“与密钥模 2^n 加运算”的差分性质研究

郑 斌　　关 杰
(信息工程大学电子技术学院　郑州　450004)

摘　要：“与密钥 K 模 2^n 加”—$Y=X+K \bmod 2^n$ 是密码算法中一个常用的基本编码环节，在 SAFER++，RC6 Phelix 等算法中有广泛的应用。该文对 $Y=X+K \bmod 2^n$ 进行了差分分析，首次给出了当差分转移概率取最大值 1，次大值 $1-1/2^{n-2}$，次小值 $1/2^{n-2}$ 以及 1/2 时，输入差，输出差及密钥的结构特点和计数公式。

关键词：密码学；差分分析；模 2^n 加；差分转移概率
中图分类号：TN918.1　　**文献标识码**：A　　**文章编号**：1009-5896(2009)11-2708-05

Differential Characteristic Probability of Added Key on Modulo 2^n Operation

Zheng Bin　　Guan Jie
(*Electronic Technology Institute*, *Information Engineering University*, *Zhengzhou* 450004, *China*)

Abstract: Added key on modulo 2^n operation—$Y=X+K \bmod 2^n$ is a code link which is often used in cipher algorithms, as SAFER++, RC6, Phelix and so on. In this paper, the $Y=X+K \bmod 2^n$ is analyzed with differential cryptanalysis. And the characters of structure, counting formulas of input and output differences and the keys is given for the first time, when the differential probability is to be 1, $1-1/2^{n-2}$, $1/2^{n-2}$, 1/2.

Key words: Cryptography; Differential cryptanalysis; Addition on modulo 2^n; Differential probability

1　引言

“与密钥 K 模 2^n 加”—$Y = X + K \bmod 2^n$ 是密码算法中一个常用的基本编码环节，该环节具有较好的非线性性质，在许多分组密码和流密码算法中有广泛的应用，例如 SAFER++[1]，RC6[1]，CAST-256[1]，Phelix[2,3]。差分密码分析[4]是针对分组密码算法提出的一种有效的分析方法。对密码算法的加密环节进行差分分析，有助于密码分析者分析密码算法抗差分攻击的强度，对于密码设计者设计抵抗差分攻击的密码算法也是十分必要的。目前公开文献中有一些关于模 2^n 加运算密码学性质的研究结果[5–9]，其中 Hiroshi Miyano 给出了一些特殊情况下此环节差分转移概率和线性相关优势的计算公式，Alexis 给出了一个多项式时间计算此环节差分转移概率的算法。

从密码分析者的角度来说，对一个算法进行差分攻击时，希望能找到高概率的差分传递链，这样自然关心算法中所使用的加密环节—$Y = X + K \bmod 2^n$ 运算中差分转移概率取值比较大的点 $(\Delta X, \Delta Y, K)$ (即输入差 ΔX，输出差 ΔY 以及密钥 K)的结构特点以及计数，同时也关心差分转移概率取值比较小的点 $(\Delta X, \Delta Y, K)$ 的结构特点以及计数，以便对算法进行不可能差分攻击。目前还没有公开文献解决此问题。

本文对 $Y = X + K \bmod 2^n$ 运算的差分分布规律进行了研究，首次给出了差分转移概率取最大值 1，次大值 $1-1/2^{n-2}$，次小值 $1/2^{n-2}$ 以及 1/2 时，$(\Delta X, \Delta Y, K)$ 的结构特点和计数公式。

2　符号说明及相关结论

2.1　符号说明

(1) $\forall X \in Z/(2^n)$，记 $X = \sum_{i=0}^{n-1} 2^i x_i$，其中 $x_i \in \{0,1\} (0 \le i \le n-1)$，则 $(x_{n-1}, \cdots, x_1, x_0)$ 是 X 的二进制表示。

本文对 X 的实数表示和二进制表示不加区分地使用，即对 Z_2^n 中的 $(x_{n-1}, x_{n-2}, \cdots, x_0)$ 和 $Z/(2^n)$ 中的 X 不加区分。

(2)引入记号“田”：X田$K = X + K \bmod 2^n$；

(3) $\mathrm{DCP}(\Delta X, \Delta Y, K)$ 表示“ X田K ”运算关于 $(\Delta X, \Delta Y, K)$ 的差分转移概率，即 $\mathrm{DCP}(\Delta X, \Delta Y, K) = \#\{X : (X田K) \oplus ((X \oplus \Delta X)田K) = \Delta Y\}/2^n$。

有时将 $\mathrm{DCP}(\Delta X, \Delta Y, K)$ 简记为 DCP；在给定某个确定 K 情况下，也记 $\mathrm{DCP}(\Delta X, \Delta Y, K)$ 为 $\mathrm{DCP}(\Delta X, \Delta Y)$。

2008-11-03 收到，2009-07-21 改回

2.2 相关结论

Alexis 在文献[6]中给出了关于此环节的一个多项式时间计算差分转移概率的算法如图 1 所示。

$\lambda = \Delta x_0 \oplus \Delta y_0 \oplus 1; \delta_0 = 0$
for $i = 0$ to $n-2$
do
case $< \Delta x_i, \Delta y_i, \Delta x_{i+1} \oplus \Delta y_{i+1} >$ of
$< 0,0,0 >: \varphi_i = 1; \delta_{i+1} = (k_i + \delta_i)/2$
$< 0,0,1 >: \varphi_i = 0; \delta_{i+1} = 0$
$< 1,1,0 >: \varphi_i = 1 - (k_i + \delta_i - 2 \cdot k_i \cdot \delta_i); \delta_{i+1} = k_i$
$< 1,1,1 >: \varphi_i = k_i + \delta_i - 2 \cdot k_i \cdot \delta_i; \delta_{i+1} = 1/2$
$< 0,1,0 >: \varphi_i = 1/2; \delta_{i+1} = k_i$
$< 0,1,1 >: \varphi_i = 1/2$
$< 1,0,0 >: \varphi_i = 1/2; \delta_{i+1} = k_i$
$< 1,0,1 >: \varphi_i = 1/2$
end case;
$\lambda = \lambda \cdot \varphi_i$;
end for;

图 1 算法 1[6]

3 结构特点和计数公式

由算法 1 可知，当给定 $\Delta X, \Delta Y$ 和密钥 K 时，最多只需经过 $n-1$ 步计算就可以得到 DCP(ΔX, $\Delta Y, K$) 的值。本文在此算法的基础上，给出了此环节一些特殊点(最大、次大、次小值等)的结构特点和计数公式，具体如下：

3.1 DCP = 1 的结构及计数

定理 1　DCP($\Delta X, \Delta Y, K$) = 1 当且仅当 (ΔX, $\Delta Y, K$) 同时满足下列条件：

条件 1：$\forall i: 0 \le i \le n-2$，$\Delta x_i \oplus \Delta y_i = 0$；

条件 2：令 $t = \max\{0 \le i \le n-2 : \Delta x_i = 1\}$，当 $t \ne n-2$ 时，$\forall i: 0 \le i \le t$，均有 $k_i = 0$；当 $t = n-2$ 时，$\forall i: 0 \le i \le n-3$，均有 $k_i = 0$，$k_{n-2} = \Delta x_{n-1} \oplus \Delta y_{n-1}$。

特别地，若 $\forall i: 0 \le i \le n-2$，均有 $\Delta x_i = 0$，则令 $t = -1$。

证明　根据算法 1，要使 DCP($\Delta X, \Delta Y, K$) =1，则 $\forall i: 0 \le i \le n-2$，必须有 $\varphi_i = 1$。那么 $< \Delta x_i, \Delta y_i, \Delta x_{i+1} \oplus \Delta y_{i+1} >$ 只能取 <0,0,0> 或 <1,1,0>，当 $i = n-2$ 时，可以取<0,0,0>，<1,1,0>或<1,1,1>。总之，$\forall i: 0 \le i \le n-2$ 要满足条件 1。

下面 $\forall i: 0 \le i \le n-3$ 考查 $\Delta x_i = 0$ 和 $\Delta x_i = 1$ 这两种情况。

情况 1：当 $\Delta x_i = 1$ 时，即 $< \Delta x_i, \Delta y_i, \Delta x_{i+1} \oplus \Delta y_{i+1} > =$<1,1,0>，这时，$\varphi_i = 1 - (k_i + \delta_i - 2 \cdot k_i \cdot \delta_i); \delta_{i+1} = k_i$。若使 $\varphi_i = 1$，那么：$k_i + \delta_i - 2 \cdot k_i \cdot \delta_i = 0$，易推得：$\delta_{i+1} = k_i = \delta_i$。

情况 2：当 $\Delta x_i = 0$ 时，即 $< \Delta x_i, \Delta y_i, \Delta x_{i+1} \oplus \Delta y_{i+1} > =$<0,0,0>，这时，$\varphi_i = 1$，$\delta_{i+1} = (k_i + \delta_i)/2$。

若 Δx_i 的取值不再涉及情况 1，即 $\forall j: i+1 \le j \le n-3$，均有 $\Delta x_j = 0$，则 k_i 可取任意值。

若 Δx_i 的取值还将涉及情况 1，即存在 $j: i+1 \le j \le n-3$，使得 $\Delta x_j = 1$，由情况 1 知：使 $\varphi_j = 1$，必有 $k_j = \delta_j$；并且因为 $\delta_0 = 0$，那么 $\forall i: 0 \le i \le j$，k_i 只能取 0；否则 δ_j 为分数，$k_j = \delta_j$ 是不可能的。

下面讨论 Δx_{n-2} 的取值情况。

当 $\Delta x_{n-2} = 1$ 时，由算法可知 $< \Delta x_{n-2}, \Delta y_{n-2}, \Delta x_{n-1} \oplus \Delta y_{n-1} >$ 可以取<1,1,1>或<1,1,0>。

当取<1,1,0>时，同情况 1 的分析，$k_{n-2} = 0$；当取 <1,1,1> 时，由于 $\varphi_{n-2} = k_{n-2} + \delta_{n-2} - 2 \cdot k_{n-2} \cdot \delta_{n-2}$，若使 $\varphi_{n-2} = 1$，易得 $k_{n-2} \oplus \delta_{n-2} = 1$，而根据上述分析可知 $\delta_{n-2} = 0$，所以 $k_{n-2} = 1$；因此这时有，$k_{n-2} = \Delta x_{n-1} \oplus \Delta y_{n-1}$。

综上所述，得条件 2。　　证毕

定理 2　满足 DCP($\Delta X, \Delta Y, K$) = 1 的 (ΔX, $\Delta Y, K$) 个数为 $(n+2) \cdot 2^n$。

证明　根据定理 1 中 t 的取值不同，分 3 种情况分别计数：

情况 1：当 $t = -1$ 时，$\forall i: 0 \le i \le n-2$，$\Delta x_i = \Delta y_i = 0$ 且 $\Delta x_{n-1} \oplus \Delta y_{n-1} = 0$，此时 ($\Delta X, \Delta Y, K$) 的个数为 $2 \cdot 2^n$。

情况 2：当 $t = n-2$ 时，$\forall i: 0 \le i \le n-3$，$\Delta x_i = \Delta y_i, k_i = 0$，但 $k_{n-2} = \Delta x_{n-1} \oplus \Delta y_{n-1}$，此时 ($\Delta X$, $\Delta Y, K$) 的个数为 2^{n+1}。

情况 3：当 $0 \le t \le n-3$ 时，$\forall i: 0 \le i \le t$，$\Delta x_i = \Delta y_i$ 且 $k_i = 0$；对 $\forall i: t+1 \le i \le n-2$，$\Delta x_i = \Delta y_i = 0$ 且 $\Delta x_{n-1} \oplus \Delta y_{n-1} = 0$。分两部分计数，$0 \le i \le t$ 部分使 ($\Delta x_i, \Delta y_i, k_i$) 满足条件的个数为 2^t；$t+1 \le i \le n-1$ 部分使 ($\Delta x_i, \Delta y_i, k_i$) 满足条件的个数为 2^{n-t}，此时计数为 $\sum_{t=0}^{n-3} 2^t \cdot 2^{n-t} = (n-2) \cdot 2^n$。

综上所述，满足 DCP($\Delta X, \Delta Y, K$) = 1 的 (ΔX, $\Delta Y, K$) 总数为 $2^{n+1} + 2^{n+1} + (n-2) \cdot 2^n = (n+2) \cdot 2^n$。　　证毕

推论 1　对于任意给定密钥 K，满足 DCP(ΔX, ΔY) = 1 的 ($\Delta X, \Delta Y$) 有 2^{s+1} 个，其中 $s = \min\{0 \le i \le n-1 : k_i = 1\}$，特别地，当 $K = 0$ 时，约定 $s = n-1$。

证明　令 $s = \min\{0 \le i \le n-1 : k_i = 1\}$，由 DCP($\Delta X, \Delta Y, K$) =1 的结构特点，选取 $\Delta X = \Delta Y$ 具有如下形式：$\forall i: 0 \le i \le s-1$，$\Delta x_i$ 可任意选取；$\forall i: s \le i \le n-2$，$\Delta x_i = 0$；而且 $\Delta x_{n-1} \oplus \Delta y_{n-1} = k_{n-2}$，特别地，$K = 0$ 等效于 $s = n-1$ 的情况，

故 $K=0$ 时，约定 $s=n-1$。因此满足 DCP(ΔX, ΔY)$=1$的$(\Delta X,\Delta Y)$计数为$2\cdot 2^{s}=2^{s+1}$。 证毕

3.2 DCP$=1-1/2^{n-2}$的结构及计数

由算法 1 易知，$1-1/2^{n-2}$是“ X田K ”运算 DCP$(\Delta X,\Delta Y,K)$所能达到的次大值，下面给出其结构特点和计数公式。

定理 3 DCP$(\Delta X,\Delta Y,K)=1-1/2^{n-2}$当且仅当$(\Delta X,\Delta Y,K)$同时满足下列条件时：

条件 1：$\forall i:0\le i\le n-3$，$\Delta x_i=\Delta y_i=0$；$\Delta x_{n-2}=\Delta y_{n-2}=1$；$k_0=1$；

条件 2：$\forall j:1\le j\le n-3$，k_j相等，且$\Delta x_{n-1}\oplus\Delta y_{n-1}=k_{n-1}\oplus k_j$。

证明 显然$\forall i:0\le i\le n-3$，都不能有$<\Delta x_i,\Delta y_i,\Delta x_{i+1}\oplus\Delta y_{i+1}>=<1,0,1>$或$<1,0,0>$或$<0,1,1>$或$<0,1,0>$，否则DCP必然小于等于1/2。

下面$\forall i:0\le i\le n-3$，考察$<\Delta x_i,\Delta y_i,\Delta x_{i+1}\oplus\Delta y_{i+1}>=<0,0,0>$或$<1,1,0>$或$<1,1,1>$的情况。通过对算法1的分析发现，$\forall i:0\le i\le n-2$，不能都有$<\Delta x_i,\Delta y_i>=<0,0>$，否则DCP不可能等于$1-1/2^{n-2}$。并且，$\forall i:0\le i\le n-2$，$<\Delta x_i,\Delta y_i>=<1,1>$不能多于 1 个，否则DCP必然小于$1-1/2^{n-2}$。

同时有且只有一个$j:0\le j\le n-2$，$<\Delta x_j,\Delta y_j>=<1,1>$，并且发现若$j\ne n-2$，DCP必然小于$1-1/2^{n-2}$；只能是$<\Delta x_{n-2},\Delta y_{n-2}>=<1,1>$。这样，$\forall i:0\le i\le n-3$，$\Delta x_i=\Delta y_i=0$。

若 DCP$=1-1/2^{n-2}$，$\delta_{n-2}=1/2^{n-2}$ 或 $1-1/2^{n-2}$，那么k_0必然为1，故满足条件1。

当$\Delta x_{n-1}\oplus\Delta y_{n-1}=0$时，若$k_{n-2}=0$，则$\forall j:1\le j\le n-3$，$k_j=0$；若$k_{n-2}=1$，则$\forall j:1\le j\le n-3$，$k_j=1$。

当$\Delta x_{n-1}\oplus\Delta y_{n-1}=1$时，若$k_{n-2}=0$，则$\forall j:1\le j\le n-3$，$k_j=1$；若$k_{n-2}=1$，则$\forall j:1\le j\le n-3$，$k_j=0$。

综上所述，得条件2。 证毕

定理 4 满足DCP$(\Delta X,\Delta Y,K)=1-1/2^{n-2}$的$(\Delta X,\Delta Y,K)$个数为16。

证明 分两种情况讨论：

情况 1：当$\Delta x_{n-1}\oplus\Delta y_{n-1}=0$时，$k_{n-2},k_{n-1}$各有两种取值，计数为8。

情况 2：当$\Delta x_{n-1}\oplus\Delta y_{n-1}=1$时，$k_{n-2},k_{n-1}$各有两种取值，计数为8。

总计数为16。 证毕

3.3 DCP$=1/2^{n-2}$的结构及计数

由算法1易知，$1/2^{n-2}$是“ X田K ”运算DCP$(\Delta X,\Delta Y,K)$所能达到的次小值，下面给出其结构特点和计数公式。

定理 5 DCP$(\Delta X,\Delta Y,K)=1/2^{n-2}$当且仅当$(\Delta X,\Delta Y,K)$同时满足下列条件：

条件 1：存在且仅存在 1 个j，$0\le j\le n-2$，使得$\Delta x_j=\Delta y_j=1$；

条件 2：$k_0=1$；

条件 3：$\forall i:0\le i\le j-1$，均有$\Delta x_i=\Delta y_i=0$；$k_i=k_j$；

条件 4：$\forall i:j+1\le i\le n-2$，$\Delta x_i\oplus\Delta y_i=1$；

特别地，当$j=n-2$时，若$\Delta x_{n-1}\oplus\Delta y_{n-1}=0$，$\forall i:0\le i\le j-1$，$k_i\oplus k_{n-2}=1$。

证明 若DCP$(\Delta X,\Delta Y,K)=1/2^{n-2}$，则$\forall i:0\le i\le n-2$，$\varphi_i\ne 0$；那么$\Delta x_0=\Delta y_0$，必然使$\varphi_0=1$。

这样$\forall i:1\le i\le n-2$，平均每个$\varphi_i=1/2$；而且由算法的结构发现平均每个φ_i最小为1/2。

这样，通过对算法的分析可以发现，若$\exists j:1\le j\le n-3$，$\Delta x_j=\Delta y_j=1$，那么$\forall i:0\le i\le j$，不能存在$\Delta x_i\oplus\Delta y_i=1$。并必须有连续$j$个$<0,0,0>$，且$k_0=1$，使$\varphi_j=1/2^{j}$。类似地，$\forall i:j\le i\le n-2$，只能有$\Delta x_i\oplus\Delta y_i=1$，否则也不能使DCP$(\Delta X,\Delta Y,K)=1/2^{n-2}$。

当$j=n-2$时，若$\Delta x_{n-1}\oplus\Delta y_{n-1}=1$，同上面分析；当$\Delta x_{n-1}\oplus\Delta y_{n-1}=0$，若$k_j=1$，$\forall i:1\le i\le j-1$，$k_i=0$；若$k_j=0$，$\forall i:1\le i\le j-1$，$k_i=1$。即$\forall i:0\le i\le j-1$，$k_i\oplus k_{n-2}=1$。 证毕

定理 6 满足DCP$=1/2^{n-2}$的$(\Delta X,\Delta Y,K)$个数为$(5\cdot 2^{2n-1}-16)/3$。

证明 由DCP$=1/2^{n-2}$中，j的位置分3种情况分别计数：

情况 1：当$1\le j\le n-2$时，分两部分计数。

$\forall i,0\le i\le j-1$，$<\Delta x_i,\Delta y_i>=<0,0>$，$k_0=1$，而且$k_i$由$k_j$决定，所以该部分的计数为1。

$\forall i:j\le i\le n-1$，仅要求$\Delta x_i\oplus\Delta y_i=1$，因此计数为$2^{2n-2j}$。

此种情况下总计数为$\sum_{j=1}^{n-3}2^{2n-2j}=(2^{2n}-2^{6})/3$。

情况 2：当$j=0$时，要求$k_0=1$，$\forall i:j+1\le i\le n-1$，$\Delta x_i\oplus\Delta y_i=1$，因此计数为$2^{2n-1}$。

情况 3：当$j=n-2$时，$\forall i,0\le i\le n-3$，$<\Delta x_i,\Delta y_i>=<0,0>$，$k_0=1$，而且$k_i$由$k_{n-2}$决定，因此计数为$2^4$。

综上所述，满足DCP$=1/2^{n-2}$的$(\Delta X,\Delta Y,K)$总数为$(2^{2n}-2^{6})/3+2^{2n-1}+2^{4}=(5\cdot 2^{2n-1}-16)/3$。 证毕

3.4 DCP$=1/2$的结构及计数

满足 DCP$(\Delta X,\Delta Y,K)=1/2$ 的 $(\Delta X,\Delta Y,K)$

取值很有特点，具体如下。

为简便起见，将下列 3 个条件统称为条件 $\boldsymbol{A}$。

条件 1：$\forall i: p \le i \le n-1$，$\Delta x_i \oplus \Delta y_i = 0$；

条件 2：令 $t=\max\{p \le i \le n-2 : \Delta x_i=1\}$，$\forall i: 0 \le i \le t$，均有 $k_i = z$；

条件 3：当 $t = n-2$ 时，$\Delta x_{n-1} \oplus \Delta y_{n-1} = k_{n-2}$。

定理 7　DCP($\Delta X, \Delta Y, K$)=1/2 当且仅当($\Delta X, \Delta Y, K$)满足下列两个条件之一：

条件 1：

(1) $\forall i: 0 \le i \le n-2$，$\Delta x_i \oplus \Delta y_i = 0$；

(2)存在且仅存 1 个 j，$1 \le j \le n-2$，使得 $\Delta x_j = 1$，$\Delta x_{j-1} = 0$，$k_{j-1} = 1$；

(3) $\forall i: 0 \le i \le j-2$，均有 k_i=0；

(4)令 $z = k_j, p = j+1$，$(\Delta x_i, \Delta y_i, k_i)$ 满足条件 $\boldsymbol{A}$。

特别地，当 $j = 1$ 时，$k_0 = 1$；当 $j = n-2$ 时，$\Delta x_{n-1}, \Delta y_{n-1}$ 任意。

条件 2：

(1)存在且仅存在 1 个 j，$1 \le j \le n-2$，使得 $\Delta x_j \oplus \Delta y_j = 1$，$\Delta x_{j-1} = \Delta y_{j-1} = 1$，$k_{j-1} = 1$；

(2) $\forall 0 \le i \ne j \le n-2$，$\Delta x_i \oplus \Delta y_i = 0$；

(3) $\forall i: 0 \le i \le j-2$，均有 k_i=0；

(4)令 $z = k_j, p = j+1$，$(\Delta x_i, \Delta y_i, k_i)$ 满足条件 $\boldsymbol{A}$。

特别地，当 $j = 1$ 时，$k_0 = 1$；当 $j = n-2$ 时，$\Delta x_{n-1}, \Delta y_{n-1}$ 任意。

证明　由于 DCP($\Delta X, \Delta Y, K$)=1/2，故对于 j：$0 \le j \le n-2$，仅存在 1 个位置，使得 φ_j 取值为 1/2；对于其它的情况，即 $\forall i: 0 \le i \le n-2, i \ne j$，均有 φ_i 取值为 1。

根据 φ_j =1/2 的可能来源可将 $<\Delta x_j, \Delta y_j, \Delta x_{j+1} \oplus \Delta y_{j+1}>$ 分成以下两种情况。

情况 1：$<\Delta x_j, \Delta y_j, \Delta x_{j+1} \oplus \Delta y_{j+1}>$=<1,1,0> 或<1,1,1>

当 $1 \le j \le n-3$ 时，若 $<\Delta x_j, \Delta y_j, \Delta x_{j+1} \oplus \Delta y_{j+1}>$=<1,1,1>，则无论 Δx_{j+1} 和 Δy_{j+1} 如何选取，均有 φ_{i+1}=1/2，这时 $\varphi_j = \varphi_{i+1}$=1/2 故排除这种情况。

当 $<\Delta x_j, \Delta y_j, \Delta x_{j+1} \oplus \Delta y_{j+1}>$=<1,1,0>时，若 $\varphi_j = 1-(k_j + \delta_j - 2 \cdot k_j \cdot \delta_j)$ =1/2 当且仅当 $k_j + \delta_j - 2 \cdot k_j \cdot \delta_j$ =1/2，必然有 $\delta_j = 1/2$，那么需要考察 $<\Delta x_{j-1}, \Delta y_{j-1}, \Delta x_j \oplus \Delta y_j>$ 的取值。

又要求 φ_{j-1}=1，若 $<\Delta x_{j-1}, \Delta y_{j-1}, \Delta x_j \oplus \Delta y_j>$ =<1,1,0>，则不能使 $\delta_j = 1/2$；那么 $<\Delta x_{j-1}, \Delta y_{j-1}, \Delta x_j \oplus \Delta y_j>$ 只能为<0,0,0>，这时 $k_{j-1} \oplus \delta_{j-1}$=1。

$\forall i: 0 \le i \le j-2$，若使 φ_i=1，类似 DCP($\Delta X, \Delta Y, K$)=1 的结构，$(\Delta x_i, \Delta y_i, k_i)$ 需要满足以下条件：

$\forall i: 0 \le i \le j-2$，$\Delta x_i \oplus \Delta y_i = 0$；$\forall i: 0 \le i \le j-2$，均有 k_i=0；

由算法的结构易得 $\delta_{j-1} = 0$，因此 $k_{j-1} = 1$。

$\forall i: j+1 \le i \le n-2$，若使 φ_i =1，令 $z = k_j$，$p = j+1$，$(\Delta x_i, \Delta y_i, k_i)$ 需要满足条件 $\boldsymbol{A}$ 即可。

特别地，当 $j = n-2$ 时，$<\Delta x_{n-2}, \Delta y_{n-2}, \Delta x_{n-1} \oplus \Delta y_{n-1}>$ 可能为<1,1,1>或<1,1,0>，所以不论 $\Delta x_{n-1} \oplus \Delta y_{n-1}$，$k_{n-2}$ 如何取值均可使 φ_{n-2} =1/2，也就是说 $\Delta x_{n-1}, \Delta y_{n-1}$ 可以任意取值。

情况 2：$<\Delta x_j, \Delta y_j, \Delta x_{j+1} \oplus \Delta y_{j+1}>$=<0,1,0>，<0,1,1>,<1,0,0>或<1,0,1>

当 $0 \le j \le n-3$ 时，$<\Delta x_j, \Delta y_j, \Delta x_{j+1} \oplus \Delta y_{j+1}>$=<0,1,1>或<1,0,1 >，则 φ_{j+1} =1/2，故排除这两种情况。

当 $<\Delta x_j, \Delta y_j, \Delta x_{j+1} \oplus \Delta y_{j+1}>$ = <0,1,0> 或<1,0,0>时，由算法易推得，若使 φ_{j-1}=1 必然有 $<\Delta x_{j-1}, \Delta y_{j-1}, \Delta x_j \oplus \Delta y_j>$=<1,1,1>。

$\forall i: 0 \le i \le j-1$，若使 φ_i =1，类似 DCP($\Delta X, \Delta Y, K$)=1 的结构，$(\Delta x_i, \Delta y_i, k_i)$ 需要满足以下条件：

$\forall i: 0 \le i \le j-2$，$\Delta x_i \oplus \Delta y_i = 0$；$\forall i: 0 \le i \le j-1$，均有 k_i=0；

由算法的结构易得 $\delta_{j-1} = 0$，因此 $k_{j-1} = 1$。

若使 φ_i =1，令 $z = k_j, p = j+1$，$(\Delta x_i, \Delta y_i, k_i)$ 需要满足条件 $\boldsymbol{A}$。

当 $j = n-2$ 时，$<\Delta x_{n-2}, \Delta y_{n-2}>$=<0,1>或<1,0>，对 $\Delta x_{n-1}, \Delta y_{n-1}$ 的取值没有任何限制。证毕

定理 8　满足 DCP = 1/2 的 $(\Delta X, \Delta Y, K)$ 的个数为 $3 \cdot (n^2 + n - 4) \cdot 2^{n-2}$。

证明　首先考察定理 7 中条件 1 的计数问题，下面分两种情况讨论：

情况 1：当 $1 \le j \le n-3$ 时，分 3 部分考虑。

$\forall i: 0 \le i \le j-1$，类似定理 1 中情况 3，满足条件的 $(\Delta x_i, \Delta y_i, k_i)$ 的计数为 2^{j-1}。

$\forall i: j+1 \le i \le n-1$，由于 $(\Delta x_i, \Delta y_i, k_i)$ 满足条件 $\boldsymbol{A}$，利用定理 1 的结果，计数为 $(n-j+1) \cdot 2^{n-j-1}$。

当 $i = j$ 时，k_j 可以取 0 或 1。

因此该情况的总计数为 $2 \cdot \sum_{j=1}^{n-3} (n-j+1) \cdot 2^{n-j-1} \cdot 2^{j-1} = (n^2 + n - 12) \cdot 2^{n-2}$。

情况 2：当 $j = n-2$ 时，类似于定理 1 中情况 2，计数为 2^{n+1}。

所以条件 1 情况下，总计数为 $(n^2 + n - 12) \cdot 2^{n-2} + 2^{n+1} = (n^2 + n - 4) \cdot 2^{n-2}$。

定理 7 中条件 2 情况下的计数类似于条件 1，

只是由于 $\Delta x_j \oplus \Delta y_j = 1$ 存在两种情况，即 $\Delta x_j = 0, \Delta y_j = 1$ 和 $\Delta x_j = 1, \Delta y_j = 0$，所以不再赘述，条件 2 下的计数为 $2\cdot(n^2+n-4)\cdot 2^{n-2}$。

综上所述，满足 $\mathrm{DCP} = 1/2$ 的 $(\Delta X, \Delta Y, K)$ 总数为 $(n^2+n-4)2^{n-2} + 2(n^2+n-4)2^{n-2} = 3\cdot(n^2+n-4)\cdot 2^{n-2}$。 证毕

4 结束语

本文对 X田K 运算的差分分布规律的结构和计数进行了研究，首次给出了差分转移概率取最大值 1，次大值 $1-1/2^{n-2}$，次小值 $1/2^{n-2}$ 以及 $1/2$ 时，$(\Delta X, \Delta Y, K)$ (差分对以及密钥 K)的结构特点和计数公式。本文的所有结论均经过 C 语言编程验证了其正确性。

本文的结论对于密码分析者和密码设计者都很有帮助。有助于密码分析者分析使用“ X田K 运算”作为加密环节的密码算法抗差分攻击的强度，以及密码设计者设计抵抗差分攻击的密码算法。

“ X田K 运算”的差分转移概率取最小值 0 以及更一般的差分值时，$(\Delta X, \Delta Y, K)$ 的结构特点十分复杂，如何给出其结构特点和计数公式还有待于进一步研究。

参 考 文 献

[1] 冯登国, 吴文玲. 分组密码的设计与分析. 第一版, 北京: 清华大学出版社, 2000: 93–110.

[2] 刘运毅, 覃团发, 倪皖荪, 张淑仪. 简评 ECRYPT 的候选流密码算法. 信息安全与通信保密, 2006, 7–9: 26–28, 30–33, 17–21.

[3] Steve Babbage and Christophe De Canni`ere. The eSTREAM Portfolio. http://www.ecrypt.eu.org/stream/portfolio_revision1.pdf, 2008, 4.

[4] Biham E and Shamir A. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 1991, 4(1): 3–72.

[5] Hiroshi Miyano. Addend dependency of differential/linear probability of addition. *IEICE Transactions on Fundamentals*, 1998, E81–A(1): 106–109.

[6] Alexis Warner Machado. Differential probability of modular addition with a constant operand. http:// eprint.iacr.org/2001/052.pdf, 2008, 5.

[7] 陈士伟, 金晨辉. 模 2 加整体逼近二元和三元模 2^n 加的噪声函数分析. 电子与信息学报, 2008, 30(6): 1445–1449.

[8] 张龙, 吴文玲, 温巧燕. mod2^n 加运算与 F_2 上异或运算差值的概率分布和递推公式. 北京邮电大学学报, 2007, 30(1): 85–89.

[9] Helger Lipmaa and Shiho Moriai. Efficient algorithms for computing differential properties of addition. In Fast Software Encryption 2001, 2002, 2335: 336–350.

郑 斌： 男，1985 年生，硕士生，研究方向为分组密码理论.

关 杰： 女，1974 年生，副教授，博士，研究方向为算法的设计与分析研究.