σ-AND 随机数生成器

曾 光 邓依群 韩文报 范淑琴
(解放军信息工程大学信息工程学院信息研究系 郑州 450002)

摘 要 提出了一种结构简单、实现快速且周期为 2^k-1 的随机数生成器:σ-AND 随机数生成器,其中 k 为 32 的倍数。σ-AND 随机数生成器用极少的异或、循环移位、与等计算机基本指令即可实现,软硬件实现效率高。同时其输出序列具有良好的伪随机性,可以作为适合软件快速实现的序列密码的驱动部分使用。

关键词 σ-LFSR,随机数生成器,快速软件实现,序列密码

σ-AND Random Number Generators

ZENG Guang DENG Yi-qun HAN Wen-bao FAN Shu-qin
(Department of Information Research, PLA Information Engineering University, Zhengzhou 450002, China)

Abstract A high efficient σ-AND random number generators (RNGs) in simple structure with period 2^k-1 was presented, where k is the multiple of 32. Software implementation of σ-AND RNGs only requires few fundamental instructions, such as XOR, Circular Rotation, AND operations. Meanwhile due to the good pseudo randomness of their output sequences, σ-AND RNGs may be used as a primitive building block in software oriented stream cipher.

Keywords σ-LFSR, Random number generator, Fast software implementation, Stream cipher

1 引言

序列密码是移动通信和网络安全领域的主流加密技术之一,研究开发高强度、高效率的序列密码是人们一直追求的目标,特别是在电子商务、网上银行等对安全性和效率要求较高的系统中,对序列密码算法的要求是很高的。近年来,随着计算机技术的飞速发展,适合软件快速实现的序列密码算法的研究备受关注。欧洲 eSTREAM 序列密码征集[1]将软件实现效率作为算法设计标准之一。在所征集到的 34 个序列密码算法中有 22 个是以软件快速实现作为设计目标的,可以看出设计适合软件快速实现的序列密码已经成为一个热点问题。值得注意的是,在各种适合软件快速实现的序列密码算法中,例如 Mugi[2], Sober[3], Snow[4], Turing[5], Rabbit[6], Helix[7], ABC[8]等,都采用了基于字的设计方式。由于每次输出的是一个字而不是一个比特,同时基于字的设计不仅可以避免大量的比特操作,还能充分利用现代处理器提供的字上的数值运算和逻辑运算,这使得软件实现效率大幅度提高。

设计适合软件快速实现的序列密码必须设计与之适应的源驱动部分。源驱动部分是序列密码的基础,为序列密码提供良好的初始伪随机序列,此部分可以看作为一个随机数生成器。任何随机数生成器只要具有输出序列伪随机性好、软件实现效率高的特点,就可以作为适合软件快速实现的序列密码的驱动部分。基于字的线性反馈移位寄存器(字 LFSR)和 T-函数[9](T-function)都是现代序列密码中常用的随机源部件。Sober, Snow, Turing, ABC 中使用了字 LFSR,而 TSC[10]使用了 T-函数作为其驱动部分。

设计结构简单、具有良好伪随机性的随机数发生器对现代序列密码的设计具有重要意义。结构简单则意味实现高效,同时也可能导致输出序列伪随机性不好。如何兼顾这两者是设计的难点之一。在处理此问题上,Xorshift 随机数发生器[11]是一个优秀的算法。本文设计的 σ-AND 随机数生成器事实上是 σ-LFSR[12,13]的特例,其设计部分采用了 Xorshift 的设计思想。σ-AND 是一个非常简单的操作:先对操作数同一个常数做与,再对操作数循环移位的结果进行异或。由于与操作和循环移位操作都是现代 CPU 的基本指令,因此 σ-AND 操作可以高效实现。σ-AND 随机数生成器重复利用 σ-AND 操作就可以达到周期 2^k-1,其中 k 为 32 的倍数。例如用 w,x,y,z 表示 4 个 32 比特随机种子,利用 3 个 σ-AND 操作即可得到周期为 $2^{128}-1$ 的字长为 32 比特随机数,其 C 程序表示如下:

$\text{tmp} = \sigma^{17}(x);\ x = y;\ y = z;\ z = w$

$w = \sigma^{6}(w) \hat{}\ ((\text{tmp}\ \&\ 0\text{xffffffff}) \hat{}\ \sigma^{3}(\text{tmp}))$

其中 $\sigma(x)$是对操作数 x 进行一次循环右移操作。这样一个 σ-AND 随机数生成器的软件效率非常高,可以在 3.0GHz 的 Pentium IV CPU 上达到 11.06Gbit/second,并且输出序列具有良好的随机性,通过了 Diehard[14]软件的绝大部分随机性测试。

到稿日期:2008-01-14 本文受国家自然科学基金 (No. 90704003),国家 973 重点研究发展规划 (No. 2007CB807902),国家 863 高技术研究发展计划 (No. 2006AA01Z425)资助。

曾 光 博士研究生,CCF 会员,主要研究方向为序列密码设计与分析;**邓依群** 教授,主要研究方向为计算机软件及应用;**韩文报** 教授,博士生导师,主要研究方向为密码学、网络安全;**范淑琴** 教授,硕士生导师,主要研究方向为密码学及其应用。

2 基本理论

设 $\beta\in F_2^{1\times m}$ 是一个 m 维的行向量，其分量取自二元域 $F_2=\{0,1\}$ 中，用 β 表示随机数生成器的种子。在计算机实现时，一般选取 $m=32$ 或 64，这样 β 恰好是一个机器字。设 $T\in F_2^{m\times m}$ 是 F_2 上的一个 $m\times m$ 级非奇异的矩阵，则一个字长为 m 比特的伪随机序列 $(x_j)_{j\geqslant 0}$ 如下：

$$x_j=\beta T^j \tag{1}$$

设初态为 $x_0=\beta$，当 $j\geqslant 1$ 时有 $x_j=x_{j-1}T$。一个有限状态的随机数生成器产生的序列一定是最终周期序列。在具体应用时，希望任意两次使用的序列存在重叠的概率应当可以忽略不计，这就必须要求序列有大的周期。关于序列的周期有如下结论。

定理 1 对于式(1)定义的随机数生成器，输出序列达到最大周期 2^m-1 的充要条件是矩阵 T 在一般线性群 $GL_m(F_2)$ 中的阶为 2^m-1。

证明：设序列的周期为 t_1，矩阵 T 的周期为 t_2。对任意的 $\beta\neq 0$，由于序列周期为 t_1，因此有 $\beta T^{t_1}=\beta$。则 $T^{t_1}+E$ 的解空间为全空间，所以必有 $T^1+E=0$，即 $T^{t_1}=E$，故 $t_2\mid t_1$。反之，若 T 的阶为 t_2，则对任意 $j\geqslant 0$ 有 $x_j=x_jT^{t_2}=x_{j+t_2}$。必有序列的周期 $t_1\mid t_2$，从而有 $t_1=t_2$ 成立，特别地取 $t_1=2^m-1$，定理成立。

由定理 1 可知，若要式(1)定义的随机数发生器达到最大周期，必须对 T 的阶有特殊限制。然而对于向量 β 和一般的非奇异矩阵 T，向量乘矩阵的运算 $\beta\cdot T$ 是比较费时的操作。但如果对 T 的形式有一定的要求，$\beta\cdot T$ 也可高效实现。

设 σ 是一个 F_2 上 $m\times m$ 的矩阵如下：

$$\sigma=\begin{pmatrix}0&1&0&\cdots&0\\0&0&1&\cdots&0\\\vdots&\vdots&\vdots&\ddots&\vdots\\0&0&0&\cdots&1\\1&0&0&\cdots&0\end{pmatrix}_{m\times m} \tag{2}$$

σ 作用在向量 β 上是对 β 循环右移一位，循环左移一位可以用 σ^{m-1} 来实现。设 $\alpha=(a_1,a_2,\cdots,a_m)$ 是 F_2 上一个 m 维向量，设 AND 是 F_2 上 $m\times m$ 的矩阵如下，事实上 AND 作用在 β 上即是向量 α 和 β 做对位与运算。

$$AND_\alpha=\begin{pmatrix}a_1&0&\cdots&0&0\\0&a_2&\cdots&0&0\\0&0&\cdots&0&0\\\vdots&\vdots&\ddots&\ddots&\vdots\\0&0&\cdots&0&a_m\end{pmatrix}_{m\times m}, \tag{3}$$

定义一个 σ-AND 操作为先将操作数和 α 做与运算，再将此结果和对操作数循环移 v 位的结果异或，即 $T=AND\alpha+\sigma^v$。一个 σ-AND 操作非常简单快速，C 语言描述为

$(\beta\&\alpha)\ \hat{}\ (\beta>>v)\ \hat{}\ (\beta<<(m-v))$

σ-AND 操作简单，可以重复利用，得到最大周期序列。例如选取 $T=(AND\alpha+\sigma^v)(AND\gamma+\sigma^u)$ 等，其中 γ 是一个 m 维的行向量。对于选定的一个矩阵 T，首先要判断行列式不等于 0，以确定是一个非奇异矩阵，然后计算矩阵的阶是否达到 2^m-1。一个初步的筛选方法是将矩阵 T 连续平方 m 次，如果结果不等于 T，则 T 的阶不可能是 2^m-1。由于矩阵 T 的特殊选取，计算两个 σ-AND 矩阵的乘积是容易的。例如将矩阵 $(AND\gamma+\sigma^u)$ 的每一行看成一个机器字，则 $(AND\alpha+\sigma^v)(AND\gamma+\sigma^u)$ 的结果是将 $(AND\gamma+\sigma^u)$ 中的行循环下移 v 行，再加上 α 中 1 所在的行。这种判断方式非常迅速，可以在几分钟之内将筛选出所有可能达到最大周期的矩阵 T。在初步筛选后，再利用下面定理确定是否为最大阶矩阵。

定理 2 若式(1)定义的输出序列达到最大周期 2^m-1，其充要条件是矩阵 T 的特征多项式 $f(x)=|xE-T|$ 为 F_2 上 m 次的本原多项式。

证明：设 $p(x)=\sum_{i=0}^d h_ix^{d-i}\in F_2[x]$ 为矩阵 T 的极小多项式，其中 $h_0=1$。则有

$$\sum_{i=0}^d h_iT^{d-i}=0 \tag{4}$$

在式(4)两边同乘以 βT^{j-d}，则有

$$\sum_{i=0}^d h_i\beta T^{j-i}=0,\text{对 } j\geqslant d \tag{5}$$

由于 $x_j=\beta T^j$，因此式(5)等价有

$$\sum_{i=0}^d h_ix_{j-i}=0,\text{对 } j\geqslant d \tag{6}$$

此式说明式(1)定义的序列可以看成 m 维 F_2 上的线性递归序列，$p(x)$ 是任意一个序列的特征多项式。若式(1)定义的序列达到最大周期 2^m-1，再由 $p(x)$ 最大次数为 m，可知 $p(x)$ 一定是 F_2 上 m 次本原多项式。再由哈密尔顿-凯莱定理可知 $f(x)\mid p(x)$，故有 $f(x)=|xE-T|$ 为 F_2 上 m 次的本原多项式。

3 σ-AND 操作的应用

本节主要讨论单字($m=32$ 或 64)上的 σ-AND 随机数生成器。首先选取 $T=(AND\alpha+\sigma^v)$ 来寻找最大周期序列，然而无论如何选取 α 和 v 都不存在符合要求的矩阵 T。于是考虑 $T=(AND\alpha+\sigma^v)(AND\gamma+\sigma^u)$ 的情形，此时找到了大量的满足要求的矩阵。为了实现简单，要求 α 和 γ 中有一个为零向量，这样可以减少一个与操作。由于与参数的变化数量巨大，在 $m=32$ 时就有 2^{32} 种可能取值。表 1 中选取的与参数 α 完全由其 Hamming 重量决定，即如果与参数的重量为 w_α，则与参数为

$$\alpha=(0,\cdots,0,\underbrace{1,1,\cdots,1}_{w\text{个}})\in F_2^m \tag{7}$$

表 1 共列出 34 个三元组 (w_α,v,u)，每个三元组表示一个阶数为 $2^{32}-1$ 的 32×32 级的矩阵 $T=(AND\alpha+\sigma^v)\sigma^u$。

表 1 部分 32 比特 σ-AND 随机数生成器

29,1,4	28,1,9	9,1,14	18,1,17	14,1,19	25,1,24	8,1,25
30,1,25	30,1,27	18,3,7	5,3,10	7,3,10	16,3,10	17,3,10
21,3,22	26,3,23	26,3,27	21,5,4	25,5,4	3,5,6	13,5,6
26,7,1	18,7,3	16,7,5	24,7,5	27,9,2	28,11,17	13,11,26
17,11,26	26,13,21	15,13,22	25,13,26	22,15,3	25,15,7	

在大量的试验数据中可以发现达到最大周期的矩阵 $T=(AND\alpha+\sigma^v)(AND\gamma+\sigma^u)$ 是成对出现的，下面的定理解释了原因。

定理 3 若矩阵 $T=(AND\alpha+\sigma^v)(AND\gamma+\sigma^u)$ 达到最大周期，则矩阵 $T_1=(AND\alpha+\sigma^{m-v})\cdot(AND\gamma+\sigma^{m-u})$ 和 $T_2=(AND\gamma+\sigma^u)(AND\alpha+\sigma^v)$ 都达到最大周期。

证明：若有可逆矩阵 P，使得 $H=PTP^{-1}$，则称 T 和 H 是相似的，易证相似矩阵有相同周期。设 P 为反对角线都为 1，其余为 0 的 $m\times m$ 级矩阵。由 $PTP^{-1}=P(AND\alpha+\sigma^v)P^{-1}\cdot P(AND\gamma+\sigma^u)P^{-1}=(AND\alpha+\sigma^{m-v})\cdot(AND\gamma+\sigma^{m-u})=T_1$，可知 T 和 T_1 相似。设 $A=(AND\alpha+\sigma^v)$，$B=(AND\gamma+$

σ^u)，由于矩阵 T 达到最大周期，因此 $|T|\neq 0$，故 $|A|\neq 0$，所以 A^{-1} 存在。由于

$$BA = (A^{-1}A)\cdot BA = A^{-1}\cdot(AB)\cdot A$$

可知 AB 和 BA 相似。

由定理 3 可知，表 1 中任意一个三元组 (w_α, v, u) 变化成 $(w_\alpha, m-v, m-u)$ 还是一个最大周期矩阵，这样又可以得到 34 个最大周期三元组，共计 68 个。再将这 68 个 $T=(AND\alpha+\sigma^v)\sigma^u$ 变成 $T=\sigma^u(AND\alpha+\sigma^v)$ 的形式，又可得到 68 个最大周期矩阵。这 136 个矩阵恰好是在 $m=32$ 的情形下，矩阵 $T=(AND\alpha+\sigma^v)(AND\gamma+\sigma^u)$ 中有一个与参数为 0 的所有最大周期矩阵。当两个与参数都不为 0 时，存在大量的最大周期矩阵。仍限定与参数由重量决定，在实际搜索中共找到 13096 个由 2 个 σ-AND 操作构成的最大周期矩阵。表 2 中列举了部分结果，表示形式为四元组 $(w_\alpha, v, w_\gamma, u)$。

表 2　与参数不为零的部分结果

3,1,16,1	31,1,2,12	9,1,3,16	28,2,5,17	1,3,19,1
16,3,24,1	19,4,3,11	26,5,1,4	9,7,27,23	1,9,2,17
20,10,6,27	18,11,11,11	11,12,20,13	29,13,1,6	1,14,12,9
16,15,15,8	15,16,26,11	9,17,2,2	3,18,28,11	16,19,1,2
22,20,20,3	28,21,24,2	1,22,4,23	16,23,21,8	14,24,3,3
30,25,30,3	9,26,13,5	13,27,29,2	13,28,6,7	2,29,21,5
16,29,21,5	11,29,13,10	19,29,23,10	19,30,28,9	7,30,9,11
18,30,3,11	1,30,16,13	22,30,31,13	16,30,7,15	1,30,6,17
15,31,8,9	1,31,3,10	20,31,20,9	30,31,5,10	2,31,8,12
4,23,30,6	22,21,2,23	29,10,22,29	2,12,18,7	3,10,1,31

当 $m=64$ 时，共找到 932 个 64×64 级的矩阵 $T=(AND\alpha+\sigma^v)(AND\gamma+\sigma^u)$ 达到最大周期，其中 α 或 γ 为 0。表 3 列举了 233 个最大周期矩阵，再经过定理 3 中的由矩阵 T 到 T_1 和 T 到 T_2 的变换可以得到所有 932 个有 1 个与参数为 0 的矩阵。

表 3　部分 64 比特 σ-AND 随机数生成器

59,1,6	35,1,16	22,1,17	62,1,23	29,1,28	47,1,28	24,1,29
38,1,29	48,1,29	63,1,34	14,1,35	59,1,36	36,1,41	54,1,51
42,1,55	24,1,57	46,1,57	30,1,59	17,1,60	49,1,60	27,3,12
16,3,15	36,3,17	58,3,19	54,3,25	43,3,26	43,3,28	61,3,28
55,3,34	38,3,35	50,3,35	49,3,38	63,3,38	15,3,40	61,3,42
56,3,43	45,3,48	18,3,51	30,3,55	30,3,57	29,3,62	45,3,62
30,3,63	35,5,4	39,5,4	24,5,7	32,5,7	41,5,10	58,5,11
60,5,13	51,5,18	32,5,23	34,5,23	38,5,23	40,5,23	44,5,23
41,5,24	28,5,39	28,5,41	63,5,42	22,5,49	44,5,49	49,5,52
61,5,52	27,5,56	18,7,3	61,7,4	56,7,11	15,7,16	21,7,16
50,7,19	54,7,19	62,7,19	62,7,23	60,7,31	59,7,34	27,7,42
63,7,46	58,7,47	51,7,62	59,7,62	58,9,1	49,9,4	53,9,4
31,9,22	35,9,22	54,9,31	58,9,35	14,9,37	22,9,37	63,9,50
39,9,62	47,11,2	32,11,3	61,11,12	29,11,22	33,11,22	24,11,25
32,11,25	45,11,30	51,11,34	16,11,35	20,11,35	32,11,41	62,11,47
63,11,54	47,11,60	46,11,61	37,11,62	22,13,7	26,13,7	34,13,9
50,13,9	15,13,24	39,13,24	41,13,24	36,13,37	25,13,44	52,13,49
56,13,57	63,13,58	60,13,59	27,13,60	22,13,61	40,13,63	42,13,63
37,15,2	53,15,2	16,15,3	24,15,3	41,15,6	45,15,6	35,15,8
47,15,8	55,15,8	61,15,20	24,15,23	28,15,23	59,15,46	52,15,51
63,15,62	55,17,2	63,17,2	31,17,12	39,17,12	20,17,21	32,17,21
40,17,35	57,17,40	23,17,56	39,17,56	62,17,59	63,19,6	54,19,33
55,19,40	55,19,42	61,19,48	46,19,61	24,19,63	49,21,4	20,21,5
63,21,10	22,21,13	38,21,13	56,21,13	20,21,17	32,21,17	52,21,31
51,21,36	46,21,37	62,21,41	56,21,45	13,23,2	15,23,2	60,23,3
31,23,6	39,23,6	57,23,10	63,23,14	60,23,15	62,23,15	13,23,16
15,23,16	35,23,16	37,23,16	56,23,19	59,23,20	57,23,28	49,23,54
61,23,60	16,25,1	52,25,3	58,25,3	16,25,13	36,25,13	54,25,17
63,25,18	60,25,19	45,25,22	30,25,45	56,25,45	54,25,53	59,25,54
49,25,58	60,25,63	47,27,4	56,27,13	63,27,22	58,27,33	62,27,45
40,27,55	51,27,58	61,29,18	61,29,22	63,29,26	61,29,28	61,29,36
58,29,39	31,29,44	51,29,44	40,29,47	56,29,55	57,29,60	61,31,10
56,31,11	63,31,30	54,31,35	60,31,39	53,31,46	59,31,48	61,31,48
54,31,57	46,31,59					

在上述所有的 σ-AND 随机数生成器中，挑选若干个用 Diehard[14] 随机性测试软件测试。例如选取表 3 中第 2 行第 3 列数据 $T=(AND_\alpha+\sigma)\sigma^{34}$，其中 α = 0x7fff ffff ffff ffff。此 σ-AND 机数生成器可输出周期为 $2^{64}-1$ 的 32 比特序列。Diehard 软件共进行 17 种随机性测试，此 σ-AND 随机数生成器输出序列通过了除矩阵秩检测之外的所有测试。矩阵秩测试是将输出序列排成一个固定维数的矩阵，将矩阵的秩看作随机变量进行测试。由于 σ-AND 随机数生成器的状态更新方式由矩阵 T 唯一决定，故前后状态之间必然存在线性关系，所以未通过此种检测。但这并不影响 σ-AND 随机数生成器的使用，因为若作为随机数使用则一次不会输出大量连续的随机数；若作为序列密码的驱动部分使用，则输出序列已经提供了良好的伪随机性，驱动部分的线弱点可以由密码的非线性部分掩盖。虽然只对少数 σ-AND 随机数生成器进行了随机性测试，但从测试结果来看，可以相信表中的 σ-AND 随机数生成器具有良好随机性。

4　大周期 σ-AND 随机数生成器构造

在实际应用中周期为 $2^{32}-1$ 或者 $2^{64}-1$ 的序列已经不能够满足现代序列密码的设计需求，这就要提供具有更大周期的序列。由于现代计算机的机器字都是 32 比特或 64 比特，因此上节的 σ-AND 操作仍然适用。可以利用 LFSR 的设计方法来设计具有更大周期的 σ-AND 随机数生成器。例如设 x,y,z,w 为 4 个 32 比特的字，选取矩阵 T 如下：

$$T=\begin{pmatrix} 0 & 0 & 0 & A \\ E & 0 & 0 & B \\ 0 & E & 0 & C \\ 0 & 0 & E & D \end{pmatrix}_{128\times 128} \tag{8}$$

其中 A,B,C,D 为 32×32 级的矩阵且可由一个或两个 σ-AND 操作完成，则有

$$(x,y,z,w)T = (y,z,w,xA + yB + zC + wD)$$

可用此种方式得到大量周期为 $2^{128}-1$ 的序列。更一般的情况，选取 T 如下：

$$T=\begin{pmatrix} 0 & 0 & 0 & A_1 \\ E & 0 & 0 & A_2 \\ \vdots & \ddots & \cdots & \vdots \\ 0 & 0 & E & A_r \end{pmatrix}_{m\times m} \tag{9}$$

其中 $A_1,\cdots,A_r$ 为 r 个 $m\times m$ 矩阵，且由一个或两个 σ-AND 操作构成。这种方式可以构造周期为 $2^{rm}-1$、字长为 m 的伪随机序列。

用上述方法在选取 $A_i(1\leqslant i\leqslant r)$ 时并不一定要求所有 A_i 都由 σ-AND 操作构成，也可选取零矩阵，这样可以进一步减少操作，从而提高效率。在所有 $m=32$、级数等于 4 的 σ-AND 随机数生成器中，最少可用 3 个 σ-AND 操作构成最大周期序列，其中有两个与参数为 0。表 4 列出了由式(8)定义的达到最大周期的部分结果，其中 $A=\sigma^e$，$B=C=0$，$D=(AND\alpha+\sigma^v)\sigma^u$，用四元组 (e,w_α,v,u) 表示矩阵 T。

表 4　部分大周期 32 比特 4 级 σ-AND 随机数生成器

1,20,7,8	1,7,12,25	2,10,16,25	3,7,9,31	3,21,22,3
4,7,5,2	5,19,11,23	6,16,9,11	7,25,3,25	8,6,20,29
9,20,19,8	10,20,9,13	11,12,1,12	12,8,6,1	13,27,3,19
14,7,3,18	15,21,6,7	16,22,7,19	17,7,5,29	18,14,1,1
19,8,1,14	20,13,1,4	21,25,1,1	22,7,1,14	23,19,2,23
24,4,1,5	25,21,1,31	25,5,2,27	25,16,3,4	26,24,1,11
27,4,3,16	28,16,1,17	29,11,1,15	30,5,1,26	31,11,1,5

此种 σ-AND 随机数生成器有大量的选取空间，对于任意给定的 e 都可以找到最大周期矩阵。当不再限制与系数为 0 时，会有更多的选择。当字长 $m=64$ 时，同样找到了大量最大周期 σ-AND 随机数生成器。此 σ-AND 随机数生成器可以产生周期为 $2^{256}-1$ 的 64 比特序列，可以满足序列密码的设计要求。表 5 中以四元组 (e,w_a,v,u) 的形式列举了部分结果。

表 5　部分大周期 64 比特 4 级 σ-*AND* 随机数生成器

1,20,1,10	2,38,1,15	3,23,1,25	4,57,1,16	5,31,1,43
6,60,2,45	7,59,2,53	8,17,3,46	9,40,5,8	10,8,5,21
11,48,5,52	12,50,7,33	13,25,7,55	14,28,8,3	15,29,8,27
16,37,9,20	17,45,9,53	18,38,10,17	19,21,10,55	20,15,11,3
21,24,11,26	22,47,11,34	23,9,11,57	24,42,12,5	25,39,12,39
26,31,13,16	27,39,13,19	28,54,13,53	29,57,14,59	30,21,1,36
31,31,1,38	32,28,2,3	33,48,3,12	34,39,3,52	35,41,4,45
36,13,5,8	37,26,5,16	38,23,5,38	39,17,7,29	40,38,7,45
41,56,9,12	42,57,9,26	43,45,10,5	44,53,11,2	45,43,11,38
46,17,11,40	47,39,9,3	48,20,8,59	49,42,7,52	50,47,7,10
51,33,6,59	52,60,5,37	53,11,5,29	54,15,5,23	55,12,5,10
56,22,5,1	57,33,4,13	58,34,3,53	59,48,3,34	60,52,3,23
61,45,2,35	62,26,1,49	63,19,1,27	63,47,1,38	

如果需要输出序列具有更大周期，还可以利用式(9)的方法构造，仍然可以得到大量的实现效率非常高的 σ-AND 随机数发生器。

结束语　本文的 σ-AND 操作不仅软件实现效率高，同时循环移位可以将字的高位信息转送到低位，进行充分的混乱和扩散，这也符合密码算法的设计思想。利用 σ-AND 操作可以构造各种各样形式简单、实现高效的 σ-AND 随机数发生器。虽然结构简单，但这些随机数发生器的输出序列在随机性测试中均有良好表现。所得结果表明 σ-AND 随机数发生器可以作为适合软件实现的序列密码的驱动部分来使用。从本文的研究可以看出，设计高效、高安全性、占用资源少的序列密码部件、甚至整个序列密码是可能的。然而本文还有许多需要进一步研究、解决的问题，例如特定形式 σ-AND 随机数发生器的构造问题。但无论如何，我们希望这种将实现效率和安全性并重的研究方法能得到广泛应用。

参 考 文 献

[1] ECRYPT, eSTREAM: ECRYPT Stream Cipher Project [EB/OL]. http://www.ecrypt.eu.org/stream/. 2007

[2] Watanabe D, Furuya S, Yoshida H, et al. A New Keystream Generator MUGI[C]// Fast Software Encryption 2002 Workshop. LNCS. Vol 2365. Berlin Heiderberg: Springer-Verlag, 2003:179-194

[3] Hawkes P, Rose G. Primitive Specification and Supporting Documentation for SOBER-t32 Submission to NESSIE [R/OL]// Proceedings of the first NESSIE Workshop. Heverlee, Belgium, 2000

[4] Ekdahl P, Johansson T. A New Version of the Stream Cipher SNOW[C]// Nyberg K, Heys H, eds. Selected Areas in Cryptography 2002 Workshop. LNCS. Vol 2595. Berlin Heidelberg: Springer-Verlag, 2003:47-61

[5] Hawkes P, Rose G. Turing: A Fast Stream Cipher[C]// Johansson T, ed. Fast Software Encryption 2003 Workshop. LNCS. Vol 2887. Berlin Heiderberg: Springer-Verlag, 2003:290-306

[6] Boesgaard M, Vesterager M, Pedersen T, et al. Rabbit: A New High-Performance Stream Cipher[C]// Fast Software Encryption 2003 Workshop. LNCS. Vol 2887. Berlin Heiderberg: Springer-Verlag, 2004:307-329

[7] Ferguson N, Whiting D, Schneier B, et al. Helix: Fast Encryption and Authentication in a Single Cryptographic Primitive[C]// Fast Software Encryption 2003 Workshop. LNCS. Vol 2887. Berlin Heiderberg: Springer-Verlag, 2004:330-346

[8] Anashin V, Bogdanov A, Kizhvatov I, et al. ABC: A new fast flexible stream cipher [R/OL]. eSTREAM, ECRYPT Stream Cipher Project. Report 2005/001. 2005

[9] Klimov A, Shamir A. A New Class of Invertible Mappings[C]// Cryptographic Hardware and Embedded Systems, LNCS 2523. 2002: 470-483

[10] Moon D, Kwon D, et al. T-function based streamcipher TSC-4 [R/OL]. ECRYPT Stream Cipher Project. Report 2006/024. 2006

[11] Marsaglia G. Xorshift RNGs[J]. Journal of Statistical Software, 2003, 8(14):1-6

[12] 曾光，何开成，韩文报. 一类三项式形式适合软件实现的 σ-LFSR [J]. 中国科学 E 辑：信息科学，2007，37(2)：209-222

[13] Zeng Guang, Han Wenbao, He Kaicheng. High Efficiency Feedback Shift Register: σ-LFSR [J/OL]. Cryptology ePrint Archive. Report 2007/114. 2007

[14] Marsaglia G. The Marsaglia Random Number CDROM with The Diehard Battery of Tests of Randomness[R/OL]. 1995. http://www.csis.hku.hk/? diehard

[15] 顾国生，韩国强，李闻. 一种基于混沌和矩阵变换的序列密码 [J]. 计算机科学，2007，34(5)：85-88