自相关性和线性复杂度的关系

高军涛[1], 胡予濮[1], 李雪莲[2]
(1.西安电子科技大学计算机网络与信息安全教育部重点实验室, 陕西西安 710071;
2.西安电子科技大学应用数学系, 陕西西安 710071)

摘 要: 自相关性和线性复杂度是衡量序列伪随机性质的两个独立的指标.针对周期为 2^n 的伪随机序列, 本文首次指出了自相关性和线性复杂度之间存在的一个关系.该关系可应用于以下两个方面: (1)由序列的线性复杂度来估计/确定序列的自相关函数值; (2)通过线性复杂度来检验给定序列族的互相关性质.进一步的, 针对一类周期为 2^n 的伪随机序列, 我们指出这类序列的自相关函数值和线性复杂度以及 k-错线性复杂度存在着关系.

关键词: 自相关性质; 线性复杂度; k-错线性复杂度; 关系
中图分类号: TN918.1 文献标识码: A 文章编号: 0372-2112 (2006) 08-1401-04

A Relationship Between Autocorrelation and Linear Complexity

GAO Jun-tao[1], HU Yu-pu[1], LI Xue-lian[2]
(1.Key Laboratory of Computer Networks & Information Security, Xidian University, Xi'an, Shaanxi 710071, China;
2.Department of Applied Mathematics of Xidian University, Xi'an, Shaanxi 710071, China)

Abstract Autocorrelation and linear complexity are two independent criterions for measuring the pseudorandom properties of sequences. For the 2^n-periodic pseudorandom sequences, we first present the relationship between autocorrelation and linear complexity. The relationship can be applied in the following two aspects: (1) Estimating/Evaluating the value of autocorrelation functions by the linear complexity; (2) Evaluating the correlation of a given sequence family by the linear complexity. Furthermore, for a sort of sequences with period 2^n, we denote that the autocorrelation is related to linear complexity and k-error linear complexity.

Key words autocorrelation; linear complexity; k-error linear complexity; relationship

1 引言

在通信和密码方面, 伪随机序列有广泛的应用.衡量序列伪随机性质的指标主要有: 周期, 线性复杂度, 自相关性质, 游程分布, k-错线性复杂度等等.对于周期为 $N=2^n$ 的二元伪随机序列 $s=s_0s_1s_2\cdots s_{N-1}\cdots$, 其线性复杂度定义为产生序列 s 的最短的线性反馈移位寄存器(LFSR)的长度, 记为 $LC(s)$.更形象地, 设序列 s 的生成函数为:

$$s^N(x)=s_0+s_1x+s_2x^2+\cdots+s_{N-1}x^{N-1}$$

则:

$$LC(s)=N-\deg(\gcd(1+x^N, s^N(x)))$$

在序列密码理论中, 线性复杂度是一个重要的复杂度指标, 一个具有低线性复杂度的序列是非常不安全的.计算线性复杂度的方法主要有文献[1]算法和文献[2]算法, 其中后者对周期为 2^n 的序列更加有效.

自相关性质是衡量序列本身和其移位序列之间相似程度的指标, 对于序列 s, 其自相关函数定义为:

$$A_s(t)=\sum_{i=0}^{N-1}(-1)^{s_i+s_{i+t}},\quad t=0,1,\cdots,N-1$$

其中下标的和都是取 mod N.

在通信中, 我们希望得到自相关性质好的序列, 即序列的自相关函数值都比较小.这样我们能比较容易的区分序列本身和它的移位序列.

线性复杂度和自相关性质是两个独立的概念, 在实际应用中通常被分别研究.对于周期为 2^n 的伪随机序列, 本文首次指出两个衡量指标之间存在着关系.这种关系可以应用于以下的两个方面:

(1)在一定条件下, 给定序列的线性复杂度, 可以确定

收稿日期: 2005-08-22; 修回日期: 2006-04-10
基金项目: 国家自然科学基金(No. 60273084); 高等学校博士点基金(No. 20020701013)

/估计序列的自相关函数值;

(2)通过线性复杂度来检验给定序列族的互相关性质.

进一步的,针对一类周期为 2^n 的二元序列,我们指出其自相关性质和线性复杂度以及 k-错线性复杂度之间存在关系,即可以用序列的线性复杂度和 k-错线性复杂度来更精确地估计/确定序列自相关函数值.

2 关系

设 c 是一个正整数,$W_H(c)$ 指 c 的二进制表示的 Hamming 重量,即 c 的二进制表示中 1 的个数. 设多项式:

$c(x)=1+x^{c_1}+x^{c_2}+\cdots+x^{c_{q-1}}$,其中 $c_1<c_2<\cdots<c_{q-1}$,我们用 $W(c(x))$ 指多项式 $c(x)$ 的 Hamming 重量,即 $W(c(x))=q$.

引理 1[3] 设 c 是一个正整数,$(1+x)^c$ 是域 $GF(2)$ 上的多项式,则

$$W((1+x)^c)=2^{W_H(c)}$$

引理 2[3] 设 $(1+x)^c f(x)$ 是域 $GF(2)$ 上的多项式,且 $f(1)=1$,c 是一个正整数,则

$$W((1+x)^c f(x))\geqslant 2^{W_H(c)}$$

文献[4]中,Kurosawa 等基于上述两个定理讨论了周期为 2^n 的二元序列线性复杂度和 k-错线性复杂度之间的关系,得到了较好的结果. 下面同样基于这两个引理给出周期为 2^n 的二元序列的线性复杂度和自相关性之间的关系.

定理 1 设 $GF(2)$ 上的二元序列 $s=s_0s_1s_2\cdots s_{N-1}\cdots$,最小周期为 $N=2^n>1$,则其自相关函数 $A_s(\tau)$ 满足下面的界:

$$|A_s(\tau)|\leqslant|2^n-2^{W_H(2^n-LC(S)+1)+1}|,\tau=2^ij+1$$

$$|A_s(\tau)|\leqslant|2^n-2^{W_H(2^n-LC(S)+2^i)+1}|,\tau=2^ij$$

证明 设序列 s 的生成函数为:$s^N(x)=s_0+s_1x+s_2x^2+\cdots+s_{N-1}x^{N-1}$. $x^\tau s^N(x)$ 表示序列 s 向右循环移动了 τ 位,其中 $x^\tau s^N(x)$ 所有项的指数都取 mod$N$. 则序列 s 的自相关函数 $A_s(\tau)$ 可以表示为:

$$A_s(\tau)=N-2W(x^\tau s^N(x)+s^N(x))$$

其中"+"表示生成函数对应项的 mod2 加法.

由于 $\{(1+x)^0,(1+x)^1,(1+x)^2,\cdots,(1+x)^{2^n-1}\}$ 是向量空间 $\{f(x)\mid\deg(f(x))<2^n\}$ 的一组基,因此对于任意的一个函数 $f(x)\in\{f(x)\mid\deg(f(x))<2^n\}$,一定存在非负的整数 $t_1,t_2,\cdots,t_m$,使得 $f(x)=(1+x)^{t_1}+\cdots+(1+x)^{t_m}$,其中 $0\leqslant t_1<t_2<\cdots<t_m\leqslant 2^n-1$. 因此对于序列 s 的生成函数 $s^N(x)$ 一定存在非负的整数 $t_1,t_2,\cdots,t_m$ 使得:

$$s^N(x)=(1+x)^{t_1}+(1+x)^{t_2}\cdots+(1+x)^{t_m}.$$

因为 $N=2^n$,按照线性复杂度的定义可知:

$$\begin{aligned}LC(s)&=N-\deg(\gcd(1+x^N,s^N(x)))\\&=N-\deg(\gcd((1+x)^N,s^N(x)))\\&=N-t_1\end{aligned}$$

设多项式 $g(x)=(x^\tau+1)$,其中 $\tau=0,1,\cdots,N-1$. 则 $g(x)$ 也可以由基 $\{(1+x)^0,(1+x)^1,(1+x)^2,\cdots,(1+x)^{2^n-1}\}$ 来表示. 因此

$$g(x)s^N(x)=P_0(x)+P_1(x)(x+1)^N$$

其中 $P_0(x)=\sum_{i<N}b_i(x+1)^i$,$b_i\in GF(2)$,$P_1(x)=\sum_{i<N}b'_i(x+1)^i$,$b'_i\in GF(2)$. 由于 $N=2^n$,所以 $P_1(x)(x+1)^N=P_1(x)+P_1(x)x^N$. 因此我们可以用以下的形式来表示序列 s 的自相关函数:

$$A_s(\tau)=N-2W(P_0(x))$$

我们所关心的是 $P_0(x)$ 中 $(x+1)$ 次数最低的一项,因此我们要求出多项式 $g(x)$ 在基 $\{(1+x)^0,(1+x)^1,(1+x)^2,\cdots,(1+x)^{2^n-1}\}$ 表示形式下的次数最低的一项.

下面对 $g(x)$ 按照 τ 的值分情况进行讨论:

情况 1:τ 为奇数,即 $\tau=2^ij+1$,这里 $i\in\{1,\cdots,n-1\}$,j 是一个奇数,此时

$$g(x)=(1+x)+\sum_{k=2}^{N-1}b_k(x+1)^k$$

这里 $b_k\in GF(2)$;

此时 $P_0(x)$ 的次数最低的一项为 $(x+1)^{t_1+1}$.

情况 2:τ 为偶数,即 $\tau=2^ij$,这里 $i\in\{1,\cdots,n-1\}$,j 是一个奇数,此时

$$g(x)=(1+x)^{2^i}+\sum_{k=2^i}^{N-1}b_k(x+1)^k$$

这里 $b_k\in GF(2)$.

此时 $P_0(x)$ 的次数最低的一项为 $(x+1)^{t_1+2^i}$.

由引理 2,我们有:

$W(P_0(x))\geqslant 2^{W_H(N-LC(s)+1)}$,$\tau=2^ij+1$;

$W(P_0(x))\geqslant 2^{W_H(N-LC(s)+2^i)}$,$\tau=2^ij$

设 $C^N(x)=1+x+\cdots+x^{N-1}$,序列 s 的最小周期为 $N=2^n>1$,所以有:

$$N-W(P_0(x))=W(P_0(x)+C^N(x))\geqslant 2^{W_H(N-LC(s)+1)},\quad\tau=2^ij+1;$$

$$N-W(P_0(x))=W(P_0(x)+C^N(x))\geqslant 2^{W_H(N-LC(s)+2^i)},\quad\tau=2^ij.$$

代入表达式得:

$$|A_s(\tau)|\leqslant|2^n-2^{W_H(2^n-LC(S)+1)+1}|,\tau=2^ij+1$$

$$|A_s(\tau)|\leqslant|2^n-2^{W_H(2^n-LC(S)+2^i)+1}|,\tau=2^ij$$

证毕.

推论 设 $GF(2)$ 上的二元序列 $s=s_0s_1s_2\cdots s_{N-1}\cdots$,最小周期为 $2^n>1$,$S^\tau=S_\tau S_{\tau+1}\cdots S_{N-1}S_0\cdots(\tau=1,2,\cdots,N-1)$. 序列 $t=t_0t_1t_2\cdots t_{N-1}\cdots$,是序列 s 和 S^τ 的和序列,即 $t_i=s_i+S_{i+\tau}$,即 $t_i=s_i+s_{i+\tau}$,则 $LC(t)<LC(s)$,其中"+"表示对应项的 mod2 加法. $LC(t)$,$LC(s)$ 分别表示序列 t 和序列 s 的线性复杂度.

该推论可以由定理 1 的证明过程得到.

对于和序列的线性复杂度,目前的结论是 $LC(t)\leqslant LC(s)+LC(s^\tau)=2LC(s)$,由该推论可以使这个界更紧.

3　应用

3.1　由线性复杂度来估计/确定自相关函数值

在实际应用中,有时不需要知道自相关函数确切的值,仅仅需要知道自相关函数值所处的范围就可以了. 计算最小周期为 $N=2^n$ 的序列 s 的一个自相关函数值,需要进行 N 次 mod2 加法运算,要计算所有的自相关函数值,计算复杂度为 $O(N^2)$. 而利用 Games-Chan 算法计算序列 s 的线性复杂度,其计算复杂度为 $O(N)$. 因此,我们可以利用定理 1 的结果通过计算线性复杂度来估计/确定序列的自相关函数值. 下面是一个简单的例子:

例 1　设 $s^{16}=1111010110100000$, $LC(s^{16})=10$,则由定理 1 可知:

$$|A_s(\tau)|\leqslant|16-2^{W_H(16-10+1)+1}|,\tau=2^ij+1$$

$$|A_s(\tau)|\leqslant|16-2^{W_H(16-10+2^i)+1}|,\tau=2^ij$$

因此,当 τ 为奇数时,序列的自相关函数值 $A_s(\tau)=0$;

$$-0.75\leqslant A_s(\tau)\leqslant 0.75,\ \tau=2,6,10,14;$$

$$-0.5\leqslant A_s(\tau)\leqslant 0.5,\ \tau=4,12.$$

通过计算验证如表 1.

表 1

τ	1	2	3	4	5	6	7	8
$A_s(\tau)$	0	0.25	0	-0.5	0	-0.25	0	0

注:对于最小周期为 2^n 的序列,自相关函数值满足: $A_s(\tau)=A_s(2^n-\tau)$.

因此当已知序列的线性复杂度时,我们可以确定/估计自相关函数的值,以此来减少计算量. 当有个别的自相关值超出要求范围时,可以对这些值做具体的计算. 注意到应用线性复杂度估计自相关值有一定的局限性,只有当线性复杂度的 Hamming 重量比较小的时候, $|A_s(\tau)|$ 的界才会更低一些. 同时只有当 $|A_s(\tau)|$ 上界的值为 0 时,才能确定 $A_s(\tau)$ 的值,上界为其他值的时候只能估计 $A_s(\tau)$ 的值. 利用第四部分中定理 3 的结果能使估计值更加精确.

3.2　检验序列族优劣的一个新标准

在通信应用方面,有时我们需要一个大族序列,族内序列之间的互相关函数要满足一定的条件,一般情况下,需要序列之间具有较低的互相关函数值. 对于一个已知的序列族,利用定理 1 的结果,我们只需考虑序列的线性复杂度就可以大致检验该序列族的互相关性质. 下面以两个序列为例说明检验方法.

设序列 $s=s_0s_1s_2\cdots s_{N-1}\cdots$, $t=t_0t_1t_2\cdots t_{N-1}\cdots$,两个序列都具有最小周期 $N=2^n$,序列 s 和 t 的互相关函数可以定义为:

$$C_{s,t}(\tau)=\sum_{i=0}^{N-1}(-1)^{s_i+t_{i+\tau}}$$

其中下标的和都是取 mod$N$ 的.

设序列 s 和 t 的生成函数为:

$$s^N(x)=(1+x)^{u_1}+(1+x)^{u_2}\cdots+(1+x)^{u_h},$$

$$t^N(x)=(1+x)^{v_1}+(1+x)^{v_2}\cdots+(1+x)^{v_l},$$

与定理 1 类似, $C_{s,t}(\tau)$ 可以记为: $C_{s,t}(\tau)=N-2W(x^\tau s^N(x)+t^N(x))$, x^τ 可以写成:

$$x^\tau=1+(1+x)^{k_1}+(1+x)^{k_2}\cdots+(1+x)^{k_g}$$

这时因为由 x^τ 作为生成函数的序列的线性复杂度为 2^n. 因此当 $u_1<v_1$ 时, $x^\tau s^N(x)+t^N(x)$ 中次数最低的一项就是 $(1+x)^{u_1}$,反之则是 $(1+x)^{v_1}$. 因此能得到下面的定理:

定理 2　设序列 $s=s_0s_1s_2\cdots s_{N-1}\cdots$, $t=t_0t_1t_2\cdots t_{N-1}\cdots$,两个序列都具有最小周期 $N=2^n$,线性复杂度分别为 $LC(s)$, $LC(t)$. 若 $LC(s)<LC(t)$,则序列 s 和 t 之间的互相关函数满足:

$$|C_{s,t}(\tau)|\leqslant|2^n-2^{W_H(2^n-LC(t))+1}|$$

该定理可以应用于构造满足有界互相关函数的序列族,下面举例说明:

例 2　设 $s^{16}=1101010011100111$; $t^{16}=1111010110100000$,则 $LC(s^{16})=11$, $LC(t^{16})=10$,由定理 2,可知序列的互相关函数满足:

$$|C_{s,t}(\tau)|\leqslant\frac{1}{2},\tau=0,\cdots,15.$$

实际计算结果如表 2.

表 2

τ	1,	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$C_{S,T}(\tau)$	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{2}$	0	0	0	$-\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	0	0	$-\frac{1}{2}$	0	$-\frac{1}{4}$	$-\frac{1}{4}$

对照理论结果和实际计算结果可知,当 $\tau=2,12$ 时, $|C_{s,t}(\tau)|$ 达到理论界 0.5,这说明由线性复杂度确定的界是紧的. 若可以从理论上已知序列族中所有序列的线性复杂度,则可以通过以上的方法来简单的检验一下序列之间的互相关性质.

4　进一步的结果

本部分针对一类周期为 2^n 的二元序列,基于文献[4]中的结果进一步提高了定理 1 中的界,首先来看一下文献[5]中的两个结果:

引理 3[5]　设 $n\geqslant 2, 0\leqslant t_1<t_2<\cdots<t_m\leqslant 2^n-1$. 则在 $GF(2)$ 有:

$$W((1+x)^{t_1}+(1+x)^{t_2}\cdots+(1+x)^{t_m})\geqslant W((1+x)^{t_1}+(1+x)^{t_2})$$

引理 4[5]　设 s 是周期为 $N=2^n$ 的二元序列, $LC(s)$ 为其线性复杂度. 若

$$s^N(x)=(1+x)^{2^n-LC(s)}+(1+x)^{t_2}\cdots+(1+x)^{t_m}$$

且 $W((1+x)^{2^n-LC(s)}+(1+x)^{t_2})>W((1+x)^{2^n-LC(s)})$,其中 $2^n-LC(s)<t_2<\cdots<t_m\leqslant 2^n-1, m>1$ 则

$$LC_k(s)=2^n-t_2.$$

其中 $LC_k(s)$ 指序列 s 的线性复杂度 $LC(s)$ 第一次下降时

的 k-错线性复杂度.

我们沿用文献[5]中的一个符号: 令 $a = a_m 2^m + a_{m-1} 2^{m-1} + \cdots + a_0$, $b = b_m 2^m + b_{m-1} 2^{m-1} + \cdots + b_0$ 为两个正整数, 其中, $a_m, a_{m-1}, \cdots a_0, b_m, b_{m-1}, \cdots b_0 \in GF(2)$, 定义 $a \wedge b = a_m b_m 2^m + a_{m-1} b^{m-1} 2^{m-1} + \cdots + a_0 b_0$. 由上述的两个引理可以得到下面的定理:

定理 **3** 设 s 是周期为 $N = 2^n$ 的二元序列, LC(s)为其线性复杂度. 若

$$s^N(x) = (1+x)^{2^n - LC(s)} + (1+x)^{t_2} \cdots + (1+x)^{t_m}$$

且 $W((1+x)^{2^n-LC(s)} + (1+x)^{t_2}) > W((1+x)^{2^n - LC(s)})$, 其中 $2^n - LC(s) < t_2 < \cdots < t_m \leqslant 2^n - 1$, $m > 1$ 则序列 s 的自相关函数值 $A_S(t)$ 满足下面的不等式:

若 $t = 2^i j + 1$, 且 $LC(s) - LC_k(s) > 2^i - 1$, 则:

$$|A_S(t)| \leqslant |2^n - 2^{W_H(2^n - LC(s)+1)+1} - 2^{W_H(2^n - LC(s)+2^i)+1} + 2^{W_H((2^n - LC(s)+1) \wedge (2^n - LC(s)+2^i))+2}|;$$

若 $t = 2^i j + 1$, 且 $LC(s) - LC_k(s) < 2^i - 1$, 则:

$$|A_S(t)| \leqslant |2^n - 2^{W_H(2^n - LC(s)+1)+1} - 2^{W_H(2^n - LC_k(s)+1)+1} + 2^{W_H((2^n - LC(s)+1) \wedge (2^n - LC_k(s)+1))+2}|;$$

若 $t = 2^i j + 1$, 且 $LC(s) - LC_k(s) = 2^i - 1$, 则:

$$|A_S(t)| \leqslant |2^n - 2^{W_H(2^n - LC(s)+1)+1} - 2^{W_H(2^n - LC_k(s)+2^i)+1} + 2^{W_H((2^n - LC(s)+1) \wedge (2^n - LC_k(s)+2^i))+2}|;$$

若 $t = 2^{i_1} j_1 - 1 = 2^{i_2} j_2$, 且 $LC(s) - LC_k(s) < -2^{i_1}$, 则:

$$|A_S(t)| \leqslant |2^n - 2^{W_H(2^n - LC(s)+2^{i_1})+1} - 2^{W_H(2^n - LC_k(s)+2^{i_1})+1} + 2^{W_H((2^n - LC(s)+2^{i_1}) \wedge (2^n - LC_k(s)+2^{i_1}))+2}|;$$

若 $t = 2^{i_1} j_1 - 1 = 2^{i_2} j_2$, 且 $LC(s) - LC_k(s) > 2^{i_2} - 2^{i_1}$, 则:

$$|A_S(t)| \leqslant |2^n - 2^{W_H(2^n - LC(s)+2^{i_1})+1} - 2^{W_H(2^n - LC(s)+2^{i_2})+1} + 2^{W_H((2^n - LC(s)+2^{i_1}) \wedge (2^n - LC(s)+2^{i_2}))+2}|;$$

若 $t = 2^{i_1} j_1 - 1 = 2^{i_2} j_2$, 且 $LC(s) - LC_k(s) = 2^{i_2} - 2^{i_1}$, 则:

$$|A_S(t)| \leqslant |2^n - 2^{W_H(2^n - LC(s)+2^{i_1})+1} - 2^{W_H(2^n - LC_k(s)+2^{i_2})+1} + 2^{W_H((2^n - LC(s)+2^{i_1}) \wedge (2^n - LC_k(s)+2^{i_2}))+2}|.$$

其中 $t \in \{1, 2, \cdots, 2^n - 1\}$.

该定理的证明和定理 1的证明类似, 即寻找 $P_0(x)$ 中 $(x+1)$ 次数最低的两项, 然后由引理 3来得到所要的结果. 从定理的结果可以看出这类序列 s 的自相关函数值的界不仅依赖于线性复杂度, 而且还依赖于序列的 k-错线性复杂度. 因此要更精确的估计这类序列的自相关函数值, 需要分别计算序列的线性复杂度和 k-错线性复杂度. 注意到定理 3并不适用于所有的周期为 2^n 的二元序列, 而定理 1则适合所有的周期为 2^n 的二元序列.

针对这类序列之间的互相关函数值也有类似的结论.

5 结论

本文首次指出了自相关函数和线性复杂度之间的关系: 即, 对于周期为 2^n 的二元序列, 序列的自相关函数值可以由序列线性复杂度的 Hamming 重量来界定. 这种关系可应用于以下两个方面: (1)由序列的线性复杂度来估计/确定序列的自相关函数值; (2)通过线性复杂度来检验序列族互相关性质. 进一步的, 针对一类周期为 2^n 的伪随机序列, 我们指出这类序列的自相关函数值和线性复杂度以及 k-错线性复杂度存在着关系. 显然这两个关系都可以推广到 q 元情况.

我们得到这两个关系都是基于多项式的权重不等式. 因此要改进这两个界必须首先考虑改进多项式的权重不等式.

参考文献:

[1] E R Berlekamp. Algebraic coding theory[M]. New York: McGraw-Hill, 1986.

[2] R Games, A Chan. A fast algorithm for determining the complexity of a binary sequence with period 2n[J]. IEEE Trans Inform Theory, 1983, 29(1): 144-146.

[3] J L Massey, D Costello, J Justesen. Polynomial weights and code constructions[J]. IEEE Trans Inform Theory, 1973, 19(1): 101-110.

[4] K Kurosawa, F Sato, T Sakata, W Kishimoto. A relation between linear complexity and k-error linear complexity[J]. IEEE Trans Inform Theory, 2000, 46(2): 694-698.

[5] 赵耀东, 戚文峰. 二元周期序列的线性复杂度[J]. 电子学报, 2005, 33(1), 12-16.
Zhao Yao-dong, Qi Wen-feng. On the k-error linear complexity of binary period sequences[J]. Acta Electronica Sinica, 2005, 33(1): 12-16. (in Chinese)

作者简介:

高军涛 男, 1979年生于河北临城, 西安电子科技大学计算机网络与信息安全教育部重点实验室博士生, 主要研究方向为序列密码, 信息安全. E-mail: gjt_albert@163.com

胡予濮 男, 1955年生于河南濮阳, 西安电子科技大学教授, 博士生导师, 信息保密研究所所长. 主要研究方向为密码学和信息安全. E-mail: yphu@mail.xidian.edu.cn

李雪莲 女, 1979年生于吉林公主岭市, 西安电子科技大学理学院讲师, 主要研究方向为密码学和信息安全.
E-mail: xuelian202@163.com