非接触式智能卡安全协议改进研究①

Study of Security Protocol Modification for Contactless Smart Card

冯　静　许　勇　(桂林电子科技大学 计算机与控制学院 广西 桂林 541004)

摘　要： 随着身份认证技术向硬件发展和智能卡的广泛应用，非接触式智能卡系统安全问题的重要性日益显著。本文通过分析和利用现有的认证协议和密码算法，针对非接触式智能卡与读卡器间的通信提出了一种改进的安全协议。首先描述了改进的身份认证协议；然后介绍了安全信道的构建方法和数据完整性实现过程；最后通过对协议进行安全性分析，表明本协议有效抵抗了重放攻击和中间人攻击，降低了密钥泄漏的概率，减少了密钥泄漏的危害。

关键词： 非接触式智能卡 安全协议 身份认证 Diffie-Hellman 算法

1　引言

随着智能卡技术的发展，智能卡可独立运行密码运算的自包容特性，使其在高安全性要求的场合得到了广泛的应用。目前，智能卡已广泛应用于身份合法性鉴别、数据存储或传输的私密性与完整性、信息交互的抗抵赖性以及移动计算等信息处理和信息安全领域。随着身份认证技术向硬件解决方案发展和智能卡的广泛应用，围绕着智能卡应用安全开展的理论和策略研究、芯片设计和产品开发既是学术界研究的热点，也是产业界关注的焦点。

非接触式智能卡作为智能卡技术的一个重要发展方向，卡与读卡器间的通信安全无疑是非接触式智能卡应用系统安全中的重中之重。非接触式智能卡通常含有用户的身份识别标示，通过特定的密码协议来保障其和读卡器间的安全交互。目前，非接触式智能卡存在的安全威胁主要包括如下几个方面：①智能卡的成本限制与协议安全强度之间的矛盾导致部分厂家为节约成本而舍弃安全性；②设计者对智能卡的自包容特性盲目信任，对克隆攻击威胁认识不足；③智能卡的唯一身份标示容易泄露用户隐私。

非接触式智能卡与读卡器间的信息安全包括了以下特性，即认证性、机密性和完整性。其安全应用的本质可总结为：构建安全终端(智能卡和读卡器之间的身份合法性鉴别)和搭建安全通道(在智能卡和读卡器之间搭建可信的智能卡信息交易通道)。

本文通过分析和利用现有的认证协议和密码算法，针对非接触式智能卡与读卡器间的通信提出了一种改进的安全协议。

本文所使用的符号如下：

A：读卡器；B：智能卡；P：消息明文；Ei：i 的公钥；Di：i 的私钥；Ki：秘密密钥，i 代表密钥所有者；Ks：会话密钥；Ri：i 产生的随机数；P(R)：由随机数 R 指向的身份信息；ssc：序列计数器。

2　认证协议

身份认证是指通信双方可靠地验证对方的身份。用以确保数据的真实性，阻止对手的主动攻击，如篡改或冒充等。认证往往是智能卡应用中安全保护的第一道防线。由于非接触式智能卡与读卡器间信道开放性的特点，使得身份信息在传递的过程中非常容易被泄露。因此一个安全的认证协议是非常重要的。

目前智能卡上的身份认证一般都已经使用了动态鉴别，但其安全性完全依赖于密钥的私密性，一旦密钥泄漏，系统就会处于危险中。对此本文提出了以下改进。

在非接触式智能卡中一般都存在着卡的唯一身份标识信息(如卡序列号，生产商代码等)，在本协议中，

① 基金项目:广西壮族自治区科学技术厅资助项目(桂科能 063006-5G-3)
收稿时间:2008-10-06

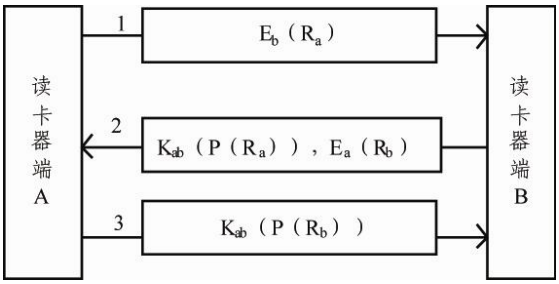

图 1　身份认证协议

对卡的身份标识信息进行扩展，使其成为一个唯一的身份标识数据块图 D(当然不能太大导致超出卡的存储范围)。当每次卡与读卡器间进行相互认证时，只使用其中的一部分进行传输，具体协议如图 1。在本协议中 A、B 预先知道了对方的公钥，并共享一个主秘密密钥 Kab。协议描述如下：

(1)A 产生一个位置随机数 R_a，并用 B 的公钥 E_b 对其进行加密后传输给 B，B 收到后用自己的私钥 D_b 进行解密得到 R_a，R_a 经过一个位置置换函数 T(位置的范围包括整个身份标识数据块图)得出 D 中相应的数据信息位置，并读出该数据。

(2)B 用共享密钥 Kab 使用 2-DES 算法加密得出的身份信息，再产生一个位置随机数 R_b，用 A 的公钥 E_a 加密 R_b，最后一起传送给 A。

(3)A 用共享密钥 K_{ab} 对消息 2 解密，将 R_a 输入与 B 中相同的位置置换函数 T 得出对应的数据信息位置，将 K_{ab} 解密后得出的身份信息与 A 得出的信息进行对比，一致则认为 B 是合法的。再用 A 的私钥 Da 对 Ea(Rb)进行解密得出 R_b，将 R_b 经过位置置换函数 T 得出对应的数据信息位置，读出该数据，用 K_{ab} 使用 2-DES 算法加密该数据并传送给 B，B 解密后对其进行验证，一致则认为 A 是合法的，完成了 A 与 B 的相互认证。

在这里，位置置换函数 T 起着非常重要的作用，它的任务是将接收到的随机数通过一系列的安全运算最终输出一个位置数，且要求这一过程只有 A、B 双方可以完成。我们可以使用 2-DES 算法生成 MAC 值的方法得出这一位置数，以位置随机数作为输入，使用共享密钥 K_{ab} 得出一个函数值，即为所需的位置数。考虑到非接触式智能卡的硬件成本限制和认证的速度，大部分的数据流量都是用 2-DES 来加密的，而现在的智能卡大部分都添加了加密协处理器，可以加快加密速度。协议中的非对称算法使用的是 ECC(椭圆曲线加密)算法，且只对两个随机数进行了加密，不会造成系统太大负担。

3　信道安全

在本协议中，每次通信都将使用一个新的随机选取的会话密钥，这样就使得利用用户的秘密密钥和公钥来发送的流量降低到最少，从而也减少了入侵者可能得到的密文数量。当会话建立后，所有的永久密钥都将退出通信过程，即使会话密钥暴露了，也可以将损害降到最低。

下面介绍基于 Diffie-Hellman 密钥交换协议的会话密钥的产生。

(1)A 产生两个大随机数 n 和 g，即 D-H 参数。这里要求 n 是一个素数，(n－1)/2 也是一个素数，g 是 n 的一个原根。这两个数可以公开的传送给 B。

(2)A 选择一个大随机数 x，x<n，x 是保密的，计算 $Y_a = g^x \bmod n$，将(n，g，Y_a)发送给 B。同样地，B 也选择一个秘密的大随机数 y，计算 $Y_b = g^y \bmod n$，并将 Y_b 作为对 A 的回应。

(3)A 通过计算 $K = Y_b^x \bmod n$ 得到了共享密钥 K_a，B 也通过计算 $K = Y_a^y \bmod n$ 得到了共享密钥 K_b。根据模算术定理，双方的计算结果是相同的。这样 A、B 就共享了一个秘密密钥 $K = K_a = K_b$。

因为 x 和 y 是保密的，一个入侵者可以利用的参数只有 n、g、Y_a 和 Y_b。因而入侵者被迫取离散对数来确定密钥。例如，要获取 B 的秘密密钥，入侵者必须先计算 y，然后再使用 B 采用的同样方法计算其秘密密钥 K。Diffie-Hellman 密钥交换算法的安全性依赖于这样一个事实：虽然计算以一个素数为模的指数相对容易，但计算离散对数却很困难。对于大的素数，计算出离散对数几乎是不可能的。

同时为了防止中间人攻击，发送 n、g、Y_a 和 Y_b 时，使用主密钥 K_{ab} 对其进行加密。具体协议如图 2。

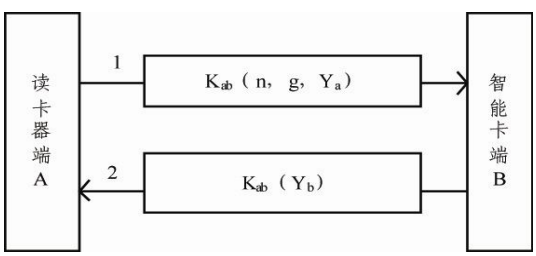

图 2　会话密钥生成协议

当然得到的 K 并不能直接用于会话密钥，因为这时的 K 只是长度不定的秘密数据串，而卡在进行加解密计算时所需的密钥长度是固定的。可以使用下面提到的 Hash 算法将可变长度的信息转化为固定长度的信息，而这个固定长度的数据串就是双方共享的会话密钥 K_s。

另外，在卡与终端进行通信时，若每次会话都重新生成一组 D-H 参数并执行相应的协商步骤，会造成通信的效率低下。因此，协议中建议采用同一组 D-H 参数来协商会话密钥，以保证执行效率。

4　数据完整性

由于非接触式智能卡与终端的通信是曝露在公开环境下的，双方在进行信息交换的时候，很容易遇到以下攻击：①篡改通信数据；②使用伪造的消息，删除或使用之前发送的消息进行重放攻击。

为了防止攻击者篡改 A、B 双方的通信数据，同时考虑到非接触式智能卡的运算效率，本协议使用 MD5 哈希算法计算数据的消息摘要得到固定长度的 Hash 值，附在密文后发送到接收方，接收方只需在解密密文后用 MD5 算法得出相应 Hash 值，并与接受到的 Hash 值相比较，结果相同则说明消息没有被篡改。

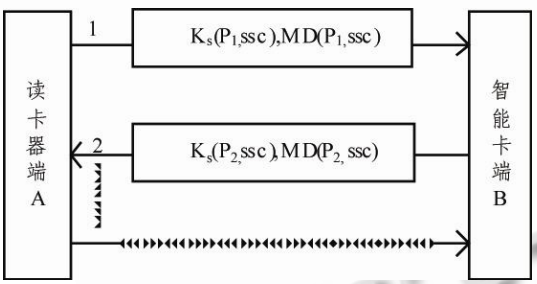

图 3　消息传输协议

而针对第二种情况，可以通过发送序列计数器机制保证信息的实时性和真实性，即在会话密钥的有效期内加入一个时间序列号。

在安全通信中使用发送序列计数器机制不是由于它本身是安全方法，只有把发送序列计数器和安全协议结合起来才有意义，否则攻击者对计数器的任何修改都将难于察觉。序列计数器的工作原理是每个消息中含有一个依赖于它被发送的时间的序列号，这使得在过程中若去掉或插入一个消息时能立即被注意到，使得接受方可采取适当的对策。

本协议中，每次会话都会产生一个唯一的共享密钥 K，它可以用于对序列计数器(ssc)进行初始化。每发送一次消息计数器就被增量。计数器的长度可以根据需要通过哈希函数进行设定。具体协议如图 3。

5　安全性分析

实际上不可能建立起一个具有完善的安全性能而不被任何人所渗透的完整系统，即使智能卡也是一样。为了保证双方通信的认证性、机密性和完整性，协议中针对这三方面进行了具体设计，希望使得它们之间的安全性可以相互叠加，即以逻辑或的关系结合在一起，当某一环节被攻击了，协议的后续操作能够有效的抵制和处理这些攻击。以下通过常见的攻击方法对本协议进行安全性分析。

(1)在身份认证阶段，本协议不仅使用了非对称算法进行身份认证，同时加入了身份信息的动态认证，安全性不只紧紧依赖于密钥的保密性，同时也依赖于用户的身份标识信息的私密性，攻击者即使通过截获的大量信息分析出一方或双方私钥，也无法完成认证。因为攻击者无法通过截获的信息来获得完整的身份标识数据块图，因为攻击者并不知道置换函数的具体过程(它被秘密的存储在卡和终端内，并不出现在信道内)，无法分析位置随机数所真正对应的位置号。有效抵制了猜测攻击。

(2)本协议基于 Diffie-Hellman 算法，使用一次一密的方法来构建安全的通信信道。在会话密钥的生成过程中，通过加密公开数据防止了中间人攻击。同时即使本次会话密钥泄露了并不会导致之前会话密钥的泄漏，保证了密钥的前向安全性。

(3)通过使用消息摘要的方式，有效防止了攻击者对消息的篡改。而在消息中加入序列计数器，则有效抵制了通过删除或使用之前发送的消息进行重放攻击。

(4)为了防止基于已知明文-密文对的攻击，在本协议的通信过程中，避免了出现对应的明文-密文对。

6　性能分析

考虑到非接触式智能卡对实时性的要求较高，协议的实现过程需要具有较高的速率。在本协议中只有在身份认证的位置随机数传递和会话密钥生成时分别使用了 ECC 和 Diffie-Hellman 这两种非对称密钥算

法。协议中的其他部分都使用了对称加密算法，计算速度很快。为了验证本协议的运算效率，模拟时钟频率为 4.9MHz，带有 DES 协处理器的智能卡，在实验中对各步骤的耗时进行了测试。ECC 密钥采用 135b，Diffie-Hellman 密钥采用 128b，对称加密算法使用 2-DES。在①②③节对协议的描述中，我们把安全协议分为 3 部分：①身份认证；②会话密钥生成；③双方的安全通信。在第一步耗时为 0.742s 左右；第二步耗时为 0.041s 左右，在此阶段 D-H 参数的生成和传递只需要一次，所以计算和通信时间不作考虑；第三步为双方的安全通信过程，由于使用了 DES 协处理器，每条消息的处理时间为 0.25ms 左右。在第一步中耗时较长，这是因为使用了非对称算法，且进行了多重置换。第二步由于使用了 Diffie-Hellman 算法进行密钥协商，耗时也较长。但总速度不超过 1s，可以认为协议能够满足实时性的要求。

7 结束

本文通过分析和利用现有的认证协议和密码算法，针对非接触式智能卡与读卡器间的通信提出了一种改进的安全协议。通过几种攻击方法对提出的协议进行验证，表明本协议可以有效抵抗重放攻击和中间人攻击；由于使用临时会话密钥，降低了密钥泄漏的概率；使用动态的身份信息，减少了密钥泄漏的危害。然而攻击的方法多种多样，本协议仍然存在安全隐患，还需要通过更有效的方法对其进行分析和改进。考虑到非接触式智能卡的特性，本文的认证协议并没有引入可信的第三认证方，只是在卡与读卡器上完成独立的相互认证。

参考文献

1 Stallings W.密码编码学与网络安全：原理与实践.北京:电子工业出版社, 2001:151－159,201.

2 Tanenbaum A S.计算机网络.北京:清华大学出版社, 2004:672－684.

3 Rankl W, Effing W.智能卡大全-智能卡的结构功能应用.北京:电子工业出版社, 2002:123－128,284－287,309－329.

4 Gothery SB, Jurgensen TM. 智能卡开发者指南.北京:电子工业出版社, 2000.

5 刘明生.IC 卡系统智能设计及多方信任计算理论研究[博士学位论文].天津:河北工业大学, 2007.

6 Messerges TS, Dabbish EA, Sloan RH. Examining smart-card security under the threat of power analysis attacks. IEEE Transactions on Computers, 2002,51(5):541－552.