ZUC序列密码算法的选择IV相关性能量分析攻击

严迎建[①] 杨昌盛[*①] 李 伟[①②] 张立朝[①③]
[①](解放军信息工程大学 郑州 450000)
[②](复旦大学微电子学院 上海 200433)
[③](天津大学电子信息工程学院 天津 300072)

摘 要：为了分析ZUC序列密码算法在相关性能量分析攻击方面的免疫能力，该文进行了相关研究。为了提高攻击的针对性，该文提出了攻击方案的快速评估方法，并据此给出了ZUC相关性能量分析攻击方案。最后基于ASIC开发环境构建仿真验证平台，对攻击方案进行了验证。实验结果表明该方案可成功恢复48 bit密钥，说明ZUC并不具备相关性能量分析攻击的免疫力，同时也证实了攻击方案快速评估方法的有效性。相比Tang Ming等采用随机初始向量进行差分能量攻击，初始向量样本数达到5000时才能观察到明显的差分功耗尖峰，该文的攻击方案只需256个初始向量，且攻击效果更为显著。

关键词：密码学；序列密码；ZUC；能量分析攻击；评估
中图分类号： TN918.4 **文献标识码**： A **文章编号**：1009-5896(2015)08-1971-07
DOI: 10.11999/JEIT141604

Chosen-IV Correlation Power Analysis Attack of ZUC Stream Cipher

Yan Ying-jian[①] Yang Chang-sheng[①] Li Wei[①②] Zhang Li-chao[①③]
[①](*PLA Information Engineering University*, *Zhengzhou* 450000, *China*)
[②](*Institute of Microelectronics*, *Fudan University*, *Shanghai* 200433, *China*)
[③](*Institute of Electronic Information Engineering*, *Tianjin University*, *Tianjin* 300072, *China*)

Abstract: To analyze the immunity of ZUC stream cipher in aspect of correlation power analysis attack, some relevant researches are conducted. In order to improve the pertinence of attack, a rapid assessment method of the attack scheme is presented, and accordingly a correlation power analysis scheme of ZUC is proposed. Finally, based on the simulation platform raised by ASIC development environment, the attack scheme is validated. Experiment results turn out that the scheme can successfully attack 48-bit key, confirming that ZUC is unable to resist the correlation power analysis attack, and the proposed assessment method of attack scheme takes effect. Compared with Tang Ming's experimental, which conducted differential power analysis of ZUC with random initial vectors and observing distinct differential power peak with 5000 initial vectors, the proposed attack scheme only uses 256 initial vectors, and gets better results.

Key words: Cryptography; Stream cipher; ZUC; Power analysis attack; Assessment

1 引言

ZUC序列密码算法由中国科学院数据通信保护研究教育中心设计，现已被采纳为3GPP LTE移动通信加密标准核心算法。该算法自发布以来受到了广泛关注，密码分析人员对其安全性进行了大量研究。2012年，文献[1]对ZUC进行了差分攻击，文献[2]对ZUC初始化阶段的安全性进行了分析，文献[3]对ZUC进行了时间攻击。2013年，文献[4]对ZUC进行了SAT分析攻击，文献[5]对ZUC进行了猜测决定(guess and determine)攻击。上述攻击均从数学分析的角度展开，目前尚未发现明显的安全漏洞，表明ZUC在抵抗代数分析攻击方面具有很好的安全性。

在物理安全性方面，文献[6]对ZUC进行了差分能量分析(Differential Power Analysis, DPA)攻击，文献[7]针对嵌入式平台下实现的ZUC算法进行了侧信道频域攻击，上述攻击属于侧信道攻击(Side Channel Attack, SCA)范畴。侧信道攻击属于交叉学科，需要同时了解密码学、统计学、测量学和微电学的相关知识体系[8]，因此针对ZUC的侧信道攻击研究较代数分析攻击要少很多。

2014-12-15收到，2015-04-14改回，2015-06-09网络优先出版
国家自然科学基金(61404175, 61302107)资助课题
*通信作者：杨昌盛 ycs3317@126.com

能量分析攻击作为侧信道攻击的重要分支之一，经过十余年的发展，先后出现了简单能量攻击(Simple Power Analysis, SPA)、DPA 攻击和相关性能量分析(Correlation Power Analysis, CPA)攻击等攻击技术，并广泛应用于分组密码和公钥密码的分析，对多种密码算法进行了有效的攻击[9,10]。尽管能量分析攻击已成为分组密码和公钥密码算法的有力分析工具，但针对序列密码的相关研究却远不及前者[11,12]。为了分析 ZUC 序列密码算法在相关性能量分析攻击方面的免疫能力，本文进行了相关研究。为了提高攻击的针对性，首先提出了攻击方案的快速评估方法，并基于此给出了 ZUC 的相关性能量分析攻击方案，最后基于专用集成电路(Application Specific Integrated Circuit, ASIC)开发工具构建的仿真环境，对攻击方案进行了验证，得到了理想的攻击结果。

2 序列密码算法功耗成分特征分析

能量分析攻击基于一个重要的假设前提：认为攻击点函数所产生的功耗 P_{F} 与芯片中其他功耗成分相互独立[13]。针对大量分组密码和公钥密码算法的攻击也证实了这一假设。然而实验发现，直接将上述攻击方法移植于序列密码算法往往并不可行。

序列密码算法的功耗成分与分组密码的类似，如图 1 所示，P_{KO}, P_{IVO} 和 P_{KIV} 分别表示仅与密钥 KEY 有关、仅与初始向量 IV 有关和同时与 KEY 和 IV 有关的功耗分量(不包括攻击点功耗 P_{F})，此外还包括随机噪声分量 P_{N} 和恒定分量 P_{C}。所不同的是，分组密码算法中普遍使用了替代-置换网络(S-P 网络)[14]，明文(或密文)在运算过程中被充分的混乱和扩散，使得攻击点功耗与其他功耗成分之间的相关性较弱。而序列密码的构造相对简单，且使用较多的线性运算，如移位、异或等，导致 P_{KIV}, P_{IVO} 与 P_{F} 之间往往存在较强的相关性。

文献[15]指出，攻击点功耗与其它功耗成分之间存在相关性是导致序列密码能量分析攻击困难的主要原因，同时还提出通过选取特定初始向量以避免或减弱功耗相关性的攻击思路。本文延续了这一思想，并结合对多种序列密码算法进行能量分析攻击

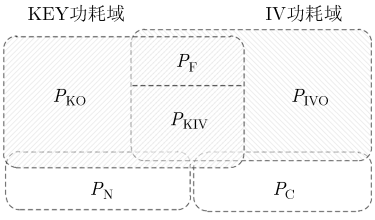


图1 序列密码算法功耗成分(仅初始化阶段)

的经验，就初始向量选取问题，总结出以下几点策略：

记攻击点函数为 $f(k_{\mathrm{P}}, iv_{\mathrm{P}})$，$k_{\mathrm{P}}$ 表示局部密钥，iv_{P} 表示局部初始向量。

(1)在解决 P_{KIV} 与 P_{F} 的相关性方面，使与 P_{KIV} 有关的初始向量比特位保持恒定，从而使 P_{KIV} 恒定；

(2)在解决 P_{IVO} 与 P_{F} 的相关性方面，引入与 iv_{P} 互补的初始向量比特位，使与初始向量有关的功耗互补，从而使 P_{IVO} 保持恒定；

(3)在解决 P_{F} 内部自身的相关性方面，可通过扩展攻击点函数中 iv_{P} 的比特位数，引入新的可变初始向量比特位来实现。

对于序列密码的能量分析攻击，攻击点和初始向量的选取是攻击方案的核心内容。而对于具体的算法，很容易找到满足基本要求的攻击点和初始向量选取方案，如果对于每一种方案都进行完整的实验，必然会带来很高的攻击成本，为了解决这一问题，本文提出攻击方案的快速评估方法。

3 攻击方案的快速评估方法

序列密码算法的功耗成分中 P_{N}, P_{C} 与 P_{F} 相互独立，而攻击过程中密钥 KEY 保持恒定，对攻击者来说，P_{KO} 相当于恒定量，也与 P_{F} 相互独立，则功耗成分中仅 P_{KIV}, P_{IVO} 可能与 P_{F} 之间存在相关性，其他的功耗分量均不影响功耗匹配结果。据此攻击点功耗与实际功耗的匹配实质上等效于 P_{F} 与 $P_{\mathrm{F}}+P_{\mathrm{KIV}}+P_{\mathrm{IVO}}$ 的匹配，故可以使用功耗模型对 P_{F} 和 $P_{\mathrm{F}}+P_{\mathrm{KIV}}+P_{\mathrm{IVO}}$ 进行建模，得出对应的攻击点模拟功耗 P_{H} 和算法整体模拟功耗 P_{U}，并根据 P_{H} 与 P_{U} 的匹配情况对攻击结果进行预判，以近似代替实验验证过程。

$P_{\mathrm{F}}+P_{\mathrm{KIV}}+P_{\mathrm{IVO}}$ 代表了所有与初始向量有关的功耗分量，记与这部分功耗有关的函数为 $g(k_{\mathrm{S}}, iv)$，k_{S} 为密钥分量，对 $P_{\mathrm{F}}+P_{\mathrm{KIV}}+P_{\mathrm{IVO}}$ 的建模就是通过功耗模型将函数 $g(k_{\mathrm{S}}, iv)$ 的输出映射为模拟功耗 P_{U}。攻击点函数 $f(k_{\mathrm{P}}, iv_{\mathrm{P}})$ 中的密钥分量 k_{P} 与函数 $g(k_{\mathrm{S}}, iv)$ 中的密钥分量 k_{S} 并不完全相同，但 k_{P} 所有可能取值都包含于 k_{S} 的取值空间，即 $k_{\mathrm{P}} \subseteq k_{\mathrm{S}}$。在对 $P_{\mathrm{F}}+P_{\mathrm{KIV}}+P_{\mathrm{IVO}}$ 建模时，理论上应遍历 k_{S} 的取值空间，但实际操作中计算量可能很大，不利于应用实施，本文提出如下解决方法。

记攻击点函数中的密钥相关量 k_{P} 的取值空间(也即猜测密钥搜索空间)为 K_{G}，$K_{\mathrm{G}}=\{k_1, k_2, \cdots, k_{\mathrm{K}}\}$。在对攻击点模拟功耗进行建模时，将猜测密钥 k_i $(1 \le i \le \mathrm{K})$ 和初始向量 iv_j $(1 \le j \le \mathrm{D})$ 依次代入攻击点函数 $f(k_{\mathrm{P}}, iv_{\mathrm{P}})$ 计算得到规模为 $\mathrm{K} \times \mathrm{D}$ 的中

间值矩阵，上述矩阵经功耗模型映射为 $\mathrm{K}\times\mathrm{D}$ 的攻击点模拟功耗矩阵，记为 $\boldsymbol{H}$，即 $\boldsymbol{H}_{i,j}=\mathrm{power\_model}(f(k_i,iv_j)),1\le i\le \mathrm{K},\ 1\le j\le \mathrm{D}$。

在对 $P_{\mathrm{F}}+P_{\mathrm{KIV}}+P_{\mathrm{IVO}}$ 进行建模时，令密钥分量 k_{S} 在猜测密钥搜索空间 K_{G} 中进行取值，即 $k_{\mathrm{S}}\in K_{\mathrm{G}}$。将 $k_{\mathrm{S}}=k_i$ ($1\le i\le \mathrm{K}$)和初始向量 iv_j ($1\le j\le \mathrm{D}$)依次代入 $g(k_{\mathrm{S}},iv)$ 计算得到规模为 $\mathrm{K}\times\mathrm{D}$ 的中间值矩阵，上述矩阵经功耗模型映射为 $\mathrm{K}\times\mathrm{D}$ 的算法整体模拟功耗矩阵，记为 $\boldsymbol{U}$，即 $\boldsymbol{U}_{i,j}=\mathrm{power\_model}(g(k_i,iv_j)),\ 1\le i\le \mathrm{K},\ 1\le j\le \mathrm{D}$。

由于 k_{S} 没有完全遍历其取值空间，故上述关于算法整体功耗的模拟并没有包含所有可能情况，但基于该方法对攻击方案进行评估是有意义的：尽管无法保证按本文提出的评估方法筛选出的攻击方案一定有效，但可以肯定的是，无法满足评估要求的攻击方案肯定是无效的，即攻击方案满足评估要求是确保攻击成功实施的必要条件。另一方面，如果能够通过选取特定的初始向量，使 P_{KIV} 和 P_{IVO} 保持恒定(方法与前一节所提到的初始向量选取策略相一致)，则算法整体模拟功耗可表述为 $P_{\mathrm{U}}=P_{\mathrm{H}}+P_{\mathrm{other}}$，其中 P_{other} 为常量。这种情形下，上述关于算法整体功耗的模拟涵盖了所有可能情况，与实际情况相符。

基于上述功耗建模，通过分析攻击点模拟功耗 P_{H} 与算法整体模拟 P_{U} 的匹配情况，对攻击方案进行评估。计算 $\boldsymbol{H}$ 中各行与 $\boldsymbol{U}$ 中各行的相关系数，得到相关系数矩阵 $\boldsymbol{C}$，即

$$\boldsymbol{C}_{i,j}=\mathrm{corrcoeff}(\boldsymbol{H}_{i,*},\boldsymbol{U}_{j,*}),\ 1\le i,j\le \mathrm{K} \tag{1}$$

式中 $\boldsymbol{H}_{i,*}$ 表示矩阵 $\boldsymbol{H}$ 的第 i 行。当矩阵 $\boldsymbol{C}$ 同时满足以下特征时，可初步判定攻击方案满足实施能量分析攻击的必要条件。

特征 1：$\forall k\in[1,\mathrm{K}]$，有且仅有 $\boldsymbol{C}_{k,k}=\max(\boldsymbol{C}_{k,*})$；

特征 2：$\forall k,j\in[1,\mathrm{K}]$且$k\ne j$，$\boldsymbol{C}_{k,j}<<\boldsymbol{C}_{k,k}$。

即：(1)当且仅当猜测密钥与实际密钥相一致时，攻击点模拟功耗与算法整体模拟功耗具有最强的相关性；(2)当猜测密码与实际密钥不一致时，攻击点模拟功耗与算法整体模拟功耗的相关性远小于猜测正确时的情况。

4　ZUC 的能量分析攻击

ZUC[16]是一种面向字(word-oriented)的序列密码算法，密钥和初始向量长度均为 128 bit，主要由 16 个 31 bit 位宽的反馈移位寄存器(Feedback Shift Register, FSR)、比特重组(Bit-Reorganization, BR)和非线性函数 F 3 部分组成，在密钥流生成阶段每个时钟周期输出 1 个 32 bit 的密钥字(key-word)。

4.1 攻击点的选取

ZUC 算法中非线性函数 F 中的 $\mathrm{S}\cdot\mathrm{L}_1(x)$ 和 $\mathrm{S}\cdot\mathrm{L}_2(x)$ 同时与密钥和初始向量有关，且与密钥有关的抽头数量较少，搜索空间小，满足作为攻击点函数的基本条件，两者均可作为攻击点。记 $X_1^{(t)}$ 和 $X_2^{(t)}$ 分别为 X_1 和 X_2 空转 t 轮后的状态值，$R_1^{(t)}$ 和 $R_2^{(t)}$ 分别为寄存器 R_1 和 R_2 空转 t 轮后的状态值，$S_i^{(t)}(m:n)$ 为空转 t 轮后寄存器组 S 中第 i 个寄存器 S_i 中的第 m 至第 n 比特状态值(令最右端为第 0 比特)，则当 $0\le t\le 4$ 时，有

$$\begin{aligned}X_1^{(t)}&=S_{11}^{(t)}(15:0)\,||\,S_9^{(t)}(30:15)\\&=d_{11+t}(7:0)\,||\,iv_{11+t}\,||\,k_{9+t}\,||\,d_{9+t}(14:7)\end{aligned}\tag{2}$$

$$\begin{aligned}X_2^{(t)}&=S_7^{(t)}(15:0)\,||\,S_5^{(t)}(30:15)\\&=d_{7+t}(7:0)\,||\,iv_{7+t}\,||\,k_{5+t}\,||\,d_{5+t}(14:7)\end{aligned}\tag{3}$$

记 $W_1^{(t)}=R_1^{(t)}+X_1^{(t)}\bmod 2^{32}$，$W_2^{(t)}=R_2^{(t)}\oplus X_2^{(t)}$，$W_{1\mathrm{H}}^{(t)}=W_1^{(t)}(31:16)$，$W_{1\mathrm{L}}^{(t)}=W_1^{(t)}(15:0)$，$W_{2\mathrm{H}}^{(t)}=W_2^{(t)}(31:16)$，$W_{2\mathrm{L}}^{(t)}=W_2^{(t)}(15:0)$，则攻击点函数可表述为 $f_1^{(t)}=\mathrm{S}\cdot\mathrm{L}_1(W_{1\mathrm{L}}^{(t)}\,||\,W_{2\mathrm{H}}^{(t)})$，$(0\le t\le 4)$；$f_2^{(t)}=\mathrm{S}\cdot\mathrm{L}_2(W_{2\mathrm{L}}^{(t)}\,||\,W_{1\mathrm{H}}^{(t)})$，$(0\le t\le 4)$。

(1)当 $t=0$ 时　由于 $R_1^{(0)}=R_2^{(0)}=0$，则有 $W_1^{(0)}=X_1^{(0)}$，$W_2^{(0)}=X_2^{(0)}$，故

$$\begin{aligned}f_1^{(0)}&=\mathrm{S}\cdot\mathrm{L}_1\left(W_{1\mathrm{L}}^{(0)}\middle\|W_{2\mathrm{H}}^{(0)}\right)=\mathrm{S}\cdot\mathrm{L}_1\left(X_{1\mathrm{L}}^{(0)}\middle\|X_{2\mathrm{H}}^{(0)}\right)\\&=\mathrm{S}\cdot\mathrm{L}_1(k_9\,||\,d_9(14:7)\,||\,d_7(7:0)\,||\,iv_7)\end{aligned}\tag{4}$$

理论上，以 f_1 为攻击点函数，通过控制第 7 字节初始向量 iv_7，可以恢复出第 9 字节密钥 k_9。同理，

$$\begin{aligned}f_2^{(0)}&=\mathrm{S}\cdot\mathrm{L}_2\left(W_{2\mathrm{L}}^{(0)}\middle\|W_{1\mathrm{H}}^{(0)}\right)=\mathrm{S}\cdot\mathrm{L}_2\left(X_{2\mathrm{L}}^{(0)}\middle\|X_{1\mathrm{H}}^{(0)}\right)\\&=\mathrm{S}\cdot\mathrm{L}_2(k_5\,||\,d_5(14:7)\,||\,d_{11}(7:0)\,||\,iv_{11})\end{aligned}\tag{5}$$

理论上，以 f_2 为攻击点函数，通过控制第 11 字节初始向量 iv_{11}，可以恢复出第 5 字节密钥 k_5。

(2)当 $1\le t<3$ 时　由于 $R_1^{(t)}=f_1^{(t-1)}$，$R_2^{(t)}=f_2^{(t-1)}$，故经过前一轮的两次攻击后，$R_1^{(t)}$ 和 $R_2^{(t)}$ 即为已知值，则以 f_1 为攻击点函数时，

$$W_{1\mathrm{L}}^{(t)}=\left(k_{9+t}\middle\|d_{9+t}(14:7)\right)+R_{1\mathrm{L}}^{(t)}\bmod 2^{16}\tag{6}$$

$$W_{2\mathrm{H}}^{(t)}=\left(d_{7+t}(7:0)\middle\|iv_{7+t}\right)\oplus R_{2\mathrm{H}}^{(t)}\tag{7}$$

故攻击点函数 $f_1^{(t)}$ 可由密钥字节 k_{9+t} 和初始向量字节 iv_{7+t} 唯一确定，因此理论上，通过选取初始向量，可以恢复出密钥字节 k_{9+t}。

同理，以 f_2 为攻击点函数时，

$$W_{2\mathrm{L}}^{(t)}=\left(k_{5+t}\middle\|d_{5+t}(14:7)\right)\oplus R_{2\mathrm{L}}^{(t)}\tag{8}$$

$$W_{1\mathrm{H}}^{(t)}=\left(d_{11+t}(7:0)\middle\|iv_{11+t}\right)+R_{1\mathrm{H}}^{(t)}+\mathrm{carry}\bmod 2^{16}\tag{9}$$

式(9)中，carry 表示计算 $W_{1\mathrm{L}}^{(t)}$ (见式 6)时产生的进位，由于 k_{9+t} 先于 k_{5+t} 被恢复出来，因此在第 t 轮以 f_2 为

攻击点函数时，carry 是已知的。故攻击点函数 $f_2^{(t)}$ 可由密钥字节 k_{5+t} 和初始向量字节 iv_{11+t} 唯一确定，因此理论上，通过选取初始向量，可以恢复出密钥字节 k_{5+t}。

由于受 f_1 中模 2^{32} 加法进位的影响，在空转阶段 $1 \le t < 3$ 的各轮攻击中，每一轮应先以 f_1 为攻击点函数，再以 f_2 为攻击点函数，依次恢复出密钥 k_{9+t} 和 k_{5+t}。

(3)当 $t \ge 3$ 时　当 $t = 3$ 时，以 f_1 为攻击点函数，所需的初始向量样本通过控制初始向量字节 iv_{10} (iv_{7+t})产生，即 iv_{10} 为可变量。而在 $t = 0$ 时，iv_{10} 被加载到寄存器 S_{10}，S_{10} 为 FSR 的抽头，因此 FSR 的反馈值(即寄存器 S_{15} 的状态更新值)受 iv_{10} 的影响，进而影响 FSR 中相关寄存器的功耗。由于 iv_{10} 对 S_{10} 的影响经过了一些非线性运算，目前暂时难以完全消除由此产生的功耗干扰(文献[13]称之为转换噪声)。作者在不消除转换噪声的情况下进行了攻击实验，错误密钥与正确密钥攻击结果的区分度很小，攻击效果并不理想，故该阶段暂不予讨论，本文仅给出 $0 \le t < 3$ 阶段的详细攻击方案。

4.2 初始向量的选取

首先对密码算法整体模拟功耗 P_{U} 和攻击点模拟功耗 P_{H} 进行建模，采用汉明距离模型，算法整体功耗以所有寄存器翻转情况为建模基准，攻击点功耗的建模以与攻击点函数有关的寄存器翻转情况为建模基准(原因分析参见文献[17])。对第 t 轮的局部密钥进行攻击时，相关功耗在第 $t+1$ 轮获得，因此第 t 轮攻击时算法整体功耗可表述为

$$P_{\mathrm{U}}^{(t)} = \mathrm{HD}\left(S^{(t+1)}, S^{(t)}\right) + \mathrm{HD}\left(R_1^{(t+1)}, R_1^{(t)}\right) + \mathrm{HD}\left(R_2^{(t+1)}, R_2^{(t)}\right) \tag{10}$$

以 S_f 表示与攻击点函数有关的寄存器状态，则空转阶段第 t 轮时攻击点功耗可表述为

$$P_{\mathrm{H}}^{(t)} = \mathrm{HD}\left(S_f^{(t+1)}, S_f^{(t)}\right) \tag{11}$$

对于某轮攻击，由于寄存器 S_i ($0 \le i \le 15$)中密钥量 k_{i+t} 和常量 d_{i+t} ($0 \le t \le 2$)是固定值，因此各寄存器中上述相关比特位的功耗为常量，即不因加载不同的初始向量而变化，故 ZUC 算法中只有与初始向量有关的寄存器的功耗可能发生变动，包括寄存器 R_1, R_2 及 S_i 中与初始向量有关的比特位。

(1)当 $t = 0$ 时　以 f_1 为攻击点函数时，由式(4)知，攻击点函数值由密钥字节 k_9 和初始向量字节 iv_7 确定，因此初始向量样本中字节 iv_7 为可变量，初始向量中其他字节均固定为 0。初始向量字节 iv_7 的变动必然会对整体功耗产生影响，为了避免对攻击的干扰，在初始向量中引入互补比特位，记为 iv_q，以使 iv_7 和 iv_q 产生的功耗之和保持恒定，则初始向量选取方案为

$$iv_i^{(0)} = \begin{cases} \left\{x \mid x \in \mathbb{F}_2^8\right\}, & i = 7 \\ \overline{iv}_7, & i = q \\ 0, & i = \text{其他} \end{cases} \tag{12}$$

其中，iv_q 的位置选取需满足以下条件：(a)不能位于 FSR 反馈函数的抽头位置；(b)不能参与攻击点函数 f_1 或 f_2 的运算。在该方案下，各寄存器组 S 的功耗保持固定，因此攻击点功耗 $P_{\mathrm{H}}^{(t)}$ 仅与寄存器 R_1 和 R_2 的功耗有关，而寄存器 R_2 的功耗为

$$\begin{aligned} P_{\mathrm{R2}}^{(0)} &= \mathrm{HD}\left(R_2^{(1)}, R_2^{(0)}\right) = \mathrm{HD}\left(f_2^{(0)}, 0\right) = \mathrm{HW}\left(f_2^{(0)}\right) \\ &= \mathrm{HW}(\mathrm{S}\cdot\mathrm{L}_2(k_5 \,||\, d_5(14:7)||d_{11}(7:0)||iv_{11})) \\ &= \mathrm{HW}(\mathrm{S}\cdot\mathrm{L}_2(k_5 \,||\, d_5(14:7)||d_{11}(7:0)||0x00)) \end{aligned} \tag{13}$$

式(13)中，由于密钥字节 k_5 在攻击中为固定值，因此寄存器 R_2 的功耗相当于常量，故攻击点功耗 $P_{\mathrm{H}}^{(t)}$ 仅与寄存器 R_1 的功耗有关。

$$\begin{aligned} P_{\mathrm{H}}^{(0)} &= \mathrm{HD}\left(R_1^{(1)}, R_1^{(0)}\right) = \mathrm{HD}\left(f_1^{(0)}, 0\right) = \mathrm{HW}\left(f_1^{(0)}\right) \\ &= \mathrm{HW}(\mathrm{S}\cdot\mathrm{L}_1(k_9 \,||\, d_9(14:7) \,||\, d_7(7:0) \,||\, iv_7)) \end{aligned} \tag{14}$$

不妨记算法中其他常量功耗为 P_{other}，则算法整体功耗为

$$P_{\mathrm{U}}^{(0)} = P_{\mathrm{H}}^{(0)} + P_{\mathrm{other}} \tag{15}$$

使与攻击点功耗 $P_{\mathrm{U}}^{(0)}$ 有关的密钥相关量 k_9 和初始向量相关量 iv_7 遍历各自的取值空间，得到攻击点模拟功耗矩阵 $\boldsymbol{H}$ 和算法整体模拟功耗矩阵 $\boldsymbol{U}$，并按评估方法计算两者的相关系数矩阵 $\boldsymbol{C}$。表 1 为第 0 轮以 f_1 为攻击点时的矩阵 $\boldsymbol{C}$。

可以看到，该方案下当且仅当猜测密钥与实际密钥一致时，攻击点功耗与整体功耗具有最大相关性，满足评估方法中的特征要求。

类似地，以 f_2 为攻击点函数时，攻击点函数值由密钥字节 k_5 和初始向量字节 iv_{11} 确定，因此初始向量样本中字节 iv_{11} 为可变量，同样引入互补比特位 iv_q，初始向量中其他字节均固定为 0，方案为

$$iv_i^{(0)} = \begin{cases} \left\{x \mid x \in \mathbb{F}_2^8\right\}, & i = 11 \\ \overline{iv}_{11}, & i = q \\ 0, & i = \text{其他} \end{cases} \tag{16}$$

攻击点功耗 $P_{\mathrm{H}}^{(t)}$ 仅与寄存器 R_2 的功耗有关，

$$\begin{aligned} P_{\mathrm{H}}^{(0)} &= \mathrm{HD}\left(R_2^{(1)}, R_2^{(0)}\right) = \mathrm{HD}\left(f_2^{(0)}, 0\right) = \mathrm{HW}\left(f_2^{(0)}\right) \\ &= \mathrm{HW}(\mathrm{S}\cdot\mathrm{L}_2(k_5 \,||\, d_5(14:7) \,||\, d_{11}(7:0)||iv_{11})) \end{aligned} \tag{17}$$

同理，通过计算相关系数矩阵 $\boldsymbol{C}$，以对方案进行评估，结果表明方案是可行的，限于篇幅不再给出具体数据。

表1 第0轮以f_1为攻击点时$\boldsymbol{H}$与$\boldsymbol{U}$的相关系数矩阵$\boldsymbol{C}$

$k_{\mathrm{P}}(\boldsymbol{H})$	$k_{\mathrm{P}}(\boldsymbol{U})$								
	0	1	2	3	…	252	253	254	255
0	1.00	0.09	0.02	0.08	…	−0.02	−0.12	−0.01	0.03
1	0.09	1.00	0.04	0.07	…	−0.01	0.02	0.04	−0.10
2	0.02	0.04	1.00	−0.05	…	−0.01	−0.01	−0.01	−0.04
3	0.08	0.07	−0.05	1.00	…	−0.02	0.01	0.04	0.01
⋮	⋮	⋮	⋮	⋮	…	⋮	⋮	⋮	⋮
252	−0.02	−0.01	−0.01	−0.02	…	1.00	−0.08	−0.08	−0.06
253	−0.12	0.02	−0.01	0.01	…	−0.08	1.00	0.08	0.03
254	−0.01	0.04	−0.01	0.04	…	−0.08	0.08	1.00	0.09
255	0.03	−0.10	−0.04	0.01	…	−0.06	0.03	0.09	1.00

(2)当$1 \le t < 3$时　根据前面选取攻击点函数时的分析，在进行第t轮攻击时，由于前$t-1$轮已经将相关密钥恢复出来，因此寄存器R_1和R_2的状态值是已知的，但不再是初始值0，因此在计算$W_{1\mathrm{H}}^{(t)}$时存在低16 bit向高位进位的情况，见式(9)，但这并不会对攻击过程产生影响，下面给出分析过程。

以f_1为攻击点函数时，待攻击密钥字节为k_{9+t}，初始向量中可变字节为iv_{7+t}及其互补字节iv_{q+t}，初始向量其余部分全为0。攻击点功耗$P_{\mathrm{H}}^{(t)}$仅与寄存器R_1和R_2的功耗有关，其中寄存器R_2的功耗为

$$\begin{aligned} P_{\mathrm{R2}}^{(t)} &= \mathrm{HD}\left(R_2^{(t+1)}, R_2^{(t)}\right) = \mathrm{HW}\left(f_2^{(t)} \oplus R_2^{(t)}\right) \\ &= \mathrm{HW}\left(\mathrm{S}\cdot\mathrm{L}_2\left(W_{2\mathrm{L}}^{(t)} \middle\| W_{1\mathrm{H}}^{(t)}\right) \oplus R_2^{(t)}\right) \end{aligned} \tag{18}$$

其中$W_{2\mathrm{L}}^{(t)}$和$W_{1\mathrm{H}}^{(t)}$的表达式见式(8)和式(9)，在一轮攻击中，k_{5+t}，iv_{11+t}，$R_{1\mathrm{H}}^{(t)}$，$R_{2\mathrm{L}}^{(t)}$和d_i均为常量，而计算$W_{1\mathrm{L}}^{(t)}$产生的进位carry与k_{9+t}有关，但并不受不同初始向量的影响，即无论是在获取实际功耗过程中，还是通过遍历猜测密钥以计算模拟功耗的过程中，由于k_{9+t}为常量，算法在加载不同初始向量进行初始化时，carry是一定的，因此寄存器R_2的功耗也是固定的。由于常量功耗对相关系数的计算没有影响，因此攻击点功耗$P_{\mathrm{H}}^{(t)}$仍然仅与寄存器R_1的功耗有关。

$$\begin{aligned} P_{\mathrm{H}}^{(t)} &= \mathrm{HD}(R_1^{(t+1)}, R_1^{(t)}) = \mathrm{HW}(f_1^{(t)} \oplus R_1^{(t)}) \\ &= \mathrm{HW}(\mathrm{S}\cdot\mathrm{L}_1(W_{1\mathrm{L}}^{(t)} \,||\, W_{2\mathrm{H}}^{(t)}) \oplus R_2^{(t)}) \end{aligned} \tag{19}$$

其中$W_{1\mathrm{L}}^{(t)}$和$W_{2\mathrm{H}}^{(t)}$的表达式见式(6)和式(7)，可见攻击点功耗由密钥字节k_{9+t}和初始向量字节iv_{7+t}唯一确定，攻击方法与$t=0$时与完全相同。

以f_2为攻击点函数时，待攻击密钥字节为k_{5+t}，初始向量中可变字节为iv_{11+t}及其互补字节iv_{q+t}，初始向量其余部分全为0。攻击点功耗$P_{\mathrm{H}}^{(t)}$仅与寄存器R_1和R_2的功耗有关，寄存器R_1的功耗表达式见式(19)，其中，$iv_{7+t}, R_{1\mathrm{L}}^{(t)}, R_{2\mathrm{H}}^{(t)}$和$d_i$均为常量，而$k_{9+t}$在同一轮攻击中已被恢复，故$R_1$的功耗为常量，则攻击点功耗$P_{\mathrm{H}}^{(t)}$仅与寄存器$R_2$的功耗有关，其表达式见式(18)，由于$k_{9+t}$为已知量，故carry为已知量，攻击点功耗由密钥字节k_{5+t}和初始向量字节iv_{11+t}唯一确定，攻击方法与$t=0$时完全相同。

综上所述，在$t=0$和$1 \le t < 3$时，初始向量选取方案是类似的，下面给出统一的表达形式，同时根据前面互补字节iv_q的选取要求给出q的取值。

(a)以f_1为攻击点函数时的初始向量选取方案

$$iv_i^{(t)} = \begin{cases} \left\{x \mid x \in \mathbb{F}_2^8\right\}, & i = 7+t \\ \overline{iv}_{7+t}, & i = 1+t \\ 0, & i = \text{其他} \end{cases} \tag{20}$$

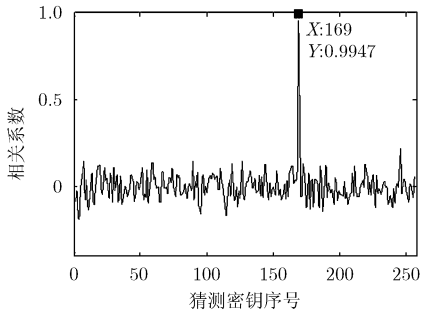
(b)以f_2为攻击点函数时的初始向量选取方案

$$iv_i^{(t)} = \begin{cases} \left\{x \mid x \in \mathbb{F}_2^8\right\}, & i = 11+t \\ \overline{iv}_{11+t}, & i = 1+t \\ 0, & i = \text{其他} \end{cases} \tag{21}$$

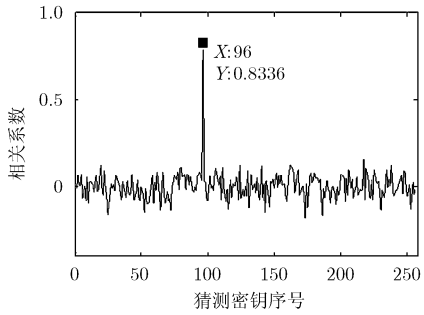
按照攻击方案，可以实施6次攻击，每次恢复1个密钥字节，共计48 bit密钥。

4.3 攻击方案验证

本文基于ASIC开发环境构建验证平台：在SMIC 65 nm工艺下，使用Design Compiler和IC Compiler工具对ZUC算法的HDL(Hardware Description Language)代码进行综合、布局布线并提取寄生参数信息，使用VCS对反标寄生参数后的ZUC网表进行仿真，得到包含所有逻辑门翻转信息的VCD文件，最后使用功耗分析工具PrimeTime PX对VCD文件进行分析，得到算法芯片加载不同初始向量样本时的总体功耗，仿真验证即以该功耗作为芯片的实际功耗数据。实验中，设定密钥为$k=$ 0x5a5b5c5d5e5fa5a6a7a8a9aaabacadae，按照前文提出的攻击方案，成功实施了6次攻击，限于篇幅，下面仅展示了前4次的攻击结果，如图2和图3所示。图中横轴为猜测密钥(k_{P})序号，从1开始，即

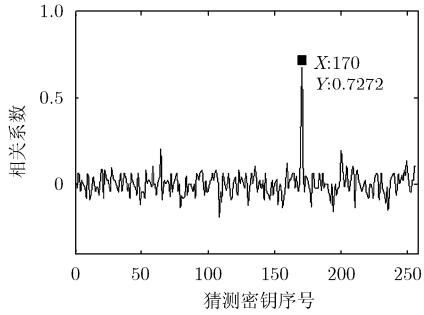


(a)以f_1为攻击点时的攻击结果

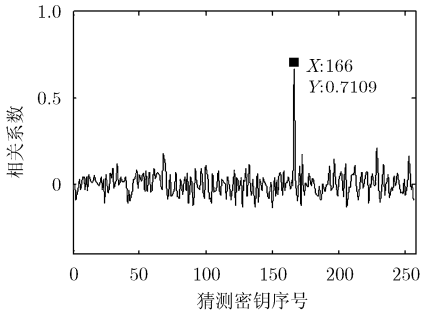


(b)以f_2为攻击点时的攻击结果

图 2 第 0 轮的攻击结果



(a)以f_1为攻击点时的攻击结果



(b)以f_2为攻击点时的攻击结果

图 3 第 1 轮的攻击结果

密钥字节 $0x00$ 对应横轴坐标 1, $0xff$ 对应 256，纵轴表示攻击时刻攻击点功耗与算法总体功耗之间的相关系数。

(1)第 0 轮($t=0$ 时)的攻击结果　第 0 轮以 f_1 为攻击点时，待攻击密钥字节为 $k_9=k[55:48]$，即 $0xa8$，十进制表示为 168。以 f_2 为攻击点时，待攻击密钥字节为 $k_5=k[87:80]$，即 $0x5f(95_{10})$。由图 2 可见，以 f_1 为攻击点时，猜测密钥序号为 169 时相关系数达到最大值 0.9947，以 f_2 为攻击点时，猜测密钥序号为 96 时，相关系数达到最大值 0.8336，表明攻击结果正确。

(2)第 1 轮($t=1$时)的攻击结果　第 1 轮攻击时，待攻击密钥字节分别为 $k_{10}=k[47:40]$ 和 $k_6=k[79:72]$，即 $0xa9(169_{10})$和 $0xa5(165_{10})$。由图 3 可见，以 f_1 为攻击点时，猜测密钥序号为 170 时相关系数达到最大值 0.7272，以 f_2 为攻击点时，猜测密钥序号为 166 时，相关系数达到最大值 0.7109，表明攻击结果正确。

文献[6]使用的验证环境与本文的相似，其采用随机初始向量样本，样本数达到 5000 时才能观察到明显的差分功耗尖峰。与之相比，本文的攻击方案只需 256 个初始向量，且攻击效果更为显著。上述实验证实了所提出的攻击方案的快速评估方法的有效性，同时也表明 ZUC 并不具备相关性能量分析攻击的免疫能力。

5 结束语

本文对 ZUC 在相关性能量分析攻击方面的免疫能力进行了研究，提出了一种有效的攻击方案。尽管同属对称密码体制，但序列密码的能量分析攻击相比分组密码更加困难。为了提高攻击的针对性，提出了序列密码能量分析攻击方案的快速评估方法，据此给出了 ZUC 的相关性能量分析攻击方案，并进行了验证，结果表明 ZUC 并不具备相关性能量分析攻击的免疫能力，同时也证实了攻击方案快速评估方法的有效性。相对于一般的攻击方案，本文所提出的方案避免了一般方案中容易出现的攻击点功耗与其他功耗成分之间存在相关性、错误猜测密钥与正确密钥攻击结果区分度低以及所需初始向量样本量过大等问题。

不足之处在于，由于单纯的侧信道攻击普遍存在可分析轮数少的局限性[18]，目前的攻击方法只能进行前 3 轮共 6 次攻击，仅恢复 48 bit 密钥，后续可结合代数分析方法进行代数旁道攻击的相关研究。

参 考 文 献

[1] Wu H J, Huang T, Phuong H N, *et al.*. Differential attacks against stream cipher ZUC[C]. Proceedings of the 18th International Conference on the Theory and Application of

Cryptology and Information Security, Beijing, China, 2012: 262–277.

[2] Zhou C F, Feng X T, and Lin D D. The initialization stage analysis of ZUC v1.5[C]. Proceedings of the 10th International Conference, Sanya, China, 2011: 40–53.

[3] Gautham S. The stream cipher core of the 3GPP encryption standard 128-EEA3: timing attacks and countermeasures[C]. Proceedings of the 7th International Conference, Beijing, China, 2011: 269–288.

[4] L afitte F, M arkowitch O, and Vav Heule D. SAT based analysis of LTE stream cipher ZUC[C]. Proceedings of the 6th International Conference on Security of Information and Networks, Aksavay, Turkey, 2013: 110–116.

[5] 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, 24(6): 1324–1333.
Guan Jie, Ding Ling, and Liu Shu-kai. Guess and determine attack on SNOW 3G and ZUC[J]. *Journal of Software*, 2013, 24(6): 1324–1333.

[6] Tang M, Cheng P P, and Qiu Z L. Differential power analysis on ZUC algorithm [OL]. IACR ePrint. http://eprint.iacr.org/2012/299.pdf. 2013-12-01.

[7] 唐明, 高剑, 孙乐昊, 等. 嵌入式平台下 ZUC 算法的侧信道频域攻击[J]. 山东大学学报(理学版), 2014, 49(9): 29–34.
Tang Ming, Gao Jian, Sun Le-hao, *et al.*. Side channel attacks in frequency domain for ZUC algorithm in embedded platform[J]. *Journal of Shandong University*(*Natural Science*), 2014, 49(9): 29–34.

[8] Reddy E K. Overview of the side channel attacks[J]. *Advanced Networking and Applications*, 2013, 4(6): 1799–1808.

[9] Paul K, Joshua J, Benjamin J, *et al.*. Introduction to differential power analysis[J]. *Journal of Cryptography Engineering*, 2011, 1(1): 5–27.

[10] 汪鹏君, 张跃军, 张学龙. 防御差分功耗分析攻击技术研究[J] 电子与信息学报, 2012, 34(11): 2774–2784.
Wang Peng-jun, Zhang Yue-jun, and Zhang Xue-long. Research of differential power analysis countermeasures[J]. *Journal of Electronics & Information Technology*, 2012, 34(11): 2774–2784.

[11] 赵永斌, 胡予濮, 贾艳艳. 一种抵抗能量攻击的线性反馈移位寄存器[J]. 西安电子科技大学学报(自然科学版), 2013, 40(3): 172–179.
Zhao Yong-bin, Hu Yu-pu, and Jia Yan-yan. New design of LFSR based stream ciphers to resist power attack[J]. *Journal of Xidian University* (*Natural Science*), 2013, 40(3): 172–179.

[12] Kumar S, Lemke K, and Paar C. Some thoughts about implementation properties of stream ciphers[C]. Proceedings of State of the Art of Stream Ciphers Workshop, Brugge, Belgium, 2004: 311–319.

[13] Stefan M, Elisabeth O, and Thomas P 著. 冯登国, 周永斌, 刘继业, 等译. 能量分析攻击[M]. 北京: 科学出版社, 2010: 45–46.

[14] 金晨辉, 郑浩然, 张少武, 等. 密码学[M]. 北京: 高等教育出版社, 2009: 149–150.
Jin Chen-hui, Zheng Hao-ran, Zhang Shao-wu, *et al.*. Cryptography[M]. Beijing: Higher Education Press, 2009: 149–150.

[15] 杨昌盛, 于敬超, 严迎建. Grain-128 同步流密码的选择初始向量相关性能量攻击[J]. 计算机应用, 2014, 34(5): 1318–1321.
Yang Chang-sheng, Yu Jing-chao, and Yan Yin-jian. Chosen initial vector correlation power attack on synchronous stream cipher Grain-128[J]. *Journal of Computer Applications*, 2014, 34(5): 1318–1321.

[16] Specification of the 3GPP confidentiality and integrity algorithms 128-EEA3 & 128-EIA3. document 2: ZUC specification version: 1.5[OL]. ETSI/SAGE Specification. http://www.gsma.com/technicalprojects/wp-content/uploads/2012/04/eea3eia3zucv16.pdf. 2011-01-04.

[17] 刘泽艺, 高能, 屠晨阳, 等. 一种抗能量分析攻击的复合寄存器系统[J]. 密码学报, 2014, 1(5): 411–421.
Liu Ze-yi, Gao Neng, Tu Chen-yang, *et al.*. A compound register system against power analysis attack[J]. *Journal of Cryptologic Research*, 2014, 1(5): 411–421.

[18] 刘会英, 赵新杰, 王韬, 等. 基于汉明重的 SMS4 密码代数旁路攻击研究[J]. 计算机学报, 2013, 36(6): 1183–1193.
Liu Hui-yin, Zhao Xin-jie, Wang Tao, *et al.*. Research on hamming weight-based algebraic side-channel attacks on SMS4[J]. *Chinese Journal of Computers*, 2013, 36(6): 1183–1193.

严迎建：　男，1973 年生，博士，教授，研究方向为安全专用芯片侧信道攻击与防护.

杨昌盛：　男，1990 年生，硕士生，研究方向为序列密码侧信道攻击与防护.

李　伟：　男，1983 年生，博士生，讲师，研究方向为安全专用芯片设计.

张立朝：　男，1979 年生，博士生，讲师，研究方向为安全 SoC 设计、嵌入式系统安全防护.