Network Security via biometric recognition of patterns of gene expression

Harry C Shaw
Telecommunication Networks & Technology Branch
NASA/Goddard Space Flight Center
Greenbelt, MD
Harry.c.shaw@nasa.gov

***Abstract*— Molecular biology provides the ability to implement forms of information and network security completely outside the bounds of legacy security protocols and algorithms. This paper addresses an approach which instantiates the power of gene expression for security. Molecular biology provides a rich source of gene expression and regulation mechanisms, which can be adopted to use in the information and electronic communication domains. Conventional security protocols are becoming increasingly vulnerable due to more intensive, highly capable attacks on the underlying mathematics of cryptography. Security protocols are being undermined by social engineering and substandard implementations by IT organizations. Molecular biology can provide countermeasures to these weak points with the current security approaches. Future advances in instruments for analyzing assays will also enable this protocol to advance from one of cryptographic algorithms to an integrated system of cryptographic algorithms and real-time assays of gene expression products.**

Keywords—network security; gene expression; transcription factors; translation;

I. INTRODUCTION

Network security is a vital component of the design of any network. There are five main requirements to be addressed in developing a secure network: Authentication, confidentiality, data integrity, non-repudiation, and access control. *In vivo*, biomolecular cellular systems of gene expression authenticate themselves through various means such as transcription factors and promoter sequences. These factors also enforce access control. They have means of retaining confidentiality of the meaning of genome sequences through processes such as control of protein expression. They are capable of establishing data integrity and non-repudiation through transcriptional and translational controls.

A suite of genomics and proteomics based authentication and confidentiality protocols are being developed to augment traditional network security approaches with concepts from molecular biology via the regulation of gene expression. These protocols are agnostic to their implementation and can be incorporated into any existing network security protocol (Secure http, SSL, TLS, IPSec, etc.) or any future network security strategy. The protocols can be implemented for implementing web-based security strategies, digital signatures, digital rights management, and general purpose encryption for data in motion or data at rest.

Initial implementations will utilize the cryptographic algorithms described below. Future implementations will take advantage of the ability to access patterns of gene expression *in vivo*. Knowledge of gene expression products (proteins and non-coding RNA) can be achieved without time consuming sequence assays. It can be done via techniques such as fluorescent labeling. In fact the use of fluorescence is one method of implementing a protein expression security protocol.

These protocols will provide new challenges for network attackers by forcing them to work in both the information security domain and the molecular biology domain. Although no security strategy is without vulnerabilities, the intent of this work is to present a completely new set of problems for network attackers which will result in higher network and information security.

II. IMPLEMENTATION OF A MOLECULAR BIOLOGICALLY BASED SECURITY PROTOCOL

Implementation of this approach utilizes the following concepts:

- A network security concept of operations based upon the processes of gene expression.
- A methodology for taking the processes of gene expression and converting them into cryptographic protocols (ciphergenes become analogs for biological genes, cipherproteins become analogs for biological proteins)
- Specific coding models for the cryptographic protocols
- Cryptographically hard sources for the patterns of gene expression called ciphercolonies. (ciphercolonies become analogs for colonies of living organisms but can also contain algorithms substituting for living organisms)
- Ultimate merging of security protocols with *in vivo* and *in vitro* realizations of ciphercolonies. Networks of ciphercolonies capable of signaling and responding to patterns of gene expression within a network and authenticating members of the network.

Security is based upon the translation of plaintext messages to and from a computationally large set of genomic and proteomic messages. Instead of relying solely on the four nucleotides and 20 amino acids as a code base, messages are generated from genomic and proteomic sequences that include the informational representation of the regulatory elements of transcription and translational networks. A single sequence can generate many messages depending upon the transcription and translation instructions. Modules can be developed and implemented in large or small systems, firewalls, routers, switches and other devices. Ultimately, the goal is a network of biologically enabled nodes and Certificate Authorities who can establish trust via evolving patterns of gene expression. Like any security protocol, the most efficient implementation requires accommodating its features early in the design phase. To accomplish that goal, designers must understand the key concepts and future IT security departments will require molecular biologists and biochemists on their staffs.

A. Gene Expression Nomenclature

Fig.1 summarizes the gene expression process using the β-globin gene [1]. The processes of transcription and translation are coded into the protocol. Each transcript (DNA, RNA, protein) has specific regions. Each region is assigned a Type and that Type is coded using the Method of Types from information theory [2]. The codes interact with each other and with codes for the molecular structures required for gene expression. This is done using defined probabilities for the intersections of the codes for each Type. This allows processes such as proteins-nucleotide and protein-protein binding to be represented as the intersection of their Types.

Even if an attacker knows, for example, that the β-globin gene has been used as a basis for creating a cryptographic code, the attacker would have to know the specific location, implementation and function of the control regions, and the gene expression products to attack a coded message. Even the process of finding the start codon in a gene is not trivial, thus finding a message encoded in exons without any further information is computationally difficult.

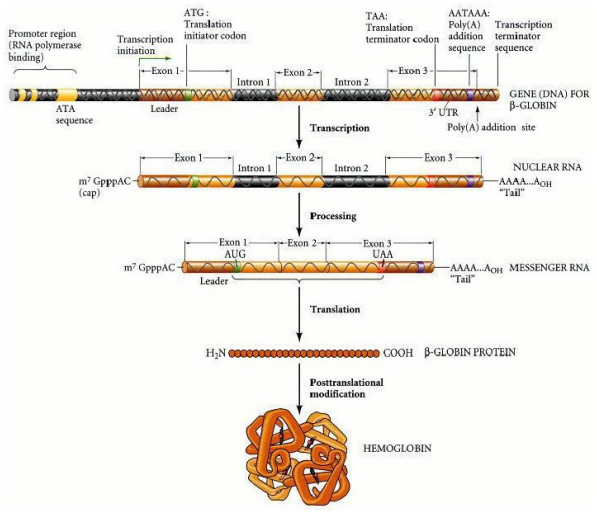

Fig. 1. Nomenclature for gene transcription and translation using β-globin as an example.

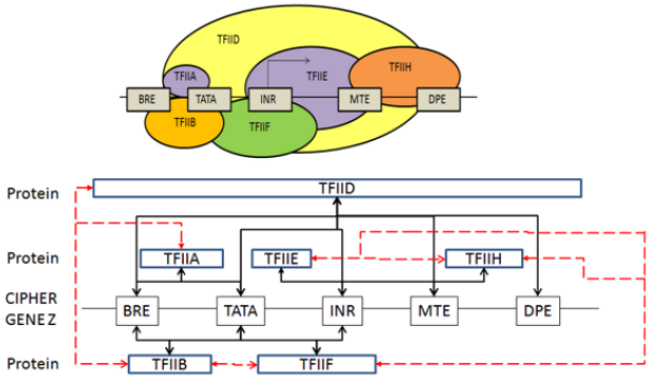

Fig. 2. Coding the transcriptional complex

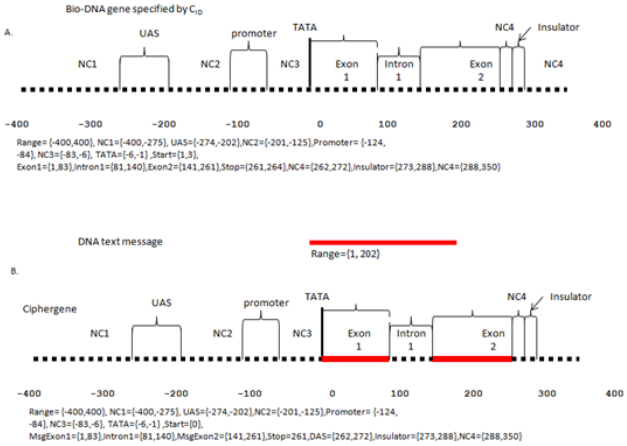

Fig. 3. Biological gene structure with a pre-coding substitution of a DNA text message into the exon regions

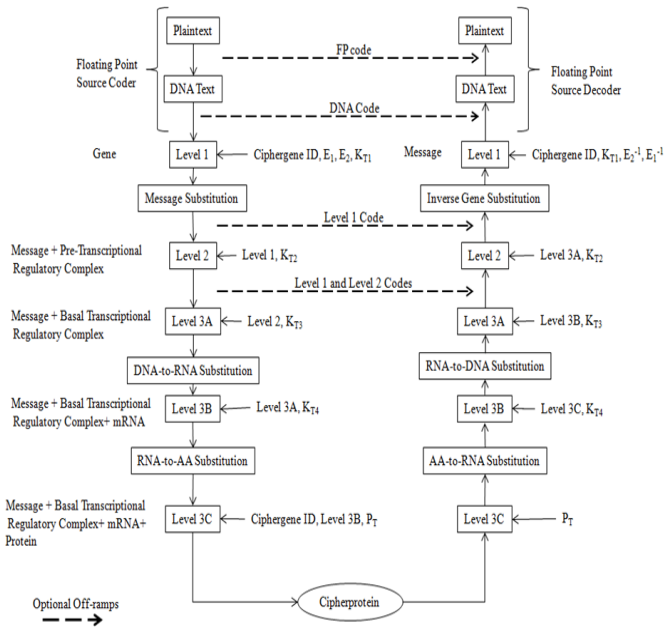

Fig. 4 Genomic Proteomic Protocol Overview

The power of the Method of Types is that it allows for certain amount of statistical variability in the interaction of the codes which mimics the variability of cellular interactions. Fig.2 provides an example of the interpretation of binding of the general transcription factor proteins to a gene undergoing transcription. In fig.2 all of the transcription factor proteins must bind to the correct gene regulatory sequences and other transcription factor proteins to permit RNA Polymerase II to bind to the entire complex and perform transcription. From a coding perspective, all of the codes for these factors have a defined probabilities of code intersection that signal successful authentication and permit subsequent operations to occur.

B. Design of the Genomic and Proteomic Protocol suite

A suite of implementations have been created to date include a one-way DNA authentication protocol, a keyed HMAC DNA authentication protocol and the genomics and proteomics cryptographic suite. The genomics and proteomics cryptographic suite begins with a plaintext substitution into selected gene motifs, followed by a floating point source coding algorithm and multiple rounds of coding on to representations of DNA-to-RNA transcription using the Type codes for the general transcription factors and RNA-to-proteins and with the Type codes for the translation regulatory factors.

Initially, a precoding step converts the plaintext input into an alphabetic string from the set of DNA bases A_D = *{A,T,C,G,MeC,H,X}*. *A, G, C,* and *T* represent the main DNA bases adenine, guanine, cytosine, and thymine. *MeC* represents 5-Methylcytosine, an epigenetic marker, *H* represents hypoxanthine, and *X* represents xanthine. *H* and *X* are mutagenic deaminations of DNA bases that occasionally occur in gene sequences. Then the protocol provides for the following steps.

- A level 1 process by which DNA text is mapped into the structure of a gene complete with introns, exons, regulatory regions, etc., to create a ciphergene. The purpose of this coding from a security perspective is that a single sequence of letters from a small alphabet can be used to represent a large set of permutations of message combinations. The decoding of such messages represents an *np*-hard problem for attackers. Fig. 3 provides a simple example of how the encoding process begins. In a real application the message could be spread across the control regions and different messages could be encoded simultaneously across different regions.
- A level 2 process by which ciphergene code is then operated on by a series of protein transcription factor codes that combine with their counterpart regulatory codes on the ciphergene to produce a new coded sequence that represents a coded transcriptional complex.
- A level 3 process is a series of operations that takes the coded transcriptional complex, which is operated on by protein and RNA polymerase codes resulting in a basal transcriptional complex code. The basal transcriptional complex code is processed by algorithms and maps the code into a messenger RNA code, called the cipher-mRNA code. The cipher-mRNA now consists only of codons of the original DNA text message and is translated into a protein code, called the cipherprotein.

The output of level 3 is the cipherprotein code that is transmitted from the sender to the receiver. The receiver applies the decryption keys to recover the cipher-mRNA and then perform all subsequent steps to reach level 2, level 1, and decoding to produce the plaintext. The process is summarized in fig. 4.

The protocol uses a series of encryption and decryption matrices, E_1, E^{-1}, E_2, E^{-2}, a series of encryption keys derived from pre-shared secret genomic sequences (K_{T1}, K_{T2}, K_{T3}, P_T), and additional tools from information theory to accomplish coding, encrypting, decoding and decrypting the successive levels of data [3]

III. ESTABLISHING AND UTILIZING PATTERNS OF GENE EXPRESSION

A. Utilization of gene expression pathways

A pattern of gene expression is created by an organism going through the processes of DNA transcription and RNA translation across the many genes within the genome. Genes are always expressed within the context of overall cellular requirements. Thus, genes are expressed in response to stimuli indicating a need for expression. Not all genes are expressed all the time.

Eukaryotic organisms (yeast, plants, animals, etc.) have more complex mechanisms and options for regulating gene expression than prokaryotes (bacteria). However, both prokaryotic and eukaryotic processes can be used in these protocols. Each pathway of gene expression contributes to an overall pattern of gene expression. These patterns of gene expression can be represented as sets of random variables that vary with time. The interaction between the patterns of gene expression by different organisms and colonies of organisms can also be represented as sets of random variables. Thus, they can be modeled using probabilistic and stochastic processes. The more complex the organism, the greater the diversity of the pattern of gene expression which will contribute to diffusion and confusion of the codes generated by the protocols. Mutation processes increase the security provided these protocols.

B. Implementation of the protocols in living systems.

These protocols are designed for eventual implementation in cellular organisms and colonies, when the technology is ready. By keeping the coding rules consistent with mechanics of gene expression, it is expected that there will eventually be instruments that read the cryptographic instructions and produce gene expression products *in vivo*. Networks will interface with each other over time, such that, as a minimum a level of phenotypic recognition can be established between networks. Mutation and variation play an important role in the security aspects. A Man-In-The-Middle attacker that has not been in constant contact with the colonies will be unable to match the patterns of gene expression that have evolved over time between 2 or more networks that recognize each other.

NASA/GSFC Space Network Project.

This leads to self-authenticating network interactions as shown in fig. 5.

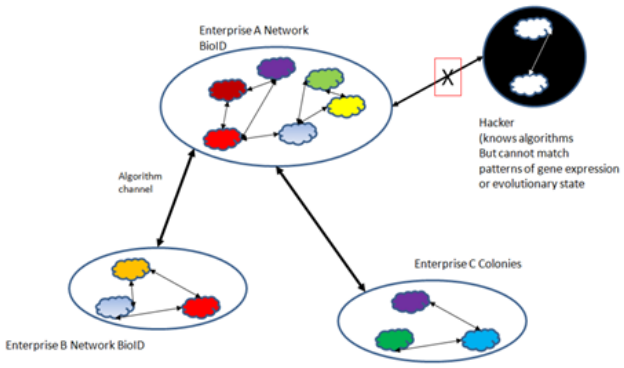

Fig. 5. Network Concept of Operations using regulation of gene expression

Networks would have appliance, called a Network BioID. Enterprises will maintain Network BioIDs that communicate with each other via communication channels (the algorithm channel). The ciphercolonies are regularly sampled to measure their patterns of gene expression and receive external stimuli to modify those patterns of expression. Patterns of gene expression occur with the expression of multiple genes which interact with each other. Gene A, produces protein A, which effects the expression of gene B, which produces protein B, etc. This creates a series of gene regulatory networks. In vivo, these regulatory networks appear in close proximity to each other, within the same cell, or colony of cells through a process of cellular signaling. In a computer network, that proximity need not be a physical proximity, but a communications channel. In vivo, the genes all exist in a physical sense within the nucleus or cellular compartment housing the DNA. In a computer network, some genes can exist in a virtual sense and these genes can communicate with the physical ones via a signaling process which alters the patterns of expression in both algorithmic and live participants.

Security rests upon maintaining continual knowledge of the state of gene expression of the underlying colonies and their interactions. For an initial implementation, it is possible to monitor and record patterns of gene expression in a laboratory over a long baseline period of time, (e.g. 1 year) and use that recorded data in place of real-time knowledge of patterns of gene expression. Additional data would be collected in parallel with consuming the recorded data is being consumed, while maintain a one year reserve of gene expression data.

C. *Incorporation into legacy networks*

A new concept such as the ones proposed in this research will not be accepted unless it can be interfaced into legacy, non-bio capable networks. In fig. 6. Alice and Bob are shown using genomic and proteomic authentication in conjunction with IPsec. In this case Alice and Bob have Network BioIDs incorporating algorithmic and live sources of gene expression and a verification method using fluorescence pattern matching when gene expression is forced by appropriate stimuli

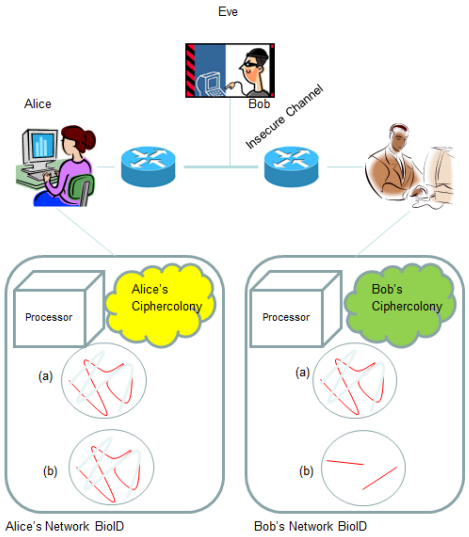

Fig. 6. Combined legacy and genomic protocol security

Alice and Bob can perform IPsec using nonces and keys derived from patterns of gene expression in their ciphercolonies unknown to them and to Eve. Alice and Bob can perform authentication via messages directing the receiver to force expression of gene(s) which can be detected optically via fluorescence, successfully as in case (a), or unsuccessfully as in case (b). Alice and Bob can send genomically or proteomically encrypted messages that cannot be decrypted without knowledge of the patterns of gene expression used as the basis of encryption. Every network node can be equipped with a Network BioID. Eve will need a background in molecular biology and cryptography as well as lab resources to attack this protocol. Coded patterns of fluorescence detection of gene expression can be formed and utilized with current technology. This type of security will require organizations to take on functions and capabilities very different from those currently used in IT departments

D. *Proteomic Authentication Messages*

An IT security official receives a remote request for access to network assets from a remote user. The security official sends the user a message coded as a protein sequence, by a regulatory network using a message-specific set of protein-DNA Type codes and a source coding scheme based upon a keyed hash function tied to a specific genome. The user successfully decrypts the message and returns the plaintext (which could be encrypted if desired) to the IT security official. The IT security official then sends a set of access credentials encrypted with a different protein and a different genome for the keyed hash code. The user successfully decrypts the message to gain access to the network. In this scheme, an attacker needs multiple levels of information at the genomic and proteomic levels to be able to decode the message by cryptanalysis means alone. The process is summarized in fig. 7.

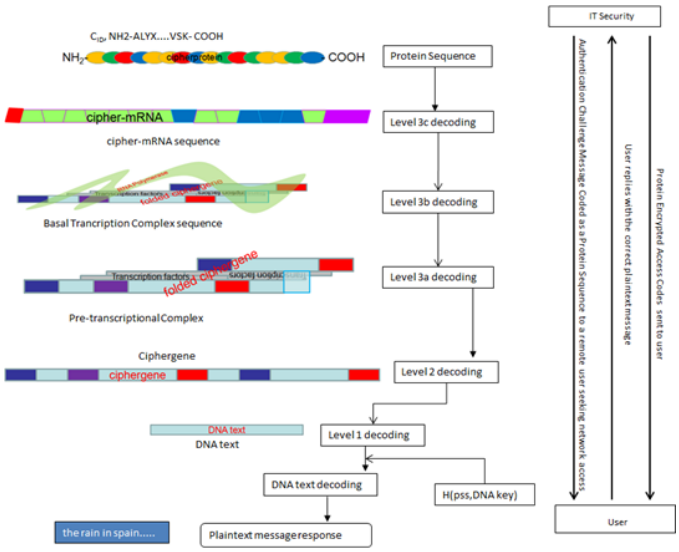

Fig. 7. Protein Coded Authentication Challenge

E. *Modulating patterns of gene expression for security*

Referring to fig. 8, let each bar represent the level of expression a group of related genes. Users A and B are passing state of expression information back and forth, but the patterns become periodic and predictable. The height of the bars corresponds to quantities of gene product expression. Note that they form a repeating pattern, in which the gene expression in the 4th time interval is the same as in the 1st time interval. In addition, assume that this pattern continues to repeat every 4th time interval. An attacker could easily discern this pattern and use it to impersonate either A, B or both. Much like a random number generator that produces the same random number sequence when provided with the same seed, this form of the concept provides no additional security.

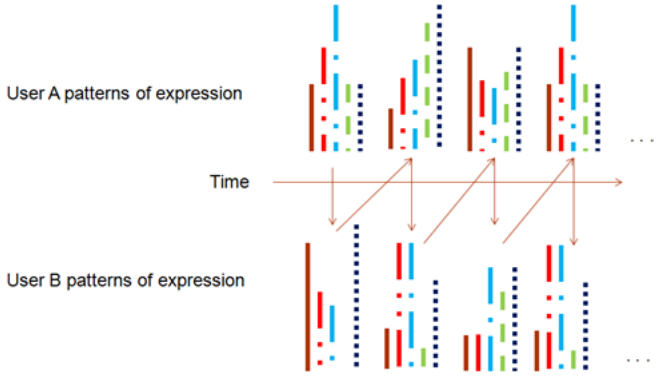

Fig. 8. Non secure ciphercolony implementation

In a secure implementation, such as fig. 9, the ciphercolonies have a heterogeneous colony of eukaryotes and prokaryotes and the patterns of gene expression are constantly being modulated by external stimuli. This creates opportunities for new groups of genes to be expressed. The patterns do not repeat as evidenced by the new patterns and the height of the bars. The stimuli can be applied independently of each other or one user can inform another user that they are becoming repetitious and either alter their behavior or be removed from the network.

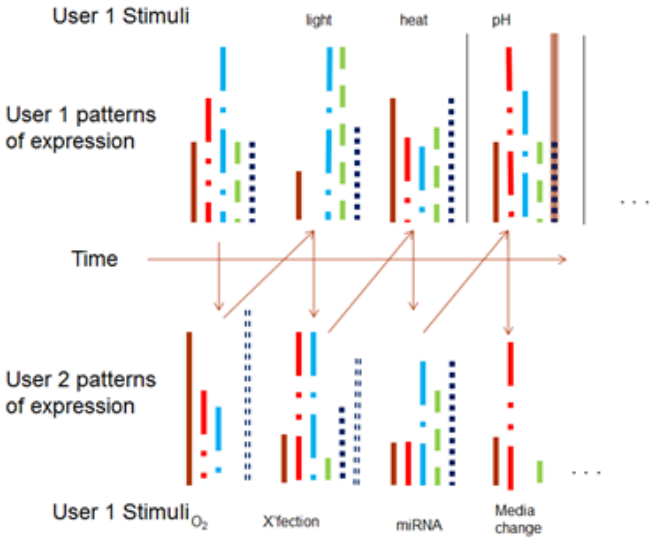

Fig. 9. Secure Ciphercolony implementation

IV. Aspects of Practical Implementation

A. *Technologies for integrating the protocols with laboratory analysis of gene expression*

The US Patent that has been secured on the technology is forward looking and assumes that full implementation will involve future technological advancements that will enhance the implementation concepts in the form of laboratory-on-a-chip devices [4]. The goal of real-time, lab-on-a-chip assays for gene expression has already been realized [5]. It is also currently possible to use techniques such as dielectrophoretic separation of assay products to create signatures of gene expression which can be used to create cryptographic codes with the genomic and proteomic protocols and low-cost devices such as the one shown in fig. 10 [6].

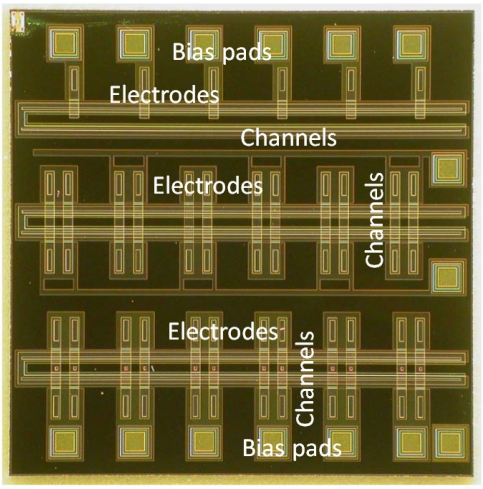

Fig. 10. Dielectrophoretic Separation Test MEMS

B. *Example of implementing protocols into a Public Key Infrastructure using a Bio-Certificate Authority*

Fig. 11 demonstrates a concept of operations for implementing the protocols within a legacy-style PKI system. The purple boxes on each slide refer to blocks in the BioID ciphercolony which may or may not be local to the user computer performing encryption. The ciphergene ID (CID) is essentially an index that points to the name of gene whose sequence, transcription, and translation features are used in the encryption process. The DNA text message is embedded into the gene sequence by the source coding protocol previously described. A given message can be encoded differently by inserting it into different genes.

The level 1 process is as follows: The Sender encrypts the CID with a Bio-CA generated public key and transmits the encrypted CID to a remote Bio-CA. The Bio-CA decrypts the CID with its private key and retrieves a Gene Sequence Key Encryption Key (GSK) for the message associated with the CID. The Bio-CA encrypts the GSK with the Sender's public key and transmits the GSK to the Sender. The Sender decrypts the GSK with its private key and retrieves the locus control region key (Bio-LCR) from the BioID ciphercolony database. The Bio-LCR is decrypted with the GSK. The DNA text is encrypted with the Bio-LCR, converting the DNA text to a ciphergene. The CID is encrypted with the public key of the sender and concatenated with the ciphergene. This completes Level 1 encryption. The ciphertext message can be sent to the receiver or sent to level 2 for further processing.

REFERENCES

[1] S.F. Gilbert, Developmental Biology. 6th edition, Differential Gene Transcription, Sunderland (MA), Sinauer Associates, 2000.

[2] T. M. Cover and J. A. Thomas, , Elements of Information Theory 2nd Ed., pp,103-347, 2006, Wiley Interscience, Hoboken, NJ

[3] Genomics and Proteomics Based Security Protocols for Secure Network Architectures, Shaw, Harry Cornel, Doctoral Dissertation, The George Washington University, 2013

[4] H. Shaw, "Integrated Genomic And Proteomic Security Protocol," U.S. Patent: 8,898,479, issued date November 25, 2014.

[5] King, Kevin R. and Wang, Sihong and Irimia, Daniel and Jayaraman, Arul and Toner, Mehmet and Yarmush, Martin L., "A high-throughput microfluidic real-time gene expression living cell array", The Royal Society of Chemistry,Lab Chip, Vol. 7, Issue 1, pp. 77-85, 2007

[6] H. C. Shaw, "Design And Simulation of a Mems Structure for Electrophoretic and Dielectrophoretic Separation of Particles by Contactless Electrodes," M.S. thesis, Electrical and Computer Engineering, George Washington Univ., Washington, DC, 2005

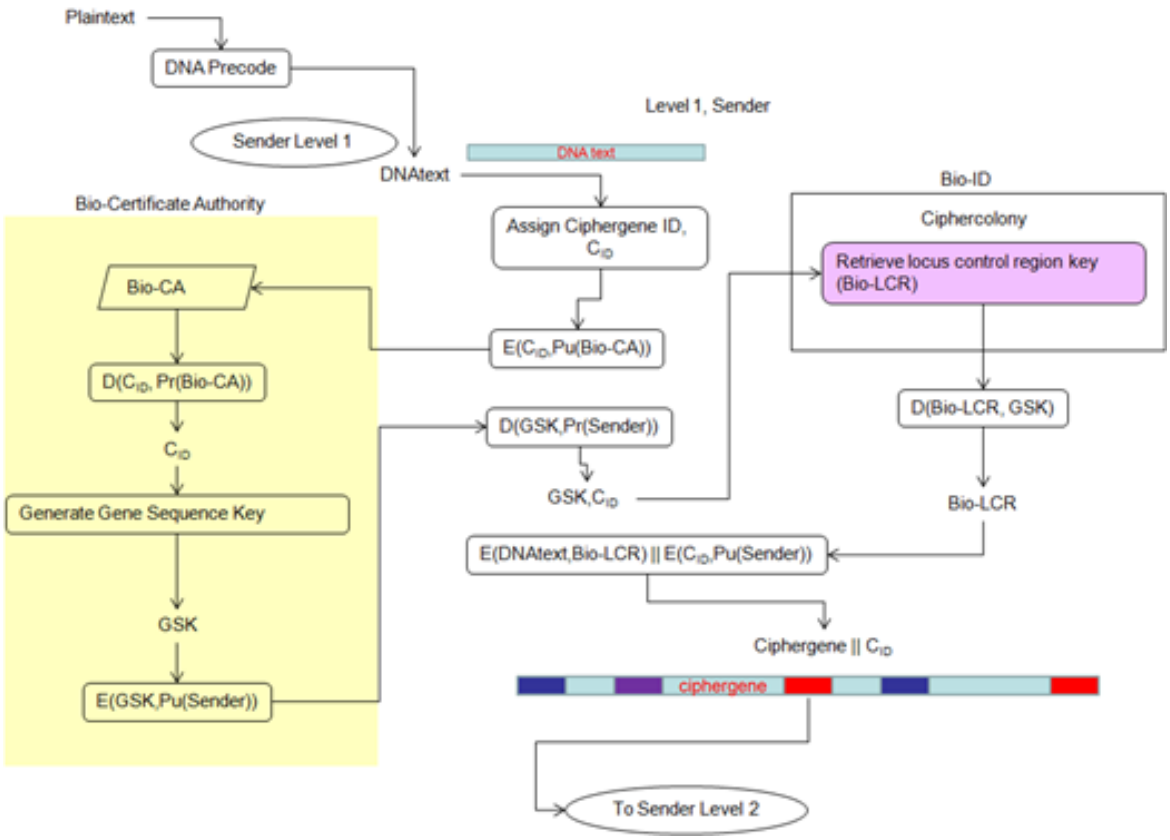

Fig. 11. A Public Key Infrastructure implementation using Bio-Certificate Authorities