基于密码技术的网上银行转账业务模型设计*

宋燕梅 李建 陈积常

南宁学院信息工程学院，南宁，530200

摘 要 针对目前网上银行转账交易业务中存在的安全问题，分析了网上银行面临的安全风险，根据网上银行系统密码安全应用需求，设计了以密码技术为基础的网上银行系统转账业务框架模型。从功能和非功能性分析了网上银行系统转账业务需求，运用密码算法、密钥管理技术、数字签名技术对网上银行转账业务系统的转账业务密码应用协议进行设计，并对协议的安全性做了分析。网上银行系统模型的测试结果表明，基于密码技术的网上银行转账业务模型实现了用户与服务端的身份鉴别、转账信息自动加密、转账信息数字签名、转账信息数字签名验证等功能，安全性达到了设计目标。

关键字 网上银行，密码技术，转账业务，密码协议，身份鉴别

Design of Transfer Business Model Based on Cryptography Technology for Online Banking

Song Yanmei Li Jian Chen Jichang

School of Information Engineering Nanning University
Nanning 530200,China;
943667593@qq.com

Abstract—Aiming at the secure problems in transaction business of online banking, the risk of security faced with online banking was analyzed. According to the requirement of cipher security application of online banking, the framework model of transaction business of online banking system based on cipher technology was designed. From the functional and non-functional analysis of the online banking system transfer business needs, using the password algorithm, key management technology, digital signature technology, the transfer cryptography application protocol of online banking system transfer business was designed, and the security of the protocol was analyzed. The test results of the online banking system model show that the online bank transfer business model based on cryptography technology realizes the functions of identity authentication of the user and the server, automatic encryption of transfer information, digital signature of transfer information, digital signature verification of transfer information, etc., The security reaches the difficulty level of calculating the discrete logarithm of elliptic curve and achieves the design goal.

Keyword—Online Banking, Password technique, Money transfer business, Cryptographic protocol；identification

1 引 言

目前，部分研究人员对网上银行系统的安全性问题进行了研究。文献[4]对网上银行认证技术进行应用研究，提出了一种改进的网上银行认证技术方案；文献[5]设计了一种基于指纹识别和PKI技术网上银行身份认证系统；文献[6]设计实现了一个基于公开密钥基础设施的网上银行网站；文献[7]和[8]研究了基于动态口令的网上银行安全认证方法。以上的研究仅仅只是针对用户身份认证的研究，没有提出对交易过程中传输数据的安全保障，或是没有具体提出保证交易安全的密码技术。

也有部分研究人员提出了网上银行系统交易安全方案。文献[9]基于网络渗透思想，采用自动化脚本编写、运行脚本对网络漏洞进行检测、平台汇总并反馈结果等方式，设计实现了一个网上银行企业级信息安全管理中心。文献[10]分析了网上银行网络入侵检测模式，构建了一套比较完善的动态口令认证系统。文献[11]研究了现代网上银行交易安全系统的构建原则和方法，比较分析了不同的体系结构的优缺点，采用结构化设计方法对网上银行交易安全系统进行功能模设计。文献[12]分析了基于网银转帐存在的安全性问题的总体架构，基于大机 CICS 平台，设计实现了网银转帐系统各个子系统。但是，这些方案没有真正实

* **基金资助**：本文得到 2017 年南宁学院校级重点专业（通信工程）（2017XJZDZY11)、广西民办重点专业建设（通信工程）（2021MBZDZY01)资助.

通讯作者：李建，教授，943667593@qq.com

现网上银行系统转账业务的功能，或是所用到的支撑网上银行交易的密码算法不够安全。

针对上述问题，本文提出一种基于国家商用密码技术[13]的网上银行转账业务模型，设计了转账业务密码应用协议。该模型运用 Linux 操纵系统、数据库等技术将数字签名与网上银行系统安全集成，实现可靠的转账信息身份验证、数据安全管理等功能，为保证用户身份的真实性、合法性、实现网上银行交易双方的抗抵赖、解决数据信息的保密性和完整性安全问题、降低银行服务经营成本以及提高银行服务质量提供了解决方案。

2 网上银行系统安全体系设计

随着网络技术的迅速遍及与发展，网上银行也渗透到了人们日常生活中的方方面面，人们可以时时刻刻在网上银行系统进行账号查询、转账交易等操作，因此网上银行系统的安全问题显得尤为重要。利用合规、正确和有效的密码技术保障网上银行系统的日常运行和交易过程，则密码技术主要需要对网上银行系统中的用户身份鉴别、关键数据保密性和信息完整性保护、交易活动行为不可否认性这几个方面进行保护，从而实现用户交易的安全保障。

2.1 系统总体体系结构设计

伴随着网络安全技术和计算机技术的日渐发展与成熟，仅使用防火墙防护网上银行的安全已经远远不够，网上银行系统安全防护逐步向着提供安全的防御措施转变[14][15]。综合密码应用需求分析，网上银行系统的总体设计目标是确保网上银行转账交易的安全性。从网上银行客户端转账至交易完成的过程中，应当保证转账交易信息数据的有效性，确认转账交易双方身份的真实性，保护传输数据的完整性和机密性，以及转账交易双方不可对存在的行为进行抵赖。

网上银行系统基本框架如图 1 所示。系统可以分为客户端和服务器端两大组成部分。客户端是由安全的浏览器、用于客户端用户身份鉴别的动态令牌等构成。服务器端则由 Web 服务器、应用服务器、数据服务器等通用服务器构成。服务端主要提供客户端用户的 Web 访问和网上银行业务处理。通信双方在进行交易数据时，保护传输中的交易数据的安全需要在网关和用户登录的浏览器之间创建一个安全链路通道。采用数字证书、数字签名和 SM2 公钥加密算法等密码技术对交易数据进行安全性保护。

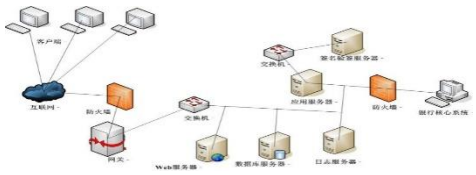

图 1 网上银行系统总体架构

2.2 系统安全技术体系设计

在系统安全体系架构设计上，本文的设计思路是：主要采用 SM4 对称算法，实现传输数据的保密性；采用数字证书，实现客户端和服务端的相互身份鉴别，保证通信双方身份的真实性；采用数字签名技术，实现发送方行为的不可否认；采用 SM3 杂凑算法，实现数据的完整性保护。系统安全架构如图 2 所示。

2.3 系统密码应用工作流程

系统密码应用工作流程如图 3 所示。

（1） 首先在通信中，需要创建安全链路通道。创建了通道后，网上银行的用户客户端的通信能得到安全保障，银行的通信也能得到安全保障，用户提交的转账交易信息数据在传输中还能得到完整性的保护，同时用户提交的转账交易信息数据在传输中也能得到很好的保密性保护。

（2）在利用动态令牌对用户身份进行认证的时，使用智能钥匙的过程与其是一样的，客户端先使用用户的账号名/账号口令与其进行协作，在两者的协作下，再与应用服务器完成鉴别身份的工作。

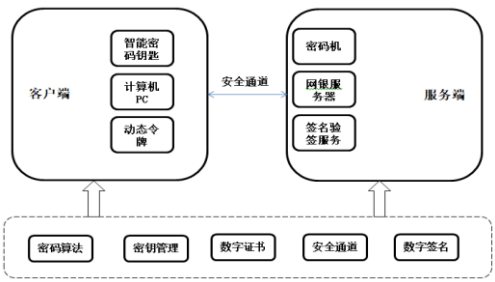

图 2 网上银行系统技术框架

（3） 在使用网上银行进行转账交易时，客户端用户先利用智能密码钥匙对交易转账信息数据进行签名得到签名转账信息数据，然后再将签名转账信息数据发送给系统应用服务器。

（4） 系统应用服务器接收到转账信息数据和签

名转账信息数据后，系统应用服务器利用金融密码机对自身新签名的转账信息数据和签名转账信息数据进行保护，然后将其发送给银行核心系统。

（5） 一旦系统应用服务器与银行核心系统之间的交易结束后，系统应用服务器利用签名验签服务器对交易信息数据文件进行数字签名，而后，系统应用服务器将其发还给客户端用户，以该签名文件当作金钱交易的凭证。

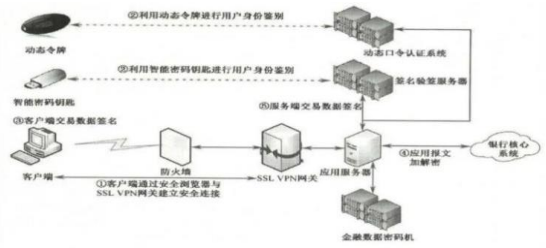

图 3 系统密码应用工作流程

3 系统转账业务密码应用协议

根据网上银行系统密码应用需求，本文为网上银行转账业务设计的安全通信协议如图 4 所示。

（1） 客户端 A 将自身的身份、时间戳、自身的证书以及自身的身份$\mathrm{ID_A}$和时间戳$\mathrm{T_0}$的签名值发送给服务端 B，即

$$\mathrm{ID_A}\|\mathrm{T_0}\|\mathrm{E_{SK_A}}[\mathrm{H(ID_A}\|\mathrm{T_0})]\ \|\mathrm{E_{SK_{CA}}}(\mathrm{ID_A}\|\mathrm{T_1}\|\mathrm{PK_A}) \quad (1)$$

（2） 服务端 B 确认发送方的身份

① 服务端 B 首先用证书中心 CA 里的公钥PK_{CA}对客户端 A 的证书PK_A进行验证，以确认客户端 A 的证书的真实性，即

$$cert_A=D_{PK_{CA}}[E_{SK_{CA}}(ID_A\|T_1\|PK_A)]=ID_A\|T_1\|PK_A \quad (2)$$

如果等式成立，则说明证书是由证书中心 CA 签发的。

② 服务端 B 用客户端 A 的公钥来验证客户端 A 的数字签名，即

$$\mathrm{H_0=D_{PK_A}[E_{SK_A}(H(ID_A\|T_0))]=H(ID_A\|T_0)} \quad (3)$$

③ 服务端 B 对客户端 A 的身份和时间戳进行哈希运算，即

$$\mathrm{H_1=H(ID_A\|T_0)} \quad (4)$$

④ 判断并比较哈希值$\mathrm{H_0}$、$\mathrm{H_1}$，如果两者相等，则服务端 B 确认了发送方就是客户端 A；如果等式不成立，则不能确认发送方的身份。

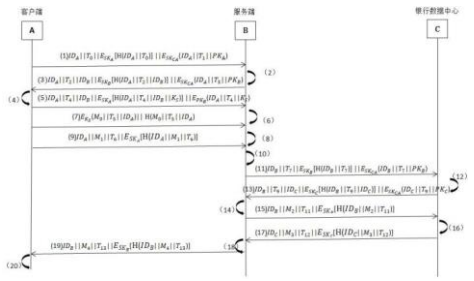

图 4 转账业务密码应用协议

（3） 服务端 B 将自身的身份、时间戳、自身的证书以及自身的身份、时间戳和客户端 A 的身份ID_A的签名值发送给客户端 A，即

$$\mathrm{ID_A}\|\mathrm{T_2}\|\mathrm{ID_B}\|\mathrm{E_{SK_B}}[\mathrm{H(ID_A}\|\mathrm{T_2}\|\mathrm{ID_B})]\ \|\mathrm{E_{SK_{CA}}}(\mathrm{ID_A}\|\mathrm{T_3}\|\mathrm{PK_B}) \quad (5)$$

（4） 客户端 A 确认发送方的身份

①客户端 A 首先用证书中心 CA 的公钥PK_{CA}对服务端 B 的证书PK_B验证，以确认服务端 B 的证书的真实性，即

$$cert_B=D_{PK_{CA}}[E_{SK_{CA}}(ID_A\|T_3\|PK_B)]=ID_A\|T_3\|PK_B \quad (6)$$

如果等式成立，则说明证书是由证书中心 CA 签发的。

② 客户端 A 用服务端 B 的公钥来验证服务端 B 的数字签名，即

$$H_2=D_{PK_B}[\mathrm{E_{SK_B}(H}(ID_A\|T_2\|ID_B))]=\mathrm{H}(ID_A\|T_2\|ID_B) \quad (7)$$

③ 客户端 A 对自身的身份、时间戳和客户端 A 的身份ID_A进行哈希运算，即

$$H_3=\mathrm{H}(ID_A\|T_2\|ID_B) \quad (8)$$

④ 比较并判断哈希值H_2、H_3，如果两者相等，则客户端 A 确认了发送方就是服务端 B；如果等式不成立，则不能确认发送方的身份。

（5） 客户端 A 将自身的身份、时间戳、服务端 B 的身份，客户端 A 对自身的身份ID_A、服务端 B 的身份、时间戳和会话密钥的签名值，以及用服务端 B 的公钥加密会话密钥、自身的身份ID_A和时间戳的值发送给服务端 B，即

$$\mathrm{ID_A}\|\mathrm{T_4}\|\mathrm{ID_B}\|\mathrm{E_{SK_A}}[\mathrm{H(ID_A}\|\mathrm{T_4}\|\mathrm{ID_B}\|\mathrm{K_S})]\ \|\mathrm{E_{PK_B}}(\mathrm{ID_A}\|\mathrm{T_4}\|\mathrm{K_S}) \quad (9)$$

（6）服务端 B 确认会话密钥

① 服务端 B 用自身的私钥解密出会话密钥、客户端 A 的身份和时间戳，即

$$D_{SK_B}[\mathrm{E_{PK_B}(ID_A}\|\mathrm{T_4}\|\mathrm{K_S})]=\mathrm{ID_A}\|\mathrm{T_4}\|\mathrm{K_S} \quad (10)$$

② 服务端 B 用客户端 A 的公钥解密客户端 A 的数字签名，即

$$H_4=D_{PK_A}[E_{SK_A}(H(ID_A||T_4||ID_B||K_S))]= H(ID_A||T_4||ID_B||K_S) \quad (11)$$

③ 服务端 B 对私钥解密得到的会话密钥进行哈希运算，即

$$H_5=H(ID_A||T_4||ID_B||K_S) \quad (12)$$

④ 服务端 B 比较判断H_4、H_5，如果两者相等，则服务端 B 可以确定协商的会话密钥在传输的过程中没有改变；如果等式不成立，则服务端 B 可以确定协商的会话密钥在传输的过程中已经改变，需要重新协商会话密钥。

（7） 客户端 A 发送使用 SM4 对称加密算法加密的数据M_0、时间戳、自身的身份信息以及使用 SM3 杂凑算法计算的数据M_0、时间戳和自身的身份信息给服务端 B，以此保护数据的机密性和完整性，即

$$E_{K_S}(M_0||T_5||ID_A)||\ H(M_0||T_5||ID_A) \quad (13)$$

（8）服务端 B 确认接收的数据

① 服务端 B 使用 SM4 对称密码算法解密数据M_0，即

$$D_{K_S}[E_{K_S}(M_0||T_5||ID_A)]= M_0||T_5||ID_A \quad (14)$$

② 服务端 B 使用 SM3 杂凑算法对数据M_0、时间戳和自身的身份信息进行哈希运算，即:

$$H_6=H(M_0||T_5||ID_A) \quad (15)$$

③ 服务端 B 比较并判断H_6、$H(M_0||T_5||ID_A)$，如果两者相等，则服务端 B 可以确定数据M_0在传输的过程中没有改变；如果等式不成立，则服务端 B 可以确定数据M_0在传输的过程中已经改变，需要重新传输数据。

（9） 客户端 A 发送信息M_1、时间戳、自身的身份信息以及自身的私钥对信息M_1、时间戳和自身的身份信息的哈希值的签名值发送给服务端 B，以防止客户端 A 对发送到 B 的转账信息进行抵赖，即

$$ID_A||M_1||T_6||E_{SK_A}[H(ID_A||M_1||T_6)] \quad (16)$$

（10）服务端 B 确认接受的信息

① 服务端 B 用客户端 A 的公钥解密签名信息，即

$$H_7=D_{PK_A}[E_{SK_A}(H(ID_A||M_1||T_6))]= H(ID_A||M_1||T_6) \quad (17)$$

② 服务端 B 对信息M_1、时间戳和自身的身份信息进行哈希计算，即

$$H_8= H(ID_A||M_1||T_6) \quad (18)$$

③ 服务端 B 比较并判断H_7、H_8，如果两者相等，则服务端 B 可以确定客户端 A 确实向服务端 B 发送了转账信息且转账信息没有被篡改；如果等式不成立，服务端 B 不能确定客户端 A 向服务端 B 发送了转账信息，或者说客户端 A 虽然已经发送了转账信息，但是转账信息在传输过程中被篡改，需要客户端 A 重新发送转账信息。

（11） 服务端 B 将自身的身份、时间戳、自身的证书以及自身的身份和时间戳的签名值发送给银行数据中心 C，即

$$ID_B||T_7||E_{SK_B}[H(ID_B||T_7)]\ ||E_{SK_{CA}}(ID_B||T_4||PK_B) \quad (19)$$

（12） 银行数据中心 C 确认发送方的身份

① 银行数据中心 C 首先用证书中心 CA 的公钥对服务端 B 的数字证书PK_B进行验证，然后就证明了服务端 B 的证书的真实性，即

$$cert_B=D_{PK_{CA}}[E_{SK_{CA}}(ID_B||T_8||PK_B)]= ID_B||T_8||PK_B \quad (20)$$

如果等式成立，则说明证书是由证书中心 CA 签发的。

② 银行数据中心 C 用服务端 B 的公钥来解密服务端 B 的数字签名，即

$$H_9=D_{PK_B}[E_{SK_B}(H(ID_B||T_7))]= H(ID_B||T_7) \quad (21)$$

③ 银行数据中心 C 对服务端 B 的身份和时间戳进行哈希运算，即

$$H_{10}= H(ID_B||T_7) \quad (22)$$

④ 判断并比较哈希值H_9、H_{10}，如果两者相等，则银行数据中心 C 确认了发送方就是服务端 B；如果等式不成立，则不能确认发送方的身份。

（13） 银行数据中心 C 将自身的身份、时间戳、自身的证书以及自身的身份、时间戳和服务端 B 的身份的签名值发送给服务端 B，即

$$ID_B||T_9||ID_C||E_{SK_C}[H(ID_B||T_9||ID_C)]\ ||E_{SK_{CA}}(ID_C||T_9||PK_C) \quad (23)$$

（14）服务端 B 确认发送方的身份

① 服务端 B 首先用证书中心 CA 的公钥对银行数据中心 C 的证书验证，以确认银行数据中心 C 的证书的真实性，即

$$cert_C=D_{PK_{CA}}[E_{SK_{CA}}(ID_C\|T_{10}\|PK_C)]=ID_C\|T_{10}\|PK_C \quad (24)$$

如果等式成立，则说明证书是由证书中心 CA 签发的。

② 服务端 B 用银行数据中心 C 的公钥来解密银行数据中心 C 的数字签名，即

$$H_{11}=D_{PK_C}[E_{SK_C}(H(ID_B\|T_9\|ID_C))]= H(ID_B\|T_9\|ID_C) \quad (25)$$

③ 服务端 B 对自身的身份、时间戳和数据中心 C 的身份进行哈希运算，

$$H_{12}= H(ID_B\|T_9\|ID_C) \quad (26)$$

④ 比较并判断哈希值H_{11}、H_{12}，如果两者相等，则服务端 B 确认了发送方就是银行数据中心 C；如果等式不成立，则不能确认发送方的身份。

（15） 服务端 B 将自身的身份、时间戳、交易信息，服务端 B 的身份、时间戳和交易信息的签名值发送给银行数据中心 C，即

$$ID_B\|M_2\|T_{11}\|E_{SK_B}[H(ID_B\|M_2\|T_{11}) \quad (27)$$

（16） 银行数据中心 C 确认交易信息

① 银行数据中心 C 用服务端 B 的公钥解密数字签名，即

$$H_{13}=D_{PK_B}[E_{SK_B}(H(ID_B\|M_2\|T_{11}))]= H(ID_B\|M_2\|T_{11}) \quad (28)$$

② 银行数据中心 C 对接收的交易信息进行哈希运算，即

$$H_{14}=H(ID_B\|M_2\|T_{11}) \quad (29)$$

③ 比较判断H_{13}、H_{14}，如果两者相等，则银行数据中心 C 可以确定服务端 B 发送了交易信息且交易信息没有被篡改；如果等式不成立，则银行数据中心 C 不可以确定服务端 B 发送了交易数据信息，或者说服务端 B 虽然发送了交易数据信息，但是交易数据信息在传输过程中被窜改，需要重新发送交易数据信息。

（17） 银行数据中心 C 将自身的身份、时间戳、交易信息以及时间戳、自身的身份和交易信息的签名值发送给银行数据中心 C，即

$$ID_C\|M_3\|T_{12}\|E_{SK_C}[H(ID_C\|M_3\|T_{12})] \quad (30)$$

（18） 服务端 B 确认从数据中心发送过来的交易信息

① 服务端 B 用银行数据中心 C 的公钥解密签名信息，即

$$H_{15}=D_{PK_C}[E_{SK_c}(H(ID_C\|M_3\|T_{12}))]= H(ID_C\|M_3\|T_{12}) \quad (31)$$

② 服务端 B 对交易信息进行哈希计算，即

$$H_{16}= H(ID_C\|M_3\|T_{12}) \quad (32)$$

③ 服务端 B 比较并判断H_{15}、H_{16}，如果两者相等，则服务端 B 可以确定银行数据中心 C 确实向服务端 B 发送了交易信息且交易信息没有被篡改；如果等式不成立，服务端 B 不能确定银行数据中心 C 向服务端 B 发送了交易信息，或者说客户端 A 虽然已经发送了交易信息，但是交易信息在传输过程中被篡改，需要银行数据中心 C 重新传输交易信息。

（19） 服务端 B 发送转账交易信息、时间戳、自身的身份以及加密自身的身份、转账交易信息、时间戳生成的签名值给客户端 A，即

$$ID_B\|M_4\|T_{13}\|E_{SK_B}[H(ID_B\|M_4\|T_{13})] \quad (33)$$

（20） 客户端 A 确认从服务端接收的转账信息

① 客户端 A 用服务端 B 的公钥解密签名，即

$$H_{17}=D_{PK_B}[E_{SK_B}(H(ID_B\|M_4\|T_{13}))]= H(ID_B\|M_4\|T_{13}) \quad (34)$$

② 客户端 A 对转账交易信息进行哈希运算，即

$$H_{18}= H(ID_B\|M_4\|T_{13}) \quad (35)$$

③ 比较并判断H_{17}、H_{18}，如果两者相等，则服务端 B 不能对已经发送的转账交易信息抵赖；如果等式不成立，则客户端 A 不能确认服务端 B 是否发送了转账交易信息。

3.2 密码应用协议的安全性分析

（1） 数字证书安全性分析。协议采用了数字证书以确认用户的身份，应用公钥密码技术建立 CA 到客户端的信任链路。在通信的各个环节中，利用数字证书确认对方身份的真实性，从而让双方能够对彼此信任。首先建立信任锚，也就是要有自签根证书 CA，根证书 CA 再为各个用户签发证书。根证书的生成需要计算根证书中的用户名、使用期限、部门代码、公钥信息哈希值，再用 CA 的私钥对需要计算的内容加密即可。因为计算的内容是采用根证书 CA 的私钥加密，且根证书 CA 的私钥只有根证书才能拥有，确保了根证书 CA 私钥的保密性，所以证书的签名值拥有唯一性的这一特点，也能防止入侵者对证书进行伪造。如果黑客想要伪造证书，需要找到哈希函数的碰撞，用穷搜索攻击对密钥进行攻击，其复杂度达到了$O(2n)$，1Gbps 的链路上需要 25 万年。所以，伪造证书是不可

实现的。

（2） SM2 算法安全性分析。协议采用 SM2 椭圆曲线公钥密码算法的数字签名算法鉴别了通信双方的身份, 采用 SM2 椭圆曲线公钥密码算法的公钥加密算法加密通信双方的会话密钥。在应用数字签名算法和公钥加密算法时，通信双方需要先获得向根证书 CA 申请的数字证书与 CA 的公钥证书。

数字签名包括签名数据和验证数据两部分。发送方对发送的数据进行哈希运算，通过自生成的私钥对数据的摘要进行签名。因为发送方的私钥只有发送方才拥有，则确认了发送方的身份，防止了他人的冒充，且不能对这一行为进行抵赖；接收方通过发送方的数字证书的公钥对签名进行解密得到数据哈希值，接收方对接收到的原数据进行哈希运算，比较两个哈希值是否一致，从而验证了传输数据是否完整，保障了传输数据的篡改。当通信双方受到中间人攻击时，因为数字签名具有认证发送方的功能，所以对数据的签名有效防止了第三方假冒成通信方或是伪造成通信方。

在运用公钥加密算法时，因为接收方的私钥是保密的，只有接收方才能查看到会话密钥，所以公钥加密保证了会话密钥的机密性，保证了会话密钥只有通信双方拥有。当通信双方受到第三方攻击时，即使中间人截获了会话密钥，中间人仍然无法获得会话密钥。因此，公钥加密能够为通信双方提供足够的保密性。

（3） SM3 密码杂凑算法安全性的分析。协议采用 SM3 算法对通信双方的传输数据进行完整性认证。发送方对数据进行哈希运算发给接收方，接收方则对解密得到的哈希值和原数据哈希运算得到的哈希值比较并判断两者是否一致，检验传输数据是否有被篡改。SM3 密码杂凑算法需要经过填充和迭代压缩，生成的长度有 256bit，在遇到穷搜索攻击时，也能有效保护数据的完整性。

（4） SM4 密码算法安全性分析。协议采用 SM4 算法对通信双方的传输信息数据进行加密。发送方使用 SM4 加密算法对数据进行加密，而接收方利用协商好的会话密钥，使用相同的密码对数据进行解密。SM4 分组算法的数据分组长度为 128 比特密钥，分组长度为 128 比特，当遇到差分攻击时，又因为 SM4 密码算法采用的是 32 轮迭代结构，攻击人也无法查看传输数据的内容。因此，SM4 算法确保了数据的机密性[15]。

（5） 时间戳的作用分析。时间戳在各个通信环节中充当着唯一标识的时间，因为有时间戳，当遇到第三方截获了双方的历史的通信报文时，能防止通信中受到重放攻击的威胁。

3.3 系统的样机实现与性能分析

为了验证本文提出的网上银行转账模型和系统转账业务密码应用协议的可行性和有效性，本文设计实现了一个相应的网上银行系统转账业务样机系统。该系统主要包括了用户转账身份鉴别功能、转账业务电子单自动加密、转账业务电子单数字签名、转账业务电子单数字签名验证等功能模块。

（1） 用户转账身份鉴别模块

该模块的功能是：用户在进行转账时，用户与服务端需要相互鉴别彼此的身份。即用户与服务端相互发送自身的数字证书和签名数字证书给对方，以此表明身份，实现双方的身份认证。

用户、服务端接收到对方的数字证书和签名数字证书后，先使用根证书 CA 里的公钥（rootcert.pem）对数字证书进行验证，以此检验证书的真伪，验证成功后，使用接收到的数字证书的公钥验证签名数字证书，如果验证通过，则证明了对方的身份。

（2） 转账业务电子单自动加密模块

该模块的功能是：当服务端接收到用户发送的转账数据后，自动加密接收到的转账数据。该模块使用 GmSSL 以及 SM4 算法自动加密转账数据，得到转账加密数据：endsm4 文件。SM4 算法为密码体制中的对称密码体制，无论是加密算法还是密钥扩展算法都是采用 32 轮非线性迭代结构，SM4 有很好的保密性，确保了转账数据的安全，保护了用户的隐私。

（3） 转账业务电子单数字签名模块

数字签名简单来说就是传统的手工签字与印章，能够解决转账信息数据被伪造、发送方抵赖行为、转账信息数据被冒充和转账信息数据被篡改问题，数字签名对保证网上银行转账交易安全有着重要的作用。

该功能模块的数字签名过程为：先使用哈希函数对转账数据（transfer.txt）进行摘要运算，再使用用户的私钥(clientkey.key)对其摘要签名，最后得到转账数据签名文件(transfersm3sm2.sig)。

（4） 转账业务电子单数字签名验证模块

对应转账业务电子单数字签名，该功能模块实现验证本地转账信息数据是否由用户发送、转账信息数据是否有被篡改。

该模块的处理过程大致如下：服务端接收到用户发送的转账信息数据后，需要先用 SM4 算法对加密转账数据（transfersm4.sms）进行解密，得到了用户发送过来的原转账数据并保存在 dsm4 文件；然后再对解密得到的转账数据信息（dsm4）进行哈希运算，利用从用户接收到的摘要转账数据文件（transfersm3）与其进行摘要对比，以对比结果来检验转账数据是否有被篡改，如果对比结果一致，则转账数据没有被篡改且表明了转账数据得到了很好的安全保护；最后利用解密得到的转账数据（dsm4）以及用户证书的公钥（pubkey2.pem）验证签名转账信息数据（transfersm3sm2.sig），如果验证成功，则表明了转账数据确实由用户发送，如果验证失败，则证明转账数据不是由用户发送或是转账数据遭受了篡改，应重视。

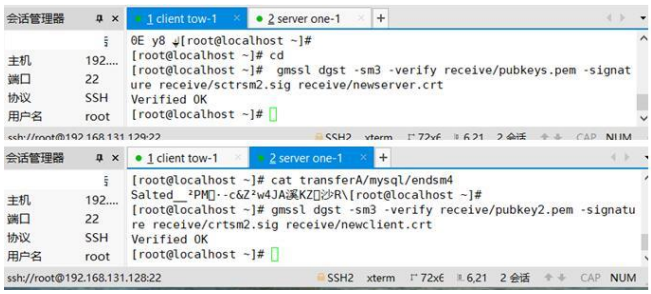

图 5 用户转账身份验证测试结果

（5） 样机系统的性能测试

样机系统开发完毕后，我们通过用例测试，对相关的功能进行单元测试，再利用测试结果分析优化代码、减少错误。测试的内容包括用户转账身份验证用例测试、转账业务电子单自动加密用例测试、转账业务电子单数字签名测试、转账业务电子单数字签名验证测试、数字签名验证用例测试、登录日志生成与自动加密用例测试等。

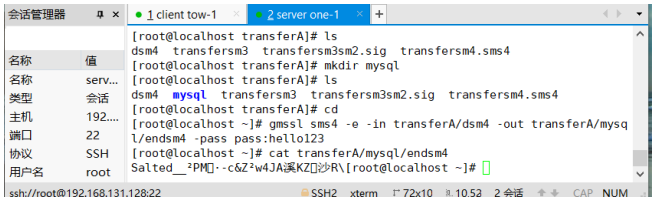

图 6 转账业务电子单自动加密测试

各个模块的测试结果见图 5-图 8。测试的结果表明，利用本文提出的网上银行系统转账业务框架模型和转账业务密码应用实现的样机系统运行正常、安全可靠，具备了用户与服务端的身份鉴别功能、转账信息自动加密功能、转账信息数字签名功能、转账信息数字签名验证功能，安全性达到了求椭圆曲线离散对数的困难水平，实现了设计目标。

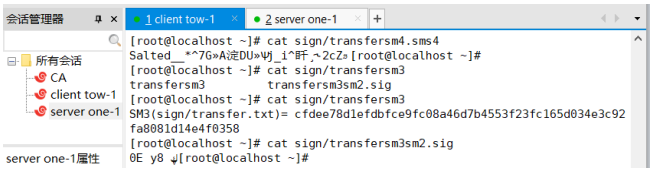

图 7 转账业务电子单数字签名测试结果

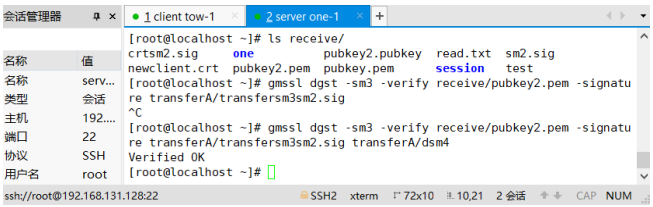

图 8 转账业务电子单数字签名验证测试结果

4 结束语

本文从网上银行功能需求分析着手，使用 GmSSL 的加密数据包、数字签名技术以及 Mysql 数据库等技术，提出了一种基于密码技术的网上银行系统转账业务框架模型，设计了网上银行转账业务密码应用协议，分析了协议的安全性。最后实现了具有相互身份鉴别、数字签名等功能的网上银行系统。系统实现运用了 Linux 操作系统、数据库等技术将数字签名与网上银行系统安全集成，实现了可靠的转账信息身份验证、数据安全管理等功能，为保证用户身份的真实性与合法性、实现网上银行交易双方的抗抵赖、解决数据信息的保密性和完整性安全问题、降低银行服务经营成本以及提高银行服务质量提供了一种安全可靠的解决方案。

参 考 文 献

[1] 李伟. 量子保密通信在银行安全系统中的应用及其关键技术的研究[D]. 华东交通大学, 2015.

[2] 褚学恭. 浅谈网上银行的安全威胁和风险防范[J]. 科技创新导报, 2020, 17(8): 241-242

[3] J. A. Ojeniyi, E. O. Edward, S. i M. Abdulhamid. Security Risk Analysis in Online Banking Transactions: Using Diamond Bank as a Case Study[J]. International Journal of Education and Management Engineering, 2019, 9(2): 1-14

[4] 陈肖华. 改进的网上银行认证技术及应用研究[D].广西大学,2013.

[5] 余庆. 基于指纹识别和PKI的网上银行身份认证系统设计[D].浙江工业大学,2011.

[6] 丛婧. 基于公开密钥基础设施的网上银行网站设计与实现[D].湖南大学,2013.

[7] 钱学洪. 基于动态口令的网上银行安全认证研究[D].电子科技大学,2011.

[8] S. S. Hari,C. Kavinkumar,G. K. Niketh, et al. Security of One Time Passwords in Online Banking Systems[J]. International Journal of Recent Technology and Engineering,2019. 7(5s3): 319-324

[9] 张波.网上银行信息安全系统的开发与实现[D].长沙：湖南大学，2015

[10] 李响.网上银行安全机制的研究与实现[D].成都：电子科技大学，2014

[11] 王钦.网上银行交易安全分析与系统设计[D].长沙：湖南大学，2014

[12] 顾杰超.基于 CICS 的网上银行安全转帐子系统的设计和研究[D].上海：复旦大学，2014

[13] 王胤, 谢宗晓.《网上银行系统信息安全通用规范》概述及修订分析[J].中国质量与标准导报,2020,(1):13-15

[14] 全艳.从网上银行安全看网络金融安全防范[J].金融经济, 2018,(4):67-68

[15] 沈明珠, 路雨桐, 徐逸楠.“互联网+”时代下银行卡的网上支付安全问题研究[J]. 经济研究导刊,2017,(26): 189-192