A Pseudorandom Bit Generator Based on Block Upper Triangular Matrices

Rafael Álvarez, Joan–Josep Climent, Leandro Tortosa, and Antonio Zamora

Departament de Ciència de la Computació i Intel·ligència Artificial. Universitat d'Alacant, Campus de Sant Vicent, Ap.Correus 99, E–03080, Alacant, Spain.
afa@afaland.com {jcliment,tortosa,zamora}@dccia.ua.es

Abstract. The popularity of the Web has created a great marketplace for businesses to sell and showcase their products increasing the need for secure Web services such as SSL, TLS or SET. We propose a pseudorandom bit generator that can be used to create a stream cipher directly applicable to these secure systems; it is based on the powers of a block upper triangular matrix achieving great statistical results and efficiency.

1 Introduction

A pseudorandom generator [4] is a deterministic algorithm that takes a random sequence of bits of length k, called seed, and generates a sequence of bits of length l, the pseudorandom sequence, being l very large compared to k. The output sequence is not really random, it is simply generated in such a way that it cannot be distinguished from a real random sequence. The size of the seed must be such that 2^k is big enough to prevent successful exhaustive key space search attacks. Also, the period of the sequence must be larger than l; otherwise, the sequence would repeat, not appearing as random anymore. Our proposal is a new pseudorandom bit generator that can be used as a stream cipher directly (a Vernam cipher), which could then be the private key cryptosystem of any Web security system such as SSL, TLS or SET; or be the base to create more sophisticated cryptographic algorithms.

2 Description of the Pseudorandom Bit Generator

Our generator is based on the powers of block upper triangular matrices defined over $\mathbb{Z}_p$, with p prime. Consider matrix M defined as

$$M = \begin{bmatrix} A & X \\ O & B \end{bmatrix}, \tag{1}$$

where A is an r × r matrix, B is an s × s matrix, X is an r × s matrix and O denotes the s × r zero matrix.

The following result is the base of the pseudorandom generator.

J.M. Cueva Lovelle et al. (Eds.): ICWE 2003, LNCS 2722, pp. 299–300, 2003.

Table 1. Statistical test results

Length	Monobit	Serial	Poker	Runs	Autocorrelation	Linear Complexity
$2{\cdot}10^4$	0.012	1.579	243.1	8.441	0.800	10001
$2{\cdot}10^5$	1.095	1.451	239.1	26.550	0.789	100000
$2{\cdot}10^6$	0.814	3.313	207.2	37.590	0.807	1000000

Theorem 1. *Let M be the matrix given in equation (1). Taking h as a nonnegative integer and if* $0 \le t \le h$ *then*

$$M^h = \begin{bmatrix} A^h & X^{(h)} \\ O & B^h \end{bmatrix}, \; \mathrm{X}^{(\mathrm{h})} = \begin{cases} 0 & if\ h = 0 \\ A^t X^{(h-t)} + X^{(t)} B^{h-t} & if\ h \ge 0 \end{cases}$$

To obtain the pseudorandom bit sequence, we build A and B using primitive polynomials (see [5]) and choose randomly X, the seed of the sequence. From theorem 1 we have a succession of matrices $X^{(h)}$, for h = 2, 3, . . ., adding all elements of each matrix we compute a new element $x^{(h)}$, for h = 2, 3, . . ., in $\mathbb{Z}_p$, from which we take the least significant bit to conform the output sequence. The period of the sequence is determined by the least common multiple of the periods of A and B (see [5]).

3 Results

The algorithm has been checked with five different statistics: monobit, serial, poker, runs, and autocorrelation (see [4]); and with the computation of the linear complexity [1, 3]. In table 1 we can see that the results are particularly good.

4 Conclusions

Using primitive polynomials to generate the diagonal blocks and, taking very small primes as well as small matrix sizes, we can produce very efficiently bit sequences with very high periods, great statistical properties and high linear complexities.

References

1. Berlekamp, E. R.: Algebraic Coding Theory. McGraw Hill, New York (1968)
2. Freier, A. O., Karlton, P., Kocher, P. C.: The SSL Protocol, Version 3.0. Internet Draft, Netscape, March (1996)
3. Massey, J. L.: Shift-Register Synthesis and BCH Decoding. IEEE Transactions on Information Theory, 15 (1969) 122–127
4. Menezes, A., van Oorschot, P., Vanstone, S.: Handbook of Applied Cryptography. CRC Press, Boca Raton, FL,(2001)
5. Odoni, R. W. K., Varadharajan, V., Sanders, P. W.: Public Key Distribution in Matrix Rings. Electronic Letters, 20 (1984) 386–387