A New Random Number Generator

Subhash Kak

I investigated the cryptographic properties of d-sequences many years ago in a series of papers [1-3]. The binary d-sequence is generated by means of the algorithm:

$$a(i) = 2^i \bmod p \bmod 2 \qquad (1)$$

where p is a prime number (for details, see [1-3]). The maximum length (period p-1) sequences are generated when 2 is a primitive root of p. When the binary d-sequence is of maximum length, the bits in the second half of the period are the complements of those in the first half.

It is easy to generate d-sequences, which makes them attractive for many engineering applications.

It was shown in [2] that it is easy to find i given $\log_2 p$ bits of a(i). Therefore, d-sequences cannot be directly used in random number generator (RNG) applications.

However, by adding together two or more different d-sequences (obtained by using primes p_1, p_2, …) mod 2, we are able to introduce non-linearity in the generation process, and the resulting sequence becomes a good candidate for use as random sequence.

For convenience, we will now consider only terms in the sum. If the individual sequences are maximum length, then the period of the sum will be

$$\text{lcm } (p_1\text{-}1)\ (p_2\text{-}1) \qquad (2)$$

But for randomly chosen primes we do not know if the starting number is a primitive root, therefore, the actual period would be a divisor of lcm $(p_1\text{-}1)\ (p_2\text{-}1)$.

A power exponent

Mathematically, let the seed by equal to S, which is relatively prime to each p_i, and the order of S does not divide $(p_i\text{-}1)$ for all i. Then the power-exponent RNG generates bits according to the algorithm:

$$\begin{aligned} a(0) &= S \bmod p_1 \bmod 2 \oplus S \bmod p_2 \bmod 2 \\ a(1) &= S^2 \bmod p_1 \bmod 2 \oplus S^2 \bmod p_2 \bmod 2 \\ a(2) &= S^4 \bmod p_1 \bmod 2 \oplus S^4 \bmod p_2 \bmod 2 \qquad (3) \\ &\ldots\ldots \end{aligned}$$

where $\oplus$ means modulo 2 addition.

An even stronger RNG would be one where the two terms are added to different powers as shown below:

$$a(0) = S \bmod p_1 \bmod 2 \oplus S^k \bmod p_2 \bmod 2$$
$$a(1) = S^2 \bmod p_1 \bmod 2 \oplus S^{2k} \bmod p_2 \bmod 2$$
$$a(2) = S^4 \bmod p_1 \bmod 2 \oplus S^{4k} \bmod p_2 \bmod 2 \qquad (4)$$
$$\ldots\ldots$$

Since the seed S would be randomly chosen, the period of the sequence will be less than lcm $(p_1\text{-}1)$ $(p_2\text{-}1)$ if it is not a primitive root simultaneously of p_1 and p_2.

One may replace p_1 and p_2 by n_1 and n_2 that are product of primes. For better security, the two primes should each be congruent to 3 mod 4.

Exponents other than 2 of generators (3) and (4) may also be used.

References

1. Kak, S., and Chatterjee, A., 1981. On Decimal Sequences. *IEEE Transactions on Information Theory*, IT-27: 647 – 652.

2. Kak, S., 1985. Encryption and error-correction coding using D sequences. *IEEE Transactions on Computers*, C-34: 803-809.

3. Kak, S., 1987. New results on d-sequences. Electronics Letters, 23: 617.

4. Mandhani, N., and S. Kak. 2005. Watermarking using decimal sequences. *Cryptologia.* 29: 50-58; http://arxiv.org/abs/cs.CR/0602003

February 5, 2006