Survey of Cellular Automata Based Hash Functions

Jun-Cheol Jeon

Department of Computer Engineering at Kumoh National Institute of Technology, Gumi, Korea
jcjeon@kumoh.ac.kr

Abstract. A cellular automata based schemes are very useful to design hash functions with a low hardware complexity because of its logical operation attribute and parallel property. In this paper, we discuss some hash functions based cellular automata.

Keywords. cryptography, hash function, cellular automata,

1 Introduction

Any message authentication or digital signature mechanism can be viewed as having fundamentally two levels [1]. At the lower level, there must be some sort of function that produces an authenticator: a value to be used to authenticate a message. This lower-level function is then used as primitive in a higher-level authentication protocol that enables a receiver to verify the authenticity of a message.

Cryptographic hash functions play an important role in modern cryptography. The basic idea of cryptographic hash functions is that a hash-value serves as a compact representative image (sometimes called an imprint, digital fingerprint, or massage digest) of an input string, and can be used as if it was uniquely identifiable with that string [2].

In the last two decades, a wide variety of applications on CA has been proposed. Major applications can be categorized under the following broad headings: simulation of physical systems, biological modeling involving models for self-reproduction, image processing, language recognition, computer architectures, error correcting codes, block and stream cipher cryptography, and fractals and chaos.

Cellular Automata (CA) are among the oldest model of natural computing, dating back over half a century. The first CA studies by John von Neumann in the late 1950s were biologically motivated [3]: the goal was to design self-replicating artificial systems that are also computationally universal. Wolfram [4] pioneered the investigation of CA as mathematical models for self-organizing statistical systems and suggested the use of a simple two-state, three-neighborhood CA with cells arranged linearly in one dimension. CAs are dynamic systems in which space and time are discrete. A CA consists of an array of cells, each of which can be in one of a finite number of possible states, updated synchronously in discrete time steps, according to a local, identical interaction rule.

In [5], Daemen et al. have persisted in vulnerability of scheme from [6] together with a new CA based hash function. Another research on CA based hash function has been reported by Mihaljevic et al. [7] based on their previous report in [2]. They have proposed a family of fast dedicated one-way hash functions based on linear CA over GF(*q*) in 1999. Jeon in [8] proposed a stronger CA based hash function. They used only CA functions to make confusion and diffusion and provided various experimental results. In this paper, we review their architecture and discuss some pros and cons.

2 Cellular Automata Based Hash Functions

The first result of the CA application for one-way hash function design has been reported in [6]. The vulnerability of the scheme from [6] is presented together with a result for new CA based hash function called *Cellhash* by Daemen et al. in 1991 [5]. However this scheme did not provide any specific neighborhood and rules. It means that the scheme is not well defined and designed by CA theory.

Mihaljevic et al. proposed another research on a CA based hash function in [7]. Their proposed function follows the model for iterated hash functions, and employs the Davis-Mayer principle. In this scheme, CA operations with primitive characteristic polynomial are used only twice in Step 2 and 4 of the compression function in [7], and other nonlinear functions are from HAVAL [9]. Actually it is hard to say that the scheme is a CA based hash function.

Though the mentioned papers have persisted in their security and advantages, they did not provide enough comprehension on security and experimental results. Moreover the previous works did not use specific rules so that it is hard to determine the characteristics of their schemes.

In [8], a stronger CA based hash function has been suggested. They used only CA functions to make confusion and diffusion and provided various experimental results. This scheme has very good at performance in tests and used only CA based operations so that the operations are only based on logical operations. However, this scheme also did not deal with security problem significantly.

3 Conclusion

In many studies, they have proposed various hash algorithms for specific environments. In order to use the algorithms on small silicon area, extremely dedicated and tiny architectures are demanded. For satisfying the demand, a CA theory has been used as a basic computational component. In this paper, we discuss some typical CA based hash functions. Each scheme has its own pros and cons. But they are still insufficient in minifying and security aspect. Thus well-defined and designed CA based hash function is exceedingly required.

Acknowledgements. This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology (2011-0014977).

References

1. Stallings W.: Cryptography and Network Security: Principles and Practice second edition, Prentice Hall Inc., 1999.
2. Mihaljecvic M., Zheng Y., Imai, H.: A Cellular Automaton Based Fast One-Way Hash Function Suitable for Hardware Implementation, proceeding of PKC’98, LNCS 1431, pp. 217-233 (1998).
3. Neumann J. von,: The Theory of Self-Reproducing Automata, A. W. Burks, ed., Univ. of Illinois Press, Urbana and London (1966).
4. Wolfram S.: Statistical Mechanics of Cellular Automata, Review of Modern Physics, vol. 55, pp. 601-644 (1983).
5. Daemen J., Govaerts R., Vandewalle J.: A Framework for the Design of One-Way Hash Functions Including Cryptanalysis of Damgard’s One-Way Function Based on a Cellular Automaton, proceeding of Asiacrypto’91, LNCS 739, pp. 82-96 (1993).
6. Damgarrd I. B.: A Design Principle for Hash Functions, proceeding of Crypto’89, LNCS 435, pp. 416-442 (1989).
7. Mihaljecvic M., Zheng Y., Imai H.: A Family of Fast Dedicated One-Way Hash Functions Based on Linear Cellular Automata over GF(q), IEICE Transactions on Fundamentals, Vol. E82-A, No. 1 (1999).
8. Jeon J. C.: One-Way Hash Function Based on Cellular Automata, LNEE 215, pp. 21-28, (2012).
9. Zheng Y., Pieprzyk J., Sebery J.: HAVAL - A One-Way Hashing Algorithm with Variable Length of Output, proceeding of Auscrypt’92, LNCS 718, pp. 83-104 (1993).