Massively parallel concept for cryptanalysis of RSA in a bio-computation framework

Gordon Cichon, Galbadrakh Battsogt, and Tseren-Onolt Ishdorj*

School of Information and Communication Technology
Mongolian University of Science and Technology
Ulaanbaatar, Mongolia
{cichon,tseren-onolt}@must.edu.mn

Abstract. The paper exposes a concept for cryptanalysis of RSA encryption using a bio-computation paradigm. A very high degree of parallelism is required, and we hope to benefit from quantum-mechanic entanglement, if the implementation technology is small enough. We implement the computation using HP/LP-neurons in membrane computing. A System-C model of the system will be developed in the next step.

Introduction

Investigation of cryptography and cryptanalysis are in the center of not only classic computer science research but also in the new computing paradigms such as bio-computation [3,4,10], and quantum computation [1,7] well. RSA encryption is based on a public encryption key that is the product of two large prime numbers [9].

[2] has investigated using membrane computing for RSA encryption. For this method, he has applied the MUST Adder [8], as well as extended by new modules. The MUST Adder is implemented using HP- and LP-neurons [11].

As the next step, we consider cryptanalysis of RSA.

RSA Cryptanalysis

For cryptanalysis of RSA, we consider the following conceptual model: (see Fig. 1).

As a first step, we employ a sequencer that is based on the MUST Adder in HP- and LP-neurons in membrane computing. This sequencer generates a large number of integer numbers which are represented individually as instances at the membrane.

The next step is a decimation operation at the first membrane. This will be realized using the sieve algorithm. By a large number of sieve steps, we eliminate all number instances that do not posses the prime property.

The surviving instances will then be collected in a large soma. We will need a significantly larger number of such instances, depending on the bit width of

[*] Corresponding author.

the RSA key. This is an excellent application of membrane computing, since at the molecular level, 1g of soma my host up to 10^{23} prime instances, which corresponds to roughly 76 bits. [**?**]

At the exit of the soma, we place a large number of MUST Multipliers, each of which is capable of multiplying two prime instances.

The second membrane functions as selector to perform a selection operation designed to match the desired encryption key of RSA. This selection operator constitutes a barrier to the exit of any number instances from the soma membrane.

Successfully overcoming the barrier releases a certain amount of target energy. The larger the energy, the more likely is the transition through the barrier, according to quantum mechanics.

We hope that we will, one day, build our cryptanalytic system at such a small scale that the soma is able to exist in the state of quantum mechanical superposition. Then, we hope to benefit from the properties of the quantum mechanic tunnel effect. This effect will make it more likely for the desired instance to exit from the membrane barrier, the more energy is being released by the transition. Then, we can make the system faster, by increasing the energy reward for the correct result to exit.

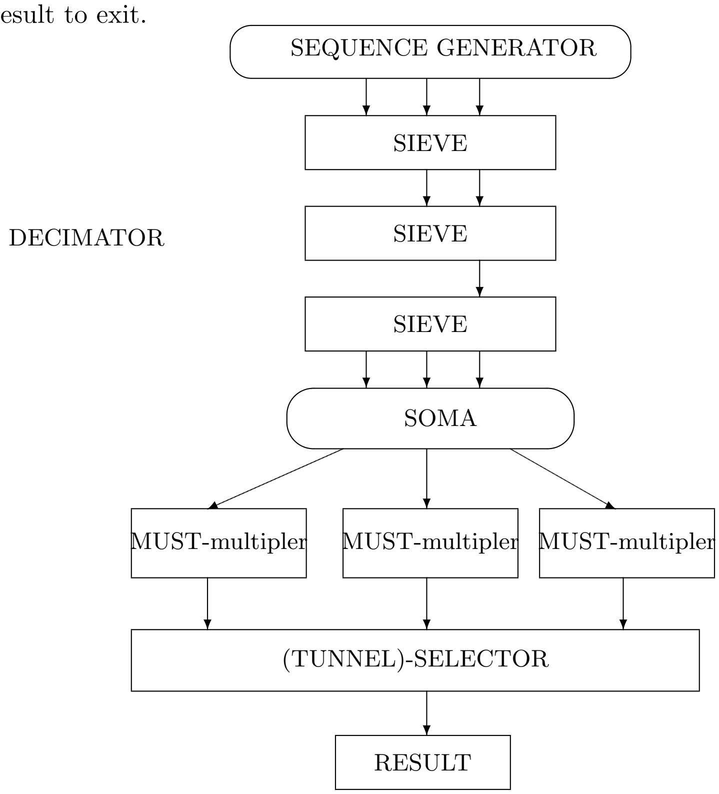

Fig. 1. RSA cryptanalysis conceptual scheme using a bio-computation framework.

Conclusion

In this approach, we hope to develop and leverage the unique quantum mechanic effects [7] in the context of biochip [6]. This works efficiently in a highly parallel fashion of SN P systems [5].

References

1. William Buchanan and Alan Woodward. Will quantum computers be the end of public key encryption? *Journal of Cyber Security Technology*, 1(1):1–22, 2017.
2. Ganbat Ganbaatar, Dugar Nyamdorj, Gordon Cichon, and Tseren-Onolt Ishdorj. Implementation of rsa cryptographic algorithm using sn p systems based on hp/lp neurons. *Journal of Membrane Computing*, 3(1):22–34, 2021.
3. Ping Guo and Wei Xu. A Family P System of Realizing RSA Algorithm. In Maoguo Gong, Linqiang Pan, Tao Song, and Gexiang Zhang, editors, *Bio-inspired Computing – Theories and Applications*, pages 155–167, Singapore, 2016. Springer Singapore.
4. Noorul Hussain, Chithralekha Balamurugan, and Rajapandian Mariappan. A novel dna computing based encryption and decryption algorithm. *Procedia Computer Science*, 46:463–475, 12 2015.
5. Mihai Ionescu, Gheorghe Păun, and Takashi Yokomori. Spiking Neural P Systems. *Fundamenta Informaticae*, 71(2):279–308, August 2006.
6. Tseren-Onolt Ishdorj, Otgonnaran Ochirbat, and Chuluunbandi Naimannaran. A μ-fluidic biochip design for Spiking Neural P systems. *International Journal of Unconventional Computation*, 2020.
7. Vasileios Mavroeidis, Kamer Vishi, Mateusz Zych, and Audun Jøsang. The impact of quantum computing on present cryptography. *International Journal of Advanced Computer Science and Applications*, 9, 03 2018.
8. Otgonnaran Ochirbat, Tseren-Onolt Ishdorj, and Gordon Cichon. An error-tolerant serial binary full-adder via a Spiking Neural P system using HP/LP basic neurons. *Journal of Membrane Computing*, 2(1):42–48, March 2020.
9. R.L. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21:120–126, 1978.
10. X. Wang and Q. Zhang. DNA computing-based cryptography. In *2009 Fourth International on Conference on Bio-Inspired Computing*, pages 1–3, 2009.
11. Zihan Xu, Matteo Cavaliere, Pei An, Sarma Vrudhula, and Yu Cao. The stochastic loss of spikes in Spiking Neural P systems: Design and implementation of reliable arithmetic circuits. *Fundamenta Informaticae*, 134(1-2):183–200, 2014.