An innovative data security method using elliptic curve cryptography

S. Benatmane[1], **D. Behloul**[2]
[1]USTHB, Bab ezzouar, Algeria
[2]USTHB, Bab ezzouar, Algeria
benatmanesara34@gmail.com, dbehloul@yahoo.fr

The study of applying mathematics to encrypt and decrypt data for safe communication is known as cryptography. It enables the user to send data over an insecure network such that only the intended recipient may read it. The current public key cryptography methods used to provide secure data transfer are RSA and Elliptic Curve Cryptography. To provide a higher level of security, current DNA-based cryptography techniques require more processing time and power as well as larger key sizes. As a result, the public key cryptography approach is constrained. A new cryptographic system that uses DNA Computing to give first level security with a smaller key size and reduced computational overhead is proposed in order to get around this restriction. The low computation ECC encryption and decryption technique offers the second level of security. The uniqueness of this suggested system is how it uses the benefits of both DNA and ECC computation to offer a high level of data protection. The effectiveness of the cryptography technique is next evaluated in comparison to other cryptographic schemes already in use.

Another well-known public key cryptography method is the elliptic curve cryptosystem (ECC), which was proposed by Miller and Koblitz in 1986 and 1987, respectively [2]. ECC uses a reduced key size while yet offering the same level of protection as RSA. The security level offered by an ECC-160 bit key is equivalent to that of a 1024 bit RSA key. As a result, the reduced key size of ECC allows for greater compactness, which has a number of benefits for circuit space, memory needs, power consumption, performance, and bandwidth. Additionally, IEEE 1363 and NIST both give the ECC key size. Point scalar multiplication, also referred to as the ECC operation, can be carried out using a variety of elliptic curve arithmetic methods [3]. After Adleman (1994) conducted research in the area of DNA computing, the idea of DNA cryptography was introduced. Along with DNA computer research, a new branch of cryptography called DNA coding has emerged recently. Modern biotechnology is used to create the instruments for DNA cryptography, which is based on DNA, a material that can carry information. DNA cryptography uses the tremendous parallelism and high storage density properties of DNA to accomplish the encryption procedure [5]. The DNA-encoded plaintext, which combines mathematical and molecular biology procedures to produce the final cipher text, is the reason why cryptography and molecular biology are combined [7]. In this approach, plaintext is encoded or decoded using DNA computing, while encryption and decryption are performed using ECC.

In terms of security, the suggested DNA-ECC hybrid cryptosystem outperforms the currently used Elliptic Curve Cryptography and DNA cryptography. Because it uses an Elliptic Curve Cryptography mechanism for encryption and a DNA cryptographic mechanism for encoding. As a result, the suggested system has two levels of security, the first of which is in the encoding phase and the second of which is in the encryption phase. Comparatively to other cyberspace cryptographic systems, it uses a tiny key size for encryption (because ECC is used for encryption, the key size is the ECC's key size). Given that it has two levels of protection, it is hardly breakable by an eavesdropper.

The ECC algorithm and DNA computing theory are combined in this research to create a revolutionary encryption method. DNA Computing's implementation of elliptic curve cryptography has several advantages over conventional methods. in the form of faster processing, less memory, and more compact keys. The suggested system also contains two levels of encryption, one using ECC and the other DNA encoding. To test the viability of the suggested cryptographic technique, a DNA-ECC embedded system based on the theories presented in this research may be created utilizing an embedded FPGA system.

1. Kumar M., Iqbal A. & Kumar P. A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie-Hellman cryptography. Signal Processing, 2016, 125, 187-202.

2. Koblitz N., Menezes A. & Vanstone S. The state of elliptic curve cryptography. Designs, codes and cryptography, 2000, 19, 173-193.

3. Hankerson D., Menezes A. J. & Vanstone S. Guide to elliptic curve cryptography. Springer Science & Business Media, 2006.

4. Bos J. W., Halderman J. A., Heninger N., Moore J., Naehrig M., & Wustrow E. Elliptic curve cryptography in practice. In Financial Cryptography and Data Security: 18th International Conference, FC 2014, Christ Church. Springer Berlin Heidelberg, 2014, pp. 157-175.

5. Li X. S., Zhang L. & Hu Y. P.. A novel generation key scheme based on DNA. In 2008 International Conference on Computational Intelligence and Security. IEEE, 2008, Vol. 1, pp. 264-266.

6. Kumar A., Tyagi S. S., Rana M., Aggarwal N. & Bhadana P. A comparative study of public key cryptosystem based on ECC and RSA. International Journal on Computer Science and Engineering, 2011, 3(5), 1904-1909.

7. Sadeg S., Gougache M., Mansouri N. & Drias H. An encryption algorithm inspired from DNA. In 2010 International Conference on Machine and Web Intelligence. IEEE, 2010, pp. 344-349.