



一种基于公钥的低成本 RFID 双向认证协议^{*}

魏丽丽,董庆宽,丁文秀

(西安电子科技大学综合业务网理论及关键技术国家重点实验室 西安 710071)

摘要:基于目前资源消耗最少的 RFID 公钥认证方案 cryptoGPS 协议,提出了一种低成本双向认证协议,采用有效的密钥管理方法、改进的快速 Rabin 加密算法、低汉明重量(LHW)模值以及轻量级流密码算法 Grain V1,并设计使用新型低资源乘法器完成标签的大数模乘,在节省资源的同时克服了 cryptoGPS 密钥管理不灵活和认证单向性的缺点。安全性分析和基于 Design Compiler 平台 Smic 0.25 μm 工艺的仿真结果表明,该方案有足够的安全性且标签只需 4 530 个门即可完成双向认证,适用于资源受限的 RFID 系统。

关键词:RFID;公钥密码;cryptoGPS;双向认证协议

doi: 10.3969/j.issn.1000-0801.2013.10.012

A Low-Cost PKC-Based RFID Mutual Authentication Protocol

Wei Lili, Dong Qingkuan, Ding Wenxiu

(State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China)

Abstract: Based on the PKC-based RFID authentication protocol cryptoGPS which costs the least resource currently, a low-cost mutual authentication protocol which has a flexible key-management and can realize a mutual authentication was proposed. It adopted a new key-management scheme, an optimized fast Rabin encryption algorithm, low Hamming weight modulus and a lightweight stream cipher algorithm Grain V1, moreover, a new low-cost multiplier was designed to achieve the modulus multiplication on large numbers. The security analysis and simulation experiments carried out on Design Compiler with Smic 0.25 μm technique show that this scheme is secure enough and in which the tag just needs 4 530 gates, it is suitable for RFID system.

Key words: RFID, public key cryptography, cryptoGPS, mutual authentication protocol

1 引言

RFID(射频识别)技术是物联网中一种采用非接触方式识别目标的自动识别技术,是一种简单的无线通信系统,主要由标签(tag)、读写器(reader)和后台服务器(back-end server)³部分组成,RFID的非接触识别和人工干预、存储量大、操作方便等优点,使其被广泛应用于生产、物流、供应链、交通、医疗、跟踪等领域的数据收集和处

理。读写器与标签的无线传输通信信道很容易遭受侦听、阻截、篡改等各种攻击,使得 RFID 系统的安全和隐私问题非常严重,限制了 RFID 技术的广泛应用。欧洲委员会在 2009 年 5 月发布的关于 RFID 安全与隐私的建议提到: RFID 应用需要以安全的方式操作,高性能、低成本的 RFID 设备安全解决方案亟待研究。

采用密码技术设计安全的认证协议,成为保护 RFID 系统安全的重要方法,但 RFID 标签的计算能力与存储资

^{*} 国家自然科学基金资助项目(No.61373172),陕西省自然科学基金基础研究计划基金资助项目,中央高校基本科研业务费基金资助项目(No.K50511010009)



源十分有限,麻省理工学院自动识别中心在2001年的研究表明,在当前的技术条件下,在设计5美分标签时,集成电路芯片的成本不应该超过2美分,用于安全和隐私保护的门电路数量不能超过2 500~5 000^[1],随着科技的进步,这个限制可能逐渐宽泛,但仍无最新数据。这对密码技术在RFID认证协议的应用提出了严格的要求。

用于RFID认证协议的密码技术主要有对称密码与公钥密码。对称密码技术的低耗能、节省资源、计算速度快等优点十分有利于RFID环境,比如一些典型的基于散列的对称密码认证协议:Hash-locking协议^[2]、Randomized Hash-locking协议^[3]与Hash chain协议^[3]。Feldhofer提出基于AES分组密码的询问—响应协议^[4]比较有效,在0.35 μm CMOS工艺下实现需要3 595个门,功耗为8.15 μA (100 kHz)。这些方案虽然具有较好的资源优势,但密钥分配不灵活的缺点严重限制了RFID的应用范围和提供服务的形式,且往往需要后台数据库的搜索,不适用于大规模的应用。

基于公钥密码算法的认证方法密钥存储、密钥管理系统简单灵活,能够克服对称密钥方法的缺点,但复杂的计算使传统的公钥密码技术在资源有限的低成本标签上难以实现。近期的一个研究趋势是在标签上存储更多的信息以满足应用需求,并且标签的门数和容量可以在原有基础上适当提高,这也为公钥密码在RFID认证中的应用增加了可行性。

在使用公钥密码算法设计认证协议中,选择恰当的密码算法,改进或避免使用公钥密码中的复杂运算,又或者采用预计算或委托计算等方法,均成为降低标签资源的有效方法。参考文献[5]提出了基于NTRU的公钥认证方案,其最小安全方案中芯片的面积低于3 000个门,但只提供57 bit的安全性,不适用于当前的RFID领域,且只实现了单向认证;参考文献[6,7]研究了基于二次剩余(Rabin体制)的RFID认证方案,具有很好的安全性,但标签的计算需要两次至少1 024 bit的模平方运算和散列运算,其实现面积在10 000门以上,远超出RFID标签的计算能力。

椭圆曲线密码算法在安全性、密钥长度和计算速度上的优势,使其成为RFID认证算法的研究热点。参考文献[9~13]给出了标量乘和ECDSA算法在GF(2^m)有限域上的实现,但是其实现面积都在10 000门以上,不适用于低成本的标签;由Girault、Poupard和Stern提出的基于ECC的GPS方案^[13]的身份识别协议,在ISO/IEC 9798-5中被标准化^[14]。基于GPS方案,McLoone和Robshaw等提出了cryptoGPS认证方案^[15],该方案中标签仅需要一个160 bit的乘法计算,

参考文献[16]引入低汉明重量(LHW)乘法后,标签的计算量进一步减小,所需GE数量降低,但方案需要使用很长的随机数,需要后台服务器搜索,且只实现了单向认证,不能提供对认证后标签数据机密性的保护。参考文献[17]中比较了各种低成本cryptoGPS架构的性能,指出cryptoGPS方案是现有的基于公钥密码的认证方案中最省资源的设计,适用于低成本的RFID标签。参考文献[18]是cryptoGPS方案的几个改进版,标签的计算量小、安全度高,但也只实现了单向认证。

上述基于公钥的认证方案均没有考虑密钥管理问题,尽管不需要读写器和标签共享私钥,但是读写器必须存储每一个标签的认证公钥,这使得读写器在认证时需要查找后台数据库,没有体现出公钥密码、密钥管理高度的灵活性。另外,以上方案只完成了读写器对标签的单方向认证,而没能实现双方的互相认证,限制了方案的实际应用。

本文综合计算能耗、资源和成本开销等因素,采用有效的密钥管理方法,基于cryptoGPS方案,提出一种有效的低成本RFID认证方案,本文的主要贡献如下。

- 实现了标签和读写器的双向认证。
- 提出了有效的公钥管理方案,无需后台数据库存储标签公钥,也无需后台搜索,有利于对新增标签的管理,提高了认证速度;
- 给出了改进的快速Rabin加密算法,改进后的算法能够快速高效地完成数据加密,保证标签与读写器通信的安全性,并降低标签的计算成本。
- 方案中的读写器公钥 n 和ECC算法的模值 q 使用LHW模值,有效降低了标签的计算量,并给出了该类模值的生成方法。
- 设计使用新型低资源乘法器,完成标签上耗费资源较多的乘法运算,能够有效节省标签的资源,降低标签的成本。

2 相关算法

2.1 cryptoGPS协议

cryptoGPS协议^[17]基于公钥密码中的椭圆曲线密码(ECC)算法,将标签上复杂的倍点计算采用预计算并存储多组优待券coupons的方式实现,认证时可直接选取coupons。这种方法避免了标签上的复杂计算,降低了标签所耗资源,使得cryptoGPS协议可以很好地用于RFID认证中。协议具体细节如图1所示。

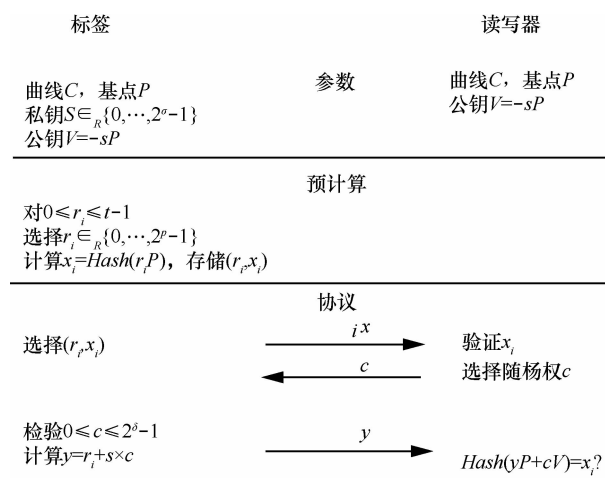


图 1 基于椭圆曲线的 cryptoGPS 认证协议

虽然该方案中的标签以很少的资源实现了认证,但它只实现了读写器对标签的单向认证。另外,方案缺乏必要的密钥管理措施,后台数据库需要存储每一个标签的公钥,而且公钥的查找需要访问后台数据库。该密钥管理方法没有体现公钥密码、密钥管理方便灵活的优势,限制了 RFID 的应用范围和提供服务的形式。

2.2 改进的快速 Rabin 加密算法

Rabin 加密算法^[7]简述如下:设 p, q 为两个大素数,且满足 $p \equiv q \equiv 3 \pmod{4}$, $n = pq$, n 为公钥, p, q 为私钥。设待加密消息为 m , 加密后生成的密文为 $c = m^2 \pmod{n}$; 解密密文 c , 则对 $m < n$ 解关于 m 的二次同余方程 $m^2 = c \pmod{n}$ 。

为适用于低成本的 RFID 标签,本方案中提出一种改进的 Rabin 型加密算法,其参数选择同 Rabin 算法,设加密函数为 $En_{Rabin}(f)$, 输入 128 bit 明文 f , 输出 1 024 bit 的密文 f' 。加密时,首先将明文 f 扩展成 1 024 bit 的消息 f' , 扩展方法是:将 1 024 bit 分成 128 个 8 bit, 将 f 的每一位依次嵌入每个字节的最低位,该字节的其余位均为 0。即明文 f 中的每个 0 字节扩展为 00000000, 1 字节扩展为 00000001。再对编码后的消息进行 Rabin 加密,得到密文 $C = f'^2 \pmod{n}$ 。

解密时,从方程 $C = f'^2 \pmod{n}$ 中可解出 4 个根 $\pm u, \pm v$, 根据 f' 的 LHW 特点,从解密的 4 个根中确定正确的根;再根据 f 的编码方式提取出 128 bit 的明文 f 。

这种编码方式,共有 2^{128} 种明文,满足抵抗穷搜索攻击的要求,由于 Rabin 算法所基于的困难问题等价于大整数分解,1 024 bit 的模值可确保加密算法的安全性不受到影响,并且 1 024-128=996 bit 的消息冗余使得这种编码方式可以解决解密不唯一的问题。另外,由于编码后明文的低

汉明重量数据特点,可简化计算,有效节省硬件资源。

2.3 LHW 模值生成算法

Rabin 加密的公钥 n 设定为 1 024 bit LHW 数值,其前 500 bit 最高位为 1,其余都为 0,后 524 bit 为随机值;其中模值 $n = pq$, p 和 q 均为模 4 余 3 的大素数, $p-1$ 有大素因子,并要求 $p-1$ 与 $q-1$ 的最大公因子 $\gcd(p-1, q-1) < B$, B 是一个较小的数值。

该 LHW 模值 n 的生成过程如下:首先,随机选取 524 bit 的随机值 r' ,并令初始模值 $n' = 1 \parallel 0^{499} \parallel r'$, 其中 0^{499} 表示 499 个 0。然后随机生成一个 512 bit 的模 4 余 3 的大素数 p ,且要求 $p-1$ 有大素因子;再计算 $q' = n'/p$ 确定 q 的取值范围,通过对 q' 增加或者减少并进行素性检验,使其满足模 4 余 3 的素数,并将该数记作 q ,且要求 $\gcd(p-1, q-1) < B$;最后,由 $n = pq$ 来确定 n 。

以下为利用上述算法生成的一组 n 和 p, q , 为节省篇幅,这里只给出 n 和 p ,并用 16 进制数表示如下:

$p = A60A5DC04C7B90542CEBBC50D5C60CB7C8A9F184$
 $F710DBFBFBFA0D79E75C2BA56F8E85FABF7C1A0F97D768$
 $35BDB 55DDCA7C401B9AEF35555E01B35EBFADEEBB7$
 $n = 8 \parallel 0^{124} \parallel 2BA03B985E504EBA6930C3C073E564455B645$
 $28B89412694E9D214718D1B916DB1F6A2692EDE38E01EDF$
 $5F5706D3B567861CF1F86D42C4C968E72A07BBB6D4AF9$

3 低成本 RFID 认证协议设计

3.1 初始设置及密钥管理

本文基于 cryptoGPS 协议提出一种低成本 RFID 双向认证协议,协议的初始设置及密钥管理方法如下。

(1) 设 $E_q(a, b)$ 为 $GF(q)$ 上的椭圆曲线, P 是该曲线上的一个基点, $s \in_R \{0, \dots, 2^p-1\}$ 是标签的秘密钥, $V = -sP$ 是标签的公钥,这里 q 是一个 LHW 值,如第 2.3 节所述。

(2) 系统为标签与读写器分配的唯一标识码 ID_{tag} 和 ID_r 。认证服务器(或 CA)为标签签署的证书 $Cert_{tag} = \{\text{版本号}, ID_{tag}, V, V = -sP, \text{CA 的签名}\}$, 将标签的私钥 s 和证书 $Cert_{tag}$ 存储在标签上。

(3) 认证服务器预先计算 m 个二元组 $Coupon_i = (r_i, r_iP)$ 作为优待券存储在标签上,其中 r_i 是随机数, $r_i \in_R \{0, \dots, 2^p-1\}$, $i = 1, 2, \dots, m$ 。

(4) 认证服务器采用第 2.3 节所述的方法生成 λ 个读写器公钥 $n_1, n_2, \dots, n_\lambda$, 其中 n_i 是两个大素数的乘积,有效长度为 524 bit。假设标签拥有 w bit 的处理器,认证服务器



预计算蒙哥马利算法中的参数 $n_i^{-1} \bmod 2^w$, $i=1, \dots, \lambda$, 最后在标签上预存储 λ 个模值对 $(n_i, n_i^{-1} \bmod 2^w)$ 。

(5) 方案中以 Grain V1 算法作为随机数产生器 prng() 和对称加密算法 E。

本方案采用低汉明重量模值使标签可以在有限的空间存储更多的读写器公钥, 而不需要设计读写器证书, 同时读写器可以验证标签的证书, 这种密钥管理方法使得只有拥有标签存储模值的读写器才有读取标签的权限, 无需后台数据库存储标签公钥 V , 避免了对后台数据库的查找, 有利于对新增标签的管理, 提高了认证速度, 充分体现了公钥密码算法密钥管理方便灵活的特点, 为双向认证提供了基础。

3.2 认证协议

本文提出了一种基于公钥的低成本 RFID 双向认证协议, 协议中伪随机数产生器 PRNG 和加密算法 E 均使用序列密码算法 Grain V1 实现, 种子密钥长度采用 128 bit, 具体细节如图 2 所示。

认证过程包括以下步骤。

步骤 1 读写器采用轻量级序列密码算法 Grain V120 生成随机数 r_s , 并将询问信号 Q 、随机数 r_s 、读写器公钥 n_r 与读写器的身份 ID_r 发送给标签。

步骤 2 标签收到数据后, 检查读写器公钥 n_r 是否为标签所预存储的模值, 如果是, 则该公钥 n_r 是合法的; 后利用种子密钥 k_0 生成 1 个 128 bit 的伪随机数 f , 计算 $C_1 = \text{EnRabin}(f)$, $C_2 = E_f(r_s P \parallel r_s \parallel \text{Cert}_{\text{tag}})$; 发送 $C_1 \parallel C_2$ 给读写器。

步骤 3 读写器收到 $C_1 \parallel C_2$ 后, 利用私钥从 C_1 中解密

出 f , 再利用 f 从 C_2 中解密得 $r_s P$ 、 r_s 和 Cert_{tag} , 验证 r_s 及证书并获得标签的公钥和 ID; 若验证通过, 再截取标签证书 Cert_{tag} 的连续 160 bit 数据 $\text{Cert}_{\text{tag}}'$, 并加密有 $C_3 = E_f(\text{Cert}_{\text{tag}}')$; 选择 32 bit 询问值 c , 将 $C_3 \parallel c$ 发送给标签。

步骤 4 标签解密消息获得数据 $\text{Cert}_{\text{tag}}'$ 和随机数 c , 验证数据 $\text{Cert}_{\text{tag}}'$ 是否为标签证书 Cert_{tag} 的某连续 160 bit, 如果是, 则标签对读写器的认证成功; 然后计算 $y = r + (s \times c) \bmod q$, 并将 y 值发送给读写器。

步骤 5 读写器收到数据后, 利用公钥 $V = -sP$ 对标签进行认证, 验证 $yP + cV = Q$, 如果验证通过, 则读写器对标签的认证成功, 则实现了双向认证, 并建立了会话密钥 f 用于传送后续数据。

4 协议的安全性

标签与读写器之间的无线信道容易受到攻击者的窃听与攻击, 需着重保护, 本节通过阐述本协议如何抵抗 RFID 系统常见的几种攻击手段, 对协议的安全性做具体分析, 并在表 1 中与 cryptoGPS 方案的安全性能做比较, 具体分析如下。

表 1 与 cryptoGPS 协议的安全性能比较

安全性能	cryptoGPS 协议	本协议
双向认证性	—	✓
抗位置追踪	✓	✓
数据保密性	—	✓
前向安全性	✓	✓
抗重放攻击	✓	✓

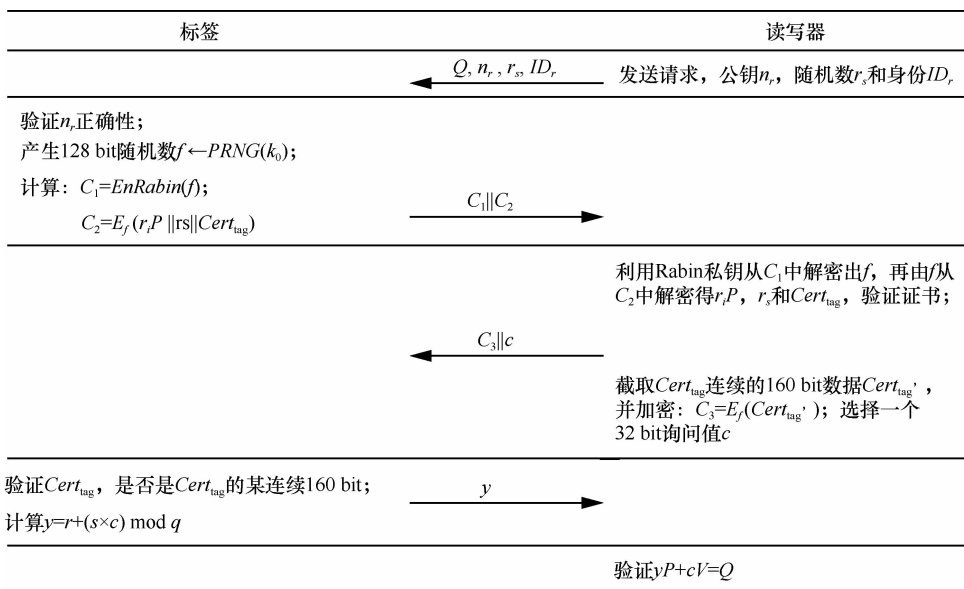


图 2 基于公钥的低成本 RFID 双向认证协议

(1) 双向认证性

本方案采用有效的密钥管理方法,由 LHW 模值生成算法产生的模值 n 作为读写器公钥,并将生成的若干个模值存储在标签上,标签用读写器公钥加密随机数 f ,读写器若能解密成功,且标签对截取的证书有效 160 bit 验证成功,则完成了对读写器的身份合法性认证;后读写器向标签发送随机询问值,并利用公钥对标签的身份进行认证,认证成功后则实现了标签与读写器的双向认证。这种有效的密钥管理和分发模式实现了标签与读写器的双向认证,可以有效防止非法读取和假冒攻击。

(2) 抗位置追踪

标签的身份等所有标识性信息在传输过程中均被加密,且标签在每次认证过程选择不同的预计算二元组 coupon,并生成不同的随机数,因此标签在每次通信中输出的信息都是随机的,攻击者无法根据固定的输出来对标签进行位置追踪。除了保护标签的位置隐私,也可以确保通信数据的隐私性。

(3) 数据保密性

本方案提供了标签与读写器的认证和密钥协商功能,并支持对称加密。在协议的步骤 2 中,标签与读写器首先进行会话密钥 f 的协商,之后用会话密钥加密后续通信数据,保证数据的安全性。与 cryptoGPS 方案相比,本协议增加了会话密钥的协商过程,提升了协议的安全性能。协议中的对称加密及伪随机数的选取采用面向硬件的轻量级 Grain V1 流密码算法实现,保证标签和读写器间所有后续通信数据的保密性和安全性,防止被窃听。

(4) 抗重放攻击

攻击者事先截获标签与读写器之间的通信信息,当读写器与标签再次通信时,攻击者利用先前截获的信息伪装成合法的实体与其他实体进行通信。本方案中,由于采用了安全的流密码算法产生随机数,并及时更新种子密钥,可确保标签和读写器每次认证中产生的随机数不同,使得攻击者不能利用之前截获的信息伪装成合法标签或读写器进行通信,从而可以有效防止重放攻击。

(5) 前向安全性

如果一个非法用户可以破坏一个标签,拥有它现在保存的全部数据,那么就可以追踪该标签以前的会话,这种攻击方法成为前向攻击。在本方案中,如果攻击者获得了某一次通信的会话密钥 f ,则获得了标签的证书等信息,由于标签每次选择的会话密钥 f 及随机数都与之前的不同,

又由于存储的优待券是椭圆曲线上的点乘运算,难以获得每次数据的相关性,也不能获得标签私钥的任何信息,因此攻击者不能根据截获的标签的某次输出而推测之前的输出,追踪标签以前的会话,从而保证了协议的前向安全性。

5 协议的实现及性能

5.1 大数乘法器的设计

方案中标签主要的资源消耗在于大数乘法上,因为传统的蒙哥马利大数乘法占用较多的资源,远远超过了 RFID 标签的计算能力,不能用于资源受限的 RFID 环境中。方案中为尽可能地降低标签所需资源完成 1 024 bit 的大数乘法,采用流水线设计的思想,使用多个乘法单元并行计算,并利用移位寄存器间接实现数据移位的功能,设计出一种新型低资源高效大数乘法器。

对于 1 024 bit 的大数乘法的实现,首先采用最节省资源的移位相加方法设计一个 $8 \times 1\,024$ bit 乘法单元如图 3 中虚线所示,再利用 4 个 $8 \times 1\,024$ bit 乘法单元并行计算,利用移位寄存器存储来间接实现数据移位,后经求和运算来实现一次 $32 \times 1\,024$ bit 的乘法计算,经过 32 次这样的计算过程可完成一次 1 024 bit 的大数乘法运算。 $32 \times 1\,024$ bit 乘法单元结构如图 3 所示。

利用图 3 所示结构实现 1 024 bit 大数乘法的流程按如下步骤进行。

步骤 1 第一个时钟输入 4 个 8 bit 数据,分别与 $128 \times 8 = 1\,024$ bit 乘数相乘。8 bit 乘法器输出的高 8 bit 为进位,返回下一时钟计算,低 8 bit 存入移位寄存器作为输出,存入数据前,移位寄存器由控制信号清零,利用相差 8 bit 的移位寄存器存储数据,间接实现移位操作。移位寄存器输出的数据输入 8 bit 加法器,进位 c 作为下一个时钟的加法器输入,其余 8 bit 输出与下一个寄存器输出相加,重复加法过程,最后将输出存储。计算方法如图 4 所示。

步骤 2 将 $32 \times 1\,024$ bit 乘法器的输出存入 RAM 中。第一次计算结束后,RAM 中的数据从低地址输出,经过一个 32 bit 的移位寄存器(初始清零),与第二次 $32 \times 1\,024$ bit 乘法器输出的 8 bit 数据做加法运算,结果再存入 RAM,进位返回参与下一次加法运算。做 32 次这样的计算可实现 1 024 bit 的乘法运算,其中使用的 32 bit 移位寄存器,可实现数据的移位 32 bit。

步骤 3 将每次 $32 \times 1\,024$ bit 乘法器的输出结果做移位(32 bit)相加,该加法器的结构如图 5 所示。

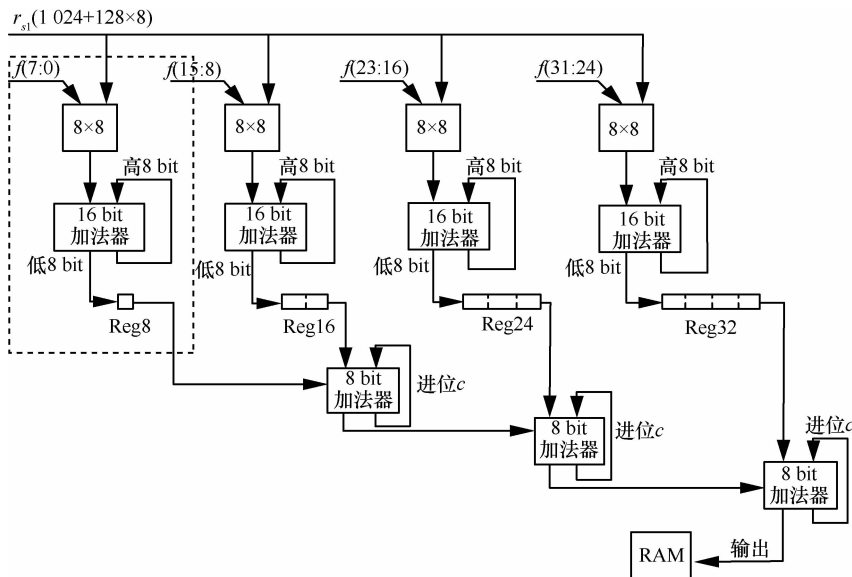


图3 32x1 024 bit 乘法单元结构

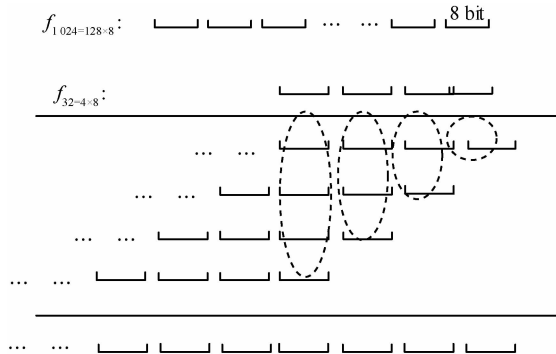


图4 计算方法示意

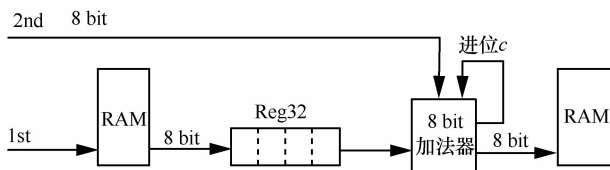


图5 加法器结构

对该乘法器的资源情况分析如下。

该乘法器用了4个8x1 024 bit的乘法器单元,3个8 bit加法器和加法器中的一个8 bit加法器,每个8x1 024 bit乘法器单元由一个8 bit乘法器(图3中8x8)和一个16 bit加法器构成。基于 Synopsys Design Compiler 使用 Smic 0.25 μm CMOS 工艺的仿真实验结果表明,8 bit的乘法器需要528个门实现,16 bit加法器要165个门,因此一个8x1 024 bit乘法器单元需693个门实现。综合结果表明该大数乘法器结构共需要3 080个门,与传统蒙哥马利乘法相比,有效节省了资源,适用于资源受限的RFID标签。表2为低资源乘

法器资源情况。

表2 低资源乘法器资源情况分析

单元	8x8 bit 乘法器	16 bit 加法器	8x1 024 bit 乘法器单元	8 bit 加法器	总数
面积 (等效门/0.25 m)	528	165	693	77	3 080

5.2 性能分析

本节通过在 Altera Quartus II 环境中对协议进行功能仿真,并使用 Synopsys 公司的综合工具 Design Compiler,采用 Smic 0.25 μm CMOS 工艺库在 500 kHz 时钟频率下对方案进行综合,对协议的性能做具体分析,并在表3中与 cryptoGPS 方案的性能进行比较。

表3 与 cryptoGPS 方案的性能比较

设计	面积(等效门)	时钟数(clk)	时间(ms)
cryptoGPS(0.13 μm^2)	7 494	6 794	13.59
本方案(0.25 μm)	4 530	4 184	8.37

比较结果可说明本方案在采用灵活的密钥管理方法实现双向认证,并在保证协议安全性的同时,具有较大的资源优势,能较好地适用于资源受限的RFID环境。

协议步骤2中耗费资源的操作有随机数的生成、快速 Rabin 加密 EnRabin 和流密码加密 E,详细如下。

- 该步骤中的随机数生成和流密码加密均采用面向硬件的轻量级流密码算法 Grain V1 实现,标签完成这些操作占用的门数为1 450²⁰。
- 改进的快速 Rabin 加密 EnRabin $(f)=f^2 \bmod n$ 中 1 024 bit LHW 数据平方运算 f^2 ,采用第5.1节所述的

低资源乘法器标签需要 3 080 个门面积实现该计算。

- Rabin 加密中 $\text{mod } n$ 的计算, 根据蒙哥马利算法分析可知, 该取模运算占用资源的主要是一个 32×32 bit 和 32×512 bit 的乘法运算, 可利用第 5.1 节所述的乘法器实现, 不额外增加占用门数。

协议中步骤 4 中的计算 $y=r+(s \times c) \bmod q$, 其中, 加法运算与 $\text{mod } q$ 的计算很简单, 占用的门数可忽略不计, 其主要耗费资源的计算是一个 160×32 bit 的乘法 $s \times c$, 该运算也可采用上述乘法器实现, 不额外增加占用门数。

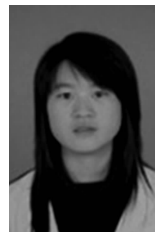
6 结束语

本文综合 RFID 系统的限制因素及各种密码算法的计算复杂性, 基于 cryptoGPS 协议, 提出一种基于公钥的低成本 RFID 认证协议, 实现了标签与读写器的双向认证, 满足标签的低成本要求, 并且能够抵抗现有的各种攻击手段, 符合 RFID 系统的安全需求。方案同 cryptoGPS 协议一样, 仍然使用存储 coupon 对的方法进行认证, 限制了标签的使用次数, 这将是下一步研究需要解决的问题。

参考文献

- Sarma S E. Towards the 5 Cent Tag. Technical Report. MIT-AUTOID-WH-006, MIT-AUTOID Center, 2001
- Weis S A, Sarma S E, Rivest R L, *et al.* Security and privacy aspects of low-cost radio frequency identification systems. Proceedings of First International Conference on Security in Pervasive Computing, Boppard, Germany, 2003: 201~212
- Avoine G, Oechslin P. A scalable and provably secure hash based RFID protocol. Proceedings of the 2nd IEEE International Workshop on Pervasive Computing and Communication Security, Kauai Island, Hawaii, USA, 2005
- Feldhofer M, Dominikus S, Wolkerstorfer J. Strong authentication for RFID systems using the AES algorithm. Proceedings of Cryptographic Hardware and Embedded Systems-CHES'04, Santa Barbara, CA, USA, 2004:357~370
- Gaubatz G, Kaps J P, Ozturk E. State of the art in ultra-low power public key cryptography for wireless sensor networks. Proceedings of the 3rd Int'l Conference on Pervasive Computing and Communications Workshops (PerCom 2005 Workshops), 2005:146~150
- Yeh T C, Wu C H, Tseng Y M. Improvement of the RFID authentication scheme based on quadratic residues. Computer Communications, 2010(5)
- Chen Y L, Chou J S, Sun H M. A novel mutual authentication scheme based on quadratic residues for RFID systems. Computer Networks, 2008,52(12): 2373~2380
- Braun M, Hess E, Meyer B. Using elliptic curves on RFID tags. International Journal of Computer Science and Network Security IJCSNS, 2008(2)
- Kumar S S, Paar C. Are standards compliant elliptic curve cryptosystems feasible on RFID. Proceedings of Workshop RFID Security, Graz, Austria, 2006
- Furbass F, Wolkerstorfer J. ECC processor with low die size for RFID applications. Circuits and Systems, New Orleans, LA, USA, 2007: 1835~1838
- Batina L, Seys S, Singelee D, *et al.* Hierarchical ECC-based RFID authentication protocol RFIDSec 2011, Amherst, Massachusetts USA, 2012:183~201
- Batina L, Lee Y K, Seys S, *et al.* Extending ECC-based RFID authentication protocols to privacy-preserving multi-party grouping proofs. Personal and Ubiquitous Computing, 2012(3)
- Girault M. Self-certified public keys. Proceedings of Eurocrypt' 91, Brighton, UK, 1992:490~497
- ISO/IEC. International Standard ISO/IEC 9798 Part 5: Mechanisms Using Zero-Knowledge Techniques, 2004
- McLoone M, Robshaw M J B. Public key cryptography and RFID tags. Proceedings of the 7th Cryptographers' Track at the RSA Conference on Topics in Cryptology, San Francisco, CA, USA, 2007:372~384
- Poschmann A, Robshaw M J B, Vater F, *et al.* Lightweight cryptography and RFID: tackling the hidden overhead. TIS, 2010(2)
- O'Neill M, Robshaw M O N N. Low-cost digital signature architecture suitable for RFID tags. IET Computers & Digital Techniques, 2010(1)
- McLoone M, Robshaw M J B. New architectures for low-cost public key cryptography on RFID tags. Proceedings of 2007 ISCAS, New Orleans, LA, USA, 2007
- Rabin M O. Digitalized Signatures and Public Key Functions as Intractable as Factorization. MIT/LCS/TR-212, Massachusetts Institute of Technology, 1979
- Hell M, Johansson T, Meier W. Grain-a stream cipher for constrained environments. International Journal of Wireless and Mobile Computing, 2007(1)

[作者简介]



魏丽丽, 女, 西安电子科技大学硕士研究生, 主要研究方向为基于公钥的射频识别认证技术。

董庆宽, 男, 博士, 西安电子科技大学副教授、硕士生导师, 中国电子学会高级会员, 中国密码学会会员, 主要研究方向为密码学、网络与信息安全、移动 IPv6 网络安全技术和 RFID 认证技术。

丁文秀, 女, 西安电子科技大学硕士研究生, 主要研究方向为基于公钥的射频识别认证技术。

(收稿日期: 2013-07-29)