卫星电话 GMR-2 流密码算法碰撞特性分析

李瑞林，胡娇，唐朝京
（国防科技大学电子科学学院，湖南 长沙 410073）

摘　要：研究了卫星电话 GMR-2 流密码算法的碰撞特性，以算法的 F 组件为桥梁，通过分析密钥差分与算法 F 组件输出碰撞以及 F 组件输出碰撞与密钥流字节碰撞之间的联系，最终得到密钥差分与密钥流碰撞之间的关系。研究表明，对于相同的帧号，当密钥对只在某一个字节上有差分，且差分的前 4 bit 与后 4 bit 相等时，该密钥对将以高概率使密钥流发生碰撞。实验结果显示，密钥流碰撞概率为 $2^{-8.248}$，远远高于理想碰撞概率 2^{-120}。这再次证明了 GMR-2 加密算法存在较大的安全隐患。

关键词：卫星电话；流密码；GMR-2；碰撞分析
中图分类号：TN918
文献标识码：A
doi: 10.11959/j.issn.1000-436x.2018026

Collision analysis of the GMR-2 cipher used in the satellite phone

LI Ruilin, HU Jiao, TANG Chaojing
College of Electronic Science, National University of Defense Technology,Changsha 410073, China

Abstract: A collision property analysis of the GMR-2 cipher used in the satellite phone was presented. By using the F-component as a bridge, the link between the difference of the key byte and the collision of the output of F as well as the link between the collision of the output of F and the collision of keystream byte were analyzed, which finally revealed the relationship between the difference of the original key byte and the keystream collision. The theoretical analysis showed that for a random frame number, a special chosen key pair could lead to a keystream collision with a high probability, when the key pair has only one byte difference in which the most significant 4 bit of the difference was equal to the last significant 4 bit. The experimental result shows that the keystream collision probability is $2^{-8.248}$, which is far higher than the ideal collision probability 2^{-120}. This proves once again, that there exists serious potential security hazards in the GMR-2 cipher.

Key words: satellite phones, stream cipher, GMR-2, collision analysis

1　引言

伴随着 2G、3G 和 4G 技术的快速发展，移动通信已经十分普遍，但在某些偏远地区如沙漠地带、海洋、高山等，仍然难以构建完整的移动蜂窝网络。卫星移动通信的出现很好地弥补了陆地蜂窝网络通信的缺点，能够在某些极端环境下提供可靠的通信。随着军民融合卫星移动通信系统的建设[1]，中国正式迈入卫星移动通信的“手机时代”[2]。

在传统的蜂窝移动通信中，为实现安全通信，人们往往采用加密算法来抵御各种窃听风险。比较著名的密码算法包括 A5、SNOW 和 ZUC 等，人们对这些算法进行了深入的安全性评估[3~11]。随着卫

收稿日期：2017-08-06；**修回日期**：2017-12-25
通信作者：李瑞林，securitylrl@gmail.com
基金项目：国家自然科学基金资助项目（No.61402515, No.61702536）
Foundation Item: The National Natural Science Foundation of China (No.61402515, No.61702536)

星移动通信的发展，卫星电话所采用的加密机制的可靠性也备受关注。目前，国际上常用的卫星通信标准主要由国际标准组织 ETSI 提出，包括 GMR-1 和 GMR-2。但 ETSI 官方发布的 GMR 标准并未公开相关密码算法的具体信息，无法对其安全性进行评估。2012 年 1 月，德国 Driessen 等[12,13]学者使用逆向工程的方法恢复出 GMR-1 和 GMR-2 加密算法。结果显示，2 种算法均属于流密码算法，其中，GMR-1 加密算法是 GSM 标准中 A5/2 加密算法的变种版本，因此，许多针对 A5/2 算法的攻击方法也适用于 GMR-1 加密算法；GMR-2 加密算法则是全新设计的，但该算法的安全性无法达到预期标准，目前，已有学者提出并实现了 2 种针对该加密算法的攻击方法。文献[13]根据算法的密钥编排特性，提出了基于“读碰撞技术”的攻击方法，该攻击方法需要 50~65 B 的明文。文献[14]提出了动态猜测决定攻击方法，根据每一次的分析结果动态地猜测下一次的分析状态，仅需要 15 B 的明文。

本文主要研究 GMR-2 算法密钥差分与输出密钥流碰撞之间的关系。根据算法密钥编排特点，该文以算法的 F 组件为桥梁，通过研究密钥差分与 F 组件输出碰撞之间的关系以及 F 组件输出碰撞与密钥流字节碰撞之间的关系，最终得到密钥差分与密钥流碰撞之间的关系。分析结果表明，对于同一个帧号，当输入密钥对只在某一个字节上有差分，且差分满足前 4 bit 与后 4 bit 相等时，发生强密钥流碰撞的概率约为 $2^{-8.314}$。实验结果表明，密钥流碰撞概率约为 $2^{-8.248}$，远远高于理想碰撞概率 2^{-120}。本文研究再次表明 GMR-2 流密码算法存在较大的安全隐患，无法达到预期安全要求。

2　GMR-2 流密码算法简介

2.1　GMR-2 流密码算法结构

GMR-2 加密算法属于流密码算法，其密钥长度为 64 bit。如图 1 所示，GMR-2 算法内部状态包括 8 B 移位寄存器 $S=(S_7,S_6,\cdots,S_0)$、8 B 的原始密钥寄存器 $K=(K_7,K_6,\cdots,K_0)$、一个开关比特 $t\in\{0,1\}$、一个计数器 $c\in\{0,1,\cdots,7\}$，并通过 F、G、H 这 3 个组件对内部状态进行变换。在每一个时钟拍 l，GMR-2 算法生成 1 B 的密钥流 Z_l。

本文主要符号对照如表 1 所示。

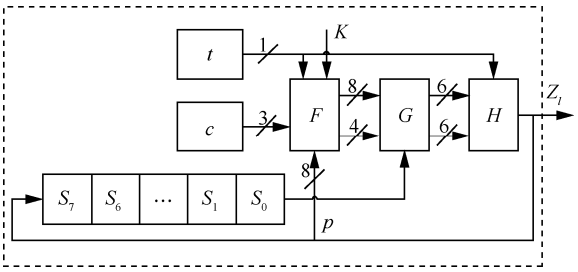


图 1　GMR-2 流密码算法结构

表 1　　**符号对照**

符号	含义
$\oplus$	异或，即按比特模 2 加
ΔX	2 bit 序列的异或差分，即 $\Delta X=X\oplus X^*$
$\Delta a\to\Delta b$	差分 Δa 能产生差分 Δb
$X\Vert Y$	2 bit 序列的级联
Γ	$\Gamma=\{\delta\Vert\delta:\delta\in\{0\text{x}1,0\text{x}2,\cdots,0\text{xf}\}\}$

2.2　GMR-2 流密码算法的组件

2.2.1　F 组件

图 2 为 F 组件，该组件的输入项包含开关比特 t、计数器 c、反馈字节 p 和 8 B 的密钥 $K=(K_7,K_6,\cdots,K_0)$，每一个时钟拍由高位复用器和低位复用器分别从 K 中选一个特定的密钥字节进行操作。输出包含 8 bit 的 O_0 和 4 bit 的 O_1，具体定义如式(1)所示。

$$\begin{cases} O_0=(K_{\tau_1(\alpha)}>>>\tau_2(\tau_1(\alpha)))_8 \\ O_1=\begin{pmatrix}\big(\big((K_c\oplus p)\gg 4\big)\,\&\,0\text{x}0\text{F}\big)\\ \oplus\big((K_c\oplus p)\,\&\,0\text{x}0\text{F}\big)\end{pmatrix}_4 \end{cases} \tag{1}$$

这里，α 定义为

$$\alpha=N(t,K_c\oplus p)=\begin{cases}\big((K_c\oplus p)\,\&\,0\text{xf}\big)_4, & t=0\\ \big(\big((K_c\oplus p)\gg 4\big)\,\&\,0\text{xf}\big)_4, & t=1\end{cases} \tag{2}$$

其中，$p=(p_7,p_6,\cdots,p_0)\in\{0,1\}^8$，$0\leqslant c\leqslant 7$，$t=c\bmod 2$，$p$ 为上一时钟拍生成的密钥流字节，$\tau_1:\{0,1\}^4\to\{0,1\}^3$ 和 $\tau_2:\{0,1\}^3\to\{0,1\}^3$ 为 2 个查表函数。对于任意的 $\alpha\in\{0,1\}^4$、$\tau_1(\alpha)$ 和 $\tau_2(\tau_1(\alpha))$ 的取值如表 2 所示。

2.2.2　G 组件

如图 3 所示为 G 组件，它以组件 F 的输入 O_0 和 O_1 以及移位寄存器 S_0 作为输入，输出为 6 bit 的

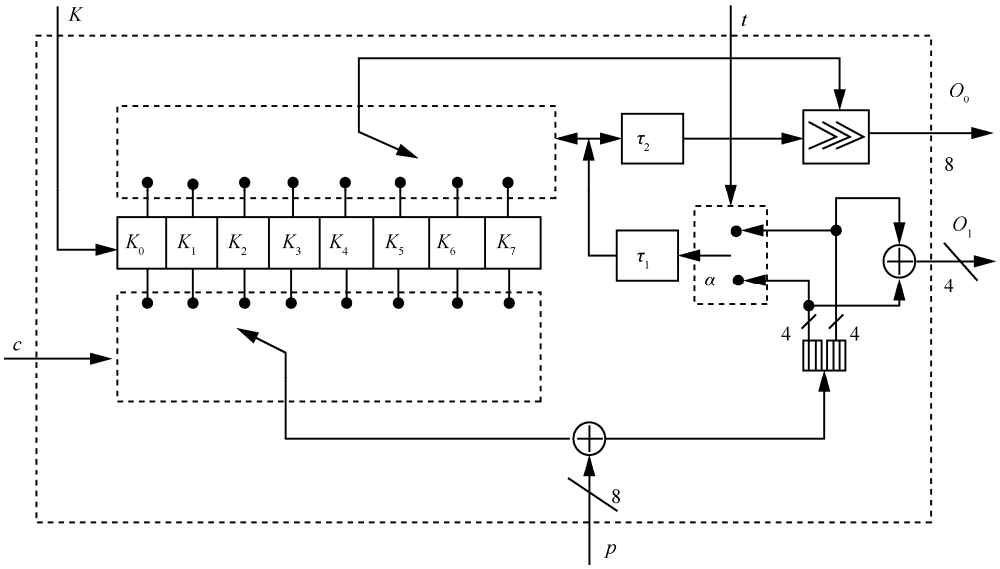


图 2 *F* 组件内部结构

表 2 $\tau_1(\alpha)$和 $\tau_2(\tau_1(\alpha))$的取值

α	$\tau_1(\alpha)$	$\tau_2(\tau_1(\alpha))$
(0,0,0,0), (1,1,1,1)	2	6
(0,0,0,1),(1,1,0,0)	5	3
(0,0,1,0),(1,0,0,1)	0	4
(0,0,1,1),(1,0,1,0)	6	2
(0,1,0,0), (1,0,0,0)	3	7
(0,1,0,1), (1,1,0,1)	7	1
(0,1,1,0), (1,1,1,0)	4	4
(0,1,1,1), (1,0,1,1)	1	5
(0,0,0,1), (1,1,0,0)	5	3

O_0'和 6 bit 的O_1'，其中，β_1、β_2和β_3为 3 个线性变换函数。*G* 组件整体上可视为一个仿射变换，该变换可以表示为

$$\begin{cases} O_0' = & (O_{0,7} \oplus O_{0,4} \oplus S_{0,5}, \\ & O_{0,7} \oplus O_{0,6} \oplus O_{0,4} \oplus S_{0,7}, \\ & O_{0,7} \oplus S_{0,4}, O_{0,5} \oplus S_{0,6}, \\ & O_{1,3} \oplus O_{1,1} \oplus O_{1,0}, O_{1,3} \oplus O_{1,0})_6 \\ O_1' = & (O_{0,3} \oplus O_{0,0} \oplus S_{0,1}, \\ & O_{0,3} \oplus O_{0,2} \oplus O_{0,0} \oplus S_{0,3}, \\ & O_{0,3} \oplus S_{0,0}, O_{0,1} \oplus S_{0,2}, O_{1,2}, O_{1,0})_6 \end{cases} \tag{3}$$

2.2.3 *H* 组件

如图 4 所示为 *H* 组件，该组件由 DES 算法中 2 个 6 进 4 出的𝕊盒并列构成（$\mathbb{S}_2$盒和$\mathbb{S}_6$盒），但是𝕊盒的查表过程与 DES 算法不同。假设𝕊盒的 6 bit

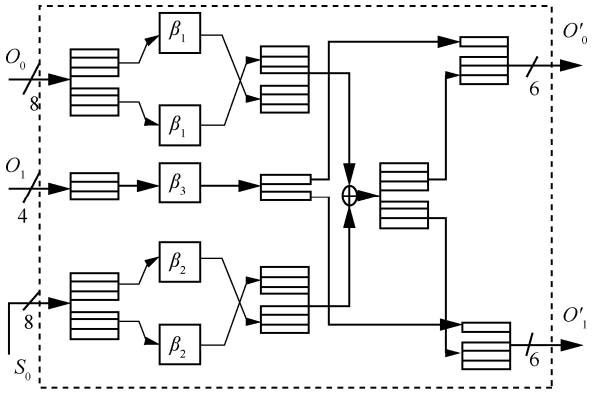


图 3 *G* 组件内部结构

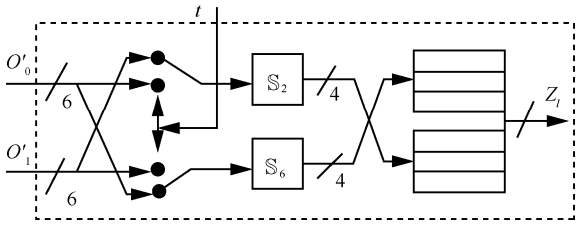


图 4 *H* 组件内部结构

输入为$(x_5,x_4,x_3,x_2,x_1,x_0)_2$，则 GMR-2 算法将$(x_5,x_4,x_3,x_2)$作为𝕊盒输入的列指标，而将$(x_1,x_0)$作为𝕊盒输入的行指标。*H* 组件将 *G* 组件 2 个 6 bit 的输出分别作为以上 2 个𝕊盒的输入，并在开关位置 *t* 的控制下，最终生成 1 B 的密钥流如式(4)所示。

$$Z_l = \begin{cases} \left(\mathbb{S}_2(O_1'), \mathbb{S}_6(O_0')\right)_8, & t=0 \\ \left(\mathbb{S}_2(O_0'), \mathbb{S}_6(O_1')\right)_8, & t=1 \end{cases} \tag{4}$$

2.3 工作模式

如文献[2]中所述，GMR-2 加密过程分为 2 个阶段：初始化阶段和密钥流生成阶段。

1) 初始化阶段

主要完成各寄存器的初始化工作。

① 将 22 bit 的帧号 $N \in \{0,1,2,\cdots\}$ 按照一定规则填充到移位寄存器 $S=(S_7,S_6,\cdots,S_0)$ 中，同时将 8 B 的密钥 K 放入组件 F 的密钥寄存器中。

②令 $t=0$， $c=0$， $p=0$。

③将该装置运行 8 拍，直至移位寄存器 S 中的值全部更新，但这 8 拍不生成密钥流。

2) 密钥流生成阶段

初始阶段结束之后，开始生成有效密钥流。每一帧走 15 拍产生 15 B 的密钥流，15 拍结束后帧号自动增加，之后对第 N+1 帧重新进行初始化，再产生 15 B 的密钥流，依次进行下去。若令 $Z_l^{(N)}$ 表示第 N 帧的第 l 拍生成的密钥流字节，且假设帧号从 0 开始，那么生成的有效密钥流可以记为

$$Z'=\left(Z_8^{(0)},Z_9^{(0)},\cdots,Z_{22}^{(0)};Z_8^{(1)},\cdots Z_{22}^{(1)};Z_8^{(2)},\cdots\right) \quad (5)$$

假设加密过程运行完第 l 拍，GMR-2 的状态将发生如下变化。

1) 根据当前的 S_0、c 和 t，输出 1 B 的密钥流 Z_l。

2) $t=c \bmod 2$， $c=(c+1) \bmod 8$。

3) 移位寄存器 S 右移 1 B：$S_i=S_{i+1}$，$0 \leqslant i \leqslant 6$，$S_7=Z_l$，并有 $p=S_7=Z_l$，用于下一拍密钥流 Z_{l+1} 的生成过程。

3 *F* 组件碰撞与密钥流碰撞关系

给定 2 组帧号和密钥 (N,K)、(N,K^*) 为简化分析过程，本文假设密钥对 (K,K^*) 仅在第 c 个字节存在差分 $\Delta K_c \neq 0$， $0 \leqslant c \leqslant 7$，其他字节均相等。在分析碰撞关系之前先给出下列关于碰撞的定义。

定义 1　F 组件输出碰撞。在第 $l\left(0 \leqslant l \leqslant 22\right)$ 拍时，根据密钥对 (K,K^*) 计算分别得到对应的 O_0、O_1 和 O_0^*、O_1^*，若同时满足：1) ΔO_0=0；2) ΔO_1=0 时，则称 F 组件在第 l 拍时发生输出碰撞。

定义 2　F 组件中间碰撞。在第 $l\left(0 \leqslant l \leqslant 22\right)$ 拍时，根据密钥对 (K,K^*) 计算分别得到对应的 O_1、$\tau_1(\alpha)$ 和 O_1^*、$\tau_1(\alpha^*)$，若同时满足：1) ΔO_1=0；2) $\Delta\tau_1(\alpha)$=0 时，则称 F 组件在第 l 拍时发生中间碰撞。

定义 3　密钥流字节碰撞。在第 $l\left(0 \leqslant l \leqslant 22\right)$ 拍时，根据密钥对 (K,K^*) 计算分别得到对应输出密钥流字节 Z 和 Z^*，若 ΔZ=0，则称 GMR-2 在第 l 拍发生密钥流字节碰撞。

定义 4　密钥流碰撞。根据密钥对 (K,K^*) 分别生成 2 帧密钥流，若对于 $8 \leqslant l \leqslant 22$，均有 ΔZ_l=0，则称 GMR-2 发生密钥流碰撞。

为更好地利用概率模型研究 GMR-2 流密码算法的密钥流碰撞特性，本文给出以下定义。

定义 5　强密钥流碰撞。根据密钥对 (K,K^*) 分别生成 2 帧密钥流，若对于 $0 \leqslant l \leqslant 22$，均有 ΔZ_l=0，则称 GMR-2 发生强密钥流碰撞。

根据上述定义，本文有以下结论。

结论 1　已知密钥对 (K,K^*) 只在第 c 个字节存在差分 $\Delta K_c \neq 0$，$0 \leqslant c \leqslant 7$，假设在第 $l(0 \leqslant l \leqslant 22)$ 拍，密钥对使 F 组件发生中间碰撞，若 $\tau_1(\alpha) \neq c$，那么 (K,K^*) 将进一步使 F 组件发生输出碰撞；若 $\tau_1(\alpha)=c$，那么 F 组件将不会发生输出碰撞。

证明　已知 F 组件发生中间碰撞，即 ΔO_1=0，$\Delta\tau_1(\alpha)$=0，由于 (K,K^*) 只在第 c 个字节存在差分，那么当 $\tau_1(\alpha) \neq c$ 时，说明高位复用器选择的密钥字节不存在差分，因此，根据式 (1) 有 $\Delta O_0=O_0 \oplus O_0^*=(K_{\tau_1(\alpha)} >>> \tau_2(\tau_1(\alpha))) \oplus (K_{\tau_1(\alpha)} >>> \tau_2(\tau_1(\alpha)))=0$，即 F 组件发生输出碰撞；当 $\tau_1(\alpha)=c$ 时，根据式 (1) 有 $\Delta O_0=O_0 \oplus O_0^*=(K_c >>> \tau_2(\tau_1(\alpha))) \oplus ((K_c \oplus \Delta K_c) >>> \tau_2(\tau_1(\alpha)))=\Delta K_c >>> \tau_2\left(\tau_1\left(\alpha\right)\right) \neq 0$, 即 F 组件不会发生输出碰撞。

根据 GMR-2 流密码算法的加密过程及文献[4]，本文有以下 2 条性质。

性质 1　G 组件为线性变换，输入与输出一一对应，因此，有 O_0 与 H 中 $\mathbb{S}_2$ 与 $\mathbb{S}_6$ 的列指标相互决定，O_1 与 H 中 $\mathbb{S}_2$ 与 $\mathbb{S}_6$ 的行指标相互决定。

性质 2　若 $\mathbb{S}$ 盒的输出和对应的行指标唯一，那么可以唯一确定 $\mathbb{S}$ 盒的列指标。

根据上述 2 条性质，本文给出如下命题。

命题 1　在第 $l(0 \leqslant l \leqslant 22)$ 拍，若密钥对 (K,K^*) 使 ΔO_1=0，且 $\Delta S_0=0$，那么密钥流字节碰撞等价于 F 组件输出碰撞。

证明　充分性。若密钥对 (K,K^*) 使输出密钥流

字节碰撞，即 $\mathbb{S}$ 盒的输出唯一，由于 $\Delta O_1=0$，即 O_1 唯一确定，根据性质 1，则 H 中 $\mathbb{S}_2$ 与 $\mathbb{S}_6$ 的行指标唯一确定，再依次根据性质 1 和性质 2，本文可以得到 $\Delta O_0=0$，即 F 组件输出碰撞。

必要性。若密钥对 (K,K^*) 使 F 组件输出碰撞，即 $\Delta O_0=0$，$\Delta O_1=0$，由于 $\Delta S_0=0$，根据性质 1，则一定有 H 中 $\mathbb{S}_2$ 与 $\mathbb{S}_6$ 的输入碰撞，因此，输出密钥流字节碰撞。

综上所述，命题 1 得证。

观察加密过程可以发现，GMR-2 流密码算法主要分为 3 个部分，其中，F 组件扮演密钥编排作用，与密钥关系最为密切。

4 F 组件碰撞特性分析

本节分析 F 组件在第 l 拍时的碰撞特性，F 组件使用了 K_c 和 $K_{\tau_1(\alpha)}$ 2 B 的密钥，其中，K_c 根据计数器依次选定，而 $K_{\tau_1(\alpha)}$ 的选取较为复杂，需要根据式(2)以及表 2 计算出下标 $\tau_1(\alpha)$ 后才能选定。由于密钥差分仅存在于第 c 个字节，$0\leqslant c\leqslant 7$，因此，本节将分 $l \bmod 8=c$ 和 $l \bmod 8\neq c$ 2 种情况来分析碰撞特性，并假设在每一拍均满足 $\Delta p=0$。

4.1 第 $l(0\leqslant l\leqslant 22, l \bmod 8=c)$ 拍 F 组件输出碰撞概率

将式(1)按位重写为

$$O_1=\boldsymbol{k}_h\oplus\boldsymbol{k}_l\oplus\boldsymbol{p}_h\oplus\boldsymbol{p}_l \tag{6}$$

其中，$\boldsymbol{p}_h=(p_7,p_6,p_5,p_4)^{\mathrm{T}}$，$\boldsymbol{k}_h=(K_{c,7},K_{c,6},K_{c,5},K_{c,4})^{\mathrm{T}}$，$\boldsymbol{k}_l=(K_{c,3},K_{c,2},K_{c,1},K_{c,0})^{\mathrm{T}}$。因此，当 p 固定时，若 $(K_{c,i+4},K_{c,i})$ 2 个比特同时改变，O_1 的值将不会变化，其中，$0\leqslant i\leqslant 3$。定义式(1)的输入密钥差分 $\Delta K_c=\Delta\boldsymbol{k}_h\|\Delta\boldsymbol{k}_l=\left(\boldsymbol{k}_h\oplus\boldsymbol{k}_h^*\right)\|\left(\boldsymbol{k}_l\oplus\boldsymbol{k}_l^*\right)$，则当 ΔK_c 满足 $\Delta\boldsymbol{k}_h=\Delta\boldsymbol{k}_l$，即差分的前 4 bit 与后 4 bit 相等时，有 $\Delta O_1=0$，将此时对应 ΔK_c 的集合记为 $\Gamma=\left\{\delta\|\delta:\delta\in\{0\mathrm{x}1,0\mathrm{x}2,\cdots,0\mathrm{xf}\}\right\}$。

根据式(2)，如果 p 已知，那么在每一拍中，t=1 时，由 K_c 的前 4 bit 可计算出 α；t=0 时，由 K_c 的后 4 bit 可计算出 α。因此，当 $\Delta p=0$，且 $\Delta K_c\in\Gamma$ 时，则 $\Delta\alpha=\delta\oplus\Delta p=\delta$。表 3 给出了当查表函数 τ_1 的输出差分 $\Delta\tau_1(\alpha)=0$ 时，输入差分 $\Delta\alpha$ 的概率分布。

表 3 当输出差分为 0 时，输入差分 $\Delta\alpha$ 的概率分布

$\Delta\alpha$	$IN_{\tau_1(\alpha)}(\Delta\alpha,\Delta\tau_1(\alpha))$	$N_{\tau_1(\alpha)}(\Delta\alpha,\Delta\tau_1(\alpha))$	$\Pr_{\tau_1(\alpha)}(\Delta\alpha\to\Delta\tau_1(\alpha))$
0	0~15	16	1
8	5,6,13,14	4	0.25
9	3,10	2	0.125
11	2,9	2	0.125
12	4,7,8,11	4	0.25
13	1,12	2	0.125
15	0,15	2	0.125
其他	$\varnothing$	0	0

其中，

$$\begin{aligned}
&IN_{\tau_1(\alpha)}\left(\Delta\alpha,\Delta\tau_1(\alpha)\right)\\
&=\left\{\alpha\in\{0,1\}^4:\tau_1(\alpha\oplus\Delta\alpha)\oplus\tau_1(\alpha)=\Delta\tau_1(\alpha)\right\},\\
&N_{\tau_1(\alpha)}\left(\Delta\alpha,\Delta\tau_1(\alpha)\right)=\#IN_{\tau_1(\alpha)}\left(\Delta\alpha,\Delta\tau_1(\alpha)\right),\\
&\Pr_{\tau_1(\alpha)}\left(\Delta\alpha\to\Delta\tau_1(\alpha)\right)\\
&=\Pr_{\alpha\in\{0,1\}^4}\left(\tau_1(\alpha\oplus\Delta\alpha)\oplus\tau_1(\alpha)=\Delta\tau_1(\alpha)\right)\\
&=\frac{N_{\tau_1(\alpha)}\left(\Delta\alpha,\Delta\tau_1(\alpha)\right)}{2^4}
\end{aligned}$$

根据表 3，本文可以得出以下命题。

命题 2 给定密钥对 $\left(K,K^*\right)$，假设密钥对仅在第 c 个字节上存在差分 ΔK_c，$0\leqslant c\leqslant 7$，且 $\Delta K_c=\delta\|\delta\in\Gamma$，若第 $l\left(0\leqslant l\leqslant 22, l \bmod 8=c\right)$ 拍时有 $\Delta p=0$，则此时 F 组件发生输出碰撞的概率为

$$\begin{aligned}
\Pr_{l \bmod 8=c}(c,\delta)=&\Pr_{\tau_1(\alpha)}(\delta\to 0)\Pr\left(\tau_1(\alpha)\neq c\middle|\delta\to 0\right)+\\
&\left(1-\Pr_{\tau_1(\alpha)}(\delta\to 0)\right)\times\frac{1}{2^8}
\end{aligned}\tag{7}$$

其中，$\Pr_{\tau_1(\alpha)}(\delta\to 0)$ 取值如表 3 所示，$\Pr(\tau_1(\alpha)\neq c|\delta\to 0)$ 表示在满足 $\Pr_{\tau_1(\alpha)}(\delta\to 0)$ 的 α 值中，恰好没有选中差分密钥字节位置 c 的概率，取值如表 4 所示。

证明 因为 $\Delta K_c\in\Gamma$，$\Delta p=0$，一定有 $\Delta O_1=0$，$\Delta\alpha=\delta$，则此时发生 F 组件中间碰撞的概率等于 $\Pr_{\tau_1(\alpha)}(\delta\to 0)$，未发生 F 组件中间碰撞的概率等于 $\left(1-\Pr_{\tau_1(\alpha)}(\delta\to 0)\right)$。接下来，分 2 种情况讨论。

情形 1 若 F 组件发生中间碰撞，则根据结论 1 可知，F 组件进一步发生输出碰撞的概率为 $\Pr\left(\tau_1(\alpha)\neq c|\delta\to 0\right)$，即在 $IN_{\tau_1(\alpha)}(\delta,0)$ 的 α 中满足

$\tau_1(\alpha)\neq c$ 的概率。以 $\Delta\alpha=\delta=8$ 为例，则 $\alpha\in IN_{\tau_1(\alpha)}(8,0)=\{5,6,13,14\}$，根据表 2，得到 $\tau_1(\alpha)\in\{4,7\}$，则 $c\in\{4,7\}$ 时，$\Pr(\tau_1(\alpha)\neq c|\delta\to 0)=0.5$，$c\in\{0,1,2,3,5,6\}$ 时，$\Pr(\tau_1(\alpha)\neq c|\delta\to 0)=1$，如表 4 第 1 行所示，类似可完整构造出表 4。

表 4　$\Pr_{\tau_1(\alpha)}(\tau_1(\alpha)\neq c|\delta\to 0)$ 取值

δ	c=0	c=1	c=2	c=3	c=4	c=5	c=6	c=7
8	1	1	1	1	0.5	1	1	0.5
9	1	1	1	1	1	1	0	1
11	0	1	1	1	1	1	1	1
12	1	0.5	1	0.5	1	1	1	1
13	1	1	1	1	1	0	1	1
15	1	1	0	1	1	1	1	1
其他	0	0	0	0	0	0	0	0

情形 2　若 F 组件没有发生中间碰撞，即 $\Delta\tau_1(\alpha)\neq 0$。由于 $\Delta K_c\in\Gamma$ 且满足 $\Delta O_1=0$，此时 F 组件发生输出碰撞的概率为

$$\begin{aligned}&\Pr(\Delta O_0=0)\\&=\Pr\left(K_{\tau_1(\alpha)}>>>\tau_2(\tau_1(\alpha))=K_{\tau_1(\alpha^*)}>>>\tau_2(\tau_1(\alpha^*))\right)\\&=\frac{1}{2^8}\end{aligned}$$

综合上述 2 种情况，命题 2 得证。

4.2　第 $l(0\leqslant l\leqslant 22, l\bmod 8\neq c)$ 拍 F 组件输出碰撞概率

接下来，分析第 $l(0\leqslant l\leqslant 22, l\bmod 8\neq c)$ 拍时，F 组件的输出碰撞概率。本文给出以下命题。

命题 3　给定密钥对 (K,K^*)，假设密钥对仅在第 c 个字节上存在差分 ΔK_c，$0\leqslant c\leqslant 7$，且 $\Delta K_c=\delta\|\delta\in\Gamma$，若第 $l(0\leqslant l\leqslant 22, l\bmod 8\neq c)$ 拍时有 $\Delta p=0$，则此时 F 组件发生输出碰撞的概率为

$$\Pr_{l\bmod 8\neq c}=\frac{7}{8}\tag{8}$$

证明　由于 (K,K^*) 只在第 c 个字节存在差分，其他字节均相等，即在第 $l(0\leqslant l\leqslant 22, l\bmod 8\neq c)$ 拍时有 $\Delta K_{l\bmod 8}=0$。由于 $\Delta p=0$，则根据式(1)和式(2)有 $\Delta O_1=0$，$\Delta\alpha=0$，从而 $\Delta\tau_1(\alpha)=0$，即在第 $l(0\leqslant l\leqslant 22, l\bmod 8\neq c)$ 拍一定有 F 组件发生中间碰撞。因此，根据结论 1，F 组件发生输出碰撞的概率为 $\Pr_{l\bmod 8\neq c}=\Pr(\tau_1(\alpha)\neq c)=\frac{7}{8}$。

5　GMR-2 流密码算法强密钥流碰撞特性分析

上一节研究了 F 组件碰撞特性，本节研究 GMR-2 算法的碰撞特性，为更好地利用第 4 节的结果，本文主要研究 GMR-2 算法的强密钥流碰撞特性。

本文约定，在第 N 帧密钥流生成的第 $l(0\leqslant l\leqslant 22)$ 拍，令 $Z_l^{(N)}$ 表示第 N 帧密钥流第 l 拍的密钥流字节值，$S_i^{(l)}$ 表示移位寄存器 S_i 在第 l 拍的值，p_l 表示第 l 拍的 p 值。那么 $8\leqslant l\leqslant 22$ 时，$p_l=S_7^{(l)}=Z_{l-1}^{(N)}$，$S_0^{(l)}=S_i^{(l-i)}=p_{l-7}=Z_{l-8}^{(N)}$，即 p 等于前一拍生成的密钥流字节，$S_0^{(l)}$ 等于 8 拍前生成的密钥流字节。因此，本文可以得出以下内部关系。

1) 若在第 $l(0\leqslant l\leqslant 21)$ 拍发生密钥流字节碰撞，则在第 $l+1$ 拍一定有 $\Delta p_{l+1}=0$。

2) 若在第 $l(0\leqslant l\leqslant 14)$ 拍发生密钥流字节碰撞，则在第 $l+8$ 拍一定有 $\Delta S_0^{(l+8)}=0$。

3) 若 $\Delta N=0$，根据初始化过程可知 $\Delta p_0=0$，且 $0\leqslant l\leqslant 7$ 时，有 $\Delta S_0^l=0$。

根据上述内部关系，本文给出以下命题。

命题 4　给定 2 组帧号和密钥 (N,K)、(K,K^*)，假设密钥对 (K,K^*) 仅在第 c 个字节上存在差分 ΔK_c，$0\leqslant c\leqslant 7$，且 $\Delta K_c=\delta\|\delta\in\Gamma$，若每个密钥流字节发生碰撞的概率是相互独立的，则 GMR-2 流密码算法强密钥流碰撞概率为

$$\Pr_1(c)=\sum_{\delta=1}^{15}\Pr(c,\delta)\tag{9}$$

其中，

$$\Pr(c,\delta)=\begin{cases}\Pr_{l\bmod 8=c}(c,\delta)^3(\Pr_{l\bmod 8\neq c})^{20}, & c\neq 7\\ \Pr_{l\bmod 8=c}(c,\delta)^2(\Pr_{l\bmod 8\neq c})^{21}, & c=7\end{cases}\tag{10}$$

这里，$\Pr_{l\bmod 8=c}(c,\delta)$ 根据式(7)计算得到，$\Pr_{l\bmod 8\neq c}$ 根据式(8)计算得到。

证明　令 $\Pr(c,\delta)$ 为密钥对仅在第 c 个字节存在差分 ΔK_c，且 $\Delta K_c=\delta\|\delta$ 时，GMR-2 流密码算法发生强密钥流碰撞的概率，则根据全概公式，将 δ 从 1~15 遍历，即可得到

$$\Pr_1(c)=\sum_{\delta=1}^{15}\Pr(c,\delta)$$

下面，分析 $\Pr(c,\delta)$ 的计算过程。注意到强密钥流碰撞意味着每一拍均发生密钥流字节碰撞，由命题 4 条件，每个密钥流字节发生碰撞的概率是相互独立的，则 $\Pr(c,\delta)$ 等于各密钥流字节碰撞概率的乘积。每生成一帧密钥流一共运行 23 拍，令 $\Pr_l(c,\delta)$ 表示第 $l(0\leqslant l\leqslant 22)$ 拍时的密钥流字节碰撞概率，则

$$\Pr(c,\delta)=\prod_{l=0}^{22}\Pr_l(c,\delta)$$

下面，进一步分析 $\Pr_l(c,\delta)$ 的计算过程。综合前述 3 条 GMR-2 算法内部关系可得，若 $\Delta N=0$，且从第 0 拍到第 22 拍依次发生密钥流字节碰撞，那么在第 $l(0\leqslant l\leqslant 22)$ 拍，均有 $\Delta p_l=0$ 和 $\Delta S_0^{(l)}=0$ 成立。同时由 $\Delta K_c\in\Gamma$，可知在第 $l(0\leqslant l\leqslant 22)$ 拍，一定满足 $\Delta O_1=0$。因此命题 1~命题 3 的条件全部满足，本文可以利用命题 1~命题 3 的结论。

根据命题 1，密钥流字节碰撞概率等于 F 组件输出碰撞概率，进一步根据命题 2 和命题 3，可将这 23 拍分为 $l\bmod 8=c$ 和 $l\bmod 8\neq c$ 这 2 种情况。

1) 在第 $l(0\leqslant l\leqslant 22, l\bmod 8=c)$ 拍时，有 $\Pr_l(c,\delta)=\Pr_{l\bmod 8=c}(c,\delta)$；

2) 在第 $l(0\leqslant l\leqslant 22, l\bmod 8\neq c)$ 拍时，有 $\Pr_l(c,\delta)=\Pr_{l\bmod 8\neq c}$。

最终得到

$$\begin{aligned}\Pr(c,\delta)&=\prod_{l=0}^{22}\Pr_l(c,\delta)\\&=\prod_{l=0}^{22}\Pr_{l\bmod 8=c}(c,\delta)\prod_{l=0}^{22}\Pr_{l\bmod 8\neq c}\\&=\begin{cases}\Pr_{l\bmod 8=c}(c,\delta)^3(\Pr_{l\bmod 8\neq c})^{20}, & c\neq 7\\ \Pr_{l\bmod 8=c}(c,\delta)^2(\Pr_{l\bmod 8\neq c})^{21}, & c=7\end{cases}\end{aligned}$$

最后，本文分析给出的强密钥流碰撞发生的前提条件，即给定 2 组帧号和密钥 (N,K)、(N,K^*)，假设密钥对 (K,K^*) 仅在第 c 个字节上存在差分 ΔK_c，$0\leqslant c\leqslant 7$，且 $\Delta K_c=\delta\|\delta\in\Gamma$。假设随机生成一个密钥对，那么该条件发生的概率为 $2^{-56}\times 2^{-4}\times 8=2^{-57}$，因此，满足该条件的密钥对数目有 $2^{64}\times 2^{64}\times 2^{-57}=2^{71}$ 对，说明实际情况中存在一定数量满足该条件的密钥对。

6 实验分析

为验证碰撞概率，本文对每个位置 $0\leqslant c\leqslant 7$ 分别进行了 2^{28} 次实验。实验中，帧号与密钥均随机生成，且满足密钥对 (K,K^*) 仅在第 c 个字节上存在差分 ΔK_c，$0\leqslant c\leqslant 7$，且 $\Delta K_c=\delta\|\delta\in\Gamma$，得到强密钥流碰撞概率的理论分析值 $\Pr_1(c)$ 与实验值 $\Pr_1(c)^*$。实验同时统计了发生密钥流碰撞的概率，记作 $\Pr_2(c)^*$。概率值对比如表 5 所示，其中，表格的第 5 列表示通过实验得到的密钥流碰撞概率与强密钥流碰撞概率的差值。观察分析表 5 可得到以下结论。

表 5 碰撞概率对比

c	$\Pr_1(c)$	$\Pr_1(c)^*$	$\Pr_2(c)^*$	$\Pr_2(c)^*-\Pr_1(c)^*$
0	$2^{-8.544}$	$2^{-8.456}$	$2^{-8.455}$	$2^{-19.488}$
1	$2^{-9.077}$	$2^{-8.996}$	$2^{-8.994}$	$2^{-18.899}$
2	$2^{-8.544}$	$2^{-8.456}$	$2^{-8.455}$	$2^{-19.488}$
3	$2^{-9.077}$	$2^{-9.000}$	$2^{-8.998}$	$2^{-19.209}$
4	$2^{-9.077}$	$2^{-8.940}$	$2^{-8.938}$	$2^{-18.950}$
5	$2^{-8.544}$	$2^{-8.492}$	$2^{-8.491}$	$2^{-19.508}$
6	$2^{-8.544}$	$2^{-8.454}$	$2^{-8.453}$	$2^{-19.536}$
7	$2^{-6.817}$	$2^{-6.795}$	$2^{-6.791}$	$2^{-15.230}$
平均值	$2^{-8.314}$	$2^{-8.250}$	$2^{-8.248}$	$2^{-17.719}$

1) 当密钥对 (K,K^*) 仅在一个字节上存在差分，且该密钥字节差分的前 4 bit 与后 4 bit 相等时，发生强密钥流碰撞的概率理论平均值约为 $2^{-8.314}$，而实验得到的强密钥流碰撞概率为 $2^{-8.250}$，略高于理论值。这一方面可能由于实验样本不够充分而造成；另一方面，也可能是由于命题 4 中计算密钥流字节碰撞概率时的独立性假设不完全满足所造成。

2) 当密钥对 (K,K^*) 的差分位置在 K_7 时，发生强密钥流碰撞的概率最高。

3) 密钥流碰撞概率与强密钥流碰撞概率差距微弱，说明 GMR-2 流密码算法强密钥流碰撞是密钥流碰撞的主概率事件。

4) 若将 GMR-2 加密算法的密钥流生成器视为 22 bit 的帧号 N 与 64 bit 的密钥 K 到 120 bit 的密钥流 Z 的映射函数，则一个理想安全的密钥流生成器要求：对于不同的(N, K)，输出 15 B 密钥流发生碰撞的概率应该为 2^{-120}。但实验得到的密钥流碰撞概率为 $2^{-8.248}$，远远高于 2^{-120}。这也再一次说明 GMR-2

算法的碰撞特性明显，安全性较弱。

7　结束语

作为卫星加密电话中使用的加密算法，GMR-2 流密码的 3 个组件分别承担了密钥编排、线性变换和非线性变换的功能。本文通过分析 F 组件的碰撞特性与密钥流碰撞之间的关系，得出了特定密钥差分使 GMR-2 流密码算法发生密钥流碰撞的概率，并通过实验进行了验证。实验得到的高碰撞概率再次证明了 GMR-2 流密码算法的安全性较弱，存在较大的安全隐患。

参考文献：

[1] 何元智. 军民融合重大举措—天通一号卫星移动通信系统[C]// 2016 中国卫星应用大会.2016.
HE Y Z. A Milestone of civil-military integrated satellite communication: tiantong-01 system[C]//China Satellite Conference 2016. 2016.

[2] 2016 中国卫星应用若干重大进展[J]. 卫星应用, 2017(1):32-39.
Significant progress in Chinese satellite applications in 2016 [J]. Satellite Application, 2017(1): 32-39

[3] 李磊. 移动通信 GSM 中密码算法安全性研究[D]. 郑州: 解放军信息工程大学, 2012.
LI L. Research on security of cryptographic algorithm in GSM[D]. Zhengzhou: PLA Information Engineering University, 2012.

[4] 关杰, 丁林, 刘树凯. SNOW 3G 与 ZUC 流密码的猜测决定攻击[J]. 软件学报, 2013(6):1324-1333.
GUAN J, DING L, LIU S K. Guess and determine attack on SNOW 3G and ZUC[J]. Journal of Software, 2013(6):1324-1333.

[5] 吴泳钢，古天龙，徐周波. SNOW 3G 加密算法的 BDD 攻击[J]. 桂林电子科技大学学报, 2016, 36 (3) :199-203.
WU Y G, GU T L, XU Z B. BDD attack on SNOW 3G encryption algorithm[J]. Journal of Guilin University of Electronic Technology, 2016, 36 (3) :199-203.

[6] BARKAN P, BIHAM E, KELLER N. Instant cipher-text only cryptanalysis of GSM encrypted communication[J]. Journal of Cryptology, 2008, 21(3): 392-429.

[7] BIRYUKOV A, SHAMIR A, WAGNER D. Real time cryptanalysis of A5/1 on a PC[M]//Fast Software Encryption, Springer Berlin Heidelberg, 2000: 1-18.

[8] DUNKELMAN O, KELLER N, SHAMIR A. A practical-time attack on the A5/3 cryptosystem used in third generation GSM telephony[C]// Icar Crgptology Eprint Archive. 2010: 393-410.

[9] WU H, HUANG T, NGUYEN P, et al. Differential attacks against stream cipher ZUC[C]//International Conference on the Theory and Application of Cryptology and Information Security. 2012: 262-277.

[10] ZHANG B, XU C, MEIER W. Fast correlation attacks over extension fields, large-unit linear approximation and cryptanalysis of SNOW 2.0[C]//Cryptology Conference. 2015: 643-662.

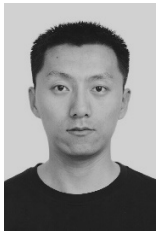
[11] ZHOU C, FENG X, LIN D. The Initialization stage analysis of ZUC v1.5[C]//Cryptology and Network Security. 2011: 40-53.

[12] DRIESSEN B, HUND R, WILLEMS C, et al. Don't trust satellite phones: a security analysis of two satphone standards[C]//Security and Privacy (SP). 2012: 128-142.

[13] DRIESSEN B, HUND R, WILLEMS C, et al. An experimental security analysis of two satphone standards[J]. ACM Transactions on Information & System Security, 2013, 16(3):1-30.

[14] LI R, LI H, LI C, ET AL. A low data complexity attack on the GMR-2 Cipher Used in the Satellite Phones[C]//FSE. 2013: 485-501.

[作者简介]



李瑞林（1982-），男，山西太原人，博士，国防科技大学讲师，主要研究方向为密码学与信息安全。

胡娇（1993-），女，湖南岳阳人，国防科技大学硕士生，主要研究方向为密码学与信息安全。

唐朝京（1962-），男，江苏常州人，博士，国防科技大学教授，主要研究方向为网络空间安全与对抗。