布尔函数的统计独立性

何良生
(信息工程大学电子技术学院　郑州 450002)

摘　要　定义在同一定义域上的两个布尔函数可能存在多种关系，本文研究它们之间的统计独立性，这种性质可以用于布尔置换的构造。本文给出了利用布尔函数的汉明距离判定两个布尔函数是否统计独立的充分必要条件，给出了寻找与某个已知布尔函数统计独立的布尔函数的算法，并分析了这种算法的有效性。

关键词　密码学，布尔函数，统计独立

On the Statistical Independence of Boolean Functions

HE Liang-Sheng
(School of Electronics Technology, Information Engineering University, Zhengzhou 450002)

Abstract　Two Boolean functions defined on the same domain may have veriety of relationships. This paper studies their statistical independence, which is useful in the construction of Boolean permutations. This paper gives a necessary and sufficient condition for judging two Boolean functions to be statistical independent, and gives an algorithm for finding Boolean functions who are statistical independent of the given one, and an analysis of the effectiveness of the algorithm is given.

Keywords　Cryptography, Boolean function, Statistical independence

1　引言

在现代密码学中，分组密码具有极其重要的应用，特别是在新兴的电子商务中，保密通信所用工具几乎全是分组密码。分组密码一般包括两类，对称分组密码(又称为传统分组密码)和非对称分组密码(又称为公钥密码)。在这些密码中，加密和解密变换分别是从明文消息空间(所有可能消息所组成的集合)到密文消息空间(所有可能的密文所组成的集合)的一对一映射和逆映射。在对称分组密码中，这种映射由一个随机选取的密钥所控制，而在非对称分组密码中，公钥和私钥的选取过程决定了如何对给出的某一映射找到其逆映射。

有趣的是，许多密码都采用了明文和密文分组长度相同的情况，这就导致了明文空间与密文空间相同，即它们都是包含所有长度为分组长度的数组的集合。为叙述方便我们记这个集合为 M。由于不管对什么明文，加密后再通过解密能唯一恢复原来的明文，这就要求加密必须是定义在集合 M 上的一个置换，而解密就是对应的逆置换。但是，由于集合 M 很大，比如含有 2^{128} 或更多个元素，能构造用于加密的置换必须具有一定的结构，这就使得对给定的一个置换，即使它有显式表达式(如 RSA[1])，如果没有其它信息，要找到它的逆置换也是在计算上不可实现的。

因此，置换与分组密码有着密不可分的关系。如果能找到一种灵活的可用显式表示的大集合上的置换，以及在其它一些信息帮助下可构造出逆置换，则这种置换表示法可成为构造新型密码体制的一种方法。在这些置换的表示中，用布尔函数方法来表示置换 就是其中的一种。用这种方法构造的置换称为布尔置换，它已被应用于密码体制的构造中[2]。因此，布尔置换的构造问题一直是密码学中的重要课题之一。最近，文[3]中给出了布尔置换的一种构造方法，其中用到布尔函数统计独立的概念。本文的主要目的是研究布尔函数之间的统计独立性，这种统计独立性的研究将为布尔置换的构造算法的实现提供理论依据。首先我们简单介绍这种建立在布尔函数统计独立概念上的布尔置换的构造方法。

2　布尔置换的构造算法

设 $GF(2)$ 为只有两个元素 0 和 1 的有限域，该域上的加法运算记为⊕，相当于逻辑异或(XOR)，乘法运算等价于实数域上的乘法。$GF(2)$ 上的 n 维向量空间记为 $GF^n(2)$。从 $GF^n(2)$ 到 $GF(2)$ 上的映射可以看作 $GF(2)$ 上 n 个输入一个输出的函数，记为 $f(x_1,x_2,\cdots,x)$，其中每一个 x_i 都是一个布尔变元，即其可能的取值为 0 或 1。为书写方便，通常将此函数记为 $f(x)$。我们称 $f(x)$ 为 n 个变元的布尔函数。将 m 个布尔函数 $f_1(x),f_2(x),\cdots,f_m(x)$ 组合在一起，则构成 $GF^n(2)$ 到 $GF^m(2)$ 上的映射。当 $m=n$ 且该映射为一一变换时，该函数组称为一个 n 元布尔置换，记为

$$P(x)=[f_1(x),f_2(x),\cdots,f_n(x)]$$

当一组布尔函数构成一个布尔置换时，它们必须满足一定的性质。利用这些性质可以判断给定的一组布尔函数是否构成一个布尔置换。

引理 1[4]　设 $f_1(x),f_2(x),\cdots,f_n(x)$ 为一组 n 个变元的布尔函数，则 $P(x)=[f_1(x),f_2(x),\cdots,f_n(x)]$ 构成一个布尔置换的充分必要条件为，对任意 $c=(c_1,c_2,\cdots,c_n)\in\{0,1\}^n$，$\sum_{i=1}^n c_i f_i(x)$ 是一个平衡布尔函数，其中 $\sum$ 表示模 2 和。

引理 1 是用来判定一组布尔函数构成布尔置换的有效方法。我们将用这一方法来判定本文给出的方法所构造的布尔函数组是否真正构成一个布尔置换。

对于布尔置换的构造问题，在文[5]中给出了一种方法，其算法描述如下：

何良生　研究员，主要研究方向为信息安全和密码学。

算法 1[5]

1)设 $P_1=[g_1,g_2,\cdots,g_{n-1},]$,$P_2[h_1,h_2,\cdots,h_{n-1}]$为由算法 5.1 构造的两个 $n-1$ 阶布尔置换,满足 $g_i\oplus x_n\neq 0$,$i=1,2,\cdots,n-1$。

2)令 $f_i(x)=g_i\oplus x_n(g_i\oplus h_i)$,$i=1,2,\cdots,n-1$;$f_n(x)=1\oplus x_n$。

3)输出 $P=[f_1,f_2,\cdots,f_n]$。

算法 1 能输出 n 元非线性布尔置换,它们的正确性已得到证明。最近文[3]中给出了一种新的构造算法,该算法的基本思想是建立在下面的定理上的。

定理 1[3] 设$[g_1(x)g_2(x)\cdots g_n(x)]$是一个布尔置换 $f_i(x)$与 $g_i(x)$统计独立,其中 $i=1,2,\cdots,k$,$k\leqslant n$,且对任意二元数组$(c_1,c_2,\cdots,c_k)\in\{0,1\}^k$,$\sum_{i=1}^{k}c_if_i(x)$与$\sum_{i=1}^{k}c_ig_i(x)$也统计独立,则$[f_1\oplus g_1,\cdots,f_k\oplus g_k,\cdots g_{k+1},\cdots g_n]$是一个新的布尔置换。

在上述定理中用到布尔函数统计独立的概念,本文的主要目的就是研究布尔函数之间的这种统计独立性。

3 布尔函数的统计独立性及其性质

首先,我们给出布尔函数统计独立性的概念。

定义 1 设 $f(x)$与 $g(x)$是两个 n 元布尔函数。若对任意 $a,b\in\{0,1\}$,都有

$$Prob(f(x)=a|g(x)=b)=Prob(f(x)=a)$$

其中 $Prob(A)$表示事件 A 发生的概率,$Prob(A|B)$表示在事件 B 发生的条件下,事件 A 发生的条件概率,则称 $f(x)$与 $g(x)$统计独立。

定义 1 讨论的情况是 $f(x)$的取值是否受 $g(x)$取值(条件)的影响,即条件概率等于绝对概率。如果条件满足,那么反过来,$g(x)$的取值是否受 $f(x)$取值的影响呢? 我们有

引理 2 设 $f(x)$与 $g(x)$是两个 n 元布尔函数,$a,b\in\{0,1\}$。若满足

$$Prob(f(x)=a|g(x)=b)=Prob(f(x)=a),$$

则必有

$$Prob(g(x)=b|f(x)=a)=Prob(g(x)=b)。$$

证明:为叙述方便,我们将两个事件记为 $A=\{f(x)=a\}$,$B=\{g(x)=b\}$。则引理的条件说明该事件满足 $Prob(A|B)=Prob(A)$。根据概率的乘法规则:

$$Prob(AB)=Prob(A|B)Prob(B)=Prob(B|A)Prob(A)$$

有

$$Prob(B|A)=\frac{Prob(A|B)Prob(B)}{Prob(A)}$$

因为

$$Prob(A|B)=Prob(A)$$

故得 $Prob(B|A)=Prob(B)$,此即

$$Prob(g(x)=b|f(x)=a)=Prob(g(x)=b)$$

故引理结论成立。

引理 2 表明,若 $f(x)$与 $g(x)$统计独立,则此时 $g(x)$与 $f(x)$亦统计独立,因此布尔函数的统计独立性是一种相互的关系。

引理 3 设 $f_1(x)$,$f_2(x)$,$g(x)$都为 n 元布尔函数。若 $f_1(x)$和 $f_2(x)$都与 $g(x)$统计独立,则 $f_1(x)\oplus f_2(x)$与 $g(x)$亦统计独立。

证明:我们只要能证明对任意 $a,b\in\{0,1\}$,有

$$Prob(f_1(x)\oplus f_2(x)=a|g(x)=b)=Prob(f_1(x)\oplus f_2(x)=a)$$

即可。当 $a=b=0$ 时,因为在二元域上的加法运算满足 $0\oplus 0=0$,$1\oplus 1=1$,故有

$$\begin{aligned}&Prob(f_1(x)\oplus f_2(x)=0|g(x)=0)\\&=Prob(f_1(x)=1|g(x)=0)Prob(f_2(x)=1|g(x)=0)\\&\quad+Prob(f_1(x)=0|g(x)=0)Prob(f_2(x)=0|g(x)=0)\\&=Prob(f_1(x)=0).Prob(f_2(x)=0)+Prob(f_1(x)=1).Prob(f_2(x)=1)\\&=Prob(f_1(x)\oplus f_2(x)=0)\end{aligned}$$

同理,当 $a=1,b=0$ 时,因为有 $0\oplus 1=1$,$1\oplus 0=1$,故有

$$\begin{aligned}&Prob(f_1(x)\oplus f_2(x)=1|g(x)=0)\\&=Prob(f_1(x)=0|g(x)=0)Prob(f_2(x)=1|g(x)=0)\\&\quad+Prob(f_1(x)=1|g(x)=0)Prob(f_2(x)=0|g(x)=0)\\&=Prob(f_1(x)=0).Prob(f_2(x)=1)+Prob(f_1(x)=1).Prob(f_2(x)=0)\\&=Prob(f_1(x)\oplus f_2(x)=1)\end{aligned}$$

这就证明了当 $b=0$ 时,无论 $a=0$ 还是 $a=1$,都满足

$$Prob(f_1(x)\oplus f_2(x)=a|g(x)=b)=Prob(f_1(x)\oplus f_2(x)=a)$$

即 $f_1(x)\oplus f_2(x)$与 $g(x)$统计独立。类似地可以证明,当 $b=1$ 时,亦有

$$Prob(f_1(x)\oplus f_2(x)=a|g(x)=b)=Prob(f_1(x)\oplus f_2(x)=a)$$

根据定义 1 知 $f_1(x)\oplus f_2(x)$与 $g(x)$统计独立。

引理 4 设 $f(x)$与 $g(x)$统计独立。若 $f(x)$是平衡布尔函数,则 $f(x)\oplus g(x)$也是平衡布尔函数。

证明:根据概率的乘法公式,有

$$Prob(f(x)=1|g(x)=1).Prob(g(x)=1)=Prob(f(x)=1,g(x)=1)$$

因 $f(x)$与 $g(x)$统计独立,我们有 $Prob(f(x)=1|g(x)=1)=Prob(f(x)=1)$,因此上式变为

$$Prob(f(x)=1).Prob(g(x)=1=Prob(f(x)=1,g(x)=1)$$

即

$$\frac{W_H(f)}{2^n}\cdot\frac{W_H(g)}{2^n}=\frac{W_H(fg)}{2^n}$$

因 $f(x)$是平衡布尔函数,即有 $W_H(f)=2^{n-1}$,则由上式得 $W_H(fg)=\frac{W_H(g)}{2}$,故有

$$W_H(f+g)=W_H(f)+W_H(g)-2W_H(fg)=2^{n-1}+W_H(g)-2\cdot\frac{W_H(g)}{2}=2^{n-1}$$

此表明函数 $f(x)\oplus g(x)$是平衡的。

4 关于布尔函数统计独立性的判定与求法

在定理 1 给出的布尔置换的构造中,用到布尔置换中部分与分量布尔函数统计独立的另外一些布尔函数。因此如何求找或构造与给定布尔函数统计独立的布尔函数是实施上述算法的关键问题之一。本节将着重讨论布尔函数统计独立性,以及对给定的布尔函数,如何构造与其统计独立的布尔函数。

未经特别说明,我们讨论的布尔函数都是 n 个变元的,则在满足 $g(x)=1$ 的条件下,满足 $f(x)=1$ 的概率为

$$\frac{Prob(f(x)=1,g(x)=1}{Prod(g(x)=1)}=\frac{W_H(fg)/2^n}{W_H(g)/2^n}=\frac{W_H(fg)}{W_H(g)}$$

而 $f(x)=1$ 的非条件概率为 $Prob(f(x)=1)=\frac{W_H(f)}{2^n}$。假定 $f(x)$ 与 $g(x)$ 独立，则上述两个概率应相等，即 $\frac{W_H(fg)}{W_H(g)}=\frac{W_H(f)}{2^n}$，由此得 $W_H(fg)=\frac{W_H(f)W_H(g)}{2^n}$。

同样如果我们考虑在 $g(x)=0$ 的条件下 $f(x)=0$ 的概率，则由

$$Prob(f(x)=0|g(x)=0)=Prob(f(x)=0$$

得到

$$W_H(\bar{f})W_H(\bar{g})=2^nW_H(\overline{fg})$$

其中 $\bar{f}(x)=f(x)\oplus 1$。注意 $W_H(g\oplus f)=W_H(f)+W_H(g)-2W_H(gf)$，故

$$\begin{aligned}W_H(\overline{fg})&=W_H(1\oplus f\oplus g\oplus fg)\\&=W_H(1\oplus f)+W_H(g\oplus fg)-2W_H(1\oplus f)(g\oplus fg)\\&=W_H(1\oplus f)+W_H(g\oplus fg)-2W_H(g\oplus fg)\\&=[2^n-W_H(f)]-[W_H(g)+W_H(fg)-2W_H(fg)]\\&=2^n-W_H(f)-W_H(g)+W_H(fg)\end{aligned}$$

由于 $W_H(\bar{f})=2^n-W_H(f)$，$W_H(\bar{g})=2^n-W_H(g)$，因此上述等式 $W_H(\bar{g})W_H(\bar{f})=2^nW_H(\overline{fg})$ 变为 $2^n[2^n-W_H(f)-W_H(g)+W_H(fg)]=[2^n-W_H(f)][2^n-W_H(g)]$，化简即为 $2^nW_H(fg)=W_H(f)W_H(g)$。

当考虑 $g(x)=1$ 的条件下 $f(x)=0$ 的概率时，则由 $Prob(f(x)=0|g(x)=1)=Prob(f(x)=0)$ 得到

$$W_H(\bar{f})W_H(g)=2^nW_H(\bar{f}g)$$

整理得：

$$[2^n-W_H(f)]W_H(g)=2^nW_H(g\oplus fg)$$

$$2^nW_H(g)-W_H(fg)=2^n[W_H(g)+W_H(g)-2W_H(fg)]$$

$$W_H(f)W_H(g)=2^nW_H(fg)$$

当考虑 $g(x)=0$ 的条件下 $f(x)=1$ 的概率时，类似地也得到 $W_H(f)W_H(g)=2^nW_H(fg)$。

综上所述，我们得到当 $f(x)$ 与 $g(x)$ 独立时，必有 $W_H(f)W_H(g)=2^nW_H(fg)$，因此我们得到 $f(x)$ 与 $g(x)$ 独立的一个必要条件。

反过来，若满足 $W_H(fg)=\frac{W_H(f)W_H(g)}{2^n}$，则

$$\begin{aligned}Prob(f(x)=1)&=\frac{W_H(f)}{2^n}=\frac{W_H(fg)}{W_H(g)}=\frac{W_H(fg)/2^n}{W_H(g)/2^n}\\&=\frac{Prob(f(x)=1),g(x)=1)}{Prob(g(x)=1)}\\&=Prob(f(x)=1|g(x)=1)\end{aligned}$$

将上述必要性的证明逆过去，我们将得到，条件 $W_H(fg)=\frac{W_H(f)W_H(g)}{2^n}$ 也是 $Prob(f(x)=0|g(x)=0)=Prob(f(x)=0)$ 的充分条件，也是 $Prob(f(x)=0|g(x)=1)=Prob(f(x)=0$ 的充分条件，也是 $Prob(f(x)=1|g(x)=0=Prob(f(x)=1)$ 的充分条件。注意在推导 $Prob(f(x)=1|g(x)=1)Prob(f(x)=1)$ 的过程中，要求 $W_H(g)\neq 0$。同样在推导其它几个结论的过程中，还要求 $W_H(\bar{g})\neq 0$，即要求 $g(x)$ 不为常数。由于独立关系的对称性，这种要求同样也适合 $f(x)$，因此我们得到

定理 2 两个非常数布尔函数 $f(x)$ 与 $g(x)$ 独立的充分必要条件是

$$W_H(f)W_H(g)=2^nW_H(fg)$$

如果有一个布尔函数为常数会怎么样？不妨假设 $g(x)=1$，则 $Prob(g(x)=0)=0$，即事件 $g(x)=$ 为不可能事件，因此以此为条件的条件事前必然为全真事件，即 $Prob(f(x)=a|g(x)=0)=Prob(f(x)=a)$ 对任意 $a\in\{0,1\}$ 都成立，因此我们得到

定理 3 常数函数与任意函数独立。

下面根据定理 2 来讨论什么样的布尔函数存在与其独立的布尔函数，有多少这样的函数，如何构造等问题。首先根据定理 2 不难看出

定理 4 若布尔函数 $f(x)$ 的汉明重量为奇数，则不存在与其独立的布尔函数。

证明：我们用反证法，假设存在与 $f(x)$ 独立的布尔函数 $g(x)$。因为 $W_H(f)$ 为奇数，则必有 $\gcd(W_H(f),2)=1$。由定理 2 知 $2^n|W_H(f)W_H(g)$，因此必有 $2^n|W_H(g)$，即 $g(x)\equiv 1$。但根据定理 3，$g(x)$ 不存在与其独立的布尔函数，此与假设矛盾。此矛盾表明定理结论正确。

定理 3 和定理 4 说明，我们只能从那些汉明重量为偶数的非常数布尔函数中寻找那些相互独立的布尔函数。假定 $f(x)$ 是这样一个函数，如何构造 $g(x)$ 使它们独立呢？根据定理 5.2，只要使 $g(x)$ 满足定理 2 即可。下列算法给出了一种求找独立函数的方法。

算法 2 输入布尔函数 $f(x)$。

1)将 $supp(f)$ 和 $supp(\bar{f})$ 均匀地分成 $t=\gcd(2^n,W_H(f))$ 组；

2)分别从两组中各任取 k 组作为 $g(x)$ 的支撑 $supp(g)$。

3)输出 $g(x)$。

算法 2 的正确性由下列定理保证。

定理 5 算法 2 所产生的函数 $g(x)$ 与输入函数 $f(x)$ 独立。

证明：根据定理 2，我们只需证明(5.2)式成立即可。从算法 2 的步骤中不难看出，在 $supp(g)$ 中，有 k 个大小为 $\frac{W_H(f)}{\gcd(2^n,W_H(f))}$ 的组是从 $supp(f)$ 中选取的，而且没有其它 $supp(f)\cap supp(g)$ 属于的元素，因此

$$W_H(fg)=k\cdot\frac{W_H(f)}{\gcd(2^n,W_H(f))}$$

因为在 $supp(g)$ 中同时还包含在 $supp(\bar{f})$ 中的 k 个大小为 $\frac{2^n-W_H(f)}{\gcd(2^n,W_H(f))}$ 的组，因此

$$\begin{aligned}W_H(g)&=W_H(fg)+k\cdot\frac{2^n-W_H(f)}{\gcd(2^n,W_H(f))}\\&=\frac{2^nk}{\gcd(2^n,W_H(f))}\end{aligned}$$

于是我们得到

$$Prob(f(x)=1|g(x)=1=\frac{W_H(fg)}{W_H(g)}=\frac{k\cdot W_H(f)}{\gcd(2^n,W_H(f))}/\frac{2^nk}{\gcd(2^d,W_H(f))}=\frac{W_H(f)}{2^n}$$

因此定理得证。

注意到在定理 5 的证明中，所用到的 $t=\gcd(2^n,W_H(f))$ 在证明中相互抵消掉，似乎对 $supp(f)$ 和 $supp(\bar{f})$ 的分割不一定要以 t 为大小。但不难发现，因为 $gcd(|supp(f)|,|supp(\bar{f})|=t$，所以 t 是可以同时整数分割 $supp(f)$ 和 $supp(\bar{f})$ 的最小单元。定理 5.5 表明算法 5.3 的正确性，但是否存在与 $f(x)$ 独立的函数不能被算法 2 来构造呢？下面的定理回答了这一问题。

定理 6 算法 2 可以构造所有与 $f(x)$ 相互独立的函数。

证明:我们需要证明任意与 $f(x)$ 相互独立的函数 $g(x)$ 都可以通过算法 2 来生成。设 $f(x)$ 与 $g(x)$ 相互独立,为书写方便,我们记 $d=\gcd(2^n,W_H(f))$。根据定理 2,我们有

$$W_H(fg)=\frac{W_H(f)W_H(g)}{2^n}=\frac{W_H(f)}{d}\cdot\frac{dW_H(g)}{2^n}$$

令 $k=\frac{dW_H(g)}{2^n}$,则 k 必为整数(否则可以推出 $W_H(fg)$ 不为整数,这显然不可能)。因此上式表明,$supp(f)$ 中有 $k\cdot\frac{W_H(f)}{d}$ 个元素包含在 $supp(g)$ 中,或者可以等价地理解为,当将 $supp(f)$ 中的元素分成大小为 $\frac{W_H(f)}{d}$ 的组时,在 $supp(g)$ 中有 k 个这样的组。更精确地,$supp(f)\cap supp(g)$ 的大小为 $k\cdot\frac{W_H(f)}{d}$(否则很容易导出矛盾结论)。如果能证明 $supp(g)$ 中另有 $supp(\bar{f})$ 中的 $k\cdot\frac{W_H(\bar{f})}{d}$ 个元素,则 $g(x)$ 就是按照算法 2 生成的。容易验证,

$$k\cdot\frac{W_H(f)}{d}+k\cdot\frac{W_H(\bar{f})}{d}=k\cdot\frac{2^n}{d}=\frac{dW_H(g)}{2^n}\cdot\frac{2^n}{d}=W_H(g)$$

这就证明了 $supp(f)$ 中的 $k\cdot\frac{W_H(f)}{d}$ 个元素和 $supp(\bar{f})$ 中的 $k\cdot\frac{W_H(\bar{f})}{d}$ 个元素构成了 $supp(g)$ 中的全部元素。故定理结论得证。

下面给出一个例子说明这种构造方法的工作原理。

例 1 4 个变元的布尔函数 $f(x)=x_1\oplus x_2x_3\oplus x_1x_2x_3\oplus x_4\oplus x_1x_4\oplus x_2x_4\oplus x_1x_2x_4$ 的支撑为 $supp(f)=\{0001,0011,0110,0111,1000,1001,1010,1011,1100,1101,1110,1111\}$,并且 $supp(\bar{f})=\{0000,0010,0100,0101\}$。将 $supp(f)$ 和 $supp(\bar{f})$ 分别分成 $\gcd(2^n,W_H(f))=4$ 组,对 $supp(f)$ 有多种不同的分法,这里随便选一种,不妨按照上述排列次序每三个一组。然后分别从 $supp(f)$ 和 $supp(\bar{f})$ 中取整数 k 组作为 $supp(g)$。当 $k=1$ 时,我们可以得到不同的 $g(x)$:

$g_1(x)=1\oplus x\oplus x_2\oplus x_1x_2\oplus x_3\oplus x_1x_3\oplus x_3x_4\oplus x_1x_3x_4$

$g_2(x)=x_3\oplus x_1x_3\oplus x_4\oplus x_1x_4\oplus x_2x_4\oplus x_1x_2x_4\oplus x_3x_4\oplus x_1x_3x_4$

$g_3(x)=x_2\oplus x_1x_3\oplus x_4\oplus x_1x_4$

$g_4(x)=x_2x_3\oplus x_1x_2x_3\oplus x_4\oplus x_1x_4\oplus x_2x_4\oplus x_2x_3x_4$

$g_5(x)=1\oplus x_2\oplus x_3\oplus x_2x_3\oplus x_4\oplus x_1x_4\oplus x_2x_4\oplus x_1x_2x_4\oplus x_3x_4\oplus x_1x_3x_4$

$g_6(x)=x_1\oplus x_1x_2\oplus x_3\oplus x_2x_3\oplus x_3x_4\oplus x_1x_3x_4$

$g_7(x)=x_1\oplus x_2\oplus x_1x_3\oplus x_2x_3\oplus x_2x_4\oplus x_1x_2x_4$

$g_8(x)=x_1\oplus x_1x_2\oplus x_1x_3\oplus x_1x_2x_3\oplus x_2x_4\oplus x_1x_2x_4$

$g_9(x)=1\oplus x_1\oplus x_2\oplus x_3\oplus x_2x_3\oplus x_1x_2x_3\oplus x_4\oplus x_1x_4\oplus x_2x_4\oplus x_3x_4\oplus x_1x_3x_4\oplus x_2x_3x_4$

$g_{10}(x)=x_1x_2\oplus x_3\oplus x_2x_3\oplus x_1x_2x_3\oplus x_1x_2x_4\oplus x_3x_4\oplus x_1x_3x_4\oplus x_2x_3x_4$

$g_{11}(x)=x_2\oplus x_1x_3\oplus x_2x_3\oplus x_1x_2x_3\oplus x_2x_4\oplus x_2x_3x_4$

$g_{12}(x)=x_1x_2\oplus x_1x_3\oplus x_2x_4\oplus x_2x_3x_4$

$g_{13}(x)=1\oplus x_1\oplus x_2\oplus x_1x_2\oplus x_3\oplus x_1x_3\oplus x_2x_3\oplus x_4\oplus x_1x_4\oplus x_2x_4\oplus x_3x_4\oplus x_1x_3x_4\oplus x_2x_3x_4$

$g_{14}(x)=x_3\oplus x_1x_3\oplus x_2x_3\oplus x_1x_2x_4\oplus x_3x_4\oplus x_1x_3x_4\oplus x_2x_3x_4$

$g_{15}(x)=x_2\oplus x_1x_2\oplus x_2x_3\oplus x_2x_4\oplus x_2x_3x_4$

$g_{16}(x)=x_1x_2x_3\oplus x_2x_4\oplus x_2x_3x_4$

例 1 仅仅给出了对 $supp(f)$ 的一种分组的情况,对于每一种分组,同样可以得到另外 16 个函数。对 $k=2,3$ 的情况同样讨论。注意当 $k=2$ 时,所构造的函数是平衡的。

结论 本文研究了布尔函数的统计独立的性质、判定、构造。利用布尔函数的汉明重量,给出了两个布尔函数统计独立的充分必要条件。进一步,对任意给定的布尔函数,如果它存在统计独立的函数的话,本文给出了一种构造所有那些与给定函数统计独立的布尔函数,并证明了其正确性和完备性。本文的结果将有利于文[3]中布尔置换构造算法的实现。

参 考 文 献

1 Shamir A, Rivest R L, Adlemen L. A method for obtaining digital signatures. Comunications of the ACM, 1979,21(2):120~126

2 Wu C K, Veredherejen V. Public Key Cryptosystems Based on Boolean Permutations and Their A lications. International Journal of Computer Mathematics,2000,74(2):167~184

3 何良生,孙红波. 布尔置换的构造,电子学报(已录用,待发表)

4 武传坤. 密码学中的布尔函数:[西安电子科技大学博士学位论文]. 1993

5 邢育森,杨义先. 密码体制中布尔置换的构造和记数. 通信学报,1998(3):74~76

6 温巧燕,等. 密码学中的布尔函数. 科学出版社,2000

(上接第 76 页)

议的不同之处在于,不同测量基的测量结果不是完全相互独立的,因此可以回收。这种构造方法在节省经典通信量和量子比特数上有显著的优势,如表 3 所示。

表 3 通信量的比较

每 n 个量子比特	经典通信量(bits)	丢弃量子数(qubits)
BB84,Ekert'91[2]	$2n$	$(1/2)n$
我们的方案	$(\log_2 3)n\approx 1.6n$	$(4/9)n$

参 考 文 献

1 Bennett C H, Brassard G. Quantum cryptography: Public-key distribution and coin tossing. In: Proc. IEEE Int. Conf. on Computers, systems, and signal processing, Bangalore, IEEE, New York, 1984. 175~179

2 Ekert A K. Quantum cryptography based on Belll's theorem. Phys Rev Lett, 1991, 67: 661~663

3 Gao Fei, Guo Fenzhuo, Wen Qiaoyan, Zhu Fuchen. Quantum key distribution without alternative measurements and rotations, Physics Letters A, 2006, 349: 53~58

4 Lo H, Chau H F. Unconditional security of quantum key distribution over arbitrary long distance. Science, 1999, 283, 2050~2056; Also available at arXive eprint quant-ph/9803006

5 Nielsen M, Chuang I. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2000. 587~591

6 Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. ,2000, 85:441~444; Also available at arXive e-print quant-ph/0003004

7 秦素娟,刘太琳,温巧燕. 基于纠缠交换和局域操作的量子秘密共享. 北京邮电大学学报,2005,28(4):74~77