●通信保密●

差分序列的性质及应用

黄建忠[①]　李超[①②]
(①国防科技大学数学与系统科学系,长沙 410073)(②中国科学院软件研究所计算机重点实验室,北京 100080)

【摘　要】给出了差分序列的若干性质,并对其在序列密码中的应用作了一些探讨。
【关键词】差分分析　差分序列　移位差分　累次差分　序列密码

The Properties and Applications of Differential Sequence

Huang Jianzhong [①]　*Li Chao* [①②]
(① Department of Mathematics and System Science of NUDT, Changsha 410073)
(② Laboratory of Computer Science of Institute of Software of Chinese Academic of Science, Beijing 10080)

【Abstract】In this paper, we give some properties of differential sequence, and discuss the applications of differential sequence in sequence cryptology.
【Keywords】differential cryptanalysis, differential sequence, shift differential, cumulate differential, sequence cryptology

1 引言

差分密码分析是已知的攻击迭代分组密码最有效的方法之一,它是 Eli Biham 和 Adi Shamir 于 1990 年提出[1,2]的。但长期以来,很少有人把这种方法应用于序列密码的设计和分析中。对此研究较早的一篇文章[3]是丁存生写的。作者给出了差分序列的若干性质,并对其在序列密码中的应用作了初步的探讨。

2 差分的基本概念

定义 1[4] 设 $f: S\to T$ 是从阿贝尔群 $(S, +)$ 到阿贝尔群 $(T, +)$ 的映射,f 在点 $a\in S$ 的差分定义为:

$\Delta_a(f(x)) = f(x+a) - f(x)$

定义 2[2] 条件同上,f 在点 $a_1, \cdots, a_i$ 的 i 阶差分定义为:

$\Delta^{(i)}_{a_1,\cdots,a_i} f(x) = \Delta_{a_i}(\Delta^{(i-1)}_{a_1,\cdots,a_{i-1}} f(x))$

这里所指的差分和高阶差分类同于上述的定义 1 和定义 2。由于这里主要讨论二元域上的序列密码,因此文章后面的差分运算如没有特别指明,均指异或运算。

定义 3[4] 设 $\underline{a_1}$ 是 $\underline{a}$ 的子序列,$\underline{b_1}$ 是 $\underline{b}$ 的子序列,则 $\Delta_{a_1,b_1} = \underline{a_1}\otimes\underline{b_1}^{-1}$ 称为序列 $\underline{a}$, $\underline{b}$ 关于子序列 $\underline{a_1}$, $\underline{b_1}$ 的截断差分,其中 $\otimes$ 表示序列集上的一个特定群运算,$\underline{b_1}^{-1}$ 表示 $\underline{b_1}$ 在此序列集上的一个特定群中的逆元。

定义 4 设 $a_1, a_2, a_3, \cdots, a_n\cdots$,为二元域上的一条序列,对其作如下运算:

$a_1, a_1\oplus a_2, a_2\oplus a_3, \cdots, a_{n-1}\oplus a_n, \cdots$,

则称此运算为移位差分,所生成的序列称为第一类差分序列。

定义 5 设 $a_1, a_2, a_3, \cdots, a_n\cdots$,为二元域上的一条序列,对其作如下运算:

$a_1, a_1\oplus a_2, a_1\oplus a_2\oplus a_3, \cdots, a_1\oplus\cdots\oplus a_{n-1}\oplus a_n, \cdots$,

则称此运算为累次差分,所生成的序列称为第二类差分序列。

3 差分序列的若干性质

在讨论差分序列的性质之前,先给出一些需要用到的定理。

引理 1[5] 设 n 级 LFSR 的特征多项式为 $f(x) = x^n + c_1x^{n-1} + \cdots + c_n(c_n\neq 0)$,则 LFSR 以 $(a_0, a_1, \cdots, a_{n-1})$ 为初态产生的 q 元序列的母函数表示为 $A(x) = \frac{g(x)}{f(x)}$,其中 $f(x)$ 为 LFSR 的联结多项式,而 $g(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$ 由初态和反馈系数 $(c_0, \cdots, c_n)$ 给出。

引理 2[5] 设 $f_1(x), \cdots, f_n(x)\in GF(q)[x]$, $f_1(x), \cdots, f_n(x)$ 两两互素,则每个有理真分式 $\frac{g(x)}{f_1(x)\cdots f_n(x)}$ 均可唯一表示成若干真分式之和:$\frac{g(x)}{f_1(x)\cdots f_n(x)} = \frac{g_1(x)}{f_1(x)} + \cdots + \frac{g_n(x)}{f_n(x)}$。

引理 3[5] 设 $s_1^\infty, \cdots, s_k^\infty$ 为 $GF(q)$ 上的 k 个周期序列,且 $r_{i1}(x)/f_{i1}(x), \cdots, r_{it}(x)/f_{it}(x)$ 分别为它们的生成函数的既约有理分式表示。再设 $t^\infty = \sum_{i=1}^{k} s_i^\infty$ 为这个序列的和序列。命:

$g(x) = \sum_{j=1}^{k} r_{ij}(x)\prod_{i\neq j} f_{ii}(x)$, $f(x) = \prod_{i=1}^{k} f_{ii}(x)$ 则有:

(1) $f_t(x) = f(x)/\gcd[f(x), g(x)]$;

收稿日期:2003-02-21。
中国科学院软件研究所计算机科学重点实验室开放基金(NO. syskf0201)和国防科技大学基础研究基金(NO. JC0202007)资助。
黄建忠:男,1973 年生,系硕士研究生。主要研究方向为编码密码理论及其应用。
李　超:男,1966 年生,教授。主要研究方向为编码密码理论及其应用。

(2) $per(t^m)=ord(f(x)/\gcd[f(x),g(x)])\le lcm[per(s_1^m),\cdots,per(s_k^m)]$，其中等号当 $f_{s1}(x),\cdots,f_{sk}(x)$ 两两互素时成立；

(3) $L(t^m)\le\sum_{i=1}^{k}L(s_i^m)$，当且仅当 $f_{s1}(x),\cdots,f_{sk}(x)$ 两两互素时等号成立。

引理 4[6] 设 F_q 为一特征为 p 的有限域，$f\in F_q[x]$ 是一个次数大于 0 且 $f(0)\neq 0$ 的多项式。设 $f=af_1^{h_1}\cdots f_k^{h_k}$ 为 f 在 $F_q[x]$ 中的标准分解式，其中 $a\in F_q$，$b_1,\cdots,b_k\in N$，且 $f_1,\cdots,f_k$ 是 $F_q[x]$ 中两两不同的首一不可约多项式。则 $ord(f)=ep^t$，其中 $e=lcm(ord(f_1),\cdots,ord(f_k))$，$t$ 是满足 $p^t\ge\max(b_1,\cdots,b_k)$ 的最小整数。

3.1 第一类差分序列的性质

定理 1 设 $\underline{a}$ 是周期为 T 的二元序列，$f(x)$ 是其极小多项式，序列 $\underline{b}$ 为 $\underline{a}$ 的第一类差分序列。如果 $(1+x)\mid f(x)$，则 $\underline{b}$ 的极小多项式为 $f(x)/(1+x)$，周期和线性复杂度不增；否则，$\underline{b}$ 的极小多项式为 $f(x)$，周期和线性复杂度不变。

证明 由引理 1，$\underline{a}$ 的母函数表示为：$A(x)=\frac{g(x)}{f(x)}$

设 $a_{-1}=0$，则 $\underline{b}$ 的母函数表示为：

$$B(x)=\sum_{i=0}^{\infty}(a_{i-1}+a_i)x^i=(1+x)\sum_{i=0}^{\infty}ax^i$$

$$=(1+x)A(x)=\frac{g(x)(1+x)}{f(x)}$$

如果 $(1+x)\mid f(x)$，设 $f(x)=(1+x)f_1(x)$，此时有：$B(x)=\frac{g(x)}{f_1(x)}$。因此由母函数的表示知 $\underline{b}$ 的极小多项式为 $f_1(x)$，再由引理 2～引理 4 知周期和线性复杂度不增。

否则，由母函数的表达式知 $\underline{b}$ 的极小多项式仍为 $f(x)$，自然周期和线性复杂度都不变。

推论 1 设 $\underline{a}$ 为 n 级 m 序列，$\underline{b}$ 为其第一类差分序列，则 $\underline{b}$ 仍为 n 级 m 序列。

3.2 第二类差分序列的性质

定理 2 设 $\underline{a}$ 是周期为 T 的二元序列，其母函数 $A(x)=\frac{g(x)}{f(x)}$，$f(x)$ 是其极小多项式，$\underline{b}$ 为 $\underline{a}$ 的第二类差分序列。如果 $(1+x)\mid g(x)$，则 $\underline{b}$ 的极小多项式为 $f(x)$，周期和线性复杂度不变；否则，$\underline{b}$ 的极小多项式为 $f(x)(1+x)$，周期和线性复杂度不减。

证明 由第二类差分序列的运算知：

$a_i=b_{i-1}+b_i$，$i=0,1,\cdots$，其中 $b_{-1}=0$

设 $\underline{b}$ 的母函数为 $B(x)$，则有：

$$A(x)=\sum_{i=0}^{\infty}ax^i=\sum_{i=0}^{\infty}(b_{i-1}+b_i)x^i$$

$$=(1+x)\sum_{i=0}^{\infty}bx^i=(1+x)B(x)$$

故 $B(x)=\frac{A(x)}{(1+x)}=\frac{g(x)}{(1+x)f(x)}$。 (1)

如果 $(1+x)\mid g(x)$，设 $g(x)=(1+x)g_1(x)$，此时 $B(x)=\frac{g_1(x)}{f(x)}$，由母函数的表示知 $\underline{b}$ 的极小多项式为 $f(x)$，周期和线性复杂度不变。

否则，由母函数的表示知 $\underline{b}$ 的极小多项式为 $f(x)(1+x)$，再由引理 2～引理 4 知周期和线性复杂度不减。

定理 3 设 $\underline{a}$ 是周期为 T 的 m 序列，$\underline{b}$ 为其第二类差分序列。则 $\underline{b}$ 的周期也为 T。

证明 由于 $\underline{a}$ 的周期为 T，故其母函数可表示为：

$A(x)=\frac{g(x)}{1+x^T}$，其中 $g(x)=c_0+c_1x+\cdots+c_{T-1}x^{T-1}$。

由定理 2 的证明过程，可以把序列 $\underline{b}$ 的母函数表示为：

$$B(x)=\frac{g(x)}{(1+x)(1+x^T)} \quad (2)$$

由 $\underline{a}$ 为 m 序列，有 $g(1)=0$，故 $(1+x)\mid g(x)$。再由(2)式和定理 2 即知 $\underline{b}$ 的周期为 T。

定理 4 对任意有限长序列 $\underline{a}$，$w(\underline{a})$ 表示其中 1 的个数，$\underline{b}$ 为其第二类差分序列。若 $w(\underline{a})$ 为偶数，则 $\underline{b}$ 的最后一比特为 0；若 $w(\underline{a})$ 为奇数，则 $\underline{b}$ 的最后一比特为 1。

证明 由定义 5 易证(略)。

3.3 两类差分序列的相互关系

由定义 4 和定义 5 容易证明下面两个定理。

定理 5 设 $\underline{a}$ 为二元域上的一条序列，$\underline{b}$ 为其第一类差分序列，$\underline{c}$ 为 $\underline{b}$ 的第二类差分序列，则 $\underline{a}$ 和 $\underline{c}$ 是相同的序列。

定理 6 设 $\underline{a}$ 为二元域上的一条序列，$\underline{b}$ 为其第二类差分序列，$\underline{c}$ 为 $\underline{b}$ 的第一类差分序列，则 $\underline{a}$ 和 $\underline{c}$ 是相同的序列。

4 差分序列在序列密码中的若干应用

4.1 对密文序列进行差分，有望提高密码攻击成功的概率

有了定理 5 和定理 6，现在来考虑一下，在唯密文攻击时，如何从密文中恢复明文和密钥。假设已知明文编码及统计特性，则可以充分利用这些编码规律和统计特性。为了讨论方便，以下不妨假设：

P：1 0 1 0 1 0 1 0 1 0 1 0 $\cdots$

K：$k_0\,k_1\,k_2\,k_3\,k_4\,k_5\,k_6\,k_7\,k_8\,k_9\cdots$

C：$c_0\,c_1\,c_2\,c_3\,c_4\,c_5\,c_6\,c_7\,c_8\,c_9\cdots$

现对 C 进行移位差分，则有：

$$\Delta C:\Delta c_i=\Delta k_i\oplus 1,\ i\ge 0 \quad (3)$$

由(3)式可以知道密钥差分序列就等于密文差分取反序列，因此要研究密钥差分序列，只需研究密文差分取反后的序列即可。当然此时还可以对 ΔC 再移位差分一次，这样就可以完全消除明文中比特 1 的影响。如果此时的密文差分序列的反馈多项式和初态能够求出，那么就可以求出整条密文差分序列。再通过密文差分序列和密钥差分序列之间的对应关系，就可以求出密钥差分序列。而上面两个定理则保证差分后的序列是可以很容易还原为原始序列的，由此就求出了原始密钥序列。至于 P 为其它情况，则只要运用截断差分的思想，再进行类似差分，同样可以求出原始密钥序列，只是会稍微复杂一些。

由此可见，对密文进行差分可以消除明文的一些影响，以获得部分密钥序列。而这对于进一步分析密码系统无疑是大有帮助的。比如 BAA[5] 攻击需要有一定量的密钥，尤其是当系统中的各个 LFSR 级数增大时，密钥量需求随之增加。此时如果辅以本文的差分分析方法，则可以保证密钥量的需求，提高攻击成功的概率。

4.2 对密文序列进行累次差分，可作为序列误码校验的一种指标

定理 4 可以作为判断序列有无误码的校验指标。即发方先把密文序列进行累次差分，然后发送给对方；收方接收到差分序列以后，先记下序列最后一比特信息，然后把该序列进行移位差分，并统计其中"1"出现的个数，若为奇数则记为 1，否则记为 0；最后与原始序列最后一比特进行比较，若相同则说明没有误码，否则说明有误码（这里假定误码率控制在一定范围之内）。虽然这种方法不能确定误码的位置，但简单易行，使用它还是值得的。比如在一些不需要确定误码位置的情形，或者仅作为一种辅助判断。

5 结束语

这里给出了差分序列的若干性质，并对其在序列密码中的应用作了初步的探讨。如何进一步地把差分分析技术应用到序列密码的分析和设计中？这是笔者下一步要研究的课题。

参考文献

1 Biham E, Shamir A. Differential cryptanalysis of DES - like cryptosys - tems. Advances in Cryptology - CRYPTO'90 Proceedings, Berlin: Springer - Verlag, 1991: 2 ~ 21

2 Biham E, Shamir A. Differential cryptanalysis of the data encryption standard. Berlin: Spring - Verlag, 1993

3 Ding C. The differential cryptanalysis and design of natural stream ciphers. Fast Software Encryption, Cambridge Security Workshop Proceedings. Berlin: Springer - Verlag, 1994: 101 ~ 115

4 冯登国. 密码分析学. 北京：清华出版社，2000

5 丁存生，肖国镇. 流密码学及其应用. 北京：国防工业出版社，1994

6 Lidl R, Niederreiter H. Finite Field. Addisonwesley Publishing Company, 1983

7 Knudsen L R. Truncated and higher order differentials, fast software encryption. 2nd Int'l Workshop Proc, Berlin: Springer - Verlag, 1995: 196 ~ 211

8 Lai X. Higher order derivations and differential cryptanalysis. Proc. Symp. on Communication, Coding and Cryptography, Monte - Verita, Ascona, Switzerland, 1994

（上接第 101 页）

和低复杂度的接收机，而 VSG 系统可能支持更宽范围的数码率但是编码设计复杂的多。

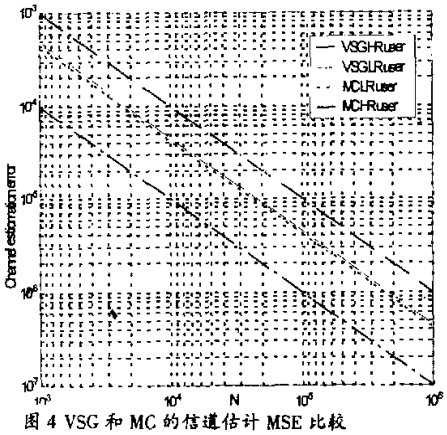

图 4 VSG 和 MC 的信道估计 MSE 比较

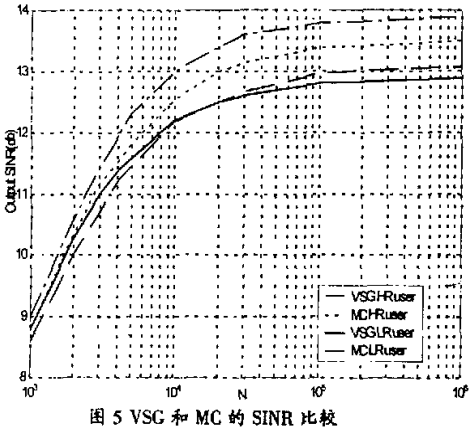

图 5 VSG 和 MC 的 SINR 比较

	VSG - CDMA	MC - CDMA
码设计复杂度	高	低
接收机复杂度	低	中等
多速率支持度	高	高

图 6 两种方案的综合比较

4 结束语

通过两种多速率方案的基本原理和性能比较，得出两者在低速率传输中具有差不多的性能，但是在检测高速用户中，如果只考虑附加高斯白噪声的情况下，MC - CDMA 的"远近问题"性能优于 VSG - CDMA，如果考虑在现实的互相关值中，VSG - CDMA 的性能优于 MC - CDMA。

参考文献

1 Mitra U. Comparison of Maximum Likelihood - based Detection for Two Multi - rate Access Schemes for CDMA Signals. IEEE Trans. Com - mun., 1999; 47(1): 64 ~ 77

2 Ottosson T, Svensson A. Performance of different multi - rate schemes in DS/CDMA systems. Proc. NRS ceminar on Radio communication networks, Sweden, 1994: 15 ~ 18

3 Groe J B, Larson L E 著. 杨家玮，刘勤，刘静译. CDMA Mobile Radio Desig. 北京：人民邮电出版社 2002: 165 ~ 166

4 Guo Z, Letsief K B. Performance of VSG - CDMA and MC - CDMA in Multirate Systems. Proc. IEEE Vehicular Technology Conference, Greece, May 2001

5 Xu Z. Asymptotic Performance of Subspace Methods for Synchronous Multirate CDMA Systems. IEEE Trans. Signal Process., 2002; 50(8): 2015 ~ 2025

差分序列的性质及应用

作者： 黄建忠， 李超
作者单位： 黄建忠(国防科技大学数学与系统科学系,长沙,410073)， 李超(国防科技大学数学与系统科学系,长沙,410073;中国科学院软件研究所计算机重点实验室,北京,100080)

刊名： 通信技术
英文刊名： COMMUNICATIONS TECHNOLOGY
年，卷(期)： 2003(10)

参考文献(8条)

1. Biham E;Shamir A Differential cryptanalysis of DES - like cryptosystems. Advances in Cryptology-CRYPTO'90 Proceedings 1991

2. Biham E;Shamir A Differential cryptanalysis of the data encryption standard 1993

3. Ding C The differential cryptanalysis and design of natural stream ciphers. Fast Software Encryption Cambridge Security Workshop Proceedings 1994

4. 冯登国 密码分析学 2000

5. 丁存生;肖国镇 流密码学及其应用 1994

6. Lidl R Niederreiter H 1983

7. Knudsen L R Truncated and higher order differentialsfast software encryption. 2nd Int'l Workshop Proc 1995

8. Lai X Higher order derivations and differential cryptanalysis. Proc.Symp. on Communication 1994

本文读者也读过(10条)