Neuro-Amorphic Construction Algorithm (NACA)

Egger Mielberg

egger.mielberg@gmail.com

29.12.2018

Abstract.
Under certain circumstances, determinism of a block cipher can lead to a disclosure of sensitive information about working mechanism of underlying machine. Unveiled restrictions of the mechanism can also give a possibility for an adversary to brute-force the cipher at a reasonable period of time.
We propose a nondeterministic algorithm operating on variable-length groups of bits with dynamically varying parts of round ciphertext. We named it as “Neuron Cipher”. It does not use as public as private key. In compared with symmetric or asymmetric encryption, it has obvious practical advantages. Among them is a “Perfect Secrecy” [4].

1. Introduction

In cryptography, there are a number of cryptographic hash functions that use deterministic algorithms with some restrictions on input data. *However, the most restrictions are realized in the deterministic algorithm, the bigger range of attacks the adversary is given*. The one who designs an authorization application should always remember that a percent of publicly presented information about the procedure of authorization is to converge to zero.

Minimizing predictability of what next step is going to be in an encryption process, we came up with a neurobiology-based solution. The basis of our research is in the field of memory formation. The principles of neurotransmission in the case of influence of dynamically changing dendrite formation. We also base on **Theory of One Synapse** [7].

The goal of this article is to present a new innovative approach of encryption mechanism. The mechanism that will allow a user, *first*, not to worry about publicly transmitted ciphertext, *second*, to get a ciphertext that makes any brute-force attacks meaningless.

2. Construction details

Neuro-amorphic structure of the algorithm is based on features of dendrites of a nerve cell and of amorphous substances. As a basis we took a simplified model of the nerve cell.

The algorithm can have as many rounds as it needs but in most practical cases, it will require not more than two or three rounds at all. In a first round, process of generating a hash consists of four stages:

Stage 1: Plaintext is split into two or more pieces, randomly. Length of each piece of the plaintext can or cannot be equal to other one's length.

Stage 2: Generating a random number of 256, 512, 1024 or more bit size.

Stage 3: Calculating a synapse value (sv) by XORing the random number and the piece of the plaintext chosen by F_{sp} (round function). The chosen piece is a primary piece (pp).

Stage 4: Calculating hashes for remaining pieces of the plaintext by using sv. Obtained hashes of all pieces including sv, form a first hash value, ciphertext, for the whole plaintext.

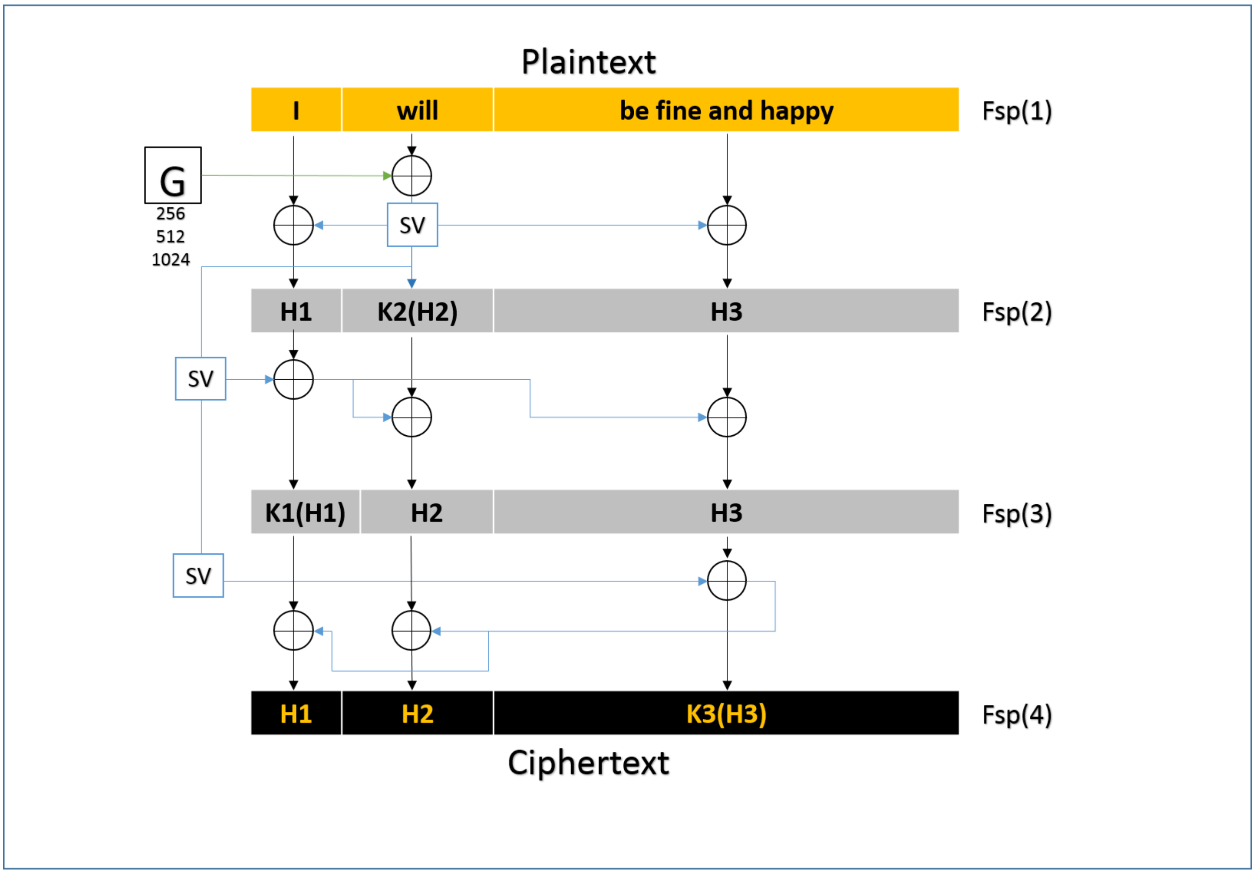


Figure 1. “Amorphic Construction”.

F_{sp} – a multi-valued function the main task of which is to take a plaintext as an argument and split it into two or N pieces of different sizes. A piece of the plaintext can be a sentence, a phrase, a word, half a word, a letter (‘s), a number (‘s), special symbol (‘s) or a combination of word and special symbol, etc.

Hash value of the plaintext is different from round to round and its length as well.

K_1, K_2, K_3,… K_N – key hashes generated by the synapse value.

H_1, H_2, H_3,… H_N – round hash values of pieces of the plaintext.

3. Mode of operation

In our case, an algorithm that provides a confidentiality is based on two components, a unique binary sequence (256, 512, 1024, etc.) and an initialization vector (iv) that is calculated by F_{sp} on a random basis.

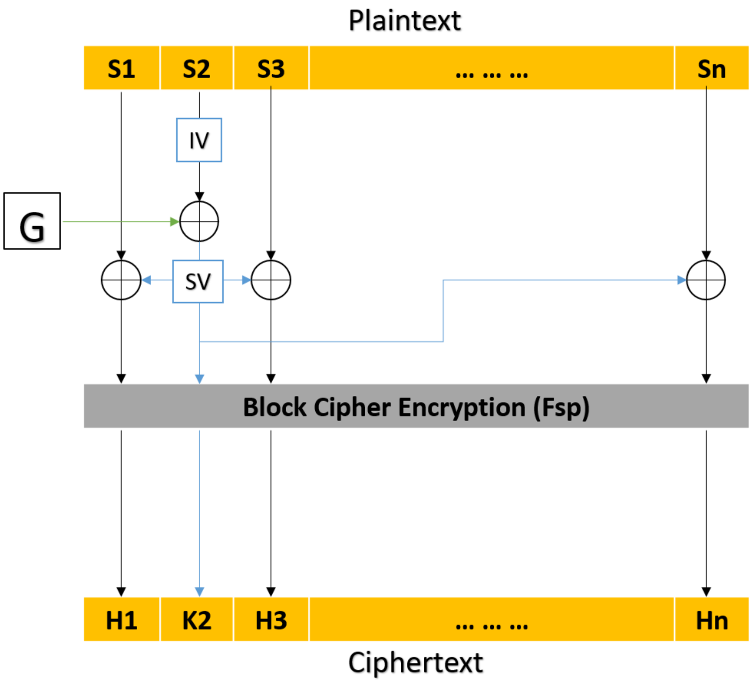


Figure 2. "Encryption mode". Cipher Neuron Chaining (CNC).

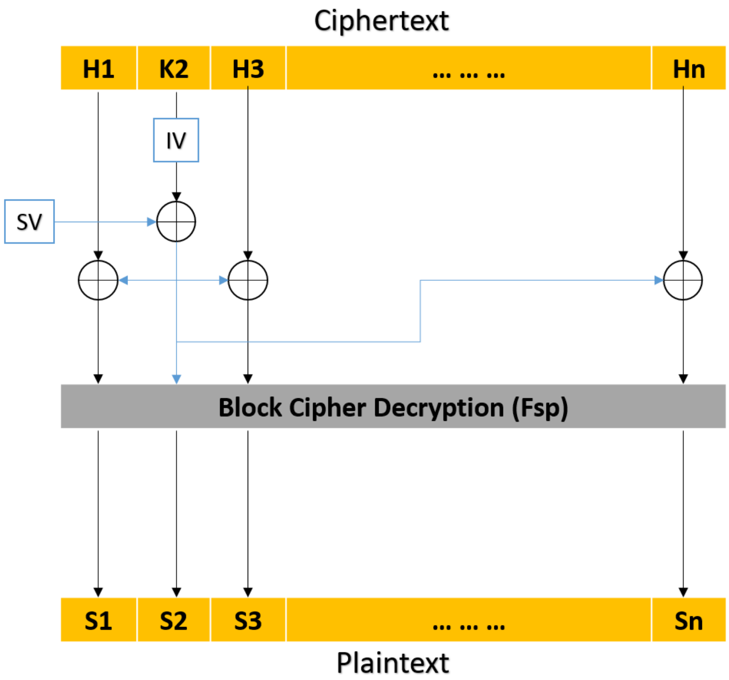


Figure 3. "Decryption mode". Cipher Neuron Chaining (CNC).

Formula for CNC encryption mode can have the following expression:

$H_0 = S_i \oplus K$, $i \in N$,

$H_j = F_{sp}(sv \oplus P_j)$, $i \neq j$, $j \in N$

Formula for CNC decryption mode can have the following expression:

$H_0 = K_i \oplus sv$, $i \in N$,

$P_j = F_{sp}(H_j \oplus K_i)$, $j \neq i$, $j \in N$, $K_i \neq K$.

In compared with CBC (Cipher Block Chaining) [1], PCBC (Propagating Cipher Block Chaining) [2] and other modes of operation, CNC has several advantages. Among them:

1. Encryption and decryption processes can be parallelized. Thus, it can result in a fast overall performance of the entire hash process.
2. K_i values are being changed in every single round. It helps reach a good level of *Avalanche effect*.
3. Confusion property is totally realized in part of dependency of H_j on sv.
4. Diffusion property is realized completely. Changes in S_i values will drastically change bits in the ciphertext (over 50%).

Also, it should be noted that, *first*, S_i value (iv) is chosen randomly by F_{sp} and *second*, the length of the ciphertext for the same plaintext is different for a single encryption process.

4. Perfect Secrecy

As [4] claims, “Perfect Secrecy is defined by requiring of a system that after a cryptogram is intercepted by the enemy the *a posteriori probabilities* of this cryptogram representing various messages be identically the same as the *a priori probabilities* of the same message before the interception”. In other words, the chances to decrypt a ciphertext for an attacker must be the same in both situations, when the attacker gets known about the ciphertext and when he or she gets known nothing about it. That is, the ciphertext gives absolutely no additional information about the plaintext.

According to Shannon’s proof, a one-time pad has the perfect secrecy property. *But a practical realization of the one-time pad has serious drawbacks*. Among them:

1. “Security place”. A place where the one-time pad is stored must be as secure as a military territory.

2. “Limit of users”. A number of people which have an access to the one-time pad as minimum as possible.
3. “Transport efficiency”. It becomes practically impossible if there is an urgent need for transportation of the one-time pad from one place in planet to another without using Internet.

As we see, non-deterministic property of NACA can eliminate above-mentioned drawbacks.

Let’s consider the following practical example (Internet version).

Suppose, agent A has to transmit to agent B some secret message “*Meet me at 8 o’clock, October 31, 7799 Broadway, New York*”. In case of a one-time pad usage, agent A must share his or her one-time pad with agent B before any message transmission.

Moreover, keeping the perfect secrecy property agent A will always need to generate and transmit a new one-time pad each time when he or she needs to send a secret message. This requirement is time-consuming and costly for both agents.

Now, imagine that a generation of the one-time pad is executed on the side of agent A. Then, in order to send a secret message agent A will not need to share his or her generated pad with agent B. In this situation, only one secret agent B has to know is a sv.

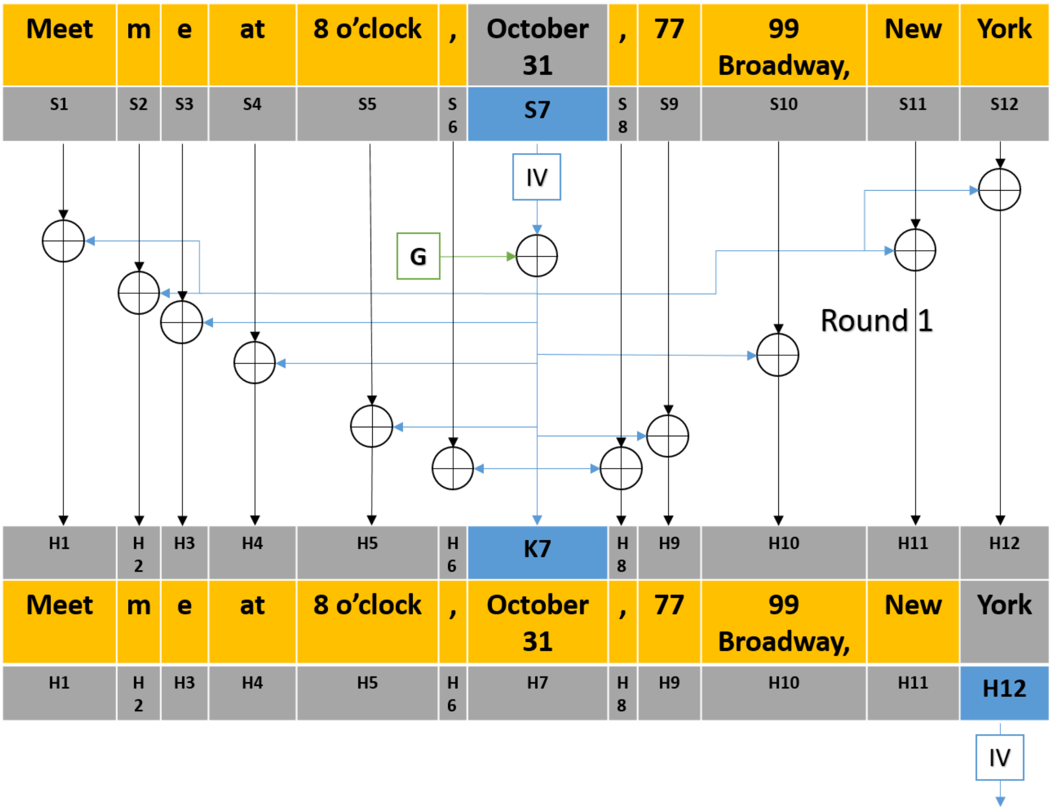


Figure 4. “Secret message”.

As seen on Figure above, snippet “October 31” (S7) is used as a iv value in Round 1. sv is generated by XORing a 256 (512, 1024, etc.) bits key and iv. Then, sv is used for generating a key hash K_7 by XORing sv and a randomly chosen new iv. For each round, there is a unique iv. Thus, the length as well as hash value of the plaintext will change from round to round. In this case, the ciphertext can be as longer as shorter than the plaintext. This property of NACA is **crucial** as it allows the ciphertext, *first*, not to be strictly tied to the following inequality $|K| \geq |C| \geq |P|$, where C is a ciphertext, P is a plaintext and K is a key hash.

[4] claims, “if a secrecy system with a finite key is used, and N letters of cryptogram intercepted, there will be, for the enemy, a certain set of messages with certain probabilities that this cryptogram could represent. As N increases the field usually narrows down until eventually there is a unique solution to the cryptogram”. In case of NACA, there is no need to worry about interception at all as a ciphertext of any plaintext can be presented publicly with no any disclosure of plaintext information.

Another **crucial** property of NACA is a set of different ciphertexts for a single plaintext. It became possible because of randomness of iv value.

5. Neural entropy

The degree of uncertainty is a crucial property of any cryptographic algorithm in part of outcome value. Ideally, an outcome (ciphertext) of the cryptographic algorithm should, *first*, be presented publicly without giving a possibility to hack it, *second*, have a unique value compared with another outcomes of the same input value (plaintext).

We believe that this two features of an outcome are self-sufficient and let the degree of uncertainty reach its maximum.

The first feature implies an absolute identity of both, *priori* and *posteriori probabilities* of the outcome. It is different from the interpretation of “Perfect Secrecy” formulated by Shannon [4]. In our case, there is no need to separate a priori probability from a posteriori one as the outcome of NACA can be unveiled as much public as a public key in asymmetric cryptography.

The second feature implies that the one-way cryptographic NACA-based function is multivariable. In other words, for any given plaintext there is an infinite set of different ciphertexts with different length.

Thus, we are coming to such a definition as “*Neural Content*” (NC):

“*A continuous random unit* X *(text, number, symbol) with probability density function* $M(x)$ *[5] and function* $NC_X(x) = \frac{1}{M^2(x)}$ *, where* $x \in X$*.*”

Continuity of X is caused by existence of infinitely-large set of possible hash values generated by F_{sp} and G.

Probability of falling X into a given interval $[a, b]$ is defined by the following formula:

$$P[a \leq X \leq b] = \int_a^b M(x)dx$$

According to the properties of NC we can formulate the definition of “*Neural Entropy*” (NE):

“*A frequency expectation expressed by the following formula:*

$$F[X] = \sum_{i=1}^{N} p_i fr(x_i),$$

where

$$p_i = p_X(x_i), x_i \in X,$$

$$fr - \ functions\ of\ frequency\ (fof),$$

$$N - total\ number\ of\ random\ variables\ of\ X$$”

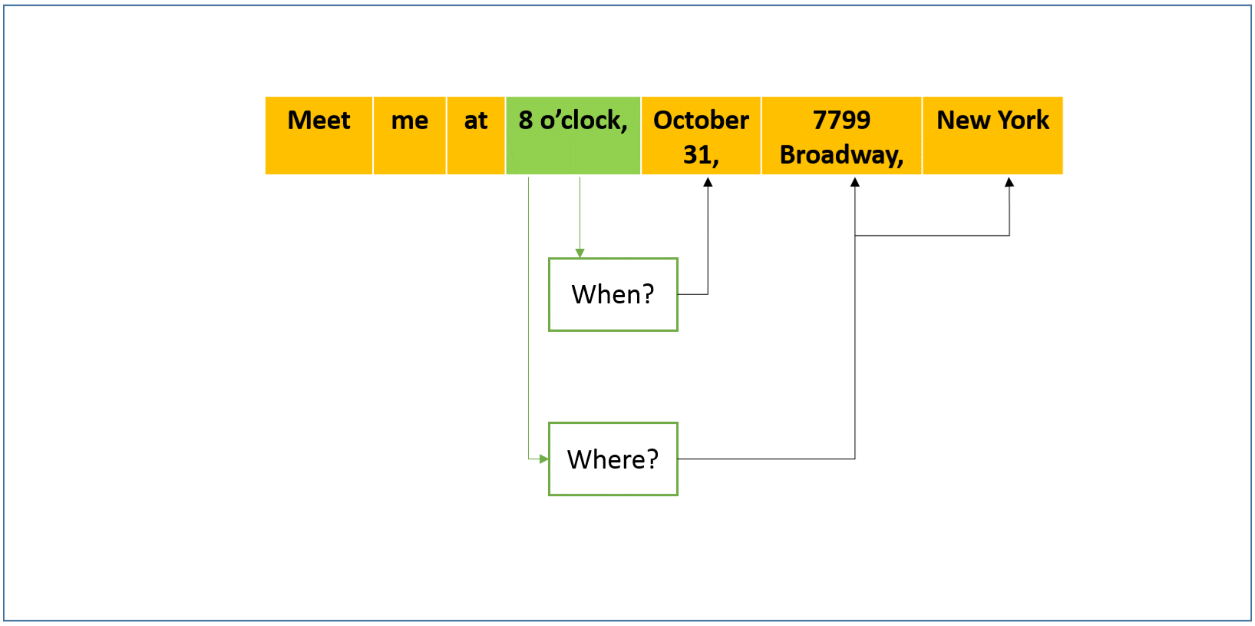
The frequency expectation $F[X]$ has a series of important properties. Among them:

1. $F[c] = c, if\ X = \{x_i\}, where\ i = \{1\}, then\ fr(x_i) = x_i\ (c \in R)$.
2. $F[X] = 0\ if\ and\ only\ if\ \forall x_i \in X, fr(x_i) = 0\ (i = \{1,2,3, \dots n\})$.
3. $F[\emptyset] = 0\ as\ fr(\emptyset) = 0$.
4. $F[X] = F[Y]\ if\ X = Y\ almost\ strong\ in\ case\ of\ fr(x_i) = fr(y_i)$.
5. $F[CX] = CF[X], where\ C\ is\ constant$.
6. $F[XY] = F[X]F[Y]\ for\ \forall X, Y \in R$ ().
7. $F[M_0] = \begin{cases} M_0,\ if\ card(M_0) = 1, where\ p = 1 \\ p\sum_{i=1}^{n} x_i\ ,\ if\ card(M_0) > 1,\ where\ p_1 = p_2 = \cdots p_n \\ 0,\ if\ card(M_0) =\ \emptyset \end{cases}$

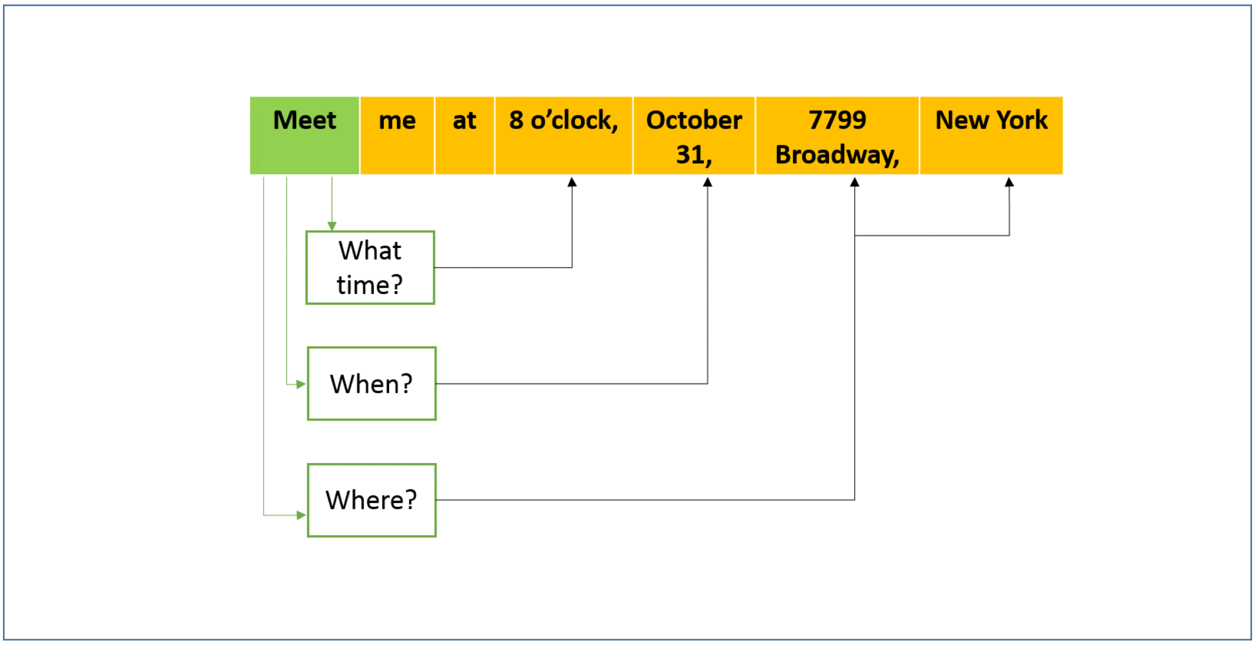
In compared with Shannon entropy that calculates an expected value of information content, “*Neural Entropy*” primarily focuses on the frequency of appearance of a random-unit-pattern. This feature of NE has a lot of practical applications.

For more technical details of the frequency expectation ($F[X]$) and probability density function ($M(x)$), see [5]. For a detailed description of NE, see [6].

6. Provable security



If an adversary is known about faces of both, agent A and agent B, he or she will only need to know "Where?".



If an adversary is familiar with the place where agent A and agent B are used to or can be, then he or she will be satisfied with only decrypted part of the plaintext “Meet”.

Neuro-amorphic function or *NAF* or *N-function* is a cryptographic nondeterministic multivalued function $N = B \to B$, where B is a set of bits and $\forall b_{1,} b_2 \in B$ $(b_1 \neq b_2,\ b_{12} - bit\ string)$.

NAF has a series of important properties. Among them:

1. There are no two identical values of codomain B for a single value of domain B.
2. It is nondeterministic ($N_k(b_i) \neq N_e(b_i), k \neq e$).
3. It is irreversible ($N^{-1}\big(N(b)\big) \neq b, \forall b \in B$).

In the context of *Neuron Cipher* and NAF, we can formulate the strict conditions for the “security” of a cryptographic algorithm:

“*An algorithm is secure if and only if the following two conditions are met:*

1. *The same message always results in a different hash.*
2. *The brute-force attack is meaningless in both directions.*”

First condition can be realized through a direct usage of NACA for any cryptographic needs.

Second condition implies a lack of information for choosing the right template or pattern for an iterative algorithm. It is about a situation when an attacker does not have any information about the nature of data that is used in an encryption internal process. For example, in case of user passwords, an attacker systematically (iteratively) checks all possible passwords until the correct one is found. In other words, the attacker knows possible variants of letters, numbers or symbols the password might be consisted of. Nondeterministic property of NACA and F_{sp} allows a user to be as much secure as possible from any brute-force attack at all.

7. Conclusion

We presented the new concept for an encryption procedure. The concept introduces a series of innovative mechanism and definitions that confront traditional deterministic concept of a cryptographic hash function. Among the main practical advantages of Neuro-Amorphic Construction Algorithm (NACA), two of them should be noted separately, “*public storage of ciphertext*” and “*brute-force attack resistance*”.

We hope that our decent work will help researchers, engineers and other users in their professional endeavors.

References

[1] C. Rackoff, S. Gorbunov, “On the Security of Cipher Block Chaining Message Authentication Code”, University of Toronto, http://people.csail.mit.edu/sergeyg/publications/securityOfCBC.pdf

[2] A. Z´uquete, P. Guede, “Efficient Error-Propagating Block Chaining”, http://www.inesc-id.pt/pt/indicadores/Ficheiros/1215.pdf

[3] C. Shannon, “A Mathematical Theory of Cryptography”, 1945, https://www.iacr.org/museum/shannon/shannon45.pdf

[4] C. Shannon, “Mathematical Theory of Cryptography”, 1949, http://pages.cs.wisc.edu/~rist/642-spring-2014/shannon-secrecy.pdf

[5] E. Mielberg, "Probability Density M-function”, to be republished, 2019

[6] E. Mielberg, "Neural Entropy", to be published, 2019

[7] E. Mielberg, "Theory of One Synapse", to be published, 2019