Current Trends on Biostatistics & Biometrics
DOI: 10.32474/CTBB.2020.02.000133
ISSN: 2644-1381

Short Communication

# Cryptography Motivated By Immune System

**Ahmed E***

*Department of Mathematics, Faculty of Science, Mansoura, Egypt*

***Corresponding author:** E. Ahmed, Faculty of Science Mathematics department, Mansoura 35516, Egypt

**Received:** January 27, 2020 **Published:** February 05, 2020

**Abstract**

A cryptography algorithm is proposed. It depends on extremal optimization which is motivated by immune system.

## Extremal optimization

Extremal optimization (EO) [1] is a metaheuristic method [2] which is quite similar to the way the immune system (IS) renews its cells. This dynamic is called extremal dynamics [3]. It can explain the long-range memory of the immune system even without the persistence of antigens. The reason is that if a system evolves according to such dynamics then the annihilation probability for a clone (a type of cells) that has already survived for time t is proportional to 1/ (1+ tc), where c is a positive constant. Therefore, the longer it lives the higher the probability that it will continue to survive. This is the memory effect observed in the immune system. Consider a system of N elements, each element assigned a single scalar variable x(i), i = 1,2…, N drawn from the fixed probability distribution function p(x). For every time step, the element with the smallest value in the system is selected and renewed by assigning a new value which is drawn from p(x). It is assumed that no two x(i) can take the same value.

### Definition 1

For the above system the typical values of x(i) increase monotonically in time. This means that any renewed element is likely to have a smaller x(i) than the bulk, and hence a shorter than average lifespan until it is again renewed. Corresponding, elements that have not been renewed for some time will have a longer than average life expectancy. This separation between the shortest and the longest-lived elements will become more pronounced as the system evolves and the average x(i) in the bulk increases.

This phenomenon is called long-time memory.

### Proposition 2

Extremally driven systems can generally be expected to exhibit long-term memory [1].

Proposed algorithm:

i. Apply public key cryptography [4,5] using binary notation to build the initial state x(i) i=1, 2,,n common to both sender A and receiver B.

ii. A chooses the matrix J(i,k) and runs the spin glass model [1] using the extremal optimization algorithm and the Hamiltonian $H = \Sigma J(i,k) \times (i) \times (k)$ Such that the final state xf(i) represents the message.

iii. A sends J(i,k) to B to derive the message.

An advantage of this algorithm is that it is applicable even for small computers.

## Conclusion

I like to comment on the present situation of post-quantum cryptography. Quantum computers have already been made by Google and IBM. They are capable of breaking the standard cryptography e.g. RSA and elliptic curve cryptography [4]. Therefore, studying post-quantum cryptography is essential. An excellent candidate is quantum cryptography, but it is local [6]. Presently one of the strongest candidates in the National Institute of Standards and Technology (NIST) competition is lattice based cryptography [7]. Google chrome already uses lattice-based cryptography. But lattice-based cryptography is known to have a gap between theory and practice. More mathematical studies are needed for it [7].

## References


1. Elettreby MF, Ahmed E, Houari Boumedien Khenous (2014) On Metaheuristic Optimization Motivated by the Immune System Applied Math 5(02): 318.
2. Blum C, Roli A (2003) ACM Computing Surveys 35(3): 268-308.
3. Boettcher S, Percus A (2001) Optimization with Extremal Dynamics Physical Review Letters 86(23): 5211-5214.
4. Jeffrey, Hoffstein, Jill, Pipher, Joseph H, et al. (2004) An Introduction to Mathematical Cryptography. Springer.
5. Knospe Heiko (2019) A course in cryptography. Pure and Applied Undergraduate. Providence RI American Mathematical Society 40: 323.
6. Mitch Leslie (2019) Quantum Cryptography via Satellite Engineering 5(3): 353-354.
7. Lidong Chen, Dustin Moody (2020) New Mission and Opportunity for Mathematics Researchers. Cryptography in the Quantum Era Advances in Mathematics of Communications 14(1): 161.




**DOI:** 10.32474/CTBB.2020.02.000133