ARIA分组密码相关性功耗分析

计 锋 王 韬 赵新杰 张金中

(军械工程学院计算机工程系 石家庄 050003)

摘 要 功耗攻击已对密码算法实现的物理安全性构成严重威胁,对其攻击和防御的研究是近年来旁路攻击的热点问题。研究了ARIA韩国国家分组密码的相关功耗分析攻击方法。阐述了ARIA密码算法,给出了密码算法功耗泄露模型及相关性分析的原理,结合ARIA算法给出了相关功耗分析的具体方法,并通过仿真实验验证了攻击的有效性。结果表明,ARIA密码中的非线性S盒查表操作功耗泄露使其易遭受相关功耗分析攻击;仿真环境下10个样本的采集和分析即可恢复ARIA主密钥。

关键词 ARIA,分组密码,相关功耗分析,S盒

中图法分类号 TP393.08 **文献标识码** A

Correlation Power Analysis on ARIA Block Cipher

JI Feng WANG Tao ZHAO Xin-jie ZHANG Jin-zhong

(Department of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003, China)

Abstract In recent years, power analysis attack has become one of the most serious threats to block ciphers implemented on integrated circuits, and the research of this field about attack and defense is a hot spot of cryptographic side channel attacks. This paper introduced correlation power analysis attack on Block Cipher ARIA which was announced by Korea National Security Institute. All its theories are based upon the physical characters, power consumption models and data-dependent power consumption. The methods and steps of CPA were presented in detail, and correct secret key of encryption algorithm was cracked successfully with experiments. Experiment results demonstrate that ARIA is vulnerable to correlation power analysis attack by nonlinear S-box lookup table in the operating leaked. Simulation environment of 10 samples are enough to obtain the 128 bit master key in a short time.

Keywords ARIA, Block cipher, Correlation power analysis, S-box

1 引言

1996年,Kocher等人提出密码设备在执行加、解密过程中会产生旁路泄露信息。利用这些泄露的信息,结合一定的方法,就有可能破解密钥,这种攻击方法又称为旁路攻击(side-channel Attack)。随后,密码学者们对其进行了广泛的研究。典型的旁路攻击手段有计时攻击、功耗分析攻击、电磁分析攻击、声音分析攻击等。同传统基于数学理论的密码分析相比,旁路攻击具有攻击成本低、攻击力强、难以防护等特点。

功耗分析攻击[1]是旁路攻击的一种重要实现方法,典型的分析方法可分为简单功耗分析(Simple Power Analysis, SPA)、差分功耗分析(Differential Power Analysis, DPA)两种。在DPA中,用计算中间值和真实功耗的相关性来代替最后一步的差分计算,就形成了相关功耗分析[2](Correlation Power Analysis, CPA)。

ARIA分组密码算法[3]是韩国于2003年提出的国家数据加密标准,其加解密采用SPN结构,分组长度为128位,支持128位、192位、256位3种密钥长度,加密轮数分别为12、14、16轮。本文主要针对128位密钥ARIA算法中的S盒查表操作进行相关功耗分析,并通过仿真实验验证攻击有效性。和实际功耗分析相比,软件仿真功耗具有无噪声和功耗波形无需对齐等特点,实验仅需少量的明文和功耗曲线,即可成功地获取轮密钥。

本文第2节给出ARIA相关功耗分析的原理;第3节详细阐述ARIA的功耗分析攻击实现、实验结果;最后为结束语。

2 ARIA相关功耗分析原理

2.1 ARIA算法实现过程

128位密钥的ARIA算法加密时共需12轮,每轮使用$ek_r(1\leqslant r\leqslant 13)$作为轮密钥,轮函数包括轮密钥异或、代换层、混淆层3部分,第12轮运算结束后使用密钥ek_{13}进行后期的白化操作。128位密钥的ARIA算法加密过程如图1所示。

到稿日期:2011-03-20 返修日期:2011-07-13 本文受国家自然科学基金(60772082),河北省自然科学基金(08M010)资助。

计 锋(1979—),男,硕士生,主要研究方向为分组密码旁路分析,E-mail:geforce05@sohu.com;王 韬(1964—),男,教授,博士生导师,主要研究方向为网络安全与对抗;赵新杰(1986—),男,博士生,主要研究方向为信息安全和密码旁路分析;张金中(1986—),男,硕士生,主要研究方向为公钥密码旁路分析。

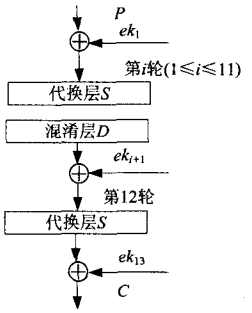

图 1　128 位密钥的 ARIA 算法轮加密过程

轮函数的代换层、混淆层以及密钥扩展可描述如下。

1) 代换层：加密时每轮使用了 4 个 S 盒 S_1，S_2 以及它们的逆 S 盒 S_1^{-1}，S_2^{-1}，对这 4 个 S 盒分别查找 4 次，奇数轮和偶数轮加密查找 S 盒的使用顺序不同。在奇数轮时，代换层为 $\{S_1, S_2, S_1^{-1}, S_2^{-1}, S_1, S_2, S_1^{-1}, S_2^{-1}, S_1, S_2, S_1^{-1}, S_2^{-1}, S_1, S_2, S_1^{-1}, S_2^{-1}\}$；在偶数轮时，代换层为 $\{S_1^{-1}, S_2^{-1}, S_1, S_2, S_1^{-1}, S_2^{-1}, S_1, S_2, S_1^{-1}, S_2^{-1}, S_1, S_2, S_1^{-1}, S_2^{-1}, S_1, S_2\}$。

2) 混淆层：混淆层 D 是一个将 16 字节输入($x_0, x_1, \cdots, x_{15}$)映射为 16 字节输出($y_0, y_1, \ldots, y_{15}$)的函数，映射关系见图 2。

3) 密钥扩展算法：将 128 比特实际密钥经过一个 3 轮 256 比特的 Feistel 密码函数后，生成 4 个初始化的值 W_0，W_1，W_2，W_3，然后将这 4 个初始化值采用两两组合方式，循环移位来生成加密时所需的子密钥 $ek_r(1\leqslant r\leqslant 13)$。

$$y_0=x_3\oplus x_4\oplus x_6\oplus x_8\oplus x_9\oplus x_{13}\oplus x_{14},\ y_8=x_0\oplus x_1\oplus x_4\oplus x_7\oplus x_{10}\oplus x_{13}\oplus x_{15}$$
$$y_1=x_2\oplus x_5\oplus x_7\oplus x_8\oplus x_9\oplus x_{12}\oplus x_{15},\ y_9=x_0\oplus x_1\oplus x_5\oplus x_6\oplus x_{11}\oplus x_{12}\oplus x_{14}$$
$$y_2=x_1\oplus x_4\oplus x_6\oplus x_{10}\oplus x_{11}\oplus x_{12}\oplus x_{15},\ y_{10}=x_2\oplus x_3\oplus x_5\oplus x_6\oplus x_8\oplus x_{13}\oplus x_{15}$$
$$y_3=x_0\oplus x_3\oplus x_7\oplus x_{10}\oplus x_{11}\oplus x_{13}\oplus x_{14},\ y_{11}=x_2\oplus x_3\oplus x_4\oplus x_7\oplus x_9\oplus x_{12}\oplus x_{14}$$
$$y_4=x_0\oplus x_2\oplus x_5\oplus x_8\oplus x_{11}\oplus x_{14}\oplus x_{15},\ y_{12}=x_1\oplus x_2\oplus x_6\oplus x_7\oplus x_9\oplus x_{11}\oplus x_{12}$$
$$y_5=x_1\oplus x_3\oplus x_4\oplus x_9\oplus x_{10}\oplus x_{14}\oplus x_{15},\ y_{13}=x_0\oplus x_2\oplus x_6\oplus x_7\oplus x_8\oplus x_{10}\oplus x_{13}$$
$$y_6=x_0\oplus x_2\oplus x_7\oplus x_9\oplus x_{10}\oplus x_{12}\oplus x_{13},\ y_{14}=x_0\oplus x_3\oplus x_4\oplus x_5\oplus x_9\oplus x_{11}\oplus x_{14}$$
$$y_7=x_1\oplus x_3\oplus x_6\oplus x_8\oplus x_{11}\oplus x_{12}\oplus x_{13},\ y_{15}=x_1\oplus x_2\oplus x_4\oplus x_5\oplus x_8\oplus x_{10}\oplus x_{15}$$

图 2　输入、输出的映射关系

2.2　功耗泄露模型

功耗分析攻击的原理为：密码设备在运行时泄露出的功耗同加密操作或加密数据之间存在相关性，而这些加密操作或加密中间数据又与密钥直接或间接相关。于是，结合一定分析方法和密码算法结构就可推断出相关的密钥。常用的功耗泄露模型有汉明距离和汉明重量模型两种[4]。汉明重量为操作数中为 1 比特个数，而汉明距离为原始操作数和结果操作数之间的变化位个数。

一般来说，设备的功耗同汉明距离成正比，具有线性的数据相关性。此外，有研究[5]指出，在某些情况下设备功耗同汉明重量也有线性相关性。二者相比，汉明距离模型能更准确地体现功耗变化，故本文仿真实验主要利用汉明距离模型对加密功耗进行模拟。为了仿真实验更接近真实环境，在采集的功耗上随机加上些小变量来模拟真实环境下的噪声情况。

2.3　相关系数计算模型

统计学中用协方差与相关性来表示一条线上两个点之间的线性关系。式(1)给出了协方差的定义，Kocher 通过计算平均值之间的距离来测量相关性[1]。

$$\begin{aligned}Cov(X,Y)&=E((X-E(X))*(Y-E(Y))\\&=E(XY)-E(X)*E(Y)\end{aligned}\tag{1}$$

本文用 Pearson 相关性系数来测量相关性，因为在使用这种方法进行测量上已经有比较完备的理论。式(2)定义了两个变量 X,Y 之间的相关性系数 ρ。

$$\rho(X,Y)=\frac{E(XY)-E(X)E(Y)}{\sqrt{Var(X)Var(Y)}}=\frac{Cov(x,y)}{\sqrt{Var(X)Var(Y)}}\tag{2}$$

式(3)定义了 Pearson 相关性系数 r。r 用于估计 N 个样本中两变量间的相关性系数 ρ，$\overline{X}$ 和 $\overline{Y}$ 分别代表两个变量的平均值。

$$r(\langle x_1,\cdots,x_i\rangle,\langle y_1,\cdots,y_i\rangle)=\frac{\sum_{i=1}^{n}(x_i-\overline{X})(y_i-\overline{Y})}{\sqrt{\sum_{i=1}^{n}(x_i-\overline{X})^2}\sqrt{\sum_{i=1}^{n}(y_i-\overline{Y})^2}}\tag{3}$$

2.4　针对 S 盒的相关分析的原理

ARIA 算法每轮进行 16 次查找 S 盒操作，每次将 8 比特的输入异或一个轮密钥字节作为 S 盒输入，得到 8 比特 S 盒输出。

针对密码 S 盒的功耗分析攻击模型如图 3 所示，P_i 和 K_i 为明文和密钥的第 i 个字节($0\leqslant i\leqslant 15$)，$P_i\oplus K_i$ 为 S 盒输入，Y_i 为查找 S 盒结果，显然 $K_i=P_i\oplus S^{-1}(Y_i)$。通常攻击者已知明文 P_i，却无法获得中间状态 Y_i，故无法直接获取密钥字节 K_i，但可通过功耗观测到 S 盒输入和输出数据之间的汉明距离变化，利用功耗相关分析[5,6]的思想对每个密钥字节 K_i 进行猜测。一个 K_i 字节从 0x00 到 0xff 共有 256 个候选值，将 K_i 代入与明文异或、查找 S 盒，记录此时的功耗情况。具体分析过程见第 3.1.2 节。

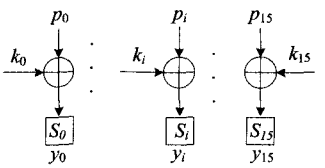

图 3　S 盒分析模型

3　ARIA 相关功耗分析仿真

3.1　CPA 攻击过程

CPA 攻击原理是计算模型与实际功率轨迹在每个位置的相关性系数，如果在某个位置的相关性系数最大，那么该位置就可以判断猜测密钥为正确值。主要步骤如下。

3.1.1　功耗信息采集

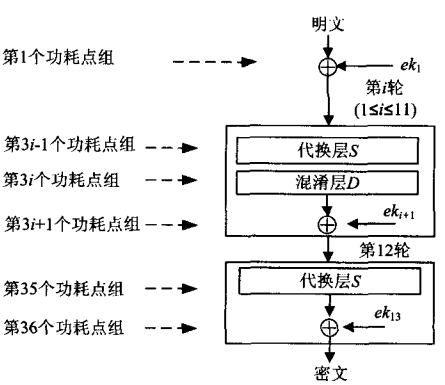

图 4　ARIA 加密功耗点选定

在 ARIA 算法加密中，在涉及数据处理的位置设定功耗

采集点。由于每个加密操作都要对128位状态按字节进行处理，故根据加密操作设定了36个功耗点组，每组对应16个功耗点，每个功耗点对应1个字节的对应功耗。如图4所示，ARIA算法加密过程中共采集了576个加密功耗点。

3.1.2 *功耗信息分析*

步骤1 获取第一轮密钥 ek_1

(1)选择一个加密操作 $F(p,k)$，该操作和明文/密文、密钥紧密相关。选择第一轮的S盒的查表操作，式(4)给出 F 函数的定义：

$$F=Pi\oplus Ki\oplus S[Pi\oplus Ki] \tag{4}$$

(2)输入 N 个随机明文 P 和第一轮密钥 ek_1 进行异或运算、第1类S盒替换，对应S盒输出，得到功耗点数组 $P[N][L]$，其中 N 为样本量，L 为每次加密功耗点数。

(3)需遍历猜测轮密钥 ek_1 的第一个字节从0x00到0xff共256种可能的取值。用第2步产生的 N 个明文 P 分别和猜测轮密钥 ek_1 的第一个字节值(共有256个可能值)执行同一个 F 函数，得到 F 函数的输入和输出字节、变化的汉明距离 $Hi[N][L]$ 矩阵，其中 i 表示 ek_1 的第一个字节的256种取值，$0\leqslant i\leqslant 255$。

(4)将 $Hi[N][L]$ 和实际功耗点 $P[N][L]$ 分别代入Pearson相关系数式(3)，计算得到 ek_1 第一个字节对应为 i 时的相关性曲线，其中 $0\leqslant i\leqslant 255$。

(5)观察这256条曲线，有最大尖峰的曲线对应的密钥值即为正确密钥候选值。因为只有正确地猜测密钥值，才能得到较为准确的功耗预测值。而只有和正确的功耗操作点相匹配，才会有最大相关性系数，

步骤2 获取第二轮密钥 ek_2

在128位获取 ek_1 后，结合明文做异或运算、第一类S盒替换、混淆变换得到第二轮的输入值。然后参考前面方法分析获取 ek_2。

步骤3 获取其他轮密钥 ek_3，ek_4

参考步骤1，步骤2分析获取 ek_3，ek_4。

步骤4 结合密钥扩展算法恢复主密钥 K

首先将 ek_1，ek_2，ek_3，ek_4 的值代入式(5)，得到 $C=W_0\oplus(W_0>>>76)$ 值。

$$\left.\begin{array}{l} ek_1=(W_0)\oplus(W_1>>>19)\quad ek_2=(W_1)\oplus(W_2>>>19)\\ ek_3=(W_2)\oplus(W_3>>>19)\quad ek_4=(W_3)\oplus(W_0>>>19)\end{array}\right\}$$

$$\Rightarrow$$

$$\begin{aligned} &ek_1\oplus(ek_2>>>19)\oplus(ek_3>>>38)\oplus(ek_4>>>57)\\ &=(W_0)\oplus(W_0>>>76)=(K)\oplus(K>>>76) \end{aligned} \tag{5}$$

通过 $C=W_0\oplus(W_0>>>76)$ 值，根据下面主密钥 K 恢复算法推导得到 W_0，即主密钥 K 值。

算法1 主密钥 K 恢复算法

```
输入:K⊕(K>>>76)
输出:K
  unsigned char K[128],cTemp;
    S_K←∅
    For each i from 0x00 to 0x01 {//对于每个密钥位的两个候选值
      For each j from 0 to 3 {//对于4个密钥异或碰撞循环
        K[j] ← i
          For each m from 0 to 31{//对于4个密钥异或碰撞循环
  中分别对应的32个密钥位
            cTemp←(K[(76*m)%128]^C[(76*m)%128])
  &0x01
    If(m! =31)
      K[(76*(m+1))%128]←cTemp;
      Else if(m==31) {
        If(cTemp ==K[j])
          Add K to S_K}}}}
```

3.2 实验结果

在普通PC机(CPU为AMD Athlon32 3000+1.81GHz，内存为1GB)上使用C++语言(Visual C++ 6.0环境)编程仿真实现了ARIA分组算法相关功耗攻击。实验中先产生10组输入随机明文和128位的随机密钥，用ARIA算法进行加密，然后利用上述针对S盒查表操作的相关功耗分析的方法，推测第一轮加密过程的轮密钥第一个字节，选取前两组的功耗点进行分析，得到256个密钥值所对应的相关功耗曲线。选取其中的4组曲线(密钥值分别为0，1，44和45)，如图5所示，当密钥字节猜测错误时，对应功耗曲线相对较为平坦；密钥值猜测正确时，对应功耗曲线会出现明显峰值，见图中红色的曲线，其密钥值为45。实验中随机产生的第一轮密钥的第一个字节为0x2D(十进制数45)，然后将第一轮密钥的其它字节也类似地推测出来，拼接得到128位的 ek_1 值。进而，通过这种方法能成功地获取ARIA加密过程中的前4轮轮密钥，结合密钥扩展即可获取ARIA主密钥。

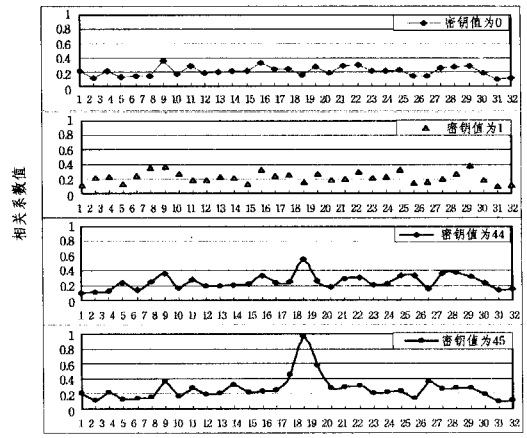

图5 正确密钥字节、错误的密钥字节相关性功耗曲线

图5中，猜测密钥所对应的相关系数约等于1，说明此时的猜测密钥和真实密钥之间有很强的相关性，这是因为相关系数和信噪比(Signal-Noise-Ratio，SNR)是具有正比关系的。信噪比的计算方法见式(6)：

$$SNR=\frac{Var(P_{exp})}{Var(P_{sw.\ noise}+P_{el.\ noise})} \tag{6}$$

式中，P_{exp} 代表观测点的功耗，$P_{sw.\ noise}$ 和 $P_{el.\ noise}$ 分别代表开关噪声和电子噪声产生的功耗。

采用的相关功耗分析方法，只需要采集10个样本的随机明文就可以分析出相关的密钥，同差分功耗分析需要大量的随机样本相比，可以节省时间和运行资源，提高工作效率。

结束语 本文对ARIA分组密码中S盒查表操作进行了相关功耗分析研究，对攻击过程进行了详细的阐述，并通过仿真实验成功获取了ARIA算法的128位轮密钥。实验结果表明，ARIA密码中S盒查表操作功耗易遭受相关功耗攻击，采集10个随机明文的功耗曲线，经分析可获取ARIA加密中的

(下转第108页)

用虚拟载波侦听方式，某一时刻只允许一对收发节点进行数据传输，吞吐量一直保持在 10.1Mbit/s 左右不变。仿真过程中，设定系统为饱和状态，实验结果表明，采用 LACT-MAC 协议较 DCF 协议网络端到端吞吐量有显著的提高。

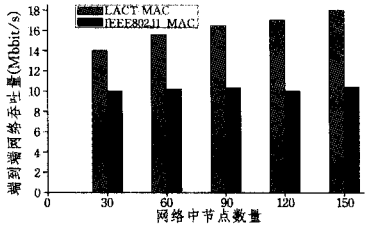

图 5　不同节点数目的 5 种仿真情景时端到端吞吐量分析

图 6 给出了 5 种不同节点数目仿真场景下平均端到端数据包传输延迟的曲线。从图 6 可以看出，802.11DCF 协议随着网络中节点数目的增加，节点间冲突会增多，导致数据重传率升高，从而使平均数据包传输延迟逐步增加。而采用 LACT-MAC 协议时，多个暴露终端可以同时进行数据传输，从而大大降低了平均数据包传输延迟。由实验结果可知 5 种仿真情况下，LACT-MAC 协议与 DCF 协议平均端到端的延迟的比值分别为 64.28%，60.60%，70%，80%和 78.57%。仿真实验证明，LACT-MAC 协议传输数据包的平均延迟远小于 802.11DCF 协议。

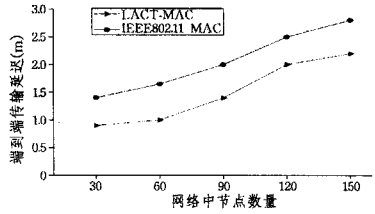

图 6　不同节点数目的 5 种仿真情景时端到端延迟分析

结束语　本文主要解决了无线传感器网络中暴露终端导致无线信道利用率低的问题。首先利用节点地理位置信息分析了暴露终端并行传输的可行性，在此基础上提出了一个高效无线传感器并行传输 LACT-MAC 协议。在 LACT-MAC 协议中，节点首先通过 GPS 或其他定位算法获取当前的地理位置信息，然后根据此位置信息识别自己暴露终端身份，只有通过并行传输检测的暴露终端才能进行并行传输调度。为了避免多个并行传输之间发生冲突，协议中增加了随机退避机制，从而减少了数据发送冲突产生的能量消耗。仿真结果表明，相比于 IEEE 802.11 DCF 协议，LACT-MAC 协议显著提高了网络的平均吞吐量，降低了数据传输延迟，并有效提高了无线传感器网络的效率和性能。

参 考 文 献

[1] Akyildiz F, Su W, Sankarasubramaniam Y, et al. A survey on sensor networks[J]. IEEE Communications Magazine, 2002, 40(8): 102-114

[2] Jiang L B, Liew S C. Improving throughput and fairness by reducing exposed and hidden nodes in 802.11 networks[J]. IEEE Transactions on Mobile Computing, 2008, 7(1): 34-49

[3] 姜志鹏，高随祥. 无线传感器网络节点定位的同心圆改进算法[J]. 计算机科学，2009，36(10)：46-49

[4] Shi Q, He C, Chen H, et al. Distributed wireless sensor network localization via sequential greedy optimization algorithm[J]. IEEE Transactions on Signal Processing, 2010, 58(6): 3328-3340

[5] Wu X, Mukherjee B, Chan S H G. MACA-an efficient channel allocation scheme in cellular networks[C]// IEEE Global Telecommunications Conference. San Francisco. CA, USA, 2000: 1385-1389

[6] Bencini L, Fantacci R, Maccari L. Analytical model for performance analysis of IEEE 802.11 DCF mechanism in multi-radio wireless networks[C]// Proc. of ICC. Cape Town, South Africa, 2010: 1-5

[7] Son I K, Mao S, Hur S M. Medium Access Control for Opportunistic Concurrent Transmissions Under Shadowing Channels[J]. Sensors, 2009, 9(6): 4824-4844

[8] Fu L, Liew S C, Huang J. Effective Carrier Sensing in CSMA Networks Under Cumulative Interference[C]// Proceedings of INFOCOM. San Diego, USA, 2010: 1-9

[9] Jiang L, Walrand J. A Distributed CSMA Algorithm for Throughput and Utility Maximization in Wireless Networks[J]. IEEE/ACM Trans on Networking, 2010, 18(3): 960-972

[10] Zhai H, Fang Y. Physical carrier sensing and spatial reuse in multirate and multihop wireless ad hoc networks[C]// Proc. IEEE INFOCOM. Barcelona, Spain, Apr. 2006: 1-12

[11] Alawieh B, Zhang Y, Assi C, et al. Improving Spatial Reuse in Multihop Wireless Networks-A Survey[J]. IEEE Commun, Surveys Tutorials, 2009, 11(3): 71-91

[12] Heuvel-Romaszko S V D, Blondia C. Enhancements of the IEEE 802.11, a MAC protocol for ad hoc network with history of power adjustment[C]// Proc IEEE Conf Wireless Netw. 2005: 48-54

[13] Zhou Y H, Nettles S M. Balancing the hidden and exposed node problems with power control in CSMA/CA-based wireless networks[A]// IEEE Wireless Communications and Networking Conference[C]. New Orleans, LA, USA, 2005: 683-688

(上接第 94 页)

前 4 轮轮密钥，结合密钥扩展即可获取 ARIA 主密钥。下一步的工作将在实际的物理加密平台上采集加密算法运行过程泄露的旁路信息，并对其进行多种功耗分析方法的研究。

参 考 文 献

[1] Kocher P C, Jaffe J, Jun B. Differential Power Analysis[A]// Proc. of the CRYPTO 1999[C]. LNCS 1109. Berlin: Springer-Verlag, 1999: 388-397

[2] Brier E, Clavier C, Olivier F. Correlation Power Analysis with a Leakage Model[A]// Joye M, Quisquater J J, eds. Cryptographic Hardware Embedded System-CHES 2004[C]. Springer-Verlag, LNCS 3156, 2004: 16-29

[3] Kwon D, Kim J, Park S. New block cipher: ARIA[A]// Proc. of the Information Security and Cryptology-ICISC'03[C]. Berlin: Springer-Verlag, LNCS 2971, 2003: 432-445

[4] Thomas M. Using Second-order Power Analysis to Attack DPA Resistant Software[A]// Proc. of the CHES 2000[C]. Berlin: Springer-Verlag, LNCS 1965, 2000: 238-251

[5] Mangard S, Elisabeth O, Thoms P. Power Analysis Attacks[M]. Berlin: Springer -Verlag, 2007: 119-165

[6] Moradi A, Mischke O, Eisenbarth T. Correlation-enhanced Power Analysis Collision Attack[A]// Mangard S, Standaert F X, eds. CHES 2010[C]. LNCS 6225, 2010: 125-139