[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/08 (2006.01)
H04L 9/06 (2006.01)
H04B 5/02 (2006.01)
H04Q 7/32 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200610118956.7

[43] 公开日 2007 年 7 月 11 日

[11] 公开号 CN 1996832A

[22] 申请日 2006.12.1

[21] 申请号 200610118956.7

[71] 申请人 上海复旦微电子股份有限公司

地址 200433 上海市国泰路 127 号复旦科技园 4 号楼

[72] 发明人 李 清 王元彪 李 蔚 邹勇波 张 纲

[74] 专利代理机构 上海新天专利代理有限公司

代理人 张静洁

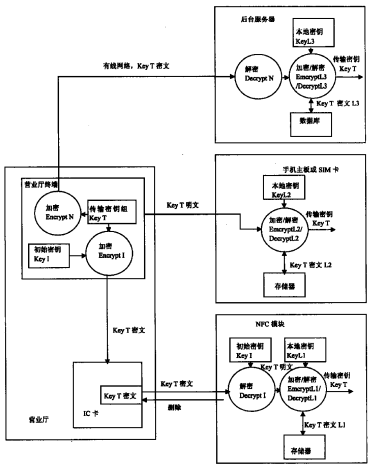
权利要求书 2 页 说明书 6 页 附图 1 页

[54] 发明名称

用于近场通讯手机的对称密钥初始化方法

[57] 摘要

本发明提供了一种用于近场通讯手机的对称密钥初始化方法，实现对称密钥在营业厅与 NFC 模块、手机和后台服务器之间的安全传递和安全存储。 传输密钥建立后，可以通过特定的密钥分散算法和随机数发生器，通过特定运算产生每次交易的会话密钥，用于对 NFC 模块与手机主板或 SIM 卡、手机主板或 SIM 卡与后台服务器之间的数据加密和解密，实现交易密钥和数据通信的安全性。



1. 用于近场通讯手机的对称密钥初始化方法，其特征在于，包含以下步骤：

步骤 1、营业厅将密钥发送给 NFC 模块；

步骤 2、营业厅将密钥发送给手机；

步骤 3、营业厅将密钥发送给后台服务器。

2. 如权利要求 1 所述的用于近场通讯手机的对称密钥初始化方法，其特征在于，所述的步骤 1 包含以下步骤：

步骤 1.1、营业厅的终端采用对称算法产生传输密钥 Key T，利用初始密钥 Key I 和对称加密算法 Encrypt I 对该传输密钥 Key T 进行加密操作，写入一张非接触 IC 卡的存储器内；

步骤 1.2、NFC 模块读取非接触 IC 卡内的存储器，获取通过初始密钥 Key I 加密后的传输密钥 Key T 密文，NFC 模块采用对称解密算法 Decrypt I，用 NFC 模块内存储的初始密钥 Key I 对获取的传输密钥 Key T 密文做解密操作后，获得传输密钥 Key T 的明文；

步骤 1.3、NFC 模块对非接触 IC 卡内存储器作写或擦操作，删除非接触 IC 卡内存储器内存储的传输密钥 Key T 密文；

步骤 1.4、NFC 模块采用第一本地密钥 Key L1 和本地加密算法 Encrypt L1 对获取的传输密钥 Key T 明文进行加密操作，并存储在 NFC 模块的存储器内；

步骤 1.5、在需要使用步骤 1.4 得到的传输密钥 Key T 时，NFC 模块将密钥密文从 NFC 模块存储器内读出，经第一本地密钥 Key L1 和解密算法 Decrypt L1 解密后得到传输密钥 Key T 的明文。

3. 如权利要求 2 所述的用于近场通讯手机的对称密钥初始化方法，其特征在于，所述的初始密钥 Key I 为固定的缺省值。

4. 如权利要求 1 所述的用于近场通讯手机的对称密钥初始化方法，其特征在于，所述的步骤 2 包含以下步骤：

步骤 2.1、营业厅终端将传输密钥 Key T 明文写入手机主板或手机 SIM 卡；

步骤 2.2、手机主板或 SIM 卡获取传输密钥后，采用第二本地密钥

Key L2 和本地加密算法 Encrypt L2 对该传输密钥 Key T 进行加密，并存储在手机或手机 SIM 卡的存储器内；

步骤 2.3、在需要使用步骤 2.2 得到的传输密钥时，手机主板或 SIM 卡将密钥密文从手机主板或 SIM 卡存储器内读出，经第二本地密钥 Key L1 和解密算法 Decrypt L2 解密后获得传输密钥 Key T 的明文。

5. 如权利要求 1 所述的用于近场通讯手机的对称密钥初始化方法，其特征在于，所述的步骤 3 包含以下步骤：

步骤 3.1、营业厅终端产生的传输密钥 Key T 经约定的加密算法 Encrypt N 加密后通过有线网络传递到后台服务器；

步骤 3.2、后台服务器获取传输密钥 Key T 密文后，采用约定算法 Decrypt N 解密后，获得传输密钥 Key T 明文；

步骤 3.3、后台服务器采用第三本地密钥 Key L3 和本地加密算法 Encrypt L3 对该步骤 3.2 得到的传输密钥进行加密，并存储在后台服务器的数据库内；

步骤 3.4、在需要使用步骤 3.3 得到的传输密钥时，将密钥密文从后台服务器的数据库读出，经第三本地密钥 Key L3 和算法 Decrypt L3 解密后获得传输密钥的明文。

用于近场通讯手机的对称密钥初始化方法

技术领域

本发明涉及一种用于近场通讯手机的对称密钥初始化方法，应用于手机安全技术领域。

背景技术

IC（集成电路）卡特别是非接触式 IC（集成电路）卡经过十多年的发展，已深入现代生活的各个角落，被广泛应用于公交、门禁、小额电子支付等领域。近年来，在轨道交通、物流管理、物品防伪、身份识别等需求推动下，非接触式 IC（集成电路）卡（或者电子标签）技术的不断进步，应用越来越普及，迫切需要各类非接触 IC（集成电路）卡（或者电子标签）识别设备。与此同时，手机经历 20 多年的迅速发展，已经几乎成为居民人手俱备的随身装置，普及率非常高，并且有向手机集成更多功能的趋势。

NFC（Near Field Communication 近场通讯）是这几年飞速发展的一种新兴技术，由 Sony、Philips 和 Nokia 提出，它使得两个电子设备直接可以进行短程的通讯，工作在 13.56MHz 频段，工作距离几个厘米。NFC 技术目标是电子设备之间的近距离通讯，主要实现三类功能：非接触 IC 卡片模拟功能；点对点数据通讯功能；读卡机模式。

NFC 手机广泛地应用于移动支付、产品防伪、追踪监管、数字签名、身份认证、信息获取等领域，除了完成非接触通讯的接口和协议之外，还必须具有通信的安全管理功能，即对密钥进行管理，对通信数据进行加密传输。

安全性较高的加密方法是采用非对称加密方法进行身份认证和对称密钥的传递，再利用对称加密方法对通信数据进行加密，这对 NFC 手机的硬件提出了很高的要求，即需要支持非对称算法和对称算法两种加密方法。目前通常使用的非对称算法是 1024/2048 位的 RSA 算法或 256 位的 ECC 算法，无法用软件实现，硬件实现的电路规模较大，而且现有的通用的手机 SIM 卡和 NFC 模块功能一般不支持。而对称算法如 3DES, AES 等，软硬件实现相对简

单，现有的通用的手机 SIM 卡和 NFC 模块功能都可以支持这些对称算法，但是，对称算法最大的障碍是密钥的安全传递。由于对称算法中加密和解密的密钥是相同的，所以，发送方和接收方需要通过一个安全的通道来交换密钥，如果密钥泄漏，加密的数据将被密钥的窃取者解密，数据的安全性也就荡然无存。因此，为了实现 NFC 手机的安全通信，首先需要解决的问题就是数据加密所需要的对称密钥在 NFC 模块、手机或手机 SIM 卡和后台服务器之间安全传递及安全存储。

由于数据传输需要在 NFC 模块、手机或手机 SIM 卡和后台服务器之间进行，因此，对称密钥需要传递并保存在 NFC 模块、手机或手机 SIM 卡和后台服务器上。电信或移动营业厅作为密钥的发行场所，终端在营业厅内向非接触 IC 卡、手机或手机 SIM 卡写入密钥的过程可以认为是安全的。营业厅与后台服务器之间采用有线网络连接，营业厅和后台服务器之间可以约定加密算法，将密钥经约定算法加密后经过有线网络传输到后台服务器的过程也是安全的。

由于手机种类繁多，NFC 模块的对外数据接口千差万别，营业厅的终端不可能具有适应各种 NFC 模块的数据接口，营业厅的终端如何将密钥传递到 NFC 模块是一个需要解决的问题。同时，在密钥写入 NFC 模块、手机或手机 SIM 卡和后台服务器之后，密钥如何存储以保证不被非法窃取，也需要提供解决方案。

发明内容

本发明提供的一种用于近场通讯手机的对称密钥初始化方法，解决了对称密钥在营业厅与 NFC 模块、手机和后台服务器之间的安全传递和安全存储问题。

为了达到上述目的，本发明提供了一种用于近场通讯手机的对称密钥初始化方法，包含以下步骤：

步骤 1、营业厅将密钥发送给 NFC 模块；

步骤 1.1、营业厅的终端采用对称算法产生传输密钥（组），利用初始密钥和对称加密算法 Encrypt I，对该传输密钥（组）进行加密操作，写入一张非接触 IC 卡的存储器内，所述的初始密钥为固定的缺省值；

步骤 1.2、NFC 模块读取非接触 IC 卡内的存储器，获取通过初始密钥加密后的传输密钥（组）密文，NFC 模块采用对称解密算法 Decrypt I（，用 NFC 模块内存储的初始密钥对获取的传输密钥（组）密文做解密操作后，获得传输密钥（组）的明文；

步骤 1.3、NFC 模块对非接触 IC 卡内存储器作写或擦操作，删除非接触 IC 卡内存储器内存储的传输密钥（组）密文；

步骤 1.4、NFC 模块采用第一本地密钥和本地加密算法 Encrypt L1 对获取的传输密钥明文进行加密操作，并存储在 NFC 模块的存储器内；

步骤 1.5、在需要使用步骤 1.4 得到的传输密钥时，NFC 模块将密钥密文从 NFC 模块存储器内读出，经第一本地密钥和解密算法 Decrypt L1 解密后得到传输密钥的明文；

步骤 2、营业厅将密钥发送给手机；

步骤 2.1、营业厅终端将传输密钥明文写入手机主板或手机 SIM 卡；

步骤 2.2、手机主板或 SIM 卡获取传输密钥后，采用第二本地密钥和本地加密算法 Encrypt L2 对该传输密钥进行加密，并存储在手机或手机 SIM 卡的存储器内；

步骤 2.3、在需要使用步骤 2.2 得到的传输密钥时，手机主板或 SIM 卡将密钥密文从手机主板或 SIM 卡存储器内读出，经第二本地密钥和解密算法 Decrypt L2 解密后获得传输密钥的明文；

步骤 3、营业厅将密钥发送给后台服务器；

步骤 3.1、营业厅终端产生的传输密钥经约定的加密算法 Encrypt N 加密后通过有线网络传递到后台服务器；

步骤 3.2、后台服务器获取传输密钥密文后，采用约定算法 Decrypt N 解密后，获得传输密钥明文；

步骤 3.3、后台服务器采用第三本地密钥和本地加密算法 Encrypt L3 对该步骤 3.2 得到的传输密钥进行加密，并存储在后台服务器的数据库内；

步骤 3.4、在需要使用该步骤 3.3 得到的传输密钥时，将密钥密文从后台服务器的数据库读出，经第三本地密钥和算法 Decrypt L3 解密后获得传输密钥的明文。

本发明提供的一种用于近场通讯手机的对称密钥初始化方法，可以将营

业厅终端产生的对称传输密钥安全地传递到 NFC 模块、手机主板或 SIM 卡及后台服务器，并可以安全地存储在 NFC 模块、手机主板或 SIM 卡及后台服务器内。传输密钥建立后，可以通过特定的密钥分散算法和随机数发生器，通过特定运算产生每次交易的会话密钥，用于对 NFC 模块与手机主板或 SIM 卡、手机主板或 SIM 卡与后台服务器之间的数据加密和解密，实现交易密钥和数据通信的安全性。

附图说明

图 1 是本发明提供的一种用于近场通讯手机的对称密钥初始化方法的流程图。

具体实施方式

以下根据图 1 具体说明本发明的一种较佳实施方式：

如图 1 所示，本发明提供了一种用于近场通讯手机的对称密钥初始化方法，包含以下步骤：

步骤 1、营业厅将密钥发送给 NFC 模块；

步骤 1.1、营业厅的终端采用对称算法（如 DES, AES 等，算法的流程步骤在相关信息安全及密码学的文献中均可查到，如“保密学一基础与应用”，作者王育民、何大可，西安电子科技大学出版社出版）产生传输密钥（组）Key T，利用初始密钥 Key I 和对称加密算法 Encrypt I（如 DES, AES 等，算法的流程步骤在相关信息安全及密码学的文献中均可查到，如“保密学一基础与应用”，作者王育民、何大可，西安电子科技大学出版社出版），对该传输密钥（组）Key T 进行加密操作，写入一张非接触 IC 卡的存储器内，所述的初始密钥 Key I 为固定的缺省值；

步骤 1.2、NFC 模块读取非接触 IC 卡内的存储器，获取通过初始密钥 Key I 加密后的传输密钥（组）Key T 密文，NFC 模块采用对称解密算法 Decrypt I（如 DES, AES 等，算法的流程步骤在相关信息安全及密码学的文献中均可查到，如“保密学一基础与应用”，作者王育民、何大可，西安电子科技大学出版社出版），用 NFC 模块内存储的初始密钥 Key I 对获取的传输密钥（组）Key T 密文做解密操作后，获得传输密钥（组）Key T 的明文；

步骤 1.3、NFC 模块对非接触 IC 卡内存储器作写或擦操作，删除非接触 IC 卡内存储器内存储的传输密钥（组）Key T 密文；

步骤 1.4、NFC 模块采用第一本地密钥 Key L1 和本地加密算法 Encrypt L1（如 DES, AES 等，算法的流程步骤在相关信息安全及密码学的文献中均可查到，如“保密学一基础与应用”，作者王育民、何大可，西安电子科技大学出版社出版）对获取的传输密钥 Key T 明文进行加密操作，并存储在 NFC 模块的存储器内；

步骤 1.5、在需要使用步骤 1.4 得到的传输密钥 Key T 时，NFC 模块将密钥密文从 NFC 模块存储器内读出，经第一本地密钥 Key L1 和解密算法 Decrypt L1（如 DES, AES 等，算法的流程步骤在相关信息安全及密码学的文献中均可查到，如“保密学一基础与应用”，作者王育民、何大可，西安电子科技大学出版社出版）解密后得到传输密钥 Key T 的明文；

步骤 2、营业厅将密钥发送给手机；

步骤 2.1、营业厅终端将传输密钥 Key T 明文写入手机主板或手机 SIM 卡；

步骤 2.2、手机主板或 SIM 卡获取传输密钥后，采用第二本地密钥 Key L2 和本地加密算法 Encrypt L2（如 DES, AES 等，算法的流程步骤在相关信息安全及密码学的文献中均可查到，如“保密学一基础与应用”，作者王育民、何大可，西安电子科技大学出版社出版）对该传输密钥 Key T 进行加密，并存储在手机或手机 SIM 卡的存储器内；

步骤 2.3、在需要使用步骤 2.2 得到的传输密钥时，手机主板或 SIM 卡将密钥密文从手机主板或 SIM 卡存储器内读出，经第二本地密钥 Key L1 和解密算法 Decrypt L2（如 DES, AES 等，算法的流程步骤在相关信息安全及密码学的文献中均可查到，如“保密学一基础与应用”，作者王育民、何大可，西安电子科技大学出版社出版）解密后获得传输密钥 Key T 的明文；

步骤 3、营业厅将密钥发送给后台服务器；

步骤 3.1、营业厅终端产生的传输密钥 Key T 经约定的加密算法 Encrypt N（如 DES, AES 等，算法的流程步骤在相关信息安全及密码学的文献中均可查到，如“保密学一基础与应用”，作者王育民、何大可，西安电子科技大学出版社出版）加密后通过有线网络传递到后台服务器；

步骤 3.2、后台服务器获取传输密钥 Key T 密文后，采用约定算法 Decrypt N（如 DES, AES 等，算法的流程步骤在相关信息安全及密码学的文献中均可查到，如“保密学一基础与应用”，作者王育民、何大可，西安电子科技大学出版社出版）解密后，获得传输密钥 Key T 明文；

步骤 3.3、后台服务器采用第三本地密钥 Key L3 和本地加密算法 Encrypt L3（如 DES, AES 等，算法的流程步骤在相关信息安全及密码学的文献中均可查到，如“保密学一基础与应用”，作者王育民、何大可，西安电子科技大学出版社出版）对该步骤 3.2 得到的传输密钥进行加密，并存储在后台服务器的数据库内；

步骤 3.4、在需要使用该步骤 3.3 得到的传输密钥时，将密钥密文从后台服务器的数据库读出，经第三本地密钥 Key L3 和算法 Decrypt L3（如 DES, AES 等，算法的流程步骤在相关信息安全及密码学的文献中均可查到，如“保密学一基础与应用”，作者王育民、何大可，西安电子科技大学出版社出版）解密后获得传输密钥的明文。

本发明提供的一种用于近场通讯手机的对称密钥初始化方法，可以将营业厅终端产生的对称传输密钥安全地传递到 NFC 模块、手机主板或 SIM 卡及后台服务器，并可以安全地存储在 NFC 模块、手机主板或 SIM 卡及后台服务器内。传输密钥建立后，可以通过特定的密钥分散算法和随机数发生器，通过特定运算产生每次交易的会话密钥，用于对 NFC 模块与手机主板或 SIM 卡、手机主板或 SIM 卡与后台服务器之间的数据加密和解密，实现交易密钥和数据通信的安全性。

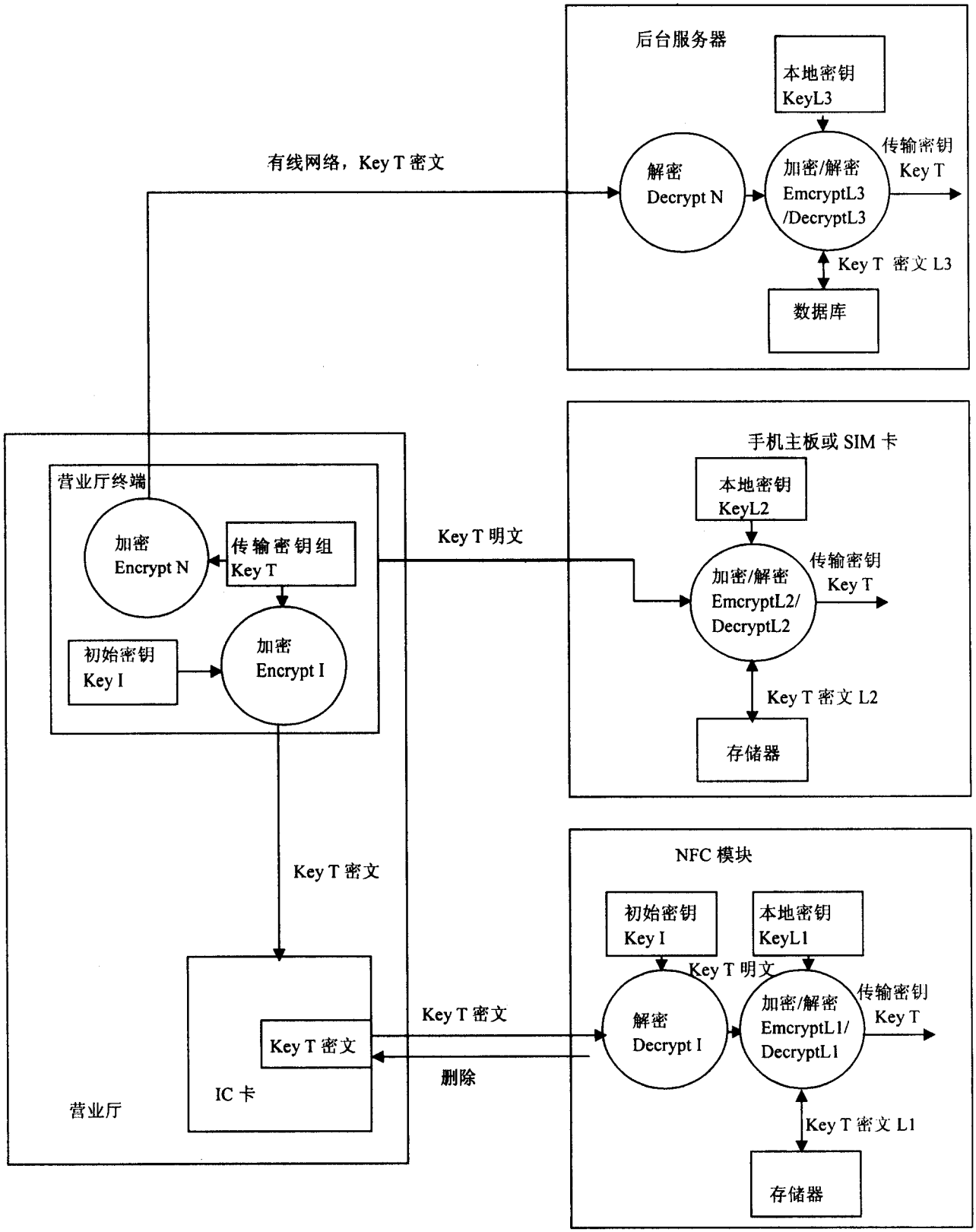

后台服务器
本地密钥
KeyL3
解密
Decrypt N
加密/解密
EmcryptL3
/DecryptL3
传输密钥
Key T
Key T 密文 L3
数据库
有线网络，Key T 密文
手机主板或 SIM 卡
本地密钥
KeyL2
加密/解密
EmcryptL2/
DecryptL2
传输密钥
Key T
Key T 密文 L2
存储器
营业厅终端
加密
Encrypt N
传输密钥组
Key T
初始密钥
Key I
加密
Encrypt I
Key T 明文
Key T 密文
NFC 模块
初始密钥
Key I
本地密钥
KeyL1
Key T 明文
解密
Decrypt I
加密/解密
EmcryptL1/
DecryptL1
传输密钥
Key T
Key T 密文 L1
存储器
Key T 密文
Key T 密文
IC 卡
删除
营业厅

图 1