一种保护芯片设计的多变量加密及其电路结构

赵险峰[1], 李 宁[1], 邓 艺[2]
(1. 中国科学院软件研究所信息安全国家重点实验室, 北京 100190;
2. 中国科学技术大学电子工程与信息科学系, 安徽合肥 230027)

摘 要: 当前普遍用分组加密保护可编程芯片的设计数据, 它们在使用前被内置密钥的电路解密, 典型地, 解密电路尺寸为 3 至 615 万门电路, 处理速度为 3 至 317 吉比特每秒(Gbps). 本文提出一种两轮多变量密码, 它的解密算法并不复合构成算法的多项式映射, 而仅连接它们, 可仅用数千至 1 万余个门电路实现, 解密速度可达到 7176 至 1316Gbps; 由于解密多项式被封装和伪装, 对多变量密码的大多攻击失效, 并且该密码系统也能够抵御不需要解密多项式的攻击, 包括插值、线性攻击和侧信道攻击等.

关键词: 知识产权保护; 芯片设计保护; 密码芯片; 信息安全
中图分类号: TP309 文献标识码: A 文章编号: 0372-2112 (2009) 06-1300-07

A Multivariate Encryption for Chip Design Protection and Its Circuit Architecture

ZHAO Xian-feng[1], LI Ning[1], DENG Yi[2]
(1. State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China;
2. Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei, Anhui 230026, China)

Abstract: Currently the design data in a programmable chip is widely protected by block cipher, and the ciphertext is deci-phered by a keyed circuit before the use of the data. Typically, the size of such a circuit is from 30 to 65 thousand gates, and the processing rate of it is from 3.10 to 3.17 Gigabits per second(Gbps). This paper proposes a 2-round multivariate cryptosystem. The algorithm of its decryption does not compose the constituent polynomial maps but only concatenates them. And with the processing rate from 7.176 to 13.16 Gbps, the decryption can be implemented by only about several or ten thousand gates. Because the decryption polynomials are encapsulated and disguised, most attacks against multivariate cryptosystems become inapplicable. And the new cryp-tosystem also resists the attacks that do not need to know the decryption polynomials, including the interpolation, linearization attack, side-channel attack, etc.

Key words: intellectual property protection; chip design protection; cryptographic chip; information security

1 引言

当前, 越来越多的集成电路是可编程的, 它们的功能由在加电时从存储器载入的设计数据确定. 由于设计数据是开发者的成果, 为保护数字设计的知识产权, 防止侵权者复制数据并仿造产品, 当前芯片制造商普遍在这类芯片中嵌入含密钥解密电路[1~4], 由芯片开发者在完成开发后加密并导入设计数据, 数据在加电时被解密并配置到芯片中去. 以上安全机制是建立在芯片及其封装对含密钥解密算法和解密后数据具有保护作用这一前提下的. 当前, 芯片集成度的提高和封装技术已使侵权者难以正确分析或探测其内部结构或数据, 因此本文在多数情况下也假设这类保护有效.

对以上解密当前主要采用了分组密码, 包括 AES (Advance Encryption Standard)[1~3]和 3DES(Triple Data En-cryption Standard)[4]等, 但它的合理性值得研究. 分组密码一般有数轮至 10 轮以上的操作, 实现电路较多地采用了查找表和乘法器等[5], 门电路规模甚至可能超过所保护的芯片. 以实现分组长度为 128 比特的 AES 为例, 当前的设计普遍采用迭代方法(即重复利用部分电路)[5]在电路尺寸和速度之间权衡, 典型地[6,7], 当逻辑门数从 615 万减少至 3 万, 处理速度从 317 吉比特每秒 (Gbps) 下降为 3 Gbps; 在较极端情况下[6], 当逻辑门数为 111 万, 速度仅为 015 Gbps. 然而, 以上由芯片封装形成的/黑箱0特性并未被利用, 本文认为它使安全机制和模型发生了变化, 因此算法及实现电路有可能在保持安

收稿日期: 2008-04-20; 修回日期: 2008-12-26
基金项目: 国家自然科学基金(No. 60573049, 60633030)

全性的前提下得到简化,速度也可以提高.

由于一些多变量密码的操作仅包含计算多项式的值[8],我们发现它们更适合以上应用. 多变量密码的功能与普通非对称密码相同,但算法构造差异大. 典型地,它用两个互逆非线性多项式作为密钥对,其中解密密钥(也称公钥)也是解密算法,设/ . 0表示映射复合,在 q 元有限域 GF(q)中,它可用多项式系统表示为

$$y = h(x) = (\ ,\ , h_i(x_1,\ ,\ , x_n),\ ,\ ) = T \cdot WS(x) \quad (1)$$

其中,映射 T 与S 是线性的, W是非线性的. 为减小密钥尺寸, W通常为二次的,因此 h 是二次多项式系统. 即使公开 y= h(x)的代数式,由于推导 h^{-1}或求解 h 均被认为是困难的,因此{T^{-1}, W^{1}, S^{-1}}可作为加密密钥(也称私钥). 虽然多变量密码是非对称的,但这并不影响它们在以上场合使用,我们称其中的解密为封装的多变量解密(PMD, Packaged Multivariate Decryption). 本文通过改造两轮多变量密码[9]提出了一种 PMD 算法及其电路结构. 分析和实验表明,在 GF(2)上 PMD 适合用简单的组合逻辑电路实现,即使采用流水线方法(即无需重复利用电路),所需门电路也仅为数千至 1 万余个,而解密速度已达到 7176 至 1316 Gbps; 由于可认为未公开公钥,主要威胁多变量密码的攻击已不适用,虽然无需利用公钥的攻击还包括插值[10~16]、线性攻击[17]和侧信道攻击[18,19]等,PMD仍可抵御它们. 获得以上性质的主要机制是, PMD 无需复合映射,而仅需连接它们,因此所需的门电路数量少,算法可通过提高多项式次数和添加映射增加安全,而攻击由于仅能分析输入和部分输出,面临攻击复合的高次多项式系统(下称虚拟复合系统),并且所需的明密文对数量远大于现实可能正确获取的数量.

2　实现 PMD的电路结构

PMD 可以用简单、高速和通用的电路结构实现,这是本文提出 PMD 的基本出发点之一. 以下定义有助于描述这类电路:

定义 1　若解密电路的输出难以被攻击者获得,称它为明文访问受限的,若它的输入难以被攻击者获得,称它为密文访问受限的.

定义 2　如果多变量解密算法用连接的方式组合映射,而不是复合它们,并需要借助封装保护这些映射,则解密算法被称为 PMD.

当前的芯片设计保护方案普遍假设被保护电路是明文访问受限的[1~4],而密文访问是不受限的. 前者反映了受保护芯片的内部结构和数据是难以分析的事实,后者反映了存储器由于要存储设计数据而必须能从外部访问的事实. 但由于芯片的工作特性等可能泄露一定的信息,因此应假设攻击者知道一定数量的明密文对. 这些假设对本文提出的 PMD(图 1) 及其电路结构也适用.

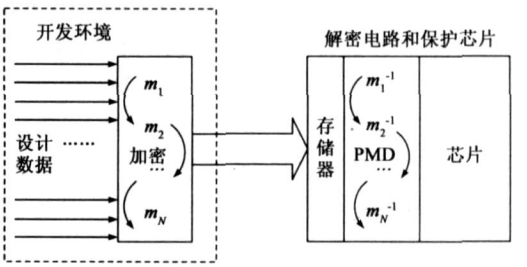

图1　PMD在当前保护体系中的位置(m_i是第i个映射,弧线箭头表示连接它们)

GF(2)上的非线性多项式映射仅包含与(AND)和异或(XOR)操作,适合用可编程与2异或门阵列实现(图 2),而线性映射可仅用异或门阵列实现. 门阵列可用 CMOS(Complementary Metal Oxide Semiconductor)管实现与和异或逻辑,其中连接点可用 E^2PROM 单元实现[20]. 在芯片开发者确定解密密钥代数式后,用写入工具导通相应连接点,这使与门阵列计算单项式,异或门阵列将它们在 GF(2)上相加. 为增加安全性并减小解密电路的尺寸,本文将采用两轮的 PMD(即有两个非线性映射). 为了减少不必要的电路,异或门在与2异或门阵列中交错布置: 由于 PMD 中每个多项式项数较少,异或门可以逐多项式交错,即每个纵线上仅设 1 个异或门,但每个横线上的异或门数量保证实现一个多项式; 对采用分区(详情见下节)的映射,由于每个多项式变元仅来自所属的分区,可按最大单项式的数量确定分块大小,逐分块交错. 以上电路结构简单,容易被标准化和批量生产,内部处理速度仅取决于信号的传播延时.

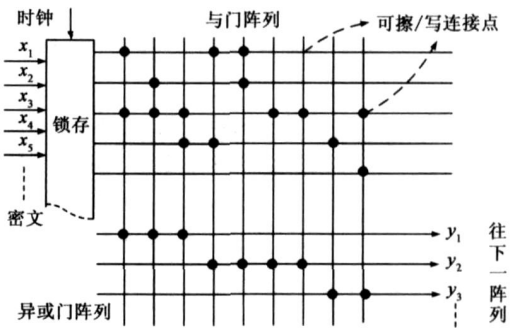

图2　用与-异或门阵列实现PMD中非线性多项式映射(实心圆点表示导通)

3　PMD算法

由于类似式(1) 的单轮多变量加密存在安全缺陷[17,21],J. Patarin 和 L. Goubin 提出了两轮多变量加密[9],相关算法被统称为 2R. 本文提出的 PMD 是一种不复合映射的新型 2R,它的首轮能够方便地通过提高多项式映射的次数提高算法安全. 以下在先给出各轮非线性映射的构造后给出 PMD 算法:

算法 1 生成二次 C^* 多项式映射及其逆映射[8]

输入参数: 两组正整数$\{n_1, \cdots, n_B\}$与$\{H_1, \cdots, H_B\}$, $n = n_1 + \cdots + n_B$ 是多项式的变元数量, 并且 $1 \leq H_i < n_i$, $1 \leq i \leq B$. $\{H_1, \cdots, H_B\}$可由芯片开发者用开发工具确定.

(1) 生成解密映射. 将输入 a 划分为 B 个分区, $a_i = (a_{i1}, \cdots, a_{in_i}) \in GF(2)^{n_i}$是第 i 个分区, 其中, $GF(2)^{n_i}$表示 n_i 个 GF(2) 上元素组成的向量集合; 令 a_i 代表 a_i 在 $GF(2^{n_i})$ 上的同态表示, 则在 $GF(2^{n_i})$ 上 C^* 映射可表示为

$$b_i = W_i(a_i) = a_i^{1+2^{H_i}} \tag{2}$$

由于 2 是 $GF(2^{n_i})$ 的特征, $a_i^{2^{H_i}}$ 关于 a_i 是线性的, 因此 $b_i = a_i^{1+2^{H_i}}$ 关于 a_i 是二次的. 令 $b_i = (b_{i1}, \cdots, b_{in_i})$ 是 b_i 在 $GF(2)^{n_i}$上的同态表示, 则 b_{ij}可以根据式(2)用 GF(2) 上关于$(a_{i1}, \cdots, a_{in_i})$的多项式表示.

(2) 生成加密映射. 因 $a_i = W_i^{-1}(b_i) = b_i^{(1+2^{H_i})^{-1}}$, a_{ij}也可类似地用 GF(2) 上关于$(b_{i1}, \cdots, b_{in_i})$的多项式表示.

算法 2 生成次数 $d_f \geq 3$ 的 Feistel 多项式映射及其逆映射

输入参数: 设变元数量 n 为偶数, 则输入为映射 $f: GF(2)^{n/2} \to GF(2)^{n/2}$, 它的次数为 d_f. f 可由芯片开发者用开发工具确定.

(1) 生成解密映射. 令 $a_l, a_r \in GF(q)^{n/2}$分别表示输入 a 的左(前)半部分和右(后)半部分, 则 Feistel 多项式映射 $\prec: GF(2)^n \to GF(2)^n$ 为

$$b = \prec(a) = (a_r, a_l + f(a_r)) \tag{3}$$

(2) 生成加密映射. 显然它是 $a = \prec^{-1}(b) = (b_r - f(b_l), b_l)$, 并且 $\prec^{-1}$总存在.

算法 3 基于 Feistel 映射与 C^* 映射的 PMD 及对应的加密

(1) 密钥生成. 生成线性映射 R, S, T: $GF(2)^n \to GF(2)^n$, 按前述算法生成 C^* 映射 $\prec$和 Feistel 映射 U; 设 $b_l, b_r \in GF(q)^{n/2}$分别表示 S 的输入 b 的前半部分和后半部分, 则要求 S 在输出上满足以下性质: 在每个 C^* 映射分区的位置范围内至少输出一个受 b_r 影响的分量(原因见 4.1.3 小节).

(2) PMD. 设 z 表示连接, 则 PMD 可以表示为

$$y = g(x) = (g_1(x), \cdots, g_n(x)) = (T \circ W \circ S \circ \prec \circ R)(x) \tag{4}$$

其中, $g: GF(2)^n \to GF(2)^n$, $g_i: GF(2)^n \to GF(2)$, $\circ$ 表示 / 记为0.

(3) 加密. 可以表示为 $x = (R^{-1} \circ U^{-1} \circ S^{-1} \circ W^{-1} \circ T^{-1})(y)$.

为减小电路尺寸并保证所需的安全性, 需为算法 3 选取大小合适的 d_f 和 n, 第 5 节通过分析与实验给出了它们的一些具体值.

4 安全性分析

2R 主要受到分解攻击的威胁, 而普通单轮多变量密码还面临更多的攻击, 但 PMD 被封装保护起来, 攻击者难以正确获得 PMD 的代数式, 因此本部分主要考虑无需代数式的攻击, 并假设攻击者能够通过读取存储器和分析芯片的执行等手段获得部分明密文对.

4.1.1 插值分类和基本插值

插值是经典的研究领域, 目的是根据已知离散点获得未知函数或其替代式, 但在有限域上的多元插值仍是当前研究的问题[10~15]. 插值也已用于攻击分组密码[16]和辅助攻击多变量密码 HFE(Hidden Fields Equations)[21], 然而本小节将指出, 当前插值面临的问题比分析 PMD 简单或与之无关, 为此需先将它们分类. 设一个未知的 k 稀疏多项式函数 h: $GF(q)^n \to GF(q)$ 为

$$h(x) = \sum_{i=1}^{k} a_i m_i(x_1, \cdots, x_n) \quad a_i \in GF(q) \setminus \{0\}, GF(q)[x_1, \cdots, x_n] \tag{5}$$

其中, $a_i \in GF(q) \setminus \{0\}$, $GF(q)[x_1, \cdots, x_n]$ 为 GF(q) 上的多项式环, $m_i(x_1, \cdots, x_n)$ 为不同的单项式, 基于 h 的部分输入输出取值(下称点值), 当前对 h 存在以下插值:

(1) 仅获得有限点值的插值[14]被称为是受限取值的, 若它得到了能根据输入计算 h 的/黑盒0[10~13], 则是非受限取值的.

(2) 插值可以精确[10~13]或非精确[14,15]还原 h, 在后一情况下, 由于获得的点值数量少或对 h 的性质缺乏了解, 即使全部已知的点值满足插值获得的 h^c, h^c 与 h 也不是相同的多项式. 如 Lagrange 法和 Newton 法是常用的插值方法, 它们获得的 hc 仅保证已知的点值是零点.

(3) 插值可以要求插值函数 h^c 符合全部的已知点值[10~14], 或要求它仅符合其中一个比例[15].

以上各类插值不全适用于攻击 PMD. 即使假设插值获得了所需数量的明密文对, 但是, 密码函数对连续的输入, 输出间的相关性弱, 因此, 若插值多项式系统 g^c 与式(4) 的 g 不同, 它对 g 的逼近效果差, 因此有:

定义 3 对 PMD 的插值攻击是, 利用获得的明密文对精确重构 PMD 虚拟复合多项式系统 $g = (g_1, \cdots, g_n): GF(2)^n \to GF(2)^n$.

最基本的插值方法是求解线性方程组, 本文称它为基本插值. 对未知多项式函数 h 的 t 个点值$\{(c_1, v_1 = h(c_1)), \cdots, (c_t, v_t = h(c_t))\}$, 算法可以取 t 个可能出现的单项式$\{m_1, \cdots, m_t\}$, 通过求解

$$M_{t \times t} \times a = \begin{bmatrix} m_{11} & \cdots & m_{1t} \\ \vdots & \ddots & \vdots \\ m_{t1} & \cdots & m_{tt} \end{bmatrix} \times \begin{bmatrix} a_1 \\ \vdots \\ a_t \end{bmatrix} = v = \begin{bmatrix} v_1 \\ \vdots \\ v_t \end{bmatrix} \tag{6}$$

获得 h 的插值多项式 $h^c = a_1 m_1 + , + a_t m_t$, 其中, $m_{ij} = m_j \mid_{x=c_i} \in GF(q)$, $\{a_1, , , a_t\}$ 是求解获得的系数, 求解的常用方法是高斯法. 虽然在理论上该方法可用于对 PMD 的插值攻击, 但 PMD 在计算上仍是安全的:

引理 1　若算法可获得足够的点值和计算能力, 通过求解 GF(2) 上线性方程组可形成对 PMD 的插值攻击.

证明　对式(4) 中的 $g_k, 1 \leqslant k \leqslant n$, 它的任意 t 个点值对应一个如式(6) 的方程 $M_{t@t} \# a = v$, 其中 $m_{ij} = m_j \mid_{x=c_i} \in GF(2), 1 \leqslant i, j \leqslant t$, t 是全部可能的 n 元单项式 $\{m_1, , , m_t\}$ 的个数. 算法可通过选取点值使 M 非奇异, 它定义了 $GF(2)^t$ 上的一个双射, 由于 g_k 的真实系数也满足该方程, 它们与通过求解获得的 a 相同.

定理 1　若引理 1 中的插值采用高斯法求解方程组并已知 $d = deg(g)$, 则重构 g 的时间复杂度为 $O(n\#(\sum_{i=1}^{d} C_n^i)^3)$, 并至少需 $\sum_{i=1}^{d} C_n^i$ 个点值(明密文对). 其中 C_n^i 是从 n 个元素中组合 i 个的数量.

证明　为重构 g 需逐一重构 $g_k, 1 \leqslant k \leqslant n$. 由于 $d = deg(g)$, 在重构 g_k 时需计算全部次数不大于 d 的 n 元单项式的系数. 由于对任意正整数 z 在 GF(2) 上有 $x_i^z = x_i$, 因此单项式的数量为 $\sum_{i=1}^{d} C_n^i$. 由于对 m 个变量线性系统的高斯法的复杂度为 $O(m^3)$, 因此重构 g 的时间复杂度为 $O(n\#(\sum_{i=1}^{d} C_n^i)^3)$. 由于由每个点值可列出每个 g_k 的一个方程, 它包含 $\sum_{i=1}^{d} C_n^i$ 个待求解系数, 求解需要列出相同数量的方程, 因此至少需要 $\sum_{i=1}^{d} C_n^i$ 个明密文对.

第 5 节将验证以上插值在 $d \geqslant 6$ 时在计算上难以威胁 PMD. 由于 GF(q) 上的 n 元系统可以在扩域 $GF(q^n)$ 上用一元系统表示[21], 以上基本的多元插值还存在对应的一元插值情况. 设 $x, y \in GF(2^n)$ 是 $x, y \in GF(2)^n$ 的同态表示, GF(2) 上的 n 元系统 $y = g(x)$ 在扩域 $GF(2^n)$ 上可表示为 $y = g(x) = \sum_{i=1}^{N} a_i x^{b_i}$, N 与 b_i 为正整数. 以下描述了对这个一元系统的基本插值情况:

定理 2　若对以上一元系统 g 的插值用高斯法求解线性方程组并已知 $d = deg(g)$, 则重构 g 在扩域上的操作复杂度为 $O((\sum_{i=1}^{d} C_n^i)^3)$, 并至少需要 $\sum_{i=1}^{d} C_n^i$ 个点值.

证明　对 $y = g(x) = \sum_{i=1}^{N} a_i x^{b_i}$, 为重构 g, 需考虑全部可能出现的 b_i. 由于 2 是域的特征, 并且 g 的输入与输出成份之间存在不大于 d 次的关系, 则 b_i 具有如下整数次幂之和的形式:

$$\underbrace{2^i, 2^j + 2^k, , , 2^l + 2^m + , + 2^w}_{d}, 0 \leqslant i, j, k, l, m, w < n \tag{7}$$

显然, 其中形如 2^i 的不同数有 C_n^1 个; 由于对任意正整数 z 有 $2^z + 2^z = 2^{z+1}$, 因此对特定的 b_i, 当它是一个 2 的幂级数和, 若它对应的幂级数和经过 $2^z + 2^z = 2^{z+1}$ 化简后仍有固定的项数 $G, 2 \leqslant G \leqslant d$, 则每个幂的次数均不同, 否则项数会继续减少. 因此, 全部 b_i 的数量为 $\sum_{i=1}^{d} C_n^i$, 因此通过高斯法求解的操作复杂度为 $O((\sum_{i=1}^{d} C_n^i)^3)$, 并至少需要 $\sum_{i=1}^{d} C_n^i$ 个点值.

由于 $GF(q^n)$ 中的操作在复杂度上是 GF(q) 中同类操作的大约 n 倍, 因此定理 2 说明, 攻击者即使能将 GF(2) 上 n 元系统转换为 $GF(2^n)$ 上等价的一元系统, 对后者基本插值的复杂度也与对前者的近似.

4.2　密码插值攻击和通用插值

插值已被用于攻击密码. T. Jakobsen 和 L. R. Knudsen 发现分组密码的明、密文子块之间存在多项式关系[16], 但他们假设加密采用简单的 S 盒和特定的子块操作. 插值也被用于辅助对 HFE 进行小秩攻击[21], 但是 HFE 通过求解方程解密, 需要控制映射复合后的密钥尺寸, 因此中间映射仅为二次系统, 而 PMD 虚拟复合系统的次数不小于 6, 第 5 部分将结合定理 1 和实验给出对后者实施基本插值的时间复杂度, 从中不难看出插值是计算上困难的.

研究人员在有限域上提出了一些精确插值方法[10~13], 但它们的性质也说明在 GF(2) 上重构多元多项式的困难. A. Dür 与 J. Grabmeier[12] 将代数编码理论用于重构 GF(2) 上的稀疏多项式, 他们将计算系数转换为解码, 但算法复杂度为 $O(2^n)$, 仅在 n 较小时适用. 一些插值利用素性和唯一分解性等性质确定/ 黑箱0中的单项式, 但这在小的有限域上难以奏效, 因此 M. Clausen 等人[10] 要求/ 黑箱0能计算扩域 $GF(q^n)$ 上的取值, 显然这并不实际, 而若/ 黑箱0仅能计算 GF(q) 上的值, 他们证明了算法的时间复杂度下限为 $8(n^{\log t})$, 所需点值数量为 $2^{\log n \# \log t}$, 其中 t 为可能的单项式数量. D. Y. Grigoriev 等人[11] 给出了一个并行插值算法, 虽然它的时间复杂度仅为 $O(\log^3 nt)$, 但需要 $O(n^2 t^6 \log^2 nt)$ 个处理器并要求/ 黑箱0能计算 $GF(q^{72\log_q(nt)+36})$ 上的值. M. A. Huang 与 A. J. Rao[13] 用/ 黑箱0构造一个以 $(p_1(y), , , p_n(y))$ 为输入的算法, 用于确定/ 黑箱0中的单项式, 其中, $p_i(y) \in GF(q)[y]$, y 是新引入的变元, 它在 GF(q) 上的操作复杂度为 $O(\log^4(td)\log p)$, 但由于 $p_i(y)$ 必须是 $GF(q)[y]$ 上的不可约元素, 当 $q = 2$, 它们只有两个,

因此方法不能扩展到 GF(2)上.

413 线性化攻击

式(4)中 T z Wz S 从整体上看是 C^* 多变量密码[8]. 由于 J. Patarin 用线性化攻击[17]破解了 C^*, 并且该攻击不需要了解解密密钥的代数式, 这里分析它对 PMD 的可能威胁.

线性化攻击利用了 C^* 的明文 x I $GF(2)^n$ 和密文 y I $GF(2)^n$ 满足双线性方程的弱点. 设 a= S(x)与 b= $T^{-1}(y)$ 分别是 < 的输入与输出, 在第 i 个分区上的输入与输出分别是 a_i, b_i I $GF(2)^{n_i}$, 令 a_i, b_i I $GF(2^{n_i})$ 分别是它们的同态表示, 根据式(2), $a_i \# b_i^{2^{H_i}} = a_i^{2^{2H}} \# b_i$. 由于 2 是 $GF(2^{n_i})$ 的特征, $a_i^{2^{2H}}$ 和 $b_i^{2^{H_i}}$ 关于 a_i 和 b_i 都是线性的, 因此 x 和 y 满足一些形如

$$\sum_{i,j} C_{ij} x_i y_j + \sum_k A_k x_k + \sum_l B_l y_l + c_m = 0 \qquad (8)$$

的方程, 其中, C_{ij}、A_k、B_l 与 c_m 是线性攻击待定的系数, 通过代入明密文对的值, 线性攻击可求解这些系数, 随后, 在已知密文情况下, 通过求解线性方程组可获得明文. 但以下定理说明 PMD 能抵御该攻击:

定理 3 对算法 3 中的 PMD, 如果 S 至少向 C^* 映射 W的每个分区输入一个受 b_r 影响的分量, 则线性攻击不适用于攻击 PMD.

证明 根据式(3), $b_r = a_l + f(a_r)$, 其中 (a_l, a_r) 是 Feistel 映射 < 的输入, 则 b_r 与 PMD 的输入 x 为次数不小于 3 的非线性关系. 设 c 与 d 分别是 W的输入和输出, 由于 W的每个分区输入了至少一个受 b_r 影响的分量, 则虽然在分区上仍存在 $c_i \# d_i^{2^{H_i}} = c_i^{2^{2H_i}} \# d_i$, 但由于 c 与 x 为次数不小于 3 的非线性关系, 这说明 x 与 PMD 的输出 y 满足次数不小于 4 的非线性方程, 即使它的关系系数可以被求解, 但在已知 y 时攻击仅能得到关于 x 次数不小于 3 的非线性方程.

414 侧信道攻击

侧信道攻击利用了密码芯片中可以检测的物理特性, 它们的变化能帮助攻击者建立统计分析模型. 当前, 可利用的物理特性主要来自功率[18]和电磁辐射[19], 但建立统计分析模型和实施攻击的原理是相似的:

算法 4 利用物理特性 W的一般化侧信道攻击

A. 建立统计分析模型

(1)准备. 获得一个能控制的密码芯片, 它仅密钥与待攻击芯片不同.

(2)选取密码算法中产生或使用的量 K. 它包含部分密钥或子密钥, 并能用以下建立的模型预测; K 有 M 个可能的取值 K_k, 1[k[M.

(3)信号检测. 取 N 个明/密文 x_i, 用以上芯片加/解密得到 N 个密/明文 y_i; 在每次操作中的 T 个时刻检测物理特性 W, 得到采样值阵列 W(i, j), 1[i[N, 1[j[T.

(4)建立预测模型. 由于 K 较难与 W有直接的关联, 因此取密码算法中间值 I, 它是关于 y_i 与 K_k 的函数, 计算得到阵列 I(i, k), 1[i[N, 1[k[M, 它记录了 I 在 y_i 与 K_k 处的取值. 对 1[i[N, 1[j[T, 建立用 I(i, k)预测 W(i, j)的模型, 其中在一次预测中 K_k 固定.

B. 现场攻击

(1)信号检测. 在被攻击芯片的 N 次加/解密中检测并记录所需的物理特性 W(i, j), 保存 N 个输出的密/明文 y_i^c; 对每个可能的 K_k 执行以下(2)~(4).

(2)计算中间值. 用 y_i^c 与 K_k 计算 $I^c(i, k)$.

(3)预测. 用前述的预测模型预测得到 $W^c(i, j)$.

(4)判定. 比较 $W^c(i, j)$ 与 W(i, j), 在满足相关性要求时输出 K_k.

从原理上看, 以上一般化的侧信道攻击不适用于攻击 PMD 芯片:

定理 4 算法 4 中的一般化侧信道攻击在原理上不适用于攻击 PMD.

证明 算法 4 中的攻击需要选取密码算法中出现的 K 以及中间值 I, 这是基于已知算法前提的, 它使攻击者知道 K 和 I 的存在性和基本性质以及 I 与 y_i 和 K_k 的关系, 也使攻击者建立的预测模型适用于攻击其它同类算法芯片. PMD 的密钥和算法进行了结合, 使侧信道攻击仅能靠猜测确定多项式形式, 并且建立的预测模型不适用于攻击其它同类芯片, 因为后者的多项式不同.

415 其它相关攻击

对多变量密码还存在一些无需公钥代数式的攻击. 差分攻击曾被用于分析多变量密码所使用多项式的性质. 然而, 它们仅适用于在分区上使用非双射的情况[9], 或依赖于算法采用的特定映射[22], 因此并不能威胁 PMD. E. Biham[23]提出了一种攻击两轮多变量密码的方法, 但它依赖分区映射采用 S 盒并需借助 S 盒的非双射性质, 而 PMD 在分区上是双射的.

前面假设芯片封装对保护含密钥解密算法是有效的, 但这里考虑攻击者通过破坏硬件搜集密钥信息的情况. 当前普遍用防篡改电路和封装技术抵御这类攻击, 我们还使 PMD 包含伪装项, 它们在计算中相互抵消, 因此在以上攻击下, 部分伪装项将混杂在攻击者的检测结果中.

5 算法实验和性能评估结果

为具体确定 PMD 的构造参数、安全性、解密速度和实现特性, 我们进行了实验和评估. 在不同 PMD 变元数量 n 和虚拟复合系统次数下, 我们先按定理 1 计算基本插值的时间复杂度和所需的明密文对数量, 据此确定

在该攻击下安全的变元数和次数, 其中, 次数的变化通过改变 Feistel 映射的次数获得. 实验用程序获得不同构造参数下的 PMD, 其中, 线性映射的每个输出组合 3 至 10 个输入, Feistel 多项式映射的每个多项式包含 3 个单项式, C^* 映射每个多项式平均和最多分别包含 9 个和 15 个单项式, 这些映射仅通过连接组合, 约 1/3 的多项式包含两个计算上抵消的伪装项. 随后实验按图 2 的电路结构估算实现两个非线性映射所需的门电路数量(每个多输入门按输入的数量计算), 按异或门阵列结构估算实现线性映射所需的门电路数量, 按信号的传输方向得到最大传播路径, 并基于当前 CMOS 芯片常见的传输延时评估了解密速度, 其中每个逻辑门和连接点的传输延时分别取为 30 和 15 皮秒(ps), 输入和输出接口的延时均取为 150ps.

表 1　对 PMD 的主要实验和评估结果

变元数 n	Feistel 映射次数	虚拟复合系统次数	基本插值复杂度	所需明密文对数(@10^5)	用上的逻辑门/连接点数	电路的逻辑门/连接点数	最大信号传播延时(ps)	速度(Gbps)
16	3	6	O($2^{45.6}$)	0.14892	681/415	2474/2208	1920	7.761
16	4	8	O($2^{49.8}$)	0.39202	729/463	2474/2208	1920	7.761
16	5	10	O($2^{51.5}$)	0.58650	777/511	2474/2208	1920	7.761
32	3	6	O($2^{65.4}$)	11.4902	1564/1032	9364/8832	2190	13.608
32	4	8	O($2^{76.5}$)	150.332	1660/1128	9364/8832	2190	13.608
32	5	10	O($2^{85.0}$)	1075.94	1756/1224	9364/8832	2190	13.608

结果显示(表 1), PMD 在简单的电路结构下能获得实用的安全性和高效的操作性能. 仅在 n= 16 和 Feistel 映射次数不大于 5 的情况下, 基本插值的复杂度已接近 O(2^{50}). 尤其是, 完成攻击需要已知数万对明密文, 在实际中攻击者难以正确获得它们, 甚至被保护的数据量小于所需的数据量. 以上具有流水线特性的 PMD 电路在 n= 16 和 n= 32 时仅包含数千至 1 万余门的电路规模, 这约是当前典型解密电路的 1/3. PMD 电路还具有处理速度快的特性, 在当前 CMOS 芯片常见的传输延时下, 当 n= 16 和 n= 32 时的速度分别可达到 7176 至 1316 Gbps, 这比当前典型解密电路的速度高出约 4 至 10 Gbps. 由于增加多项式的次数并未增加最大传输路径, 可以在不影响 PMD 处理速度的前提下进一步提高安全性.

6　结论

本文提出了一种保护数字设计的 PMD 算法以及实现它的电路结构. 分析和实验说明, 由于在芯片封装的保护下攻击者不能正确得到解密多项式, 多数对多变量密码的攻击对 PMD 失效, 而且 PMD 也能够抵御插值、线性化、侧信道分析等无需解密多项式的攻击, 并容易利用冗余项伪装. PMD 仅包括与和异或两种逻辑操作, 可用易于标准化和批量生产的门阵列实现, 而由于映射用连接组合, PMD 电路可仅包含数千至 1 万余个门电路, 而速度在当前 CMOS 电路的传输延时下已达 7176 至 1316Gbps. 相比当前典型的同类保护方法, 本文提出的方法使解密电路规模仅是原来的 1/3 左右, 速度提高了大约 4 至 10Gbps.

参考文献:

[1] CASTILLO J, HUERTA P, MARTINEZ J I. Secure IP downloading for FPGAs[J]. Microprocessors and Microsystems, 2007, 31(2): 77-86.

[2] BOSSUET L, GOGNIAT G, BURLESON W. Dynamically configurable security for SRAM FPGA bitstreams[J]. Intern J of Embedded Systems, 2006, 2(1): 73-85.

[3] Altera Corporation. Design Security in Stratix III Devices(white paper)[EB/OL]. http://www.altera.com, 2006-11.

[4] Xilinx Corporation. Virtex2Ò platform FPGA User Guide v2.1 [EB/OL]. http://www.xilinx.com, 2007-03.

[5] MCLOONE M, MCCANNY J V. System2On2Chip Architectures and Implementations for Private2Key Data Encryption [M]. New York, USA: Kluwer Academic, 2003. 28-96.

[6] Helion Technology Limited. Overview Datasheet2high Performance AES(Rijndael) Core for ASIC[EB/OL]. http://www.heliontech.com/downloads/aes-asic-helioncore.pdf, 2007-06-12.

[7] DeverSYS Corporation. Ultra High Speed AES(Rijndael) Cryptto Processor [EB/OL]. http://deversys.com/?action=project&id=43, 2008-12-10.

[8] MATSUMOTO T, IMAI H. Public quadratic polynomial2tuples for efficient signature2verification and message encryption[A]. GUNTHER C G. Proc Eurocrypt. 88[C]. LNCS, vol. 330. Berlin, Germany: Springer2Verlag, 1988. 419-453.

[9] PATARIN J, GOUBIN L. Asymmetric cryptography with S2boxes[A]. HAN Y, et al. Proc ICICS. 97[C]. LNCS, vol. 1334. Berlin, Germany: Springer2Verlag, 1997. 369-380.

[10] CLAUSEN M, DRESS A, et al. On zero2testing and interpolation of k2sparse multivariate polynomials over finite fields[J]. Theoretical Computer Science, 1991, 84(2): 151-164.

[11] GRIGORIEV D Y, KARPINSKI M, SINGER M F. Fast parallel algorithms for sparse multivariate polynomial interpolation over finite fields[J]. SIAM J Computing, 1990, 19(6): 1059-1063.

[12] DUR A, GRABMEIER J. Applying coding theory to sparse in2

terpolation[J]. SIAM J. Computing, 1993, 22(4): 695- 704.

[13] HUANG M A, RAO A J. Interpolation of sparse multivariate polynomials over large finite fields with applications[A]. TARDOS E. Proc 7th Annual ACM2SIAM Symposium on Discrete Algorithms[C]. New York, USA: ACM Press, 1996. 508- 517.

[14] ZILIC Z, VRANESIC Z G. A deterministic multivariate interpolation algorithm for small finite fields[J]. IEEE Trans Computers, 2002, 51(9): 1100- 1105.

[15] ROTH R M, BENEDEK G M. Interpolation and approximation of sparse multivariate polynomials over GF(2)[J]. SIAM J Computing, 1991, 20(2): 291- 314.

[16] JAKOBSEN T, KNUDSEN L R. The interpolation attack on block ciphers[A]. BIHAM E. Proc. FSE. 97[C]. LNCS, vol. 1267. Berlin, Germany: Springer2Verlag, 1997. 28- 40.

[17] PATARIN J. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt. 88[A]. COPPERSMITH D. Proc Crypto 95[C]. LNCS, vol. 963. Berlin, Germany: Springer2Verlag, 1995. 248- 261.

[18] MANGARD S. Hardware countermeasures against DPA) A statistical analysis of their effectiveness[A]. OKAMOTO T. Proc CT2RSA. 04[C]. LNCS, vol. 2964. Berlin, Germany: Springer2Verlag, 2004. 222- 235.

[19] AGRAWAL D, ARCHAMBEAULT B, et al. The EM side2channel(s)[A]. KALISKI JR B, et al. Proc. CHES. 02[C]. LNCS, vol. 2523. Berlin, Germany: Springer2Verlag, 2003. 29 - 45.

[20] 甘学温, 赵宝瑛, 陈中建, 金海岩. 集成电路原理与设计[M]. 北京: 北京大学出版社, 2006.

[21] KIPNIS A, SHAMIR A. Cryptanalysis of the HFE public key cryptosystem by relinearization[A]. WIENER M. Proc. CRYPTO. 99[C]. LNCS, vol. 1666. Berlin, Germany: Springer2Verlag, 1999. 19- 30.

[22] FOUQUE P, GRANBOULAN L, STERN J. Differential cryptanalysis for multivariate schemes[A]. CRAMER R. Proc. Eurocrypt 05[C]. LNCS, vol. 3494. Berlin, Germany: Springer2Verlag, 2005. 341- 535.

[23] BIHAM E. Cryptanalysis of Patarin s 22round public key system with S boxes(2R)[A]. PRENEEL B. Proc. Eurocrypt. 00[C]. LNCS, vol. 1807. Berlin, Germany: Springer2Verlag, 2000. 408- 416.

作者简介:

赵险峰 男, 1969 年 6 月生于安徽淮北, 2003 年于上海交通大学获博士学位, 2003 年至 2005 年为中国科学院数据与通信保护研究教育中心(DCS 中心)博士后, 现为中国科学院软件研究所信息安全国家重点实验室副研究员, IEEE 与中国密码学会会员. 主要研究领域为密码、信息隐藏及其在数字知识产权保护中的应用, 已发表 30 余篇论文并申请 3 项专利.

E2mail: xfzhao@is. iscas. ac. cn

李 宁 男, 1983 年 1 月生于江苏南京, 2005 年于南京大学获学士学位, 现为中国科学院软件研究所信息安全国家重点实验室硕士生, 主要研究领域为数字知识产权保护.

E2mail: lining@is. iscas. ac. cn