doi:10.11959/j.issn.1000-436x.2016254

针对 SM4 算法的约减轮故障攻击

王敏，吴震，饶金涛，凌杭
（成都信息工程大学信息安全工程学院，四川 成都 610225）

摘 要：提出了一种新型的针对 SM4 算法的约减轮故障攻击，该攻击在加密算法的后 4 轮中导入故障，诱导缩减加密算法的迭代轮数，经过对故障数据的简单筛选，最终仅需 4 个错误密文即可恢复出完整的 128 bit 初始密钥，从而实现了对 SM4 的故障注入攻击。利用该方法对无防护 SM4 算法的能量曲线进行了实际故障注入攻击的实验表明，该攻击方法行之有效，并简化了现有针对 SM4 的差分故障攻击方法，提高了攻击效率。

关键词：SM4 算法；故障注入；约减轮；故障样本筛选；分组密码
中图分类号：TP309.1 **文献标识码**：A

Round reduction-based fault attack on SM4 algorithm

WANG Min, WU Zhen, RAO Jin-tao, LING Hang
(College of Information Security Engineering, Chengdu University of Information Technology, Chengdu 610225, China)

Abstract: A novel method of fault attack based on round reduction against SM4 algorithm was proposed. Faults were injected into the last four rounds of the SM4 encryption algorithm, so that the number of the algorithm's rounds can be reduced. In known-ciphertext scenario, four traces are enough to recover the total 128 bit master key by screening these faults easily. The proposed attack is made to an unprotected SM4 smart card. Experiment shows that this attack method is efficient, and which not only simplifies the existing differential fault attack ,but also improves the feasibility of the attack.
Key words: SM4 algorithm, fault injection, round reduction, fault sample selection, block cipher

1 引言

近年来，无线局域网产品越来越多地融入人们的生活，无线局域网的安全性已经成为了当前研究的热点内容之一。作为中国国内 WAPI 的加密算法，SM4[1]算法也是官方公布的第一个商用密码算法，其安全性极大地影响信息化发展的进程。

密码设备一般是基于电子技术实现的，在运行的过程中难免会受到外界干扰，从而导致运算模块出现寄存器故障或者运算错误，利用这些故障行为产生的错误信息攻击得到密钥的方法就是故障攻击[2]。故障攻击是 1997 年由 Boneh 等最先提出的。文献[1]实现了对基于 CRT 原理实现的 RSA 算法的故障分析。Biham 等[3]借鉴差分密码分析的思想提出差分故障攻击，并用该方法实现了对 DES 算法的攻击。目前，故障攻击的方法已经得到了广泛的应用，包括分组密码[4,5]、序列密码[6]和公钥密码[7]，该方法对密码算法的安全性威胁极高。目前，针对 SM4 算法的故障攻击基本是采用差分故障[8~12]的思想，主要利用同组明文在故障注入后的错误信息和正常运行的输出之间的关系恢复出密钥。

本文针对差分故障分析中候选轮密钥的筛选

收稿日期：2016-09-01
基金项目：“核高基”国家科技大专项基金资助项目（No.2014ZX01032401-001）；国家高技术研究发展计划（“863”计划）基金资助项目（No.2012AA01A403）；四川省科技支撑计划基金资助项目（No.2014GZ0148）；四川省教育厅重点科研基金资助项目（No.13ZA0091）；成都信息工程大学科研人才基金资助项目（No.XAKYXM008）
Foundation Items: The National Science and Technology Major Project of Hegaoji (No.2014ZX01032401-001), The National High Technology Research and Development Program (863 Program) (No.2012AA01A403), The Key Technology Research and Development Program of Sichuan Province (No.2014GZ0148), The Major Scientific Research of Sichuan Educational Commission (No.13ZA0091), The Scientific Research Talent Fund of CUIT (No.XAKYXM008)

过程繁琐，提出一种针对 SM4 算法，基于约减轮思想的故障攻击方法。对 SM4 算法后 4 轮进行故障注入诱导减少轮函数的执行次数，然后利用得到的错误密文信息恢复出轮密钥，最终攻击得到初始密钥。

2　SM4 算法

2006 年，国家密码管理局将我国无线局域网产品的密码算法确定为 SM4 算法。SM4 密码算法是分组密码算法，分组长度为 128 bit，初始密钥长度为 128 bit。该密码算法采用 32 轮的非平衡 Feistel 结构迭代的设计，加密和解密的结构相同，只是轮密钥使用的顺序刚好相反。

2.1　加密算法

令 $\boldsymbol{Z}_2^e$ 表示 e bit 的向量集，$\boldsymbol{Z}_2^{32}$ 中的元素称为字。SM4 算法以字为基本单位进行加密运算。设输入明文表示为 $(X_0,X_1,X_2,X_3)\in(\boldsymbol{Z}_2^{32})$，输出密文表示为 $(Y_0,Y_1,Y_2,Y_3)\in(\boldsymbol{Z}_2^{32})$，轮密钥表示为 $rk_i\in\boldsymbol{Z}_2^{32}$，则 SM4 算法的加密流程如图 1 所示。

该算法的一次迭代运算称为轮变换，轮函数 F 为

$$\begin{aligned}&F(X_i,X_{i+1},X_{i+2},X_{i+3},rk_i)\\&=X_i\oplus T(X_{i+1}\oplus X_{i+2}\oplus X_{i+3}\oplus rk_i)\end{aligned}\tag{1}$$

其中，T 表示合成置换，包括非线性变换 τ 和非线性变换 L，即 $T(\cdot)=L(\tau(\cdot))$。τ 变换由 4 个并行的 S 盒构成，L 变换表示如下。

$$\begin{aligned}&L(x)=x\oplus(x\lll 2)\oplus(x\lll 10)\oplus\\&(x\lll 18)\oplus(x\lll 24),x\in\boldsymbol{Z}_2^{32}\end{aligned}\tag{2}$$

32 轮轮函数执行后需要进行一次反序变换 R，如图 2 所示。

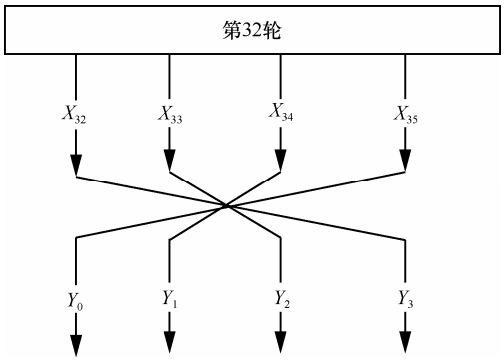


图 2　反序变换 R

2.2　密钥扩展算法

设初始密钥为 MK，系统参数为 FK，则轮密钥 rk_i 的生成过程如式(3)和式(4)所示。

$$K=(K_0,K_1,K_2,K_3)MK\oplus FK\tag{3}$$

$$rk_i=K_{i+4}=K_i\oplus L'(\tau(K_{i+1}\oplus K_{i+2}\oplus K_{i+3}\oplus CK_i))\tag{4}$$

其中，$i\in[0,31]$，CK_i 为固定参数，L' 变换表示如式(5)所示。

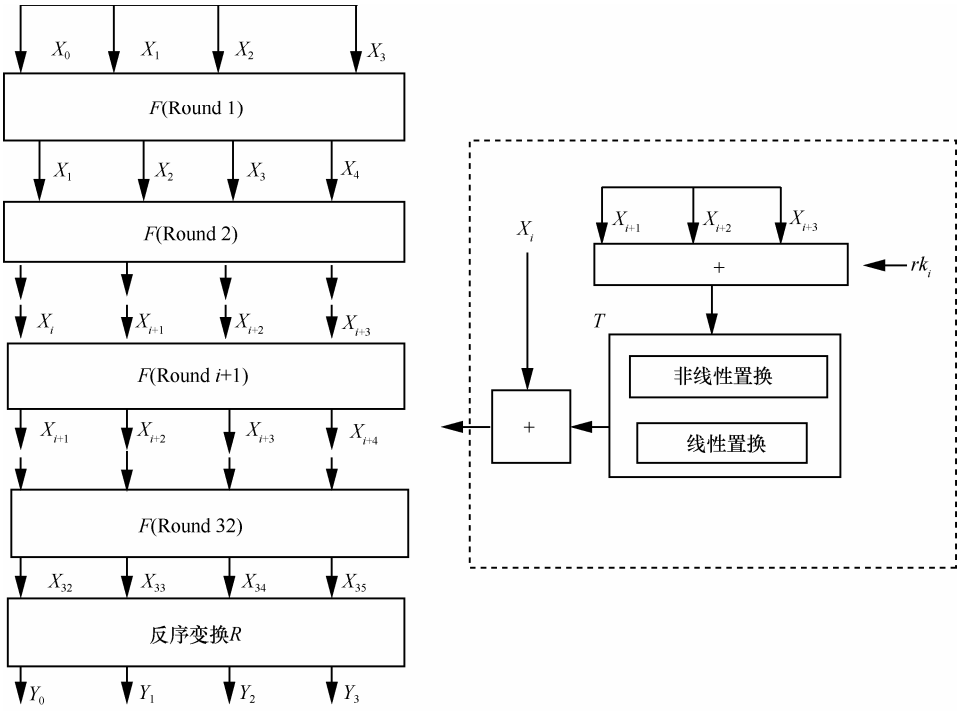


图 1　SM4 算法加密流程

$$L'(x) = x \oplus (x \lll 13) \oplus (x \lll 23), x \in \boldsymbol{Z}_2^{32} \quad (5)$$

3 针对 SM4 算法已有的故障攻击

3.1 故障模型

故障攻击一般都是基于某种故障模型进行的，目标算法的密钥能否恢复在很大程度取决于攻击者注入的故障是否符合故障模型。故障模型主要包括以下 4 个方面。

1) 故障位置

采用面向字节的随机故障模型一般都要求能够将故障引入某一个指定的数据存储单元，这种方式在实际的故障诱导过程中需要较多的注入次数。

2) 故障时机

攻击者需要控制故障发生的时刻，这样才能保证密码设备的运算在某个特定的步骤或者范围内完成注入。注入范围包括加密、解密和密钥扩展，注入步骤包括轮密钥加、*S* 盒置换等。

3) 故障效果

故障效果具体体现在故障持续度、故障注入位置是否随机、故障影响的字节大小和密码设备一次运行过程中注入的次数等方面。

4) 故障动作

常用的故障动作有 2 种：① 值重置，设定故障位置的值为特定值；② 跳过操作，跳过某个操作运算，使该操作的输入和输出相同。故障动作的实现依赖于故障注入的方式，高成本的故障注入技术（如激光束、聚离子束）能够更好地保障故障动作的实现，但是这类方法需要详细了解密码设备的实现细节，所以一般采用如电压峰值、时钟毛刺等低成本且技术水平要求不高的方式。

3.2 现有故障攻击方法

文献[8]采用面向字节的随机故障模型，结合差分分析的方法，理论上需要 32 个错误密文即可恢复 SM4 算法的 128 bit 初始密钥。针对 SM4 算法，文中在典型的差分故障攻击的基础上，率先利用加密算法中线性变换 L 的特点寻找部分输出值和输入值之间的对应关系，从而提高攻击的效率。该文的不足之处是在加密过程中特定的存储单元中诱导产生故障，这种方式故障诱导的成功率偏低。文献[9]在该文的基础上进行了改进，理论上只需要 2 个错误密文可实现攻击。

文献[10]不同于文献[8,9]，将故障的注入范围设定为密钥扩展阶段，不仅扩展了针对 SM4 算法故障攻击的注入范围，而且故障注入的位置不再需要限定在指定的存储单元中，而是待攻击轮子密钥生成过程中的任意某个存储单元。该方法成功攻击理论上需要 8 个错误密文，但是该结果的前提是最后一轮故障注入的位置必须是在第 2 个、第 3 个或者第 4 个字节上。

文献[12]在前人攻击的基础上，进一步降低了针对 SM4 算法的差分故障攻击中对故障注入位置的要求，只需要对 SM4 算法加密过程的后 4 轮进行任意位置的故障注入即可实现攻击。

根据目前的研究，基于差分思想的故障攻击，虽然故障产生位置的要求在逐渐降低，但是根据错误密文筛选候选密钥的过程比较繁琐，而且筛选的方法不具有通用性。本文所提出的方法有效解决了这个问题，而且攻击方法能够很方便地扩展到其他迭代密码算法。

4 基于约减轮的故障攻击

分组密码算法一般都是采用迭代的结构，将较弱的轮函数经过多次迭代构造出强密码函数。由此可知，分组密码的安全性与密码的轮数正相关的，因此，最直接的攻击方法就是在分组密码正常运行的过程中通过注入故障来减少密码实际运行的轮数。

基于该思想，Anderson[13]提出了通过在时钟或者芯片电源上产生毛刺来破坏循环变量或条件转移运算的实际攻击方法。2005 年，Choukri 和 Tunstall[14]通过在电源中产生毛刺对基于 AES 算法且未加防护的 Slivercard 成功实现了攻击。

故障攻击包括故障注入和故障利用 2 个部分。故障注入主要是选择一个合适的时刻将故障导入到正在运行的密码设备的某个位置。故障利用是对注入故障后产生的错误信息进行特定的分析来恢复密钥。

针对 SM4 算法的加密过程后 4 轮实施约减轮故障攻击，具体步骤如下。

步骤 1 假设密钥为 K，选定一组明文 X，采集密码设备正常运行时的功耗曲线 T，记录该组明文此时生成的密文 Y。

步骤 2 故障注入。利用步骤 1 中采集的功耗曲线区分 32 轮 SM4 密码算法运行过程中后 4 轮的时间段，对该时间段进行故障注入，诱导提前跳出轮函数正常的迭代，并获取此时的密文 Y_i。

步骤 3　故障样本筛选。SM4 算法的加密过程可以描述如下。

For *round_counter*=1 to 32
　If *round_counter*≤32
　Round Function
　round_counter+1
Reverse Function

本文的故障注入目标是诱导密码设备中控制轮函数迭代次数的寄存器中的值 *round _counter* 出现异常，也就是当 *round _counter* = 31、30、29、28 时，加密流程中判断当前迭代次数时出现故障导致直接跳转到反序变换（reverse function），此时的密文输出记为 Y_i (i=31、30、29、28)。故障筛选是通过比较故障注入时密码设备的功耗曲线和功耗曲线 T 执行的时间来完成，实际操作过程中可以查看功耗曲线中体现的加密轮数进行判断。

步骤 4　攻击第 32 轮。步骤 3 中得到了错误的密文 Y_{31}，根据反序变换 R 逆推得到第 32 轮的轮输入 R_{in_32}。

步骤 5　恢复轮密钥 rk_{32}。根据 R_{in_32} 和正常运行时的密文 Y 推断出第 32 轮的轮密钥 rk_{32}。

步骤 6　攻击第 31 轮、第 30 轮、第 29 轮。仿照步骤 4 获取第 31 轮的轮输入 R_{in_31}，根据 R_{in_31} 和对应的 Y_{31} 可以推断出第 31 轮的轮密钥 rk_{31}。同理可获得 rk_{30} 和 rk_{29}。

步骤 7　根据 SM4 算法的密钥扩展算法，利用攻击出的后 4 轮的轮密钥 rk_{32}、rk_{31}、rk_{30}、rk_{29} 恢复出初始密钥 K。

5　攻击实验与分析

本文实际攻击中涉及的功耗采集环境如表 1 所示。

表 1　功耗采集环境

设备	说明
基础设备	智能卡+ Riscure Power Tracer
数字示波器	WaveRunner 6 Zi Oscilloscopes
故障注入	Riscure VC Glitcher
侧信道分析	Riscure Inspector
服务器	DELL PowerEdge T330

5.1　原始信息采集

设置目标算法的明文信息为 01 23 45 67 89 AB CD EF FE DC BA 98 76 54 32 10，智能卡正常运行，此时生成的密文信息为 68 1E DF 34 D2 06 96 5E 86 B3 E9 4F 53 6E 42 46，采集此时的功耗曲线如图 3 所示。

5.2　故障注入

根据图 3 可区分 SM4 算法加密过程后 4 轮所处的时间段，在该时间段内对控制 32 轮循环迭代的寄存器进行故障注入。实验中执行了 1 000 次故障注入，其中，故障注入成功有 798 次，故障注入失败未影响正常工作有 202 次。部分实验结果如图 4 所示，图中白色部分表示故障注入失败，代表该算法正常工作的数据，暗灰色部分表示出现期望的错误密文，浅灰色部分表示出现其他异常。

分析图 4 中返回的期望密文数据 D2 06 96 5E 86 B3 E9 4F 53 6E 42 46 7B 93 8F 4C，与正确密文的前 96 bit 相同，可得到该数据为第 31 轮加密输出经过反序变换得到的结果。结合正确的密文推断出第 32 轮轮密钥 rk_{32}=9124A012。利用其他的错误密文，可依次获取第 31 轮轮密钥 rk_{31}=01CF72E5、第 30 轮轮密钥 rk_{30}=62293496、第 29 轮轮密钥 rk_{29}=428D3654。最后可推断出初始密钥 K，经过

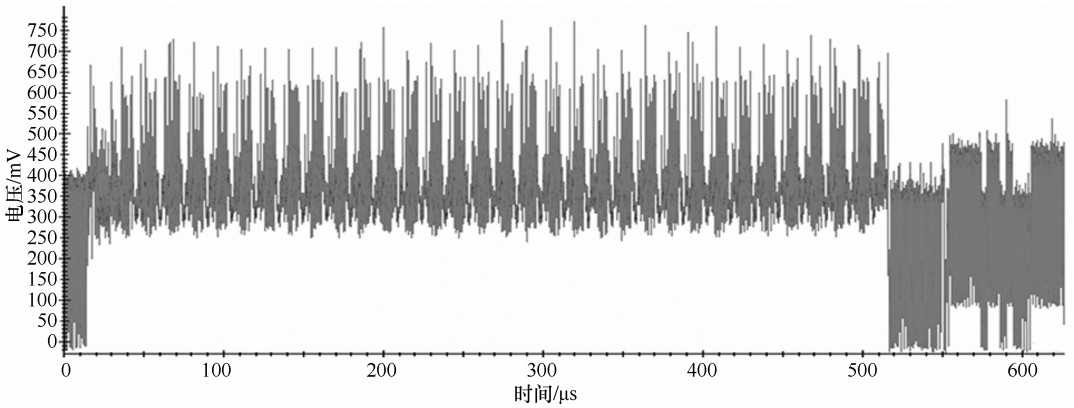


图 3　SM4 正常运行时的功耗曲线

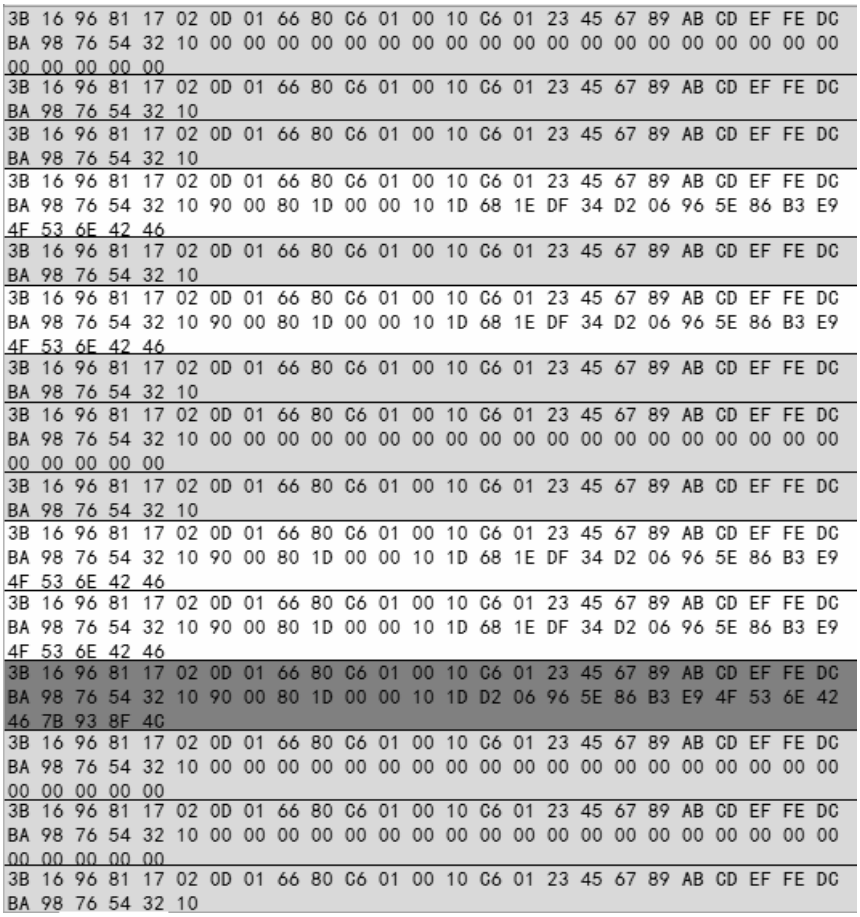


图 4　实验结果

验证采集的正确密文确认攻击成功。通过实际攻击，可以发现本文的方法有助于提高针对 SM4 算法故障攻击的实用性。

6　结束语

本文提出了一种针对 SM4 算法加密过程后 4 轮进行故障注入的约减轮攻击方法，该方法也可以扩展到加密过程前 4 轮或者中间任意位置连续 5 轮。实验结果表明，利用约减轮的思想不仅极大地降低了差分故障分析中恢复轮密钥的繁琐性，而且只需要 4 个错误密文即可攻击出 128 bit 初始密钥。同时，本文的思想还可以应用到其他分组密码的约减轮故障攻击中。下一步的研究将着重于提高故障注入的效率以便进一步提高本文方法的实用性。

参考文献：

[1] 国家商用密码管理办公室. 无线局域网产品使用的 SMS4 密码算法[EB/OL]. http://www.oscca.gov.cn/upfile/200621016423197990.pdf, 2006.
National office of business password management. SMS4 cipher algorithm for wireless local area network products[EB/OL]. http://www.oscca.gov.cn/upfile/200621016423197990.pdf, 2006.

[2] DAN B, RICHARD A, DEMILLO R, et al. On the importance of checking cryptographic protocols for faults[C]//1997:1175-1213.

[3] BIHAM E, SHAMIR A. Differential fault analysis of secret key cryptosystems[J]. Lncs, 1999,1294:513-525.

[4] JOHANNES, JEAN P S. Fault based cryptanalysis of the advanced encryption standard (AES)[M].Springer Berlin Heidelberg, 2002: 162-181.

[5] PIRET G, QUISQUATER J J. A differential fault attack technique against spn structures, with application to the AES and khazad[C]// Cryptographic Hardware and Embedded Systems-CHES 2003, International workshop. 2003:77-88.

[6] KIRCANSKI A, YOUSSEFA M. Differential fault analysis of HC-128[C]//Progress in Cyptology-africacrypt 2010, Third International Conference on Cryptology in Africa, 2010:261-278.

[7] INGRID B, BERND M, VOLKER M. Differential fault attacks on elliptic curve cryptosystems[M]. Springer Berlin Heidelberg, 2000: 131-146.

[8] 张蕾, 吴文玲. SMS4 密码算法的差分故障攻击[J]. 计算机学报, 2006, 29(9): 1596-1602.
ZHANG L, WU W L. Differential fault analysis on SMS4[J]. Chinese Journal of Computers, 2006,29(9):1596-1602.

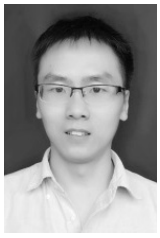
[9] LI W，GU D. An improved method of differential fault analysis on the SMS4 cryptosystem[C]//International Symposium on Data Privacy,

and E-commerce. 2007:175-180.
[10] 李玮，谷大武. 基于密钥编排故障的 SMS4 算法的差分故障分析[J]. 通信学报, 2008, 29(10): 135-142.
LI W, GU D W. Differential fault analysis on the SMS4 cipher by inducing faults to the key schedule[J]. Journal on Communications, 2008, 29(10):135-142.
[11] LI R L, SUN B, LI C, et al. Differential fault analysis on SMS4 using a single fault[J]. Information Processing Letters, 2011, 111(4): 156-163.
[12] 荣雪芳, 吴震, 王敏, 等. 基于随机故障注入的 SM4 差分故障攻击方法[J]. 计算机工程, 2016, 42(7): 129-133.
RONG X F, WU Z, WANG M, et al. Differential fault attack method on sm4 based on random fault injection[J]. Computer Engineering, 2016,42(7):129-133.
[13] ROSS A, MARKUS K. Low cost attacks on tamper resistant devices[C]. Springer, 1997:125-136.
[14] HAMID C, MICHAEL T. Round reduction using faults[J]. FDTC, 2005, 5: 13-24.

作者简介：

王敏（1977-），女，四川资阳人，成都信息工程大学讲师，主要研究方向为网络攻防、侧信道攻击与防御。

吴震（1975-），男，江苏苏州人，成都信息工程大学副教授，主要研究方向为信息安全、密码学、侧信道攻击与防御、信息安全设备设计与检测。



饶金涛（1985-），男，湖北黄冈人，成都信息工程大学助教，主要研究方向为信息安全、嵌入式系统安全、侧信道攻击与防御。

凌杭（1991-），男，湖北黄冈人，成都信息工程大学硕士生，主要研究方向为信息安全、侧信道攻击与防御。