

3G USIM 卡中安全系统的设计实现

戴 鹏, 叶兆华, 张 哲, 王新安, 张 兴

(北京大学 深圳研究生院 集成微系统科学与工程与应用重点实验室, 广东 深圳 518055)

摘 要: 设计实现了一种智能卡的安全系统, 由 128 bit AES 和 1024 bit RSA 构成, 兼顾加密速度和通信安全. 该系统在一款 3G 智能卡中应用, 采用 SMIC 0.18 μ m 混合信号工艺实现. 验证结果表明, AES 和 RSA 具有较好的加密性能, 与当前同类智能卡产品相比面积上有较大优化, 能很好满足智能卡的安全业务要求.

关键词: 智能卡; AES; RSA; 蒙哥马利

中图分类号: TN47

文献标识码: A

文章编号: 1000-7180(2011)01-0165-04

Implementation of Security System for 3G USIM Card

DAI Peng, YE Zhao-hua, ZHANG Zhe, WANG Xin-an, ZHANG Xing

(Key Lab of Integrated Microsystem Science & Engineering Applications, School of Computer and Information Engineering, Shenzhen Graduate School of Peking University, Shenzhen 518055, China)

Abstract: A encrypt system with 128 bit AES and 1024 bit RSA is introduced either for the encrypt speed or security for communication. The system is implemented by SMIC 0.18 μ m mix signal process. The result shows AES and RSA in USIM card achieve considerable performance with optimized area compared with other products, which is propitious to security application for USIM card.

Key words: USIM card; AES; RSA; Montgomery

1 引言

随着 3G 业务的开展, 智能卡在社会生活和全领域中应用日益广泛, 如身份识别、医疗卡、保险卡、电子支付等. 上述业务由于涉及到个人隐私和财产安全, 因此对智能卡的加解密安全性能提出了很高的要求.

当前密码体系中主要分为对称密钥密码系统和公开密钥密码系统.

(1) 对称密钥密码系统包含所有传统的加密系统, 如古代的恺撒挪移码、Viginere 码、单次加密簿、Enigama 密码、DES、AES^[1]、IDEA 等.

(2) 公开密钥密码系统则包含 RSA、Elgamal 密码、椭圆曲线密码以及大多数的数字签名算法.

当前智能卡应用中基本上包含了上述两种密码系统. 目前主流的智能卡包含 DES、3DES、RSA、模运算、椭圆曲线计算等硬件加解密模块. 近年来, 由

于计算机性能的飞速发展, DES 加密逐渐丧失其安全性, 而 3DES 的加密解密时间消耗较大, 效率降低, 已经不能适应实时加密需求. 因此, 在对称密钥系统中, AES 逐渐成为智能卡的主流加密系统. RSA 则是公开密钥密码系统的首选方案.

文中首先介绍智能卡的加密体系, 接着详细描述智能卡中 AES 模块和 RSA 模块的硬件实现.

2 智能卡中的加密体系

智能卡系统由对称密钥和公开密钥系统整合组成. 由于 AES 加解密速度比 RSA 要快上万倍, 数据处理带宽也大, 适合大规模数据文本的加解密; RSA 处理速度较慢, 可在公共密钥体系中传递 AES 的密钥. 文中以 RSA 加密传送 AES 密钥, 大规模数据加密采用 AES, 这样兼顾了加密速度和通信安全, 同时解决了对称密钥的密钥分配问题. 如图 1 所示.

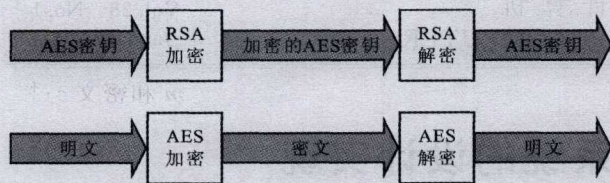


图1 智能卡中密钥系统

3 加解密模块详细设计

3.1 AES 加解密模块

AES算法由10个循环组成,每轮有一个循环密钥,来自于初始密钥。每个循环有4个基本步骤:(1)字节转换,简称BS;(2)移动行变换,简称SR;(3)混合列变换,简称MC;(4)加循环密钥,简称ARK。

AES的Rijndael算法加密简介如下:(1)ARK,使用第0个循环密钥;(2)BS、SR、MC、ARK循环9次,分别使用1~9个循环密钥;(3)最后一次循环:BS、SR、ARK,使用第10个循环密钥。解密流程为加密流程的逆过程。

智能卡系统中,首先考虑安全性,其次是面积和功耗。智能卡系统较为简单,采用并行流水设计AES会增加智能卡面积,同时智能卡处理带宽仅为1Mbps左右,选用串行AES设计完全可达系统对数据处理速度的要求,因此文中采用串行结构实现AES加解密模块。

AES模块由数据加载、操作控制、密钥扩展、加密循环和解密循环5个模块组成,如图2所示。数据加载模块加载数据;操作控制模块为一个状态机,通过操作系统设定的控制寄存器配置值控制AES模块在加密循环、解密循环及密钥扩展轮密钥等操作状态切换;密钥扩展模块每周扩展一轮密钥;加密循环模块采用非流水技术每10周期完成128bit加密;解密循环模块先进行10周期的密钥扩展,存入缓冲器后再进行11周期的解密操作。

3.1.1 加密循环模块

在加密循环模块中,需要完成行变换、加循环密钥、字节变换和混合列变换操作。其中,行变换为加密矩阵的每一行循环左移不同的位数,第0行不变,第一行循环左移1个字节,第二行循环左移2个字节,第三行循环左移3个字节;加循环密钥为状态矩阵和轮密钥进行位异或操作;混合列变换将每一列看作是在有限域GF(28)上的多项式,然后在模 $(x^4 + 1)$ 下与固定多项式 $c(x) = 03x^3 + 01x^2 + 01x + 02$ 相乘,可以表示成矩阵乘法,记为 $b(x) =$

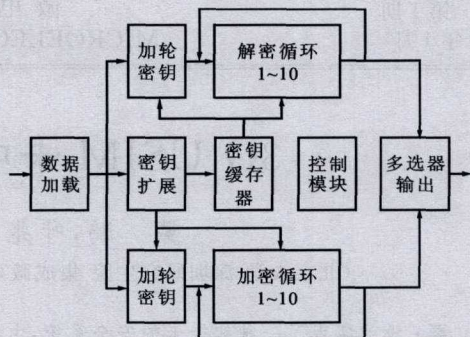


图2 AES模块总体数据流程示意图

$c(x) * a(x)$ 。上述三个操作较为简单。

字节变换将每个字节通过S-box进行非线性运算。这个S-box是可逆的,由两个变换组成:

(1)对所有子字节在有限域GF(28)求其乘法逆,且规定‘00’的逆是‘00’,‘01’的逆是‘01’。

(2)经(1)处理过的字节值进行如下仿射变换:

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

S-box的设计一般有两种实现方式:ROM查表和直接计算S-box。ROM实现比较简单,需要20个 256×8 bit的ROM,加密循环需要8个S-box,密钥扩展需要4个S-box,解密循环需要8个Inv S-box。直接计算方式设计得到的S-box面积较小,但计算算法复杂。文中采取了一种折衷方案:复用一个ROM中查表值,不同S-box采用组合逻辑选取输出S-box的查表值。这样既避免了大量的算法计算,面积比ROM实现方式减少了60%,约55万area units。

3.1.2 密钥扩展模块

AES中加解密都需要调用密钥扩展模块,加密直接使用当前产生的密钥,而解密需将所有密钥产生并存入keybuffer后再开始解密操作。

初始密钥128bit按照图3所示排成 4×4 的字节矩阵,通过矩阵再扩展出40列,前4列初始密钥记为 $K(0)$ 、 $K(1)$ 、 $K(2)$ 、 $K(3)$ 。新的列基本上是循环产生的,假设列的增加通过已经定义的 $K(i-1)$ 列来达到:

如果 i 不是4的倍数,那么 $K(i) = K(i-4) \oplus K(i-1)$;

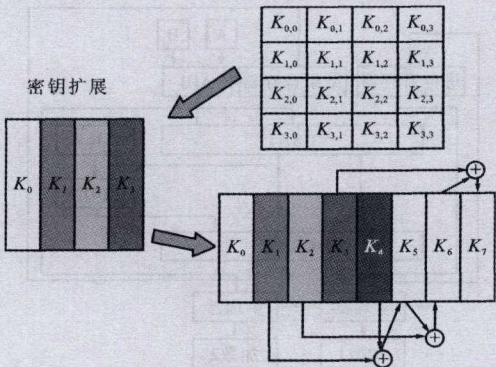


图 3 密钥扩展示意图

如果 i 是 4 的倍数,那么 $K(i) = K(i - 4) \oplus T(K(i - 1))$.

其中 $T(K(i - 1))$ 是 $K(i - 1)$ 做如下变换得到的,令列 $K(i - 1)$ 的元素是 a, b, c, d ,循环移位得到 b, c, d, a .用字节变换中 S-box 相应元素替代这些字节,得到 4 字节 e, f, g, h ,最后在有限域 $GF(28)$ 中计算循环常量: $r(i) = 00000010(i - 4)/4$,那么 $T(K(i - 1))$ 就是列向量 $(e \oplus r(i), f, g, h)$.

3.1.3 解密循环模块

解密循环为加密循环的反操作,算法基本相同.需要注意的是,解密必须等待初始密钥扩展完全之后才能进入解密循环,所以解密操作需要 20 个时钟周期才能完成,其中 10 个周期用于密钥扩展,另外 10 个周期是解密循环所用的时间.

3.2 RSA 加解密模块

RSA 模块完成 RSA 加密,解密,数字签名签署,数字签名验证,私钥产生功能.包括模幂模块,私钥产生模块.硬件的主要功能是实现型如 memodn 的模幂计算.

RSA 加解密流程如下:

(1) 产生密钥:取相异质数 p, q (保密),计算 RSA 模数 $n = p \times q$,将模数 n 公开.通过计算 $\gcd(e, (p - 1)(q - 1)) = 1$ 得到 e, e 作为加密密钥公开.通过计算 $d \times e = 1 \bmod ((p - 1)(q - 1))$ 得到解密私钥 d (保密).其中 (n, e) 作为公开密钥; (n, d) 作为私钥用来解密信息, d, p, q 保密.

(2) 加密:取公开密钥 (n, e) ,利用加密函数计算 $c = m^e \bmod n$,其中明文是 m ,密文是 c .

(3) 解密:通过解密函数计算 $m = c^d \bmod n$,解密还原成明文 m .

文中智能卡系统中 RSA 模块不支持中国剩余定理,目前只支持 n, d 形式的私钥形式.使用蒙哥马利模乘实现形如 $m^e \bmod N$ 的模幂运算. RSA 模块

由数据加载、操作控制状态机、选通控制和蒙哥马利模乘单元四个模块构成,如图 4 所示.数据加载模块用于加载 RSA 所需的公钥 n, e ,明文 m 和密文 c ;操作控制状态机模块控制蒙哥马利模乘单元操作状态切换;选通控制模块选择提供给蒙哥马利模乘单元输入数据;蒙哥马利模乘单元负责计算 $S = MM(A, B, N) = ABr \bmod N, r = 2^{-n} \bmod N$, (r 是和 N, n 相关的常数).

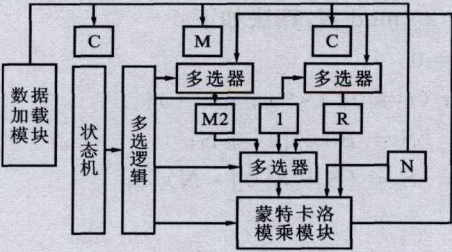


图 4 RSA 模块框图

3.2.1 操作控制状态机模块

操作控制状态机模块通过系统设定的 RSA 控制寄存器的配置信息控制当前状态以及蒙哥马利模乘单元的操作.

文中采用基于 2 的蒙哥马利算法,记为 $S = MM(A, B, N)$. 状态机主要分为: S_0 : IDLE 态; S_1 : 计算 $MM(M, C, N)$; S_2 : 计算 $MM(C, 1, N)$; S_3 : 计算 $MM(R, R, N)$; S_4 : 计算 $MM(R, M_2, N)$; S_5 : 计算 $MM(R, 1, N)$. 切换状态如图 5 所示.

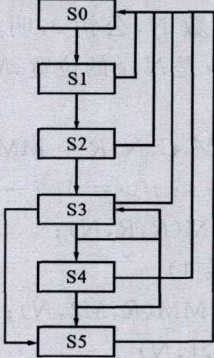


图 5 操作控制状态机图

3.2.2 蒙哥马利模乘单元

(1) L-R 二进制幂快速算法

设 $e = b_{n-1}b_{n-2} \dots b_1b_0$

$P_0 = 1$;

For ($i = n - 1; i \geq 0; i - -$) {

$P_{n-i} = P_{n-i-1} * P_{n-i-1} \bmod N$;

If ($e_i = 1$)

$P_{n-i} = P_{n-i} * m \bmod N$;

}

循环结束后得到结果： $c=Pn=m^e \bmod N$

这种方法的计算复杂度为 n 次模平方和平均为 $(n-1)/2$ 次模乘. 仅需一个模乘单元, 硬件面积小, 但是由于存在数据相关性, 不能并行运算.

(2) Montgomery 算法

基于 2 的 Montgomery 算法记为 $S = MM(A, B, N)$, A, B 是 n 位 2 进制数, $[a_{n-1}a_{n-2}\cdots a_1a_0]$ $[b_{n-1}b_{n-2}\cdots b_1b_0]$, N 是 n 位 2 进制奇数, $A < N, B < N, r = 2^{-n} \bmod N$, 算法如下:

$S = 0$

①

For ($i = 0; i < n; i++$) {

②

$S = B * A[i] + S;$

$S = (S + S[0] * N) / 2;$

}

If ($S > N$) $S = S - N;$

③

$S = MM(A, B, N) = AB r \bmod N$

算法步骤 ② 结束的时候 S 可能大于 N 所以需要加入步骤 ③, 如果要减去步骤 ③, 需要循环的次数大于等于 $n+2$, i 变化的范围是 $0-n+1$, 结果 $S = MM(A, B, N) = A * B * 2^{-(n+2)} \bmod N$.

(3) Montgomery 算法构造的 L-R 二进制幂快速算法

Montgomery 算法构造的 L-R 模幂算法只需要 1 个 Montgomery 模乘元件. 即模幂运算转化成模乘运算, 通过 Montgomery 模乘单元完成模乘运算.

算法输入: 模数 N , 公钥 e , 明文 M , 常数 $C = 2(n+2) \bmod N$, n 是 N, e 的位宽, $M, e < N, C$ 是关于 N 的常数.

$M2 = MM(M, C, N)R = MM(1, C, N);$

For ($i = n-1; i \geq 0; i--$) {

$R = MM(R, R, N);$

If ($ei = 1$)

$R = MM(R, M2, N);$ }

$R = MM(R, 1, N)$

输出 $R = Me \bmod N$.

文中采用两套 CSA 和一个 32 bit CPA 的方案, 如图 6 所示. 所有数据以保存进位的方式经过循环操作后, 最后作一次 1024 bit 加法. 这样 Montgomery 算法中 $n+2$ 个周期进行循环的时候不用处理进位, 完全并行操作, 一个周期完成一个循环. 最后整合的两个 1024 bit 数加法采用 32 bit 的 CPA 运行 32 周期, 因此完成一个模乘运算需要 $n+2+32$ 个周期.

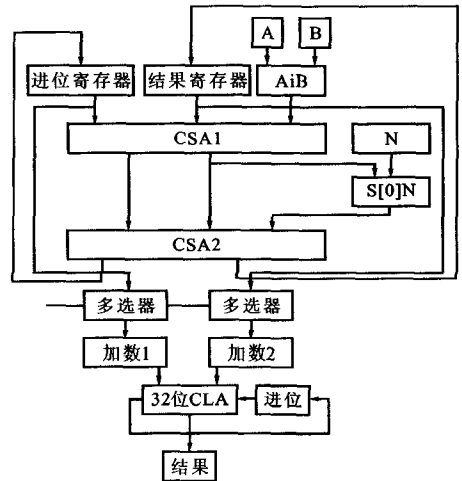


图 6 RSA 中 Montgomery 模乘单元结构图

4 芯片实现与性能评估

文中智能卡结构采用 SMIC 0.18 μ m 混合信号工艺实现了流片, 芯片面积为 3.75mm $\times$ 4.44mm, 工作频率 40MHz. 通过测试, 本芯片所有加解密功能正常.

与同类 AES 模块实现设计实现进行了比较^[2-4], 文中 AES 模块可满足智能卡需求, 达到了面积和速度的折衷.

表 1 和表 2 分别为文中 RSA 模块与现有智能卡产品的 RSA 加解密性能和面积比较. 文中 RSA 比目前市场上主流的智能卡芯片在 1024 bit 加解密性能上有所提高.

表 1 1024 bit RSA 加解密操作时间比较

产品	频率 /MHz	操作时间 /ms	工艺
ST22N144	33	242	—
ST22N144-A ^[6]			
Infineon SLE88 CX720P ^[6]	55	78	0.22 μ m CMOS
文中	40	25~50	0.18 μ m CMOS

表 2 RSA 面积比较

文献	最高工作频率 /MHz	门数 /Kgate	工艺
文献[7]	270	155	0.13 μ m
文献[8]	556	198	0.13 μ m
文献[9]	200	—	0.18 μ m
文中	100	约 130	0.18 μ m

机制存在的缺陷,采用一种监督惩罚的方法对原有激励机制进行了改进.在一个流会话期间,节点的行为被其上行节点和下行节点监控,下行节点会颁发流证书给该节点,以证明该节点提供了流数据,上行节点向该节点索要流证书以判断该节点是否给其他节点提供了流数据,若该节点被证明是自私的,则由上行节点进行惩罚.这样,克服了原有的一些等级高的节点不再共享资源的缺点,以及更好、更及时的发现系统中的自私节点.最后通过仿真实验论证了改进后的算法有效的提升了网络中节点的服务质量,更好的抑制了节点的自私行为.

参考文献:

- [1] 王洪波,马铁慧. P2P 流媒体技术原理及应用[J]. 中兴通讯技术, 2007, 13(6): 18-21.
- [2] Weihong Wang, Baochun Li. To play or to control: a game-based control-theoretic approach to peer-to-peer incentive engineering[C]//Proceedings of IEEE International Workshop on Quality of Service. USA: Berkeley, 2003: 174-192.
- [3] Hefeeda M, Habib A, Botev B, et al. PROMISE: peer-to-peer media streaming using collect cast[C]//Proceedings of the eleventh ACM international conference

on Multimedia. USA, 2003: 45-54.

- [4] Habib A, Chuang J. Incentive mechanism for peer-to-peer media streaming[C]// Proceedings of 12th IEEE International Workshop on Quality of Service. Canada, 2004: 171-180.
- [5] Yun Tang, Lifeng Sun, Meng Zhang, et al. A novel distributed and practical incentive mechanism for peer to peer live video streaming[C]// ICME 2006. Canada. Toronto, 1533-1536.
- [6] Thomas Silverston, Olivier Fourmaux, Jon Crowcroft. Towards an incentive mechanism for peer-to-peer multimedia live streaming systems[C]// Peer-to-Peer Computing. Germany: Aachen, 2008: 125-128.
- [7] 冯健, 张建华, 温乃宁. 一种基于响应度的 P2P 点播流媒体系统激励机制[J]. 微电子学与计算机, 2009, 26(6): 198-201.
- [8] 张建风, 王汝传, 徐小龙. 基于一种新的激励机制的 P2P 系统的 UML 建模[J]. 微电子学与计算机, 2008, 25(10): 175-177.

作者简介:

虞 歌 男, (1963-), 硕士, 副教授, CCF 会员. 研究方向为计算机网络.

颜 婷 女, (1985-), 硕士研究生. 研究方向为计算机网络.

(上接第 168 页)

5 结束语

文中设计实现了一种高性能, 面积优化的智能卡加解密硬件系统, 实现了 128 bit AES 和 1024 bit RSA 硬件加解密功能, 可有效支持数字签名签署, 数字签名验证等操作, 具有可靠的安全性能. 采用 SMIC 0.18 μ m 混合工艺进行了流片验证, 验证结果表明该加解密系统完全达到智能卡对高安全性的要求, 同时具有良好的加解密性能和较小的面积, 可广泛应用于 3G 智能卡芯片中.

参考文献:

- [1] 景为平, 徐晨, 陈海进. AES 密码算法的结构优化与实现[J]. 微电子学与计算机, 2007, 24(2): 36-38.
- [2] Henry Kuo, Ingrid Verbauwhede, Patrick Schaumont. A 2.29Gbits/sec, 56mW non-pipelined rijndael AES encryption IC in a 1.8V, 0.18 μ m CMOS technology[C]// IEEE 2002 Custom Integrated Circuits Conference. USA: Florida, 2002: 147-150.
- [3] Refik Sever, Nesiln Ismailiglu, Yusuf C Tekmen, et al. A high speed ASIC implementation of the rijndael algorithm

[C]// ISCAS. Las Angeles: IEEE, 2004(2): 541-545.

- [4] Lu Chihchung, Tseng Shauyin. Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter [C]// ASAP'02. USA: London, 2002: 277-285.
- [5] STMicroelectronics. ST22N144, ST22N144_A data brief, rev 2[EB/OL]. (2006-06-10)[2010-11-19]. <http://www.st.com>
- [6] Infineon Technology. SLE88CX720P preliminary short product information[EB/OL]. (2006-03-09)[2010-11-20]. <http://www.infineon.com>
- [7] Kwon T W. Two implementation methods of a 1024 bit RSA cryptoprocessor based on modified Montgomery algorithm[C]// ISCAS2001. New York: IEEE press, 2001(4): 650-653.
- [8] 刘强, 佟东, 程旭. 一款 RSA 模乘幂运算器的设计与实现[J]. 电子学报, 2005, 33(5): 156-160.
- [9] Richard Herveille. RSA specification[EB/OL]. (2003-03-10)[2010-10-15]. <http://www.opencore.com>

作者简介:

戴 鹏 男, (1983-), 博士研究生. 研究方向为微处理器体系结构设计、SOC 体系结构设计等.