



一种适用于 NFC 移动设备的双向认证安全方案

张呈钰¹, 王让定¹, 姚灵², 傅松寅¹, 左富强²

(1. 宁波大学信息科学与工程学院, 浙江 宁波 315211;

2. 宁波水表股份有限公司, 浙江 宁波 315032)

摘要: 近场无线通信 (NFC) 是一种已经被广泛应用的短距无线通信技术。其中最常见的是将 NFC 技术应用于移动支付和门禁访问控制等应用。从技术上讲, 这些应用利用 NFC 模拟卡模式将 NFC 设备模拟成银行卡或门禁卡, 然后等待外部阅读器验证。在这类应用场景下, 选取合适的安全认证方案是非常重要的。首先, 介绍了现有的 NFC 认证系统和安全方案并分析了系统安全需求和潜在的安全风险。然后, 采用 Hash、AES 和口令 *Key* 动态更新机制, 提出了一种适用于 NFC 移动设备的双向认证安全方案, 并设计了自同步机制。最后, 利用 GNY 逻辑以形式化证明的形式证明了方案的安全性, 分析表明该方案能解决伪造、重放攻击、窃听、篡改、异步攻击等安全问题。

关键词: 近场无线通信; 双向认证; 安全; 移动设备

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2017178

A mutual authentication security scheme for mobile NFC devices

ZHANG Chengyu¹, WANG Rangding¹, YAO Ling², FU Songyin¹, ZUO Fuqiang²

1. College of Information Science and Engineering, Ningbo University, Ningbo 315211, China

2. Ningbo Water Meter Co., Ltd., Ningbo 315032, China

Abstract: Near field communication (NFC) is a kind of short-range wireless communication technology which has been applied around the world. The applications of mobile payments and access control are the most common applications of NFC technology. Technically, the NFC device can be used as a bank card or an entrance card with the help of the card emulation mode of NFC, which will be validated by external reader. It is very essential to select a appropriate and safe certification scheme in this scenario. First of all, the existing NFC authentication system and security scheme was introduced and the system security requirements and potential security risks were analyzed. Then, by using Hash, AES and password *Key* dynamic updating mechanism, a mutual authentication security scheme for mobile NFC devices was proposed, and the synchronization mechanism was designed. Finally, GNY logic was used to prove the security correctness of our proposed scheme. The security analysis shows that our scheme can avoid a number of attacks, such as forgery, replay attack, eavesdropping, tampering attack, asynchronous attack and so on.

Key words: near field communication, mutual authentication, security, mobile device

收稿日期: 2017-01-22; 修回日期: 2017-06-04

基金项目: 国家自然科学基金资助项目 (No.61672302); 浙江省重中之重学科资助项目 (No.XKXL1509); 宁波市科技局产业技术创新及成果产业化重点资助项目 (No.2013B10034); 宁波市智能水表与测控技术科技创新团队项目

Foundation Items: The National Natural Science Foundation of China (No.61672302), The Key Subject Program of Zhejiang Province (No.XKXL1509), Innovation and Industrialization Key Program of Science Technology Department of Ningbo (No.2013B10034), Project of Ningbo Intelligent Water Meter and Measurement and Control Technology of Science and Technology Innovation Team



1 引言

近场无线通信 (near field communication, NFC) 技术是一种短距高频的无线电技术, 具有距离近、带宽高、能耗低、安全性高等特点。从本质上说 NFC 是在无线射频识别 (radio frequency identification, RFID) 的基础上发展而来, 是一种 RFID 的演进技术。随着智能设备的不断升级换代, 目前很多移动设备都具备 NFC 功能。移动设备和 NFC 技术的结合促使 NFC 技术从学术向应用发展, 促进了许多应用的产生, 如服务发现、移动支付、票务、门禁访问控制等。移动设备可以利用 NFC 模拟卡技术取代传统的 RFID 标签, 在设备内部生成银行卡、门禁卡、电子票等电子标签, 这样可以免去用户同时携带多个标签的麻烦, 用户只需一部移动设备, 如手机, 就可以达到支付、验证、开门的目的。传统 RFID 标签由于硬件结构、计算能力、存储空间等物理限制和成本制约, 大多采用基于逻辑运算的轻量级安全认证方案和基于 Hash 函数的安全认证协议, 很少采用基于对称加密算法或公钥加密算法的重量级安全认证方案。而移动设备集合了计算、控制、显示、联网等功能, 不仅具备强大的计算能力和通信能力, 还简化了智能硬件结构的设计与实现, 可以轻易实现传统 RFID 标签不能实现的加密算法, 进而提高系统的安全性能和抗攻击能力。

2 现有的安全认证技术

2.1 传统的 RFID 认证系统

传统 RFID 认证系统一般由 3 个部分组成:

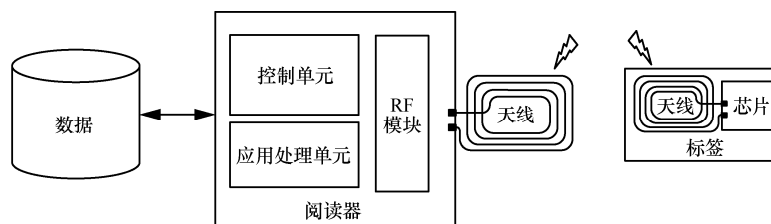


图1 传统 RFID 认证系统

阅读器、标签和后端数据库, 如图 1 所示。阅读器包括应用处理单元、RF 模块、控制逻辑单元和天线, 标签包括一定计算能力和存储能力的芯片和天线。由于受到计算、存储以及成本的限制, 一般标签仅采取简单的安全手段。而与标签相比, 读写器拥有更好的存储能力和处理计算能力, 通常可提供较好的安全解决方案^[1]。后端数据库主要用于存储和管理 RFID 标签及其相关信息, 可以部署在阅读器中, 也可以作为 RFID 应用系统的服务器独立开来。由于阅读器和后端数据库均具有强大的计算能力和存储能力, 可执行高级加密算法, 因此二者之间的通信通常认为是安全的, 可以看作是一个整体。而标签和阅读器间由于无线传输、资源受限等因素, 使得二者之间的信息传输容易受到外部干扰和恶意攻击, 存在严重的安全隐患。因此这里主要讨论标签和阅读器间的安全认证方案。

该系统的安全认证方案为三轮认证, 如图 2 所示。在阅读器发起访问后, 标签生成随机数 B 发送至阅读器; 阅读器利用简单的逻辑运算根据 B 计算出一个计算值, 再生成随机数 A 一起发给标签; 标签收到后校验 B 的计算值, 验证通过后利用同样的计算方法计算出 A 的计算值和自身 ID 一起返回至阅读器, 阅读器验证返回值, 通过则完成一次认证, 反之拒绝响应。目前许多 RFID 系统认证协议都是在三轮认证模型的基础上设计的, 研究者对认证消息的构造方式、加密函数的选择以及认证次序的设计等做了不同的研究, 由此提高认证方案的安全性和完整性, 并出现了许多不同类型的认证协议。

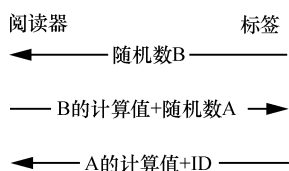


图2 传统RFID认证方案

2.2 其他相关工作

一个比较完善的认证系统安全解决方案需要具备机密性、完整性、可用性、真实性和隐私性等安全需求^[2]。而传统RFID认证方案的安全问题根源在于标签验证信息的唯一性和数据的易获得性。标签和阅读器之间的信息交互，是以明文或经简单加密的形式传输的，极易被截取。而对于系统商来说，密码及加密算法都是透明的，因为标签缺乏合理的反认证机制，无法认证阅读器的合法性。进而导致系统非常脆弱，容易受到多种安全攻击，如篡改标签、欺骗攻击、窃听攻击或异步攻击等。因此，许多研究学者基于密码技术提出了认证系统的安全协议和认证方案。典型的加强安全隐私保护的访问控制方法主要是基于单向Hash函数实现的，比如Hash锁、随机Hash锁和Hash链。也有很多论文分析了这3种方法的优缺点，如参考文献[3-5]均提到Hash锁方法，由于ID是静态的且阅读器和标签间传输的数据未经加密，因此存在追踪攻击隐私问题，窃听者可以轻易地获得标签信息；随机Hash锁方法和Hash链方法必须穷举所有记录空间，计算开销大，系统时延长，不适合标签数目较多的情况。

另外，伪随机序列也被应用到许多安全协议中。如参考文献[6]只使用按位异或和几个特殊的伪随机数构造器设计了超轻量级的安全认证协议。参考文献[7]采用部分ID、CRC校验以及ID动态更新的方法，在认证过程中随机截取不同长度的两个子ID用于认证，然而这类方法没有解决伪造、罗列攻击等问题。而参考文献[8,9]采用对称加密技术保证传输信息无法被攻击者破解，但是由于参考文献[8]加密内容依然固定，输出加密值也依然固定，

攻击者可以通过固定加密值跟踪用户的物理位置。参考文献[9]每次验证需要为每一条记录计算一次会话密钥。参考文献[10]针对NFC应用程序提出了一个使用假名方式的保护隐私安全协议，并分析了该协议能够承受各种类型的攻击，而参考文献[11]证明了该方案不能抵挡伪造攻击。

综上所述，这些方法都或多或少地存在安全性隐患以及需要穷举数据库所有记录，从而导致验证效率低的问题。

3 安全认证方案

3.1 安全性方案设计原则

认证协议设计需要符合以下几个具体原则^[12]。

- 不能未加保护传输敏感参数。如果敏感参数未加任何保护就传输，会泄露标签用户的隐私，攻击者也很容易追踪设备或发动仿冒攻击。
- 每轮认证响应信息之间不存在相关性。如果同一个标签对于相同的挑战，每次的响应都是相同的或相关的，那么攻击者就可以通过向标签发送相同的挑战来追踪某个标签。
- 为了防止重放攻击和仿冒攻击，变动信息应该由读写器和标签共同提供。
- 数据更新应同步。数据库应当存储足够信息或设置合理的数据更新条件，以保证数据同步，防止异步攻击。不少协议都是因为标签和后端数据库没有一致更新共享信息，而导致数据不同步。
- 硬件运算能力、运算时间。良好的安全协议需要权衡安全隐私保护与成本之间的问题。

3.2 安全认证方案设计

为便于描述，这里以具备NFC功能的手机为例作为认证系统中的移动设备，由手机生成电子标签替代传统的RFID标签。由于手机具有较强的计算能力和计算速度，普通标签无法完成的重量级加解密算法在手机端可以轻易实现。



3.2.1 设计思路

基于询问应答机制,充分利用阅读器的计算能力,设计了一种双向认证的安全协议,阅读器对手机的认证分两步完成,而手机对阅读器的认证仅需一步。加入口令 Key 值自动更新机制,使得保证每次验证信息变化以防止恶意追踪、重放或伪造验证信息。因为用户数据存储位置与 ID 相关,为了加快用户比对速度固定 ID 值,阅读器验证手机时需要 ID 信息,所以采用 $Hash$ 和 AES 加密方式将 ID 等验证信息加密后传输,以防窃听攻击。双方均认证用过后,阅读器最后更新记录的 Key 值和 H 值,从而防止异步攻击。

一种适用于 NFC 移动设备的双向认证安全方案如图 3 所示,表 1 列出了部分运算标识的含义。 MK 是由阅读器生成的 128 位用于 AES 加密的密钥,每个阅读器的 MK 值不能重复,初始阶段电

子标签注册时阅读器写入标签内。阅读器端数据库中每条记录除用户信息外保存 $\{H, Key, ID\}$ 字段信息,手机内电子标签保存 $\{ID, Key\}$ 字段。

表 1 运算标识说明

符号	含义
$\oplus$	异或运算
$Hash()$	单向散列函数
$ENC_{MK}()$	加密
$DEC_{MK}()$	解密
$\parallel$	连接

3.2.2 初始阶段

(1) 阅读器或管理端生成 128 位密钥 MK 用于在安全认证和数据交换过程中的加解密算法。

(2) 用户注册时,阅读器或管理端生成唯一的用户设备标识 ID 和初始 Key 值,连同密钥 MK 一起写入手机内,根据 ID 计算得到该用户数据在

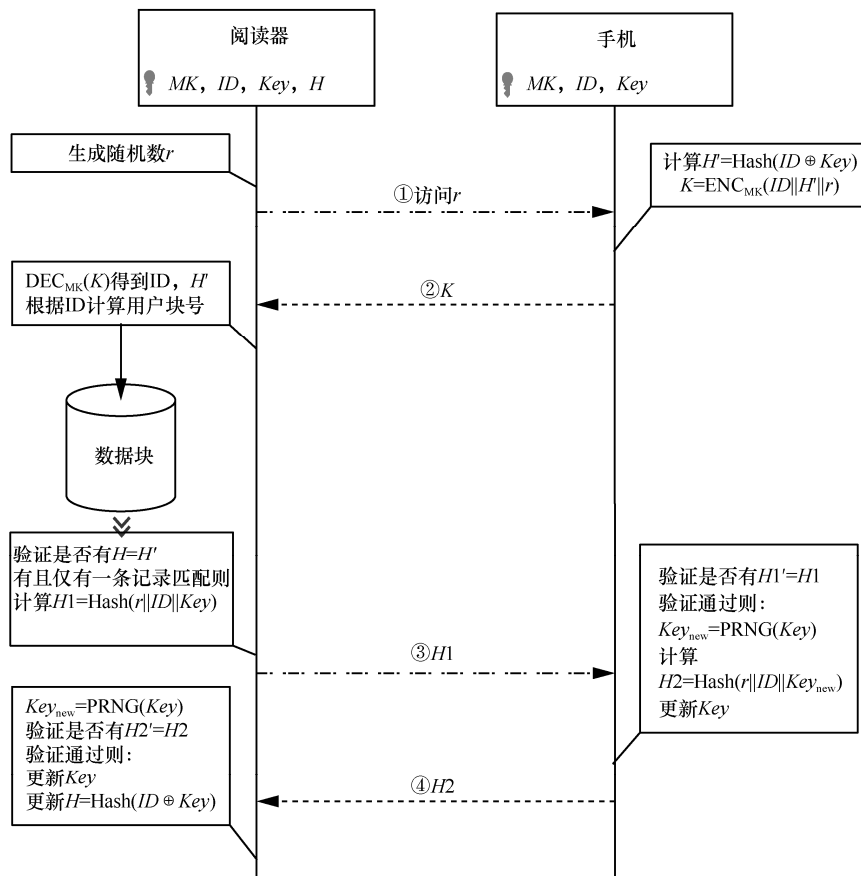


图 3 一种适用于 NFC 移动设备的双向认证安全方案

数据库内的存储位置,形成ID和所属用户块号的映射关系。

(3) 阅读器或管理端计算初始 H 值,
 $H = \text{Hash}(ID \oplus \text{Key})$ 。

3.2.3 认证过程

(1) 阅读器检测到手机后生成随机数 r , 并将其发送至手机。

(2) 手机计算 H' 和 K 值。

- 首先计算 $ID \oplus \text{Key}$, 经 Hash 运算后得到 H' 。
- $K = \text{ENC}(ID \| H' \| r)$, 连接 ID、 H' 和 r 得到一串数据, 经过 AES 加密得到 K 值。这里选取 MK 作为 AES 加密/解密密钥。
- 手机发送 K 值至阅读器。

(3) 阅读器得到 K 值后使用 MK 进行 AES 解密, 得到手机发送过来的 ID 和 H' 。根据 ID 计算得到所属用户块号, 然后按照图 4 所示的阅读器端用户比对流程进行用户比对, 比对结果如下。

- 按照 H' 比对该用户块内每条记录, 是否有记录的 $H=H'$, 如果有且仅有一条记录满足 $H=H'$, 并且接收 ID 与这条记录的 ID 相等, 则继续后续的验证步骤。
- 没有任何记录满足匹配条件, 则结束本次验证。
- 有多条记录满足 $H=H'$, 则继续比对接接收 ID 与这些记录的 ID 是否相等。没有则结束认证, 仍有多条相等则返回第一步重新验证, 只有一条满足则继续下一步认证。

用户比对通过后, 阅读器计算 $H1 = \text{Hash}(r \| ID \| \text{Key})$ 。连接 r 、ID 和 Key 后, 经过 Hash 运算后得到 $H1$, 发送 $H1$ 到手机端。

(4) 手机自行计算 $H1' = \text{Hash}(r \| ID \| \text{Key})$, 验证 $H1'$ 是否等于接收到的 $H1$, 相等则手机通过对阅读器的验证, 反之则拒绝后续响应。验证通过后, 手机端执行以下操作。

- 计算新的 Key 值, $\text{Key}_{\text{new}} = \text{PRNG}(\text{Key})$ 。旧 Key 作为随机数生成因子, 得到新的 Key

值。PRNG 为单向随机数发生器, 具有不可逆性。参考文献[13]提出了基于单向函数迭代构建伪随机数生成器, 本文中随机数输出为 Key_{new} , 定义 $G_0(\text{Key})$ 为第一个随机数输出, $G_1(\text{Key})$ 为下一个输出随机数。

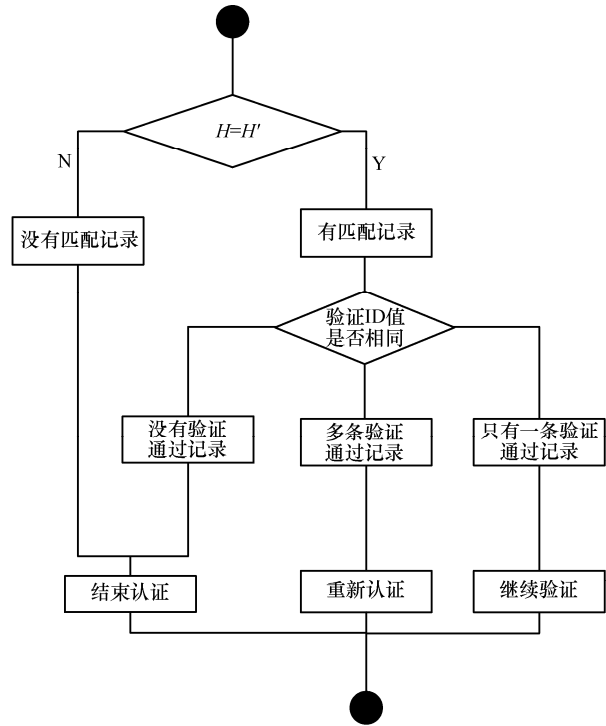


图4 阅读器端用户比对流程

假设单向函数 $f_{\text{Key}}: \{0,1\}^t \rightarrow \{0,1\}^n$, 其中 n 为 Key 的位数, t 为迭代次数, 则有:

$$f_{\text{Key}}(t) = G_t(\text{Key}) = (G_{t-1}(\dots(G_1(G_0(\text{Key})))) \quad (1)$$

所以伪随机函数 $F_n = \{f_{\text{Key}}\}_{|\text{Key}|=n}$, 其中, 单向函数的性质和生成因子的长度决定了 PRNG 的可实现性和安全性^[14]。

- 计算 $H2 = \text{Hash}(r \| ID \| \text{Key}_{\text{new}})$ 。

- 发送 $H2$ 至阅读器端。

(5) 阅读器接收到 $H2$ 后, 执行以下操作。

- 自行计算新的 Key 值, $\text{Key}_{\text{new}} = \text{PRNG}(\text{Key})$ 。
- 计算 $H2' = \text{Hash}(r \| ID \| \text{Key}_{\text{new}})$, 验证 $H2'$ 是否等于 $H2$ 。
- 验证通过则更新 Key 值和 H 值, $H = \text{Hash}(ID \oplus \text{Key})$, 验证不通过则拒绝响应, 不做更新。



虽然理论上 Hash 具有较强的抗冲突性, 很难找出任意两条消息 x 、 y , 使 $\text{Hash}(x)=\text{Hash}(y)$ 。但是实际上仍有一定的几率出现 x 、 y 不相等, 但 Hash 值相等的情况, 为了以防万一并避免重放或伪造认证标记的可能, 确保系统的安全性和顽健性, 所以建议采用如图 4 所示的比对流程。即在用户所属用户块内依次对比数据库中的 H 字段, 有且仅有一条匹配时, 本环节认证通过; 当没有匹配记录, 判定认证失败; 而如果有多条记录匹配时, 重新发起认证。

4 安全性研究

结合第 2 节分析的认证系统的安全需求, 将详细介绍针对适用于 NFC 移动设备的认证系统设计的安全认证方案。采用经典的形式化方法 GNY 逻辑对设计的认证方案进行详细的逻辑化分析和证明, 并对其安全性能进行了分析。

4.1 形式化分析和证明

因为安全协议的经典分析方法 GNY 逻辑的使用范围更加广泛, 减少了一些假设, 能够被用来分析一些使用单向函数的加密协议。所以在此使用 GNY 逻辑对上述安全认证方案进行形式化分析。表 2 列出了证明中需要用到的 GNY 逻辑符号含义及基本语法。

表 2 GNY 逻辑符号含义及基本语法

符号	含义
(X, Y)	X 连接 Y
$*X$	非起始于 X
$P \ni X$	P 拥有 X
$P \triangleleft X$	P 收到 X
$P \vdash X$	P 曾经发送 X
$P \models \#X$	P 相信 X 是新鲜的
$P \models \phi(X)$	P 相信 X 是可以识别的
$\{X\}_K$ 和 $\{X\}_K^{-1}$	传统对称密钥加密、解密
$P \xrightarrow{K} Q$	P 和 Q 共享密钥 K

GNY 逻辑推理规则具体可参考文献[15],

在此仅在图 5 中列出以下证明过程中主要使用的规则。

	$T1: \frac{P \triangleleft *X}{P \triangleleft X}$
接收规则:	$T3: \frac{P \triangleleft \{X\}_K, P \ni K}{P \triangleleft X}$
消息解析规则:	$I1: \frac{P \triangleleft \{X\}_K, P \ni K, P \models P \xrightarrow{K} Q, P \models \phi(X), P \models \#(X, K)}{P \models Q \vdash X, P \models Q \vdash \{X\}_K, P \models Q \ni K}$
	$F1: \frac{P \models \#(X)}{P \models \#(X, Y), P \models \#(F(X))}$
新鲜性规则:	$F10: \frac{P \models \#(X), P \ni X}{P \models \#(H(X, Y))}$
	$R1: \frac{P \models \phi(X)}{P \models \phi(X, Y), P \models \phi(F(X))}$
可识别规则:	$R5: \frac{P \models \phi(X), P \ni X}{P \models \phi(H(X))}$
	$R6: \frac{P \ni H(X)}{P \models \phi(X)}$

图 5 GNY 逻辑推理

(1) 形式化模型

首先, 将所设计的认证方案中每一步的交换信息列于下方, R 表示阅读器, T 表示手机 (电子标签)。

Msg1 $R \rightarrow T: r$

Msg2 $T \rightarrow R: \{ID \| H(ID \oplus Key) \| r\}_{MK}$

Msg3 $R \rightarrow T: H(ID \| r \| Key)$

Msg4 $T \rightarrow R: H(ID \| r \| Key_{new})$

为便于使用 GNY 逻辑分析, 将上述交换信息转换成形式化模型。

Msg1 $T \triangleleft *r \rightsquigarrow R \models \#r$

Msg2 $R \triangleleft * \{ID \| H(ID \oplus Key) \| r\}_{MK} \rightsquigarrow T \models R \ni MK$

Msg3 $T \triangleleft * H(ID \| r \| Key) \rightsquigarrow R \models R \xrightarrow{Key, r} T, R \models T \phi(H())$

Msg4 $R \triangleleft * H(ID \| r \| Key_{new}) \rightsquigarrow T \xrightarrow{Key} R, T \models R \phi(H())$

(2) 初始化假设和证明目标

初始化假设 $A1$ 、 $A2$ 是阅读器 R 拥有, $A6 \sim A8$

是手机(电子标签) T 拥有, A3、A4 是 R 对拥有信息新鲜性相信, A7 是 T 对拥有信息新鲜性相信, A5 和 A9 是 T 与 R 彼此相信共享密钥 MK、Key, R 可以相信 r 是 T 与 R 的秘密信息, 具体假设如图 6 所示。

A1 $R \ni \text{MK}, \text{ID}, \text{Key}$	A2 $R \ni H(\text{ID} \oplus \text{Key})$
A3 $R \models \#(r)$	A4 $R \models \#(\text{Key}), \#(\text{Key}_{\text{new}})$
A5 $R \xrightarrow{\text{MK}, \text{Key}, r} T$	A6 $T \ni \text{ID}, \text{Key}, \text{MK}$
A7 $T \models \#(\text{Key})$	A8 $T \ni H(\text{ID} \oplus \text{Key})$
A9 $T \xleftarrow{\text{MK}, \text{Key}} R$	

图 6 初始化假设

本方案的证明目标为交互双方对交互信息的新鲜性的相信, 主要有 3 个, 分别为:

$$\text{G1: } R \models T \sim \#(\{ \text{ID} \| H(\text{ID} \oplus \text{Key}) \| r \}_{\text{MK}}) \quad (2)$$

$$\text{G2: } T \models R \sim \#(H(\text{ID} \| r \| \text{Key})) \quad (3)$$

$$\text{G3: } R \models T \sim \#(H(\text{ID} \| r \| \text{Key}_{\text{new}})) \quad (4)$$

(3) 证明过程

① 证明目标 G1: $R \models T \sim \#(\{ \text{ID} \| H(\text{ID} \oplus \text{Key}) \| r \}_{\text{MK}})$

因为 Msg2 和 A5 已知, 又根据拥有规则假设 A1 和 P3 可知 $R \ni \text{MK}$, $R \ni \text{ID}$, $R \ni \text{Key}$ 。所以根据消息解析规则 I1 可知, 要证 G1 即证:

$$\text{G1.1: } R \models \varphi(\text{ID} \| H(\text{ID} \oplus \text{Key}) \| r) \quad (5)$$

$$\text{G1.2: } R \models \#((\text{ID} \| H(\text{ID} \oplus \text{Key}) \| r), \text{MK}) \quad (6)$$

因为 A2: $R \ni H(\text{ID} \oplus \text{Key})$, 根据可识别规则 R6 可得:

$$R \models \varphi(\text{ID} \oplus \text{Key}) \quad (7)$$

又根据式 (7) 和 R5 可得:

$$R \models \varphi(H(\text{ID} \oplus \text{Key})) \quad (8)$$

再根据式 (8) 和 R1 可得 $R \models \varphi(\text{ID}, H(\text{ID} \oplus \text{Key}), r)$, 即目标 G1.1 实现。

阅读器 R 接收到 T 发送的 Msg2, 根据 T1 可知 $R \triangleleft \{ \text{ID} \| H(\text{ID} \oplus \text{Key}) \| r \}_{\text{MK}}$, 因为 $R \ni \text{MK}$, 所以 R 得到 $\text{ID} \| H(\text{ID} \oplus \text{Key}) \| r$, R 只需要验证 $\#(H(\text{ID} \oplus \text{Key}))$, 验证通过则目标 G1.2 实现, 否则结束验证。因为假设 A3、A4 及 F1, 可得:

$$R \models \#(\text{ID} \oplus \text{Key}) \quad (9)$$

再根据式 (9) 和 F10 可得:

$$R \models \#(H(\text{ID} \oplus \text{Key})) \quad (10)$$

再由式 (10) 和 F1 可得 $R \models \#(\text{ID}, H(\text{ID} \oplus \text{Key}), r)$, MK), 即目标 G1.2 实现。

至此, 目标 G1 证明完毕。

② 证明目标 G2: $T \models R \sim \#(H(\text{ID} \| r \| \text{Key}))$

首先, 因为初始化假设 A7: $T \models \#(\text{Key})$ 和 F1 可知:

$$T \models \#(\text{ID}, r, \text{Key}) \quad (11)$$

在 Msg1 中, $T \triangleleft *r$, 即 $T \ni r$, 结合假设 A6 和规则 P2 可知:

$$T \ni (\text{ID}, r, \text{Key}) \quad (12)$$

其次, 已知式 (11)、式 (12), 根据 F10 可知:

$$T \models \#(H(\text{ID}, r, \text{Key})) \quad (13)$$

最后, 根据 Msg3、A9、式 (12)、式 (13) 和 I3 可以得到:

$$T \models R \sim (H(\text{ID}, r, \text{Key})) \quad (14)$$

由新鲜性的定义可得目标 G2: $T \models R \sim \#(H(\text{ID} \| r \| \text{Key}))$ 。

③ 证明目标 G3: $R \models T \sim \#(H(\text{ID} \| r \| \text{Key}_{\text{new}}))$

R 在收到 Msg4 后, 会生成新的 Key, 即:

$$R \ni \text{Key}_{\text{new}} \quad (15)$$

计算 $(\text{ID} \| r \| \text{Key}_{\text{new}})$ 的 Hash 值, 再与接收到的值比对, 一致则验证通过更新 Key 值和 H 值, 负责验证失败, 数据不做更新。所以 G3 与证明 G2 类似, 因为初始化假设 A4: $R \models \#(\text{Key}_{\text{new}})$ 和 F1 可知:

$$R \models \#(\text{ID}, r, \text{Key}_{\text{new}}) \quad (16)$$

根据式 (15) 和假设 A1 可得:

$$R \ni (\text{ID}, r, \text{Key}_{\text{new}}) \quad (17)$$

其次, 已知式 (16)、式 (17), 根据 F10 可知:

$$R \models \#(H(\text{ID}, r, \text{Key}_{\text{new}})) \quad (18)$$

最后, 根据 Msg4、A5、式 (17)、式 (18)



和 I3 可以得到 $R \equiv T \sim (H(ID, r, Key_{new}))$ ，由新鲜性的定义可得目标 G3: $R \equiv T \sim \#(H(ID \| r \| Key_{new}))$ 。

4.2 安全性分析

在 NFC 认证系统应用中，攻击者可以在任意时间对验证信息进行窃听、伪造、篡改、重放、阻塞等操作。下面针对这些常见的攻击，分析设计的认证方案的安全性。

(1) 伪造攻击

攻击者伪装成合法的手机（电子标签）试图通过验证时，阅读器检测到附件的设备信息，发出访问命令和随机数 r ，攻击者必须同时知道加密密钥 MK、设备 ID 和本轮验证 Key 值，三者缺一不可。由于这些值均经过加密后传输，攻击者很难计算得到正确的验证信息 K ，阅读器因此会拒绝响应。

(2) 重放攻击

在一轮合法的验证过程中，攻击者记录下了手机（电子标签）的响应数据，试图在下次认证中再次发送记录的响应数据给阅读器，就会发生重放攻击。在本安全认证方案中，每轮验证都会产生新的随机值 r 和新的 Key 值，如果重放上一轮的记录阅读器会识别出 r 值不同，由于 Key 的变化也找不到匹配的记录。因此本方案能保证对重放攻击具有安全性。

(3) 窃听攻击

攻击者试图通过窃听验证信息以破解加密信息从而得到原始信息时，由于阅读器和手机间的安全认证信息都采用了 Hash 算法和 AES 加密，

由于 Hash 函数具有单向性和 AES 加密的高度安全性，目前攻击者很难破解该算法得到原始信息。

(4) 对手机（电子标签）发动攻击

攻击者伪装成合法的阅读器试图篡改手机（电子标签）内的值时，首先发送访问和一个随机数 r ，随后获的手机的响应： $K = ENC_{MK}(ID \| H \| r)$ ，攻击者需要产生 $H_1 = Hash(r \| ID \| Key)$ ，由于 ID 未知并且 Key 值动态更新，电子标签对阅读器的验证失败，不会更新 Key 值。另外，即使攻击者通过各种手段得到破解密钥，解密出 ID、H 和 r 值，也无法验证通过。因为阅读器端是按照 H 值进行用户比对，H 值跟 Key 值有关，Hash 函数具有单向性，每轮 Key 都会更新，所以阅读器在数据库内找不到匹配用户，验证失败。因此可以抵抗对手机（电子标签）发动的攻击。

(5) 异步攻击

攻击者通过阻塞阅读器的访问，使得阅读器端 Key 已更新而真正的电子标签的 Key 未更新，会产生合法用户被拒绝服务的问题，因此需要防止出现阅读器和电子标签的 Key 不同步的情况。阅读器对电子标签的验证分成两步，第一步验证电子标签的 ID、Key 和 MK 的正确性，第二步验证电子标签是否能生成合法的新 Key，只有两步认证都通过后，才更新数据库中的 Key。结合上述第 4 点分析的电子标签的 Key 值更新机制，从而防止异步攻击的可能。

表 3 根据手机/标签(T)和阅读器+服务器(S)

表 3 同类的双向认证协议性能对比

协议	手机/标签 (T)	阅读器+服务器 (S)	搜索时间	交互回合	存储 T/S	通信 T+S
参考文献[1]	$3r+2RSA$	$2r+2RSA$	$T(n)$	5	$4l/2l$	$3l+3l$
参考文献[2]	$2h+r$	$n \times h+r$	$T(n)$	5	$1l/2l$	$2l+4l$
参考文献[5]	$5r$	$6r$	$T(2n)$	5	$3l/6l$	$3l+4l$
参考文献[6]	$4r+4CRC$	$3r+4CRC$	$T(2n)$	3	$2l/6l$	$5l+2l$
本文	$1AES+3h+r$	$1AES+3h+r$	$T(\frac{n}{m})$	4	$3l/4l$	$4l$

其中， h 表示单向 Hash 函数， r 表示随机数， n 表示标签数量， m 表示用户块数量，CRC 表示循环冗余校验， l 表示 ID 的长度或 Hash 输出的长度，RSA 表示公钥加密算法，AES 表示高级加密算法。

端的计算需求、存储需求、一次用户比对搜索时间、交互回合以及通信数据量 6 个方面对比了同类双向认证协议,可以看出,参考文献[1]中 T 和 S 间的计算量和通信数据量较大,而参考文献[2]虽然存储需求很小,但由此造成在每次认证时,服务器要对每一个标签计算一次 Hash,和其他协议相比,该协议计算量大且计算时间较长。参考文献[5,6]在设计协议时为了防止异步攻击,数据库里都保存了上一轮的认证信息,当最新的认证信息字段都无法与认证用户相匹配时,系统将依次对比上一轮的认证信息字段,所以对设备的存储空间要求比较高,相应地导致最坏情况下需要搜索 $2n$ 次。而本文设计的协议因为没有采用同时保存新 Key、新 H、旧 Key 和旧 H 的机制,减少了用户记录长度,节省了阅读器和手机的存储空间,也缩短了一次用户比对的搜索时间。

5 结束语

通过对射频认证系统安全需求和安全风险分析,结合基于重命名的方法和基于密码学的方法提出了一种适用于 NFC 移动设备的双向认证安全方案。该方案采用询问应答机制,充分利用 NFC 移动设备的计算存储能力,并引入口令 Key 动态更新机制改变电子标签响应读写器的方式,使其每次返回不同的数据,实现阅读器和具备 NFC 功能的移动设备的双向认证,而密码学的方法保证了电子标签数据不被非法获取。这种方案适用于多用户和需要快速验证的 NFC 认证系统。最后还利用经典的形式化方法理论证明并分析了该方案的安全性。

参考文献:

- [1] CHENG H C, LIAO W W, CHI T Y, et al. A secure and practical key management mechanism for NFC read-write mode[C]// 13th International Conference on Advanced Communication Technology (ICACT2011), February 13-16, 2011, Seoul, South Korea. [S.l.:s.n.], 2011: 1095-1111.
- [2] 丁振华, 李锦涛, 冯波, 等. 基于 Hash 函数的 RFID 安全认证协议研究[J]. 计算机研究与发展, 2009, 46(4): 583-592.

- DING Z H, LI J T, FENG B, et al. Research on Hash-based RFID security authentication protocol[J]. Journal of Computer Research and Development, 2009, 46(4): 583-592.
- [3] 曾丽华, 熊璋, 张挺, 等. Key 值更新随机 Hash 锁对 RFID 安全隐私的加强[J]. 计算机工程, 2007, 33(3): 151-153.
- ZENG L H, XIONG Z, ZHANG T, et al. Key Value renewal random hash lock for security and privacy enhancement of RFID[J]. Computer Engineering, 2007, 33(3): 151-153.
- [4] 周世杰, 张文清, 罗嘉庆, 等. 射频识别(RFID)隐私保护技术综述[J]. 软件学报, 2015, 26(4): 960-976.
- ZHOU S J, ZHANG W Q, LUO J Q, et al. Design and analysis of cryptographic protocols for RFID[J]. Chinese Journal of Computers, 2007, 33(3): 151-153.
- [5] 钱萍, 吴蒙. 一种基于 Hash 函数的 RFID 安全认证方法[J]. 电信科学, 2011, 27(10): 109-112.
- QIAN P, WU M. A security RFID authentication method based on Hash function[J]. Telecommunications Science, 2011, 27(10): 109-112.
- [6] NIU B, ZHU X, CHI H, et al. Privacy and authentication protocol for mobile RFID systems[J]. Wireless Personal Communications, 2014, 77(3): 1713-1731.
- [7] 张辉, 侯朝焕, 王东辉, 等. 一种基于部分 ID 的新型 RFID 安全隐私相互认证协议[J]. 电子与信息学报, 2009, 31(4): 853-856.
- ZHANG H, HOU Z H, WANG D H, et al. A new security and privacy on RFID mutual authentication protocol based on partial ID[J]. Journal of Electronics & Information Technology, 2009, 31(4): 853-856.
- [8] FELDHOFFER M, DOMINIKUS S, WOLKERSTORFER J. Strong authentication for RFID systems using the AES algorithm[C]//Cryptographic Hardware and Embedded Systems(CHES 2004), August 11-13, 2004, Cambridge, MA, USA. [S.l.:s.n.], 2004: 357-370.
- [9] BADRA M, BADRA R B. A lightweight security protocol for NFC-based mobile payments[J]. Procedia Computer Science, 2016(83): 705-711.
- [10] EUN H, LEE H, OH H. Conditional privacy preserving security protocol for NFC applications[J]. IEEE Transactions on Consumer Electronics, 2013, 59(1): 153-160.
- [11] HE D, KUMAR N, LEE J H. Secure pseudonym-based near field communication protocol for the consumer internet of things[J]. IEEE Transactions on Consumer Electronics, 2015, 61(1): 56-62.
- [12] 李杰. RFID 安全认证协议研究与设计[D]. 西安: 西安电子科技大学, 2012.
- LI J. Research and design on RFID security authentication protocol[D]. Xi'an: Xidian University, 2012.
- [13] GOLDREICH O, GOLDWASSER S, MICHALI S. How to construct random functions[J]. Journal of the ACM, 1986, 33(4): 792-807.
- [14] 高树静, 曲英杰, 宋廷强. 基于单向函数的伪随机数发生器[J]. 计算机研究与发展, 2015, 52(6): 1394-1399.
- GAO S J, QU Y J, SONG T Q. Pseudorandom number generators based on one-way functions[J]. Journal of Computer Research and Development, 2015, 52(6): 1394-1399.



search and Development, 2015, 52(6): 1394-1399.

- [15] LI G, NEEDHAM R, YAHALOM R. Reasoning about belief in cryptographic protocols[C]//IEEE Symposium on Security & Privacy, May 7-9, 1990, Oakland, CA, USA. New York: IEEE Computer Society, 1990: 234-248.

[作者简介]



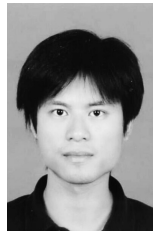
张呈钰（1992-），女，宁波大学信息科学与工程学院硕士生，主要研究方向为 NFC 应用、智能仪器仪表。



王让定（1962-），男，博士，宁波大学信息科学与工程学院教授、博士生导师，主要研究方向为多媒体通信与取证、信息安全、智能抄表及传感网络技术等。



姚灵（1953-），男，宁波水表股份有限公司技术总监、教授级高级工程师兼任中国计量协会水表工作委员会副秘书长，主要研究方向为流量仪表与精密仪器。



傅松寅（1982-），男，宁波大学信息科学与工程学院博士生、助理研究员，主要研究方向为无线传感网络、智能抄表。



左富强（1982-），男，宁波水表股份有限公司高级工程师，主要研究方向为智能水流量仪表及嵌入式系统。