

文章编号:1001-9081(2011)10-2694-03

doi:10.3724/SP.J.1087.2011.02694

高效的 RFID 双向认证协议

王明辉¹, 王建东²

(1. 盐城工学院 信息工程学院, 江苏 盐城 224051; 2. 南京航空航天大学 信息科学与技术学院, 南京 210016)

(wmh@ycit.edu.cn)

摘要:为了能有效保证射频识别(RFID)系统中用户的隐私和数据安全,采用椭圆曲线和Weil对相结合的方法来设计RFID系统的认证协议,并提出一种新型RFID双向认证协议。该协议实现了双向认证和匿名认证,并能抵抗流量分析、伪装、重放等攻击。与随机Hash锁、Hash链、New-Gen2等进行比较,该协议能够抵抗大多数已发现的攻击形式,并给出针对这些攻击的安全性分析。

关键词:椭圆曲线离散对数问题;认证协议;密钥;射频识别;隐私;Weil对

中图分类号:TP391.45; TP309.2 **文献标志码:**A

Efficient RFID mutual authentication protocol

WANG Ming-hui¹, WANG Jian-dong²

(1. School of Information Engineering, Yancheng Institute of Technology, Yancheng Jiangsu 224051, China;

2. College of Information Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing Jiangsu 210016, China)

Abstract: For effectively ensuring users' privacy and data security of the Radio Frequency Identification (RFID) system, a new RFID mutual authentication protocol was proposed in this paper, which was designed by the method of combining elliptic curves and Weil pairing. In this protocol, the mutual authentication and anonymous authentication were realized, and the traffic analysis attack, impersonation attack and replay attack were resisted. Compared with the random Hash lock, Hash chain and New-Gen2, this protocol can resist most of the attacks which have been discovered.

Key words: Elliptic Curve Discrete Logarithm Problem (ECDLP); authentication protocol; key; Radio Frequency Identification (RFID); privacy; Weil pairing

0 引言

射频识别(Radio Frequency Identification, RFID)技术是一种利用射频通信实现的非接触式自动识别技术。RFID系统由标签、读写器和数据处理系统3部分组成。标签和读写器通过无线信号进行通信,读写器向RFID标签发出命令,标签根据接收到的命令做出响应。目前RFID技术已经被广泛应用于物流和供应链管理、生产制造和装配、航空行李处理、邮件、快运包裹處理及物联网等领域。但是RFID系统也存在安全问题,容易泄漏使用者的行踪、隐私及商业机密等信息。

近些年,在RFID安全研究领域中有很多研究者致力于设计、分析轻量级的RFID认证协议,旨在使用最小的计算机能力高效地实现标签与读写器之间的单向或双向认证^[1-7]。这些研究成果分析了RFID协议中的安全问题,提出了许多新的方法和新的协议方案。经过分析发现最近提出的两个协议^[4-5]存在安全漏洞,这些缺陷能够导致协议本身受到重放攻击和标签被伪装攻击。本文指出了这些协议之所以存在安全问题的主要原因,并且提出了一个更安全高效的RFID双向认证协议。通过分析,新提出的协议能够抵抗现存的大部分攻击。

1 相关协议分析

RFID系统的安全问题呈现出来以后,研究者们提出了很多RFID认证协议,其中比较典型的是Hash锁协议^[1]、随机Hash锁协议^[2]、Hash链协议^[3]。随后研究者发现Hash锁协议依赖Hash函数是单向性,在很大程度上解决了用户的隐私

保护。然而,在认证过程中metaID始终不变,并且ID也以明文的形式通过不安全信道,所以协议很容易受到重放攻击和哄骗攻击。又因为每次标签回答的数据都是固定不变的,所以该协议不能防止位置跟踪攻击。随机Hash锁协议是Hash锁协议的改进形式,其主要目标是解决Hash锁协议的位置跟踪问题。在该协议中,标签每次回答都是随机的。然而,此协议不适合有大量标签的情况,因为阅读器需要从所有的ID标识中查找对应的标签ID,这大大增加了阅读器的计算量。不久,NTT实验室提出了一个Hash链方法,该协议中的标签集成了2个不同的Hash函数H和G。协议利用标签每次更新标识满足了不可分辨性和前向安全性。然而,Hash链协议是一个单向认证协议,它只对卡片进行认证,容易受到重传和哄骗攻击。

在上述3个协议的基础上,研究者又提出了新的基于Hash函数的RFID认证协议^[4],本文称之为New-Hash协议,该协议很好地解决了隐私保护的问题,并且能够抵抗多数攻击,但是,发现它不能抵抗字典攻击。读卡器R发送认证请求和随机数S给标签T,标签T计算 $R^i = H(key \parallel R^{i-1} \parallel S)$,发送 $R^i, H(ID \parallel S \parallel R^i)$ 给R,R再传递给服务器D,D验证T合法后,发送 $H(ID \parallel R^i)$ 给R,R再传递给T。攻击者可以在通信过程中侦听到 R^i 和 $H(ID \parallel R^i)$ 的值。而Hash函数是公开的,链接运算(\parallel)不具有加密性,因此,攻击者可以通过字典文件,攻击获得ID的值,进而跟踪标签的位置。攻击者跟踪标签和读卡器之间的认证过程,冒充读卡器对标签发出查询请求,并发送随机数S(令 $S = 0$)给标签,记录每次标签返回的 $H(ID \parallel S \parallel R^i)$ 和 R^i 的值。发起攻击的时候,使用之前记录的

收稿日期:2011-04-22;修回日期:2011-06-16。 基金项目:盐城市2009年科技发展计划项目(YK2009092)。

作者简介:王明辉(1977-)男,黑龙江绥棱人,讲师,硕士研究生,主要研究方向:信息安全、密码协议; 王建东(1945-)男,江苏南京人,教授,博士生导师,主要研究方向:人工智能、信息安全、计算复杂性。

R^i 值代替本次认证过程中的数值。因此,本协议也不能抵抗重放攻击。

最近,邓森碧等人^[5]提出了一个新的基于 Gen2 标准的 RFID 认证协议,本文称之为 New-Gen2 协议。在协议中, R 向 T 发出认证请求,并发送 n_r , T 计算 $M_1 = \text{CRC}(P \oplus (n_r \| n_t)) \oplus k$, 并且发送 (M_1, n_t) 给 R , R 转发 (M_1, n_r, n_t) 给 D 。在协议中,CRC 被当成一个单项的加密函数,忽略了 CRC 的另外一个不安全属性:对于所有的 A 和 B ,都有 $\text{CRC}(A \oplus B) = \text{CRC}(A) \oplus \text{CRC}(B)$ ^[6]。再者,攻击者通过侦听,可以获得 n_r 和 n_t ,因此,攻击者可以计算出 $\text{CRC}(n_r \| n_t), M_1 \oplus \text{CRC}(n_r \| n_t) = \text{CRC}(P) \oplus k$, 攻击者可以伪造 n_r , 在不需要知道 P 和 k 的情况下,成功地伪装了标签 T 。

从上述 RFID 认证协议的分析来看,不安全的协议主要存在如下几方面的缺陷:

1) 标签的原有信息在协议运行过程中没有被保护,直接在协议中使用。

2) 读卡器在对同一标签的多次认证过程中存在(或者隐含)一定的相关性。

3) 很多协议没有对密钥进行更新,一旦出厂密钥泄露将威胁标签中用户信息安全。同时,密钥更新时也没有注意同步更新。

4) 读卡器和标签的随机参数没有都参加认证过程,容易遭受重放攻击。

2 新的 RFID 认证协议

系统初始化之后,数据库 D 、读卡器 R 和标签 T 之间共享椭圆曲线 $E(F)$ 、加密密钥 K 、随机数生成器 $PRNG(\cdot)$ 。数据库中存储记录 $(ID_i, K_i, r_{old}, r_{new})$ 。初始 $r_{old} = r_{new} = K_i$ 。认证过程如图 1 所示,具体表述如下:

第 1 步 $R \rightarrow T$, R 选取椭圆曲线上的基点 G , 向 T 发出认证请求 $Query$, 同时将 G 发送给 T 。

第 2 步 $T \rightarrow R \rightarrow D$, T 生成随机数 d_t, k , 计算 $P_t = d_t \times G$ 作为 T 的公钥, $X = kG, m = PRNG(ID_i)$, 将 m 嵌入到椭圆曲线上, 记作点 $P_m, Y = d_t(P_m + X)$, T 将 (P_m, X, Y, P_t) 发送给 R , R 将 (X, Y, P_t, G) 发送给 D 。

第 3 步 $D \rightarrow R \rightarrow T$, 要完成对 T 的认证,首先,根据 Weil 对的性质, D 可以推导出:

表 1 RFID 认证协议的安全性比较

认证协议	密钥同步更新	相互认证	伪装攻击	重传攻击	流量分析	匿名	字典攻击	前向安全性
Hash 锁								✓
随机 Hash 锁		✓				✓		✓
Hash 链					✓	✓	✓	✓
New-Hash	✓	✓			✓	✓		✓
New-Gen2	✓	✓		✓	✓	✓	✓	✓
本文协议	✓	✓	✓	✓	✓	✓	✓	✓

注:“✓”表示具备该安全性,空白表示不具备该安全性。

3.2 复杂性比较

本文提出的认证协议是基于椭圆曲线方程和双线性对函数的。没有使用 Hash 函数是因为其计算复杂,在 EPC Class 1 Gen 2 (EPCGen2) 标准中规定不能使用 Hash 函数和加密函数^[5],而椭圆曲线上的双线性对在计算上只相当于一个二元方程。本文给出了协议间的比较(见表 2), H 表示一个 Hash 函数, G 表示一个随机数运算, W 表示一个 Weil 对计算。从比较上看,本文协议在计算性能上和现有协议有一定的可比性。

3.3 安全性分析

3.3.1 匿名

本文提出的协议实现了 RFID 系统对匿名的要求。标签的

$$e_m(Y, G) = e_m(d_t(P_m + X), G) = e_m((P_m + X), d_t G) = e_m((P_m + X), P_t) = e_m(P_m P_t) e_m(X P_t)$$

然后, D 检索数据库记录查找 ID_i , 计算出 P_m 的值,若能够满足 $e_m(Y, G) = e_m(P_m P_t) e_m(X P_t)$, 则 D 通过 T 的验证。

其次, D 完成对 T 的认证以后, D 要对密钥进行更新, 具体操作如下:

1) 若 $K_i = r_{old}$, 则 $r_{new} = PRNG(K_i)$ 。

2) 若 $K_i = r_{new}$, 则令 $r_{old} = r_{new}, r_{new} = PRNG(K_i)$; 否则验证失败。

最后, D 计算 $n = PRNG(K_i)$, 将 n 嵌入到椭圆曲线上, 记作点 P_n , D 将 P_n 发送给 R , R 计算 $P_r = d_r \times G$ 作为公钥, 选择随机数 $g, X' = gG, Y' = d_r(P_n + X')$, 并将 (P_r, X', Y') 发送给 T 。

第 4 步 T 收到数据后,验证 R 的方法和上述方法相似, T 通过验证等式 $e_m(Y', G) = e_m(P_r P_t) e_m(X' P_t)$ 是否成立, 来判断验证是否成功。因为 T 拥有椭圆曲线 $E(F)$ 和 K_i 所以可以有效计算出 P_n 。最后 T 更新密钥 $K_i = PRNG(K_i)$ 。

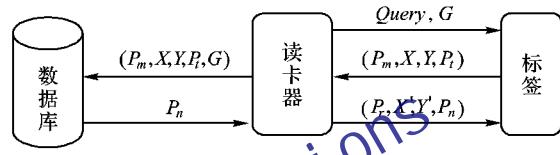


图 1 协议认证过程

3 协议性能分析

公钥密码系统的安全性一般通过该算法的抗攻击强度来反映。椭圆曲线的离散对数问题的计算难度在计算复杂度上是完全算法指数级的,而 RSA 是亚指指数级的,椭圆曲线密码(Elliptic Curve Cryptosystem, ECC)算法和其他几种公钥系统相比,其抗攻击性具有绝对优势。ECC 算法能以较短的密钥长度提供更大的安全性。例如一个 160 位的 ECC 密钥能过提供相当于一个 1 024 位的 RSA 或者 DSA 密钥所提供的安全性。为此把椭圆曲线加密引入到 RFID 认证协议中来。

3.1 安全性比较

本文提出的协议与之前提出的协议进行了比较,详见表 1。通过比较可以得出,本协议具有很好的安全性能,满足了 RFID 认证协议的需求。

表 2 RFID 认证协议的计算量比较

协议名称	标签	读卡器	数据库
Hash 锁	1H	—	—
随机 Hash 锁	1H, 1G	$(\sum ID/2)H$	—
Hash 链	2H	—	$(\sum ID/2)H$
New-Hash	3H	1G	$(\sum ID/2 + 1)H$
New-Gen2	3G	1G	2G
本文协议	3W, 2G	—	1G, 3W

注:虽然在 New-Gen2 协议中没有使用 Hash 函数,但是是标签进行了 3 次 CRC 操作,5 次异或操作;数据库进行了 4 次 CRC 操作,3 次异或操作;“—”表示没有 Hash 函数、随机数等相关操作。

身份标识 ID 存储在后端数据库和标签中，并且在整个认证过程中，标签的标识并没有被明文传输，一个随机数代替了标签的 ID ，并且随机数被嵌入到椭圆曲线上，攻击者无法把这个随机数和标签的真实身份关联起来，更无法获悉 ID 的值。

3.3.2 抵抗流量分析攻击

流量分析攻击是指对读卡器和标签的信息截取、分析，提取有用信息的过程。攻击者向标签发送多次的询问请求，接收标签返回数据。从获得的数据中分析标签的响应，达到跟踪标签的目的。在本协议中攻击者通过侦听流量，可以截获 P_m 和 X ，但由于椭圆曲线离散对数问题^[8]，攻击者没有有效办法计算出 d_i ，也无法获得标签的 ID ，更无法通过认证。

3.3.3 抵抗伪装攻击

伪装攻击是指攻击者通过被动侦听读卡器和标签之间的通信，来获取它们之间发送的数据，进而成功伪造一方通过认证。在本协议的运行过程中，攻击者获得的数据都是复合数据（随机数参与生成）。如果攻击者修改部分数据，伪装某一方参与认证，将无法通过验证，因为攻击者无法解决椭圆曲线离散对数问题（Elliptic Curve Discrete Logarithm Problem, ECDLP）。并且，认证完成后，密钥 K_i 都会进行更新。所以，协议能成功抵抗伪装攻击。

3.3.4 抵抗重放攻击

所谓的重放攻击是指攻击者在读卡器发出认证请求时，使用在前一次偷听获取到标签的消息，从而通过认证。在本协议中，攻击者通过侦听，可以获取上次通信中 R 发送给 T 的椭圆曲线的基点 G 和 T 发送给 R 的 (P_m, X, Y, P_i) ，并使用前次截获的 (P_m, X, Y, P_i) 传递给 R ，进而冒充 T 。但是， R 转发数据给 D 时，会发送本次认证过程中新选择的基点 G ，所以，认证不可能通过。因此，本协议成功抵抗重放攻击。

3.3.5 双向认证

在初始化阶段结束以后，后端数据库、读卡器和标签共享椭圆曲线方程，在消息的传递过程中，认证信息都嵌入到了椭圆曲线上，只有合法的标签和读卡器才能通过数据库的认证，也只有拥有正确的椭圆曲线方程的读卡器才能获得标签的认证。因

此，由上文的协议认证过程可知，服务器与标签的认证是相互的，只有双方的认证都通过了，才能认为协议认证成功。双向认证增强了认证的可靠性。

4 结语

本文将椭圆曲线加密与双线性对有机地结合，设计了读卡器参与下的一个 RFID 系统中标签和后端服务器之间的双向认证协议。经分析，该协议可以很好地保护数据安全和用户隐私。通过在安全性和性能两个方面的比较，本协议与之前的协议相比较，在保证性能的前提下，具有很好的安全性。

参考文献：

- [1] SARMA S E, WEIS S A, ENGELS D W. RFID systems and security and privacy implications [C]// Proceedings of the 4th International Work-shop on Cryptographic Hardware and Embedded Systems, LNCS 2523. Berlin: Springer-Verlag, 2003: 454–469.
- [2] SARMA S E, WEIS S A, ENGELS D W. Radio-frequency identification: secure risks and challenges [J]. Laboratories Cryptobytes, 2003, 6(1): 2–9.
- [3] WEIS S A, SARMA S E, RIVEST R L. Security and privacy aspects of low-cost radio frequency identification systems [M]. Berlin: Springer-Verlag, 2005: 201–212.
- [4] 袁署光, 戴宏跃, 赖声礼. 基于 Hash 函数的 RFID 认证协议 [J]. 计算机工程, 2008, 34(12): 141–143.
- [5] 李永磊, 黄照鹤, 鲁志波. EPCGen2 标准下安全的 RFID 认证协议 [J]. 计算机科学, 2010, 37(7): 115–117.
- [6] PERIS LOPEZ P, HERNANDEZ-CASTRO J C, TAPIADOR J M, et al. Weaknesses in two recent lightweight RFID authentication protocols [C]// Proceedings of Inscrypt 2009, LNCS 6151. Berlin: Springer-Verlag, 2009: 383–392.
- [7] HWU J S, CHEN R J, LIN Y B. An efficient identity-based cryptosystem for end-to-end mobile security [J]. IEEE Transactions on Wireless Communications, 2006, 5(9): 2586–2593.
- [8] KRISTIN E L, KATHERINE E S. The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences [EB/OL]. [2011-03-10]. <http://eprint.iacr.org/2008/099.pdf>.

（上接第 2673 页）

参考文献：

- [1] ASLANTAS V. An optimal robust digital image watermarking based on SVD using differential evolution algorithm [J]. Optics Communications, 2009, 282(5): 769–777.
- [2] 黄达人, 刘九芬, 黄继武. 小波变换域图像水印嵌入对策和算法[J]. 软件学报, 2002, 13(7): 1290–1297.
- [3] 陈森, 张兴周. 基于小波和伪随机变换的盲检测图像水印算法 [J]. 应用科技, 2007, 34(1): 24–27.
- [4] JOSEPH J K, RUANAIDH J J, THIERRY P. Rotation, scale, and translation invariant spread spectrum digital image watermarking [J]. Signal Processing, 1998, 66(3): 303–317.
- [5] LEE H Y, KIM H S, LEE H K. Robust image watermarking using local invariant features [J]. Optical Engineering, 2006, 45(3): 1–10.
- [6] 邓成, 高新波. 基于 SIFT 特征区域的抗几何攻击图像水印算法 [J]. 光子学报, 2009, 38(4): 1004–1010.
- [7] 单昊, 马坚伟, 杨慧珠. 自适应全尺度小波数字图像水印 [J]. 清华大学学报: 自然科学版, 2009, 49(5): 137–142.
- [8] 汪张昱, 廖铭, 陈丽亚, 等. 利用 DCT 域特征的 JPEG 图像数字水印及数字图像隐藏盲检测 [J]. 计算机应用与软件, 2008, 25(12): 271–277.
- [9] 韩亚丹, 闫德勤. 一种基于特征的抗剪裁盲水印算法 [J]. 中国图象图形学报, 2007, 12(4): 574–584.
- [10] LOWE D G. Distinctive image features from scale-invariant keypoints [J]. International Journal of Computer Vision, 2004, 60(2): 91–110.
- [11] 曲巨宝. 基于改进 CAMSHIFT 的多场景接力跟踪 [J]. 重庆师范大学学报: 自然科学版, 2010, 27(6): 69–72.
- [12] HARRIS C, STEPHENS M. A combined corner and edge detector [EB/OL]. [2010-01-01]. <http://www.bmva.org/bmvc/1988/avc-88-023.pdf>.
- [13] 路玲, 孙新德. 基于图像子块 DCT 系数对的盲检测数字水印 [J]. 郑州大学学报: 工学版, 2010, 31(2): 106–108.
- [14] 暴琳, 张尤赛. 基于 DCT 域的自适应图像数字水印盲检测算法 [J]. 信息安全与通信保密, 2005(3): 139–141.
- [15] 景丽, 肖慧敏. 基于 SIFT 特征的小波域数字图像鲁棒水印方法 [J]. 计算机应用研究, 2009, 26(2): 765–774.