanglements.

Indeed, if h_1 is encrypted, then for all $3 \le k \le r$

$$a_k = h_k - h_{k-1}. \quad (27)$$

In general, if i is fixed, $i \ge 2$, and only h_i is encrypted, then

$$a_1 = h_1 - h_2; \quad (28)$$

and for all $3 \le k \le i-1$ and $i+2 \le k \le r$

$$a_k = h_k - h_{k-1}. \quad (29)$$

Therefore, $r - 2$ blocks are cryptographically unprotected in every array.

4. Trade-off Analysis

Every block in (16)-(17) requires *four* exponentiations for encryption and decryption. In contrast, in the protocol A.2-L.2 described above, (4)-(11), the *array* of r blocks requires only one exponentiation for its encryption and decryption. Therefore, the larger the transmitted array r is, the more efficient the speed-up of A.2-L.2 is. If r = 100, then A.2-L.2 is *four hundred* times faster than the RSA algorithm.

Furtermore, if $n_B \le m \le n_A$, then the RSA digital signature algorithm (16)-(17) fails to recover the original plaintext m unless special measures are taken [4,11]. The application of entanglements (linear or non-linear transformations) is a tool that is proposed to accelerate the encryption-decryption process. Although the entanglements themselves do not provide protection, yet, when used in combination with other measures, they decrease the amount of computations necessary for the entire encryption/decryption process.

It is necessary to mention that any detailed and credible *quantification* of the trade-off between the size r of the array and cryptoimmunity requires analysis of all strategies potentially available to the intruder. Yet to *qualitatively* illustrate this point of view, let's consider an asymptotic case, where the size r of the transmitted array of plaintext blocks is very large. From one point of view, the larger r is, the more advantageous the proposed cryptosystem is. Indeed, only one entanglement is encrypted/decrypted instead of all r entanglements as it is done in the RSA, ElGamal, Rabin [6], ECC [7-9] and other PKC cryptosystems [10]. On the other hand, if the size r of the array is very large, then the intruder can invest the required time and computing resources to cryptanalyze the encrypted entanglement.

Let's consider an extreme case, where the entire message M consists of N blocks. Let's select a square nonsingular $N \times N$ matrix E, compute N entanglements $h_1, h_2, .., h_N$ using (18) and encrypt only one of them, say, h_1. For instance, if the sender transmits information regarding highly-sensitive issues of long-term national policy or the details of a major corporate policy, the intruder will invest all available resources to break the encrypted entanglement h_1 [12-18]. Therefore, for security purposes, it is safer to divide the entire file M onto several parts/arrays and securely protect each array.

5. Decryption: Reduction of Complexity

The most serious computational bottleneck of the present public-key cryptographic protocols is that they are notoriously slow and therefore cannot be used in the real-time exchange of sensitive information.

Although we are far away from completely eliminating this bottleneck, the proposed cryptosystem is a systemic tool that accelerates secure communication via open channels of the Internet or within corporate networks.

Eliminating the bottleneck mentioned above is one of major research areas today and will likely occupy hundreds of communication specialists and system designers for years ahead. Various PKC algorithms were introduced in the last thirty years. Elliptic-curve cryptography and its hyper-elliptic extension are vivid examples of this research: to accelerate the encryption/decryption process. The proposed cryptosystem is another illustration of how we can accelerate the PKC protocols if the entangled arrays rather than individual blocks are encrypted.

6. Illustrative Numeric Example

The steps A4-H4 describe a system *design* stage and the steps I4-L4 describe its implementation for signed encryption and authenticated decryption of arrays

$$m = (a_1, .., a_r):$$

A4. Let Alice and Bob select p = 1907, a generator g = 1430, (5), and $\alpha = 2/3$, (13-15);

B4. Let each Alice and Bob select two pairs of primes: $\{p_A, q_A\} = \{29, 47\}$ and $\{p_B, q_B\} = \{17, 89\}$ where

$$p_A \equiv q_A \equiv p_B \equiv q_B \equiv 2 (\text{mod } 3), \quad (30)$$

and compute their products [1]:

$$n_A := p_A q_A = 1363 \text{ and } n_B := p_B q_B = 1513; \quad (31)$$

then $\{p_A, q_A, n_A\}$ is a triad of Alice's *private* keys and $\{p_B, q_B, n_B\}$ is a triad of Bob's *private* keys;

C4. {Establishment of a secret key w}: w must satisfy the inequality $w < \alpha p$; Alice and Bob randomly select secret integers a = 7 and b = 10 respectively and compute $u := g^a \text{ mod } p = 1601$;

and $y := g^b \text{ mod } p = 1733$;

D4: Alice transmits u to Bob, who transmits y to Alice;

E4. Alice and Bob compute respectively

$$w_A := y^a \bmod p \quad \text{and} \quad w_B := u^b \bmod p. \tag{32}$$

As a result,

$$w_{AB} = w_A = w_B = g^{ab} \bmod p = 1118 \tag{33}$$

is their secret key;

F4. Alice and Bob compute a multiplicative inverse w_{AB}^{-1} of their secret key $w_{AB} : w_{AB}^{-1} = 1281$ [11];

G4. {Alice requests Bob to send his private key n_B to her}:

Bob computes *v* and sends it to Alice:

$$v := n_B w_{AB} \bmod p = 25;$$

H4. Alice recovers Bob's private key:

$$n_B = v w_{AB}^{-1} \bmod 1907 = 1513;$$

I4. Suppose that Alice and Bob select their public keys $e_A = e_B = 3$.

Consequently, $d_A e_A \bmod z_A = 1$;

and $d_B e_B \bmod z_B = 1$;

imply that $d_A = 909$; and $d_B = 1009$.

J4. Suppose Alice intends to transmit to Bob over the Internet an encrypted array

$$m := \{324, 241, 332, 108, 412\}$$

with her digital signature.

If she selects the entanglements (13), then

$$h = \{1234, 500, 568, 1350, 1588\}.$$

If $\alpha = 2/3$, then h_1 satisfies the requirement (15);

K4. Alice encrypts h_1:

$$c_1 := h_1^{e_B} \bmod n_B = 1476,$$

and transmits $(c_1, h_2, h_3, h_4, h_5)$ to Bob;

L4. Bob decrypts the ciphertext c_1:

$$x := c_1^{d_B} \bmod n_B = 1234 \ \{= h_1\};$$

M4. Using (14), Bob recovers $h = (h_1, .., h_5)$. Because nobody except Bob knows his private key n_B, only he can recover the correct values of all plaintext blocks. If the recovered message is intelligible, Bob accepts it as the authentic message from Alice.

Preliminary results of this paper are published in [19].

7. Conclusions

This paper describes a novel concept for the PKC that employs a combination of DLP, factorization and entanglements, which facilitates otherwise computationally difficult problem [12,14,19].

Let's summarize the most important issues that were described and briefly discussed in this paper:

A: In contrast with RSA, n_k is a private key of the *k*-th user, not the public key [19];

B: In another contrast, the encryption/decryption is applied not to every block of the plaintext, but to every *array* of blocks; in other words, the ***unit of protection*** is not a block, but an array of several blocks [20];

C: Within each array prior to encryption all blocks are entangled [1];

D: The advantage of entanglements is that they are interdependent; the disadvantage is that if one entanglement is corrupted, it affects the entire array. Namely, that array cannot be recovered by the receiver [2];

E: If the information is transmitted in an aggressive media and subject to networking failures or errors, the proposed cryptosystem cannot be used unless additional measures of information assurance are applied (see [21,22]).

F: As a by-product of interdependence, there is no necessity to encrypt and decrypt each block or each entanglement. Instead it is sufficient to encrypt only one of *r* entanglements [23]. This is the first advantage of the proposed protocol.

G: The application of cryptography based on a cubic-root provides the second advantage. The encryption requires only two multiplications [1];

H: The overhead of the entanglements is on the stage of information recovery: it is necessary to solve a system of *r* equations with *r* unknowns. Yet, there are many ways how to select matrix *E* that will make these computations easier. Several linear and non-linear examples of entanglements are provided above for illustration. Additional examples of entanglements are described in [20]. The proposed cryptosystem also provides a digital signature protocol.

8. Acknowledgements

The author would like to express his appreciation to I. V. Semushin for assistance and to P. Fay for comments that improved the style of this paper.

9. References

[1] B. Verkhovsky, "Entanglements of Plaintext Streams and Cubic Roots of Integers for Network Security," *Advances in Decision Technology and Intelligent Information Systems*, Vol. IX, 2008, pp. 90-93.

[2] B. Verkhovsky, "Information Assurance Protocols: Efficiency Analysis and Implementation for Secure Communication," *Journal of Information Assurance and Security*, Vol. 3, No. 4, 2008, pp. 263-269.

[3] W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, Vol. IT-22, No. 6, 1976, pp. 644-654.

[4] 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.

[5] B. Verkhovsky, "Deterministic Algorithm for Generators of Strong Primes," CS-06 Research Report, NJIT, 2006.

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

[7] V. S. Miller, "Use of Elliptic Curves in Cryptography," *Lecture Notes in Computer Science*, Vol. 218, No. 85, 1985, pp. 417-426.

[8] N. Koblitz, "Elliptic Curve Cryptosystems," *Mathematics of Computation*, Vol. 48, No. 177, 1987, pp. 203-209.

[9] N. Koblitz, A. Menezes and S. Vanstone, "The State of Elliptic Curve Cryptography," *Designs*, *Codes and Cryptography*, Vol. 19, No. 2-3, 2000, pp. 173-193.

[10] N. Koblitz, "Hyperelliptic Cryptosystems," *Journal of Cryptology*, Vol. 1, No. 3, 1989, pp. 139-150.

[11] B. Verkhovsky, "Overpass-Crossing Scheme for Digital Signature," *International Conference on Systems Research*, *Informatics and Cybernetics*, Baden-Baden, Germany, July 29-31, 2001.

[12] J. M. Pollard, "Monte Carlo Methods for Index Computation Mod P," *Mathematics of Computation*, Vol. 32, No. 143, 1978, pp. 918-924.

[13] V. I. Nechaev, "Complexity of a Deterministic Algorithm for the Discrete Logarithm," *Mathematical Notes*, Vol. 55, No. 2, 1994, pp. 165-172.

[14] A. M. Odlyzko, "Discrete Logarithms: The Past and the Future," *Designs*, *Codes and Cryptography*, Vol. 19, No. 2-3, 2000, pp. 129-145.

[15] J. M. Pollard, "Kangaroos, Monopoly and Discrete Logarithms," *Journal of Cryptology*, Vol. 13, No. 4, 2000, pp. 437-447.

[16] D. R. Stinson, "Some Baby-Step Giant-Step Algorithms for the Low Hamming Weight Discrete Logarithm Problem," *Mathematics of Computation*, Vol. 71, No. 237, 2002, pp. 379-391.

[17] M. Chateauneuf, A. Ling and D. R. Stinson, "Slope Packings and Coverings, and Generic Algorithms for the Discrete Logarithm Problem," *Journal of Combinatorial Designs*, Vol. 11, No. 1, 2003, pp. 36-50.

[18] J. Coron, D. Lefranc and G. Poupard, "A New Baby-Step Giant-Step Algorithm and Some Applications to Cryptanalysis," *Lecture Notes in Computer Science*, Vol. 3659, 2005, pp. 47-60.

[19] B. Verkhovsky, "Fast Digital Signature Hybrid Algorithm Based on Discrete Logarithm, Entanglements of Plaintext Arrays and Factorization," *7th International Conference Mathematics Modeling in Physics*, *Technology*, *Socio-Economic Systems and Processes*, Ulyanovsk, Russia, 2009, pp. 13-16.

[20] B. Verkhovsky, "Information Assurance and Secure Streaming Algorithms Based on Cubic Roots of Integers," *In the Fifth International Conference on Information Technology*: *New Generations* (*ITNG*-08), Las Vegas, USA, 2008, pp. 910-916.

[21] B. Verkhovsky, "Control Protocols Providing Information Assurance in Telecommunication Networks," *Journal of Telecommunications Management*, Vol. 2, No. 1, 2009, pp. 59-68.

[22] 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.

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

