文章编号: 1006-4710(2001)01-0043-03

离散对数伪随机序列的性质分析

王尚平[1], 王 晖[2], 王晓峰[1], 王育民[3]
(1.西安理工大学理学院,陕西 西安 710048; 2.西安仪表工业学校;
3.西安电子科技大学 ISN 国家重点实验室,陕西 西安 710071)

摘要: 提出了顺序离散对数伪随机数生成器的概念,给出了该随机数生成器生成序列的一些重要性质。利用这些性质,分析了一般离散对数伪随机数生成器生成序列的对应性质,揭示了这类序列的一些内在性质。给出了 half(·)和 lb(·)二者在离散对数伪随机数生成器上的内在关系。利用这些关系可分析离散对数伪随机数生成器的性质和规律。

关键词: 离散对数问题; 伪随机数生成器; 密码体制
中图分类号: TN918.4 **文献标识码**: A

An Analysis of Pseudo-Random Sequences Base on DL Problem

WANG Shang-ping[1], WANG Hui[2], WANG Xiao-feng[1], WANG Yu-min[3]
(1.Xi'an University of Technology, Xi'an 710048, China;
2.Xi'an School of Industrial Meter; 3.National Key Lab. On ISN, Xidian University)

Abstract: A serial pseudo-random sequences generator based on discrete logarithm is proposed, some of its characteristics is discussed. General pseudo-random sequences generator based on discreet logarithm are analyzed. The relation between function half(·) and lb(·) on discrete logarithm is presented.

Key words: discrete logarithm problem; pseudo-random sequence generator; cryptography

在现代密码学中,离散对数(Discrete Logarithm,简记 DL)问题的困难性是许多密码体制安全性基础。如 Diffe-Hellman 的密钥交换协议,ElGamal 密码体制,美国国家标准技术局(NIST)公布的数字签名标准 DSS 等。

群 G 上离散对数(DL)问题是指任意给定 $a,b\in G$,求一个 $x\in Z$,使 $a^x=b$,或证明这样的 x 不存在。若 x 存在,最小非负正整数解 $x=\log_a b$ 称为 b 关于基 a 的离散对数。

在模 p 乘法群 $G=GF(p)^*$ 上,求解 DL 问题的算法有 Silver-Pohlig-Hellman 法[2],该方法要求 $p-1$ 是光滑的,即 $p-1$ 的分解式 $p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}$ 中 $p_1,p_2,\cdots,p_k$ 均为小素数;有 Shank 的 Baby-Step-Giant-Step 法,该方法所需时间为 $O(\sqrt{p})$,当 p 充分大时,计算上实际不可行;还有指数计算(Index-Calculus)法[5],其预先计算所需时间为 $O(e^{(1+o(1))\sqrt{\ln p\ln\ln p}})$,对每个 DL 问题计算所需的时间为 $O(e^{(1/2+o(1))\sqrt{\ln p\ln\ln p}})$,该方法所需的时间也是亚指数的。还有其他的方法,但这些方法都未能在多项式时间内求解 DL 问题。故 DL 问题至今仍被认为是个困难性问题。

随机数在密码学上有重要意义。在分组密码中,加密(解密)密钥是随机数。在流密码中,密钥序列是随机数序列。在公钥密码体制实际应用中,最优非对称加密填充(OAEP)也需要随机数。在密码协议中,为防止重放攻击,需要保持信息的新鲜性,需要及时加入随机数 Nonce 及 salt 等。如何快速有效地产生伪随机数是密码学研究的重要问题之一。

收稿日期: 2000-05-29
基金项目: 国家自然科学基金资助项目(60073025),陕西省教育厅自然科学基金资助项目(00JK266)。
作者简介: 王尚平(1963-),男,西安理工大学副教授,西安电子科技大学博士研究生,研究方向为信息保密理论与电子商务的安全性。

RSA 伪随机数生成器是基于大整数分解的困难性,BBS 伪随机数生成器是基于二次剩余问题的困难性。基于 DL 问题的困难性,Blum-Micali 提出了离散对数伪随机数生成器。利用该生成器可产生二元密钥流序列,结合公钥密码体制利用数字信封技术,可构造安全高效的密码体制。

本文提出顺序离散对数伪随机数生成器的概念,给出该序列的一个重要性质。利用顺序离散对数伪随机数生成器的性质,分析一般离散对数伪随机数生成器的对应性质,揭示这类序列的一些内在性质。

1 离散对数伪随机数生成器

利用数学问题的困难性构造伪随机序列是密码学的一个重要方法。Blum-Micali 基于 DL 问题的困难性,提出了下述离散对数伪随机数生成器[1]。

设 p 是 k bit 的素数,α是 $GF(p)^*$上一个本原元。任取密钥种子 $s_0 \in GF(p)^*$,这里 $GF(p)^*$即 Z/pZ乘法群。令:

$$s_i \equiv \alpha^{s_{i-1}} \bmod p \quad (i = 1, 2, \cdots) \tag{1}$$

若 $s_i < p/2$, 则 $z_i = 0$; 若 $s_i > p/2$, 则 $z_i = 1$。

记 $f(s_0) = \{z_1, z_2, \cdots, z_l\}$,称 f 为一个(k, l) 离散对数伪随机序列生成器,以下简记 f 为 $\{z_i\}$,上述 z_i 亦可为:

$$z_i = \mathrm{half}(s_i) \quad (i = 1, 2, \cdots) \tag{2}$$

2 顺序离散对数伪随机数生成器及其性质

为了研究离散对数伪随机数生成器,首先引入顺序离散对数伪随机数生成器,记号同前。令:

$$t_i \equiv \alpha^i \bmod p \quad (i = 1, 2, \cdots) \tag{3}$$

$$\text{若 } t_i < p/2, \text{则 } a_i = \mathrm{half}(t_i) = 0; \text{ 若 } t_i > p/2, \text{则 } a_i = \mathrm{half}(t_i) = 1 \tag{4}$$

得周期为 $P-1$ 的序列,称 $\{a_i\}$为顺序离散对数生成器生成的伪随机数序列。令 b_i 是 t_i 最小比特(Least Bit),即 b_i 是 t_i 的二进制表示的最小比特位,记为:

$$b_i = \mathrm{lb}(t_i) \quad (i = 1, 2, \cdots) \tag{5}$$

得周期为 $p-1$ 的序列 $\{b_i\}$。关于序列 $\{a_i\}$与 $\{b_i\}$有下列性质(定理 1)。

定理 1 序列 $\{a_i\}$与 $\{b_i\}$具有下列关系:

$$a_i = b_{i+l} \quad (i = 1, 2, \cdots) \tag{6}$$

其中 l 满足 $\alpha^l \equiv 2 \bmod p$。

$$a_i = \mathrm{lb}(2t_i \bmod p) \tag{7}$$

对 $a_i = 0$ 及 $a_i = 1$ 两种情况分别证明如下。若 $a_i = 0$,即 $t_i < p/2$,可知 $2t_i < p$,得 $\mathrm{lb}(2t_i \bmod p) = 0 = a_i$,此时式(7)成立。又 $2t_i = 2 \cdot (\alpha^i \bmod p) \equiv \alpha^{i+l} \bmod p \equiv t_{i+l}$,可知 $b_{i+l} = \mathrm{lb}(t_{i+l}) = \mathrm{lb}(\alpha^{i+l} \bmod p) = \mathrm{lb}(2t_i \bmod p) = 0 = a_i$,此时式(6)成立。

若 $a_i = 1$,即 $t_i > p/2$,可知 $2t_i > p$,故有 $\mathrm{lb}(2t_i \bmod p) = 1 = a_i$,即式(7)成立。又同上式可得 $b_{i+l} = \mathrm{lb}(t_{i+l}) = \mathrm{lb}(\alpha^{i+l} \bmod p) = \mathrm{lb}(2t_i \bmod p) = 1 = a_i$,此时式(6)成立。

[例] 设 $p = 17$, $\alpha = 3$ 是 $GF(17)^*$的本原元,序列 $\{a_i\}$与 $\{b_i\}$的对应关系见表 1。

表 1 序列 $\{a_i\}$与 $\{b_i\}$对应关系示例

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
t_i	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1
a_i	0	1	1	1	0	1	1	1	1	0	0	0	1	0	0	0
b_i	1	1	0	1	1	1	1	0	0	0	1	0	0	0	0	1
$2t_i$	6	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2
$\mathrm{lb}(2t_i)$	0	1	1	1	0	1	1	1	1	0	0	0	1	0	0	0

注意到表 1 中 $\alpha^{14} \equiv 2 \bmod 17$,故 $l = 14$,显然有 $a_i = b_{i+14}$ $(i = 1, \cdots, 16)$,这里注意序列 $\{b_i\}$的周期是

$p-1=16$，且 $a_i=\mathrm{lb}(2^{t_i})$ $(i=1,\cdots,16)$。

3 离散对数伪随机数生成器的性质

首先分析顺序离散对数伪随机数生成器与离散对数伪随机数生成器之间关系。利用式(1)及式(3)可得：

$$s_i \equiv \alpha^{-1} \bmod p = t_{s_{i-1}} \tag{8}$$

令：

$$x_i = \mathrm{lb}(2^{s_i} \bmod p) \quad (i=1,2,\cdots) \tag{9}$$

则由定理1可得：

$$z_i = \mathrm{half}(s_i) = \mathrm{half}(t_{s_{i-1}}) = a_{s_{i-1}} = b_{s_{i-1}+l}$$

即：

$$z_i = b_{s_{i-1}+l} \quad (i=1,2,\cdots) \tag{10}$$

又：

$$z_i = b_{s_{i-1}+l} = \mathrm{lb}(\alpha^{-1+l} \bmod p) = \mathrm{lb}(2^{s_i} \bmod p) = x_i$$

即：

$$z_i = x_i \quad (i=1,2,\cdots) \tag{11}$$

综上所述，我们证明了下述定理。

定理2 关于离散对数伪随机数生成器生成的序列有下列关系：

$$z_i \triangleq \mathrm{half}(s_i) = \mathrm{lb}(2^{s_i} \bmod p) \triangleq x_i \quad (i=1,2,\cdots) \tag{12}$$

$$z_i \triangleq \mathrm{half}(s_i) = b_{s_{i-1}+l} \quad (i=1,2,\cdots) \tag{13}$$

这样，我们得到了离散对数伪随机数生成器生成序列 $\{z_i\}$ 与序列 $\{x_i\}$ 及顺序离散对数伪随机数生成器生成序列 $\{b_i\}$ 之间的一些内在关系。

4 结 语

本文通过引入顺序离散对数伪随机数生成器，并研究了其重要性质，以此为工具给出了离散对数伪随机数生成器产生序列之间的一些性质。这些性质揭示了离散对数伪随机数生成器的一些内在规律，给出了函数 $\mathrm{half}(\cdot)$ 与 $\mathrm{lb}(\cdot)$ 二者之间在离散对数伪随机数生成器上的关系。利用这些关系可分析离散对数伪随机数生成器的性质和规律。

参考文献：

[1] M Blum, S Micali. How to generate cryptographically strong sequence of pseudo-random bits[J]. SIAM Journal on Computing, 1984, 13: 850－864.

[2] S C Pohlig, M E Hellman. An improved algorithm for computing logarithms over GF(p) and its cryptography significance[J]. IEEE Transactions on Information Theory, 1978, 24: 106－110.

[3] D M Gordon, K S McCurley. Massively parallel computation of discrete logarithms[A]. Lecture Notes in Computer Science, No740[C]. Berlin: Springer, 1993. 312－323.

[4] V Shoup. Lower bounds for discrete logarithms and related problems[A]. In Advances in Cryptology-Eurocrypt '97, Lecture Notes in Computer Science, No1233[C]. Berlin: Springer, 1997. 256－266.

[5] O Schirokauer, D Weber, Th F Denny. Discrete logarithms: the effectiveness of the index calculus method[A]. A Logarithmic Number Theory-ANTS Ⅱ, Lecture Notes in Computer Science, No1122[C]. H Cohen, Editor, 1996. 223－231.

(责任编辑 韩星明 王卫勋)