A New Pseudo-Random Generator Based on Gollmann Cascades of Baker-Register-Machines

Dominik Jochinger and Franz Pichler

Systems Theory, Johannes Kepler University Linz,
Altenberger Str. 69, A-4040 Linz, Austria

Abstract. In this paper, we present a new pseudo-random sequence generator, constructed by the generalized discrete Baker transformation. This new generator is called Cascaded Baker Register Machine (CBRM), which uses the sensitivity of chaotic behaviour and allows the application of automata- and shift-register theory. It is shown that a CBRM has good properties of randomness, such as large periods and high linear complexity. It can provide high cryptographic security with fast encryption speed, and can be realized effectively by both hardware and software.

1 Introduction

Chaos theory has been established since 1970s by many different research areas, such as physics, mathematics, biology and chemistry, etc. The most well-known characteristics of chaos is the so-called "butterfly-effect" (the sensitivity to the initial conditions), and the pseudo-randomness generated by deterministic equations. Many fundamental characteristics of chaos, such as the mixing property and the sensitivity to initial conditions, can be connected with "confusion" and "diffusion" property in good ciphers. The well-mixing transformations (permutations) used in secrecy systems can be constructed by the basic "stretch-and-fold" mechanism of the Baker transformation, which implies chaos. The first paper about ciphers with dynamical systems was Wolfram's paper published in Crypto'85 [1], in which he introduced a cellular automata based cryptosystem.

In this paper, we propose a new pseudo-random-generator based on the generalized discrete Baker transformation, which is used for creating complex, key-dependent permutations. Most of today's symmetric encryption schemes rely on complex substitution while the important role of permutation is neglected.

We suggest a 256-bit key to define the initial condition of the generator, therefore a brute force attack by key exhaustion seems to be impossible.

2 The Generalized Discrete Baker Transformation

We introduce the generalized discrete Baker transformation following the paper of Pichler and Scharinger [2]:

By N_0^n we denote the subset $N_0^n := \{0,1,2,...,n-1\}$ of integers. With π we denote a list of non-negative integers $\pi = \{n_1, n_2, ..., n_k\}$ with the following properties:

R. Moreno Díaz et al. (Eds.): EUROCAST 2005, LNCS 3643, pp. 311 – 316, 2005.

(1) $\sum_{i=1}^{i\le k} n_i = n$ and

(2)each number n_s ($s = 1, 2, \ldots, k$) divides n

The transformation $T_{n,\pi} : N_0^n \times N_0^n \to N_0^n \times N_0^n$ is a discrete finite version of the generalized baker transformation. $T_{n,\pi}$ is defined as follow:

Let the numbers q_s ($s = 1, 2, \ldots, k$) be defined by $q_s = \frac{n}{n_s}$. Then

$$T_{n,\pi}(x,y) = \left(q_s(x - N_s) + y \bmod q_s, \frac{1}{q_s}(y - y \bmod q_s) + N_s \right)$$

for $(x,y) \in [N_s, N_s + n_s) \times N_0^n$ where $N_1 := 0$ and $N_s := n_1 + \ldots + n_{s-1}$ for s = 2, …, k.

It is easy to see, that $T_{n,\pi}$ maps from $N_0^n \times N_0^n$ the vertical strips $[N_s, N_s + n_s) \times N_0^n$ ($s = 1, 2, \ldots, k$) into the corresponding horizontal strips $N_0^n \times [N_s, N_s + n_s)$.

3 Structure of Baker-Permutation

The generalized discrete Baker transformation is a permutation of n^2 data items. Figure 1 gives a schematic view of a Baker permutation with partition $\pi = \{2, 2\}$ and $n = 4$.

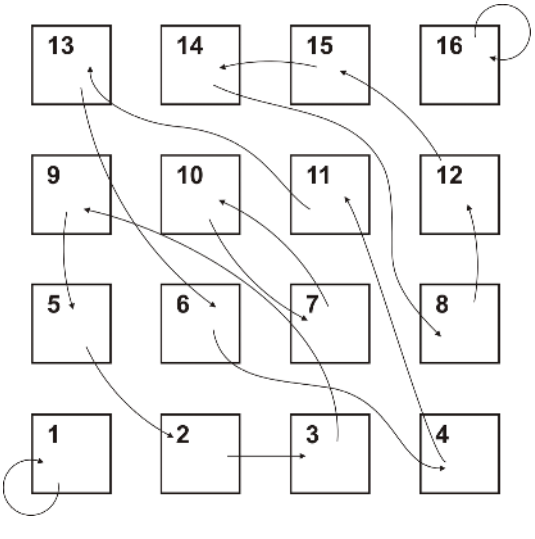

Fig. 1. Baker-permutation

The properties of the permutations defined by the discrete Baker-transformation correspond to a typical random permutation in the sense of Feller [5], [6].

Computer experiments, done for the Baker-permutation with many different partition keys π, demonstrate that the average length of cycles and the average number of different cycles have values similar to those for random permutations.

4 Cascaded Baker Register Machine (CBRM)

The building blocks of a CBRM are given by Baker-Register-Machines (BRM). The blockdiagram of a BRM is shown in figure 2. A BRM consists of *n* register cells and a binary clock-controlled input *x*.

The BRM is initialized with the *n*-bit parameter (*K1*) and the partition-parameter π.

Figure 3 shows a single stage of the CBRM. The input bit a_t clocks the BRM, and then is XORed to the output from the BRM. The *delay* assures that the addition takes place after each clock step.

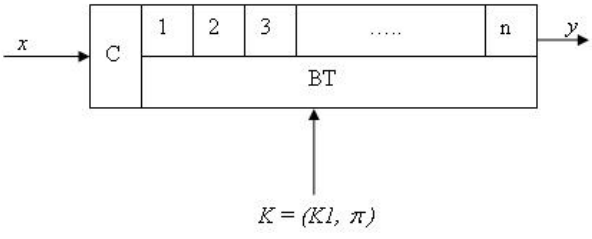

Fig. 2. Blockdiagram of a BRM

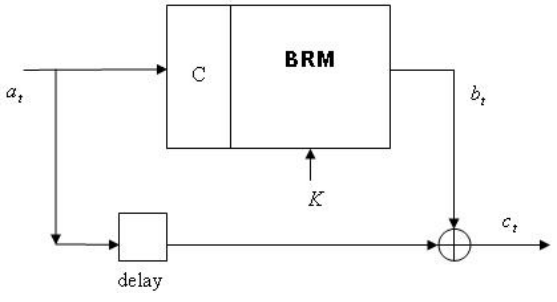

Fig. 3. A stage of the cascade

A nice representation of a BRM can be done by using several feedback-shift-registers. This can be seen as follows.

To determine the cycles of the Baker-transformation n^2 steps are needed. Each cycle, however, can be realized by a feedback-shift-register of cycle length.

To achieve a scalar output from the BRM the feedback-shift-registers of a BRM with exception of the two registers of length 1 (which correspond to the fix points) are output-coupled by a XOR-Operation.

Only one XOR-operation and several shift operations are needed for a single iteration of a Baker-Register-Machine.

The CBRM is defined similar to the well known Gollmann cascade [7], [8] of k stages. It consists of a sequence of k stages of Baker-Register-Machines (BRM), of same length.

By irregular clocking of the individual BRMs and by the cascaded structure we obtain non-linear effects in the output sequence.

A Cascaded Baker Register Machine (CBRM) with 3 stages is shown in figure 4.

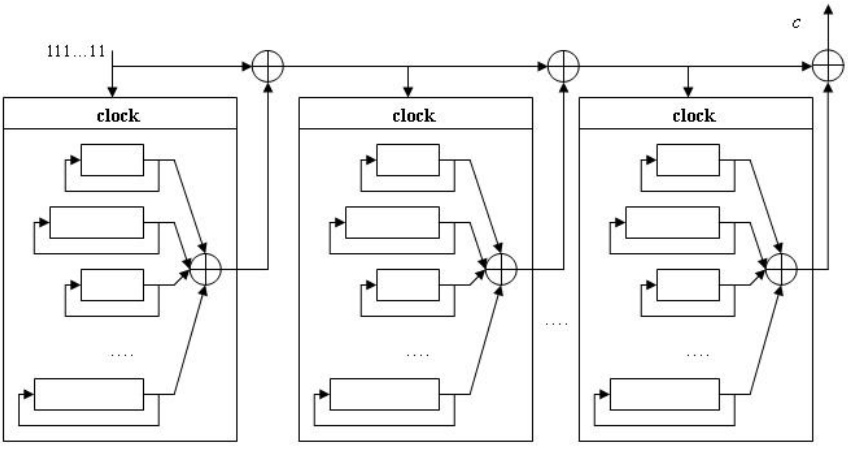

Fig. 4. Cascaded Baker Register Machine with 3 stages

5 Selection of the Partition-Parameter

The partition-parameter π can serve as a customer specific key. It is needed to initialize a Baker-Register-Machine. A selected key π determines the cyclic length of the BRM. Not every possible partition-key leads to a secure cyclic length. The table below shows some acceptable partitions of a 16×16 Baker map and their cyclic length.

Table 1. Some acceptable partitions

Partition	Cyclic length
(8,4,4)	622440
(4,4,8)	622440
(4,4,4,2,2)	1680
(4,4,2,2,4)	55440
(4,2,2,4,4)	55440
(2,2,4,2,2,2,2)	55440
(2,2,2,2,4,2,2)	55440

6 Randomness Properties

An analysis of the CBRM shows that it has many good statistical properties. For example n-gram distributions are uniform.

Another nice property of a BRM is that the generated sequences are highly sensitive to the initial key. By statistical analysis, we found that changing one bit in the encryption key *K1* caused 49.4% of the bits to change in the corresponding cipher-image. Theoretically half of the bits should change, in order to hide any information about the key from leaking.

The linear complexity profile of the CBRM algorithm is staying very close to be optimal.

The cycle length (period) of the CBRM depends on the partition key, as mentioned above. It is difficult to give a general formula to compute the exact cycle length of the CBRM. However, for the case that the length of the individual shift registers is known, a formula for this computation can be given as follows:

Let r be the number of the feedback-shift-registers that realize the Baker-Register-Machine, σ_i (i =1, 2, …, r) the length of the shift-register i, and k the number of cascaded stages. Then the cycle length of the CBRM is given by:

$$L = \mathrm{lcm}\left(\sigma_1, \sigma_2, ..., \sigma_r\right)^k$$

As an example L for n = 256, k = 10, π ={4, 4, 8}. We get L = 622440^{10} $\approx 8.7 \cdot 10^{57}$. Such a length is enough for many practical applications.

7 Conclusion

In this paper, we propose a new pseudo random generator based on the generalized discrete Baker transformation, which has good properties with respect to speed and security.

It can be demonstrated that the CBRM has good statistical properties as required in cryptography.

In the future, we will investigate further facts concerning cryptographic security (e.g. resistance against state identification attacks).

CBRM's have been simulated and tested by VHDL (hardware) and JAVA™ (software) implementation.

However, to evaluate the possibility for the application of the Baker-transformation in stream ciphering further cryptological research is needed.

Note: This paper is a part of the progressing PhD thesis of the first author.

References

1. Stephen Wolfram, "Cryptography with cellular automata", In Advances in Cryptology – Crypto'85, Lecture Notes in Computer Science vol. 0218, pp. 429-432, Springer-Verlag, Berlin, 1985.
2. Franz Pichler, Josef Scharinger, "Ciphering by Bernoulli-Shifts in Finite Abelian Groups", Contributions to General Algebra (ed. G. Pilz), Hölder-Pichler-Tempsky, pp. 249-256, Wien, 1995.

3. Josef Scharinger, “Experimentelle harmonische Anaylse von Bäcker-dynamischen 2D Systemen und ihre Anwendung in der Kryptographie“, PhD thesis, Johannes Kepler Universität Linz, 1994.
4. Josef Scharinger, Franz Pichler, “Bernoulli-Chiffren“, Elektrotechnik und Informationstechnik (e&i), 111. Jg, 1994, Heft 11, pp. 576-582.
5. W. Feller, “An Introduction to Probability Theory and Its Applications”, pp. 242-243, John Wiley, New York, 1957.
6. N. J. A. Sloane, ”Encrypting by Random Rotations“, Cryptography (ed. Thomas Beth) , Lecture Notes in Computer Science 149, pp. 71-128.
7. Dieter Gollmann, “Kaskadenschaltungen taktgesteuerter Schieberegister als Pseudozufallszahlengeneratoren“, PhD thesis, Johannes Kepler Universität Linz, VWGÖ-Verlag, Wien, 1986.
8. Bruce Schneier, ”Applied Cryptography, Protocols, Algorithms and Source Code in C, Second Edition“, John Wiley and Sons, pp. 445-446, 1995.