

1. 基于近场通信的移动钱包安全支付方法,用于具有NFC功能的移动钱包、具有NFC功能的消费POS结算终端、认证机构以及银行账户管理平台组成的支付系统,其特征在于,依次包括如下步骤(1)至步骤(12):

(1) 消费POS结算终端和移动钱包分别发送信用签证请求给认证机构,由认证机构分别生成消费POS结算终端和移动钱包的信用签证证书集合,并将信用签证证书集合分别发送给消费POS结算终端和移动钱包;其中:

所述消费POS结算终端标记为POS,移动钱包标记为Wallet,认证机构标记为TSM,消费POS结算终端的信用签证证书集合标记为Cert(TSM_{POS}),移动钱包的信用签证证书标记为Cert(TSM_{Wallet});消费POS结算终端信用签证证书集合Cert(TSM_{POS})和移动钱包信用签证证书集合Cert(TSM_{Wallet})分别由如下公式表示:

$$\text{Cert}(\text{TSM}_{\text{POS}}) = \{\text{Cert}^1(\text{TSM}_{\text{POS}}), \text{Cert}^2(\text{TSM}_{\text{POS}}), \dots, \text{Cert}^m(\text{TSM}_{\text{POS}})\};$$

$$\text{Cert}(\text{TSM}_{\text{Wallet}}) = \{\text{Cert}^1(\text{TSM}_{\text{Wallet}}), \text{Cert}^2(\text{TSM}_{\text{Wallet}}), \dots, \text{Cert}^m(\text{TSM}_{\text{Wallet}})\}; m \geq 3;$$

其中,m表示消费POS结算终端以及移动钱包可用的信用签证证书个数,所述消费POS结算终端信用签证证书集合中的各信用签证证书以及所述移动钱包信用签证证书集合中的各信用签证证书遵循遍历使用规则且均限制使用一次;

(2) 消费POS结算终端在银行账户管理平台注册收款账户和账户密码,移动钱包在银行账户管理平台注册付款账户和支付密码,并由消费POS结算终端和移动钱包分别发送金融签证请求给银行账户管理平台,由银行账户管理平台分别生成消费POS结算终端和移动钱包的金融签证证书集合,并将金融签证证书集合分别发送给消费POS结算终端和移动钱包;其中:

所述银行账户管理平台标记为BANK,消费POS结算终端的金融签证证书集合标记为Cert(BANK_{POS}),移动钱包的金融签证证书集合标记为Cert(BANK_{Wallet}),消费POS结算终端金融签证证书集合Cert(BANK_{POS})和移动钱包信用签证证书集合Cert(TSM_{Wallet})分别由如下公式表示:

$$\text{Cert}(\text{BANK}_{\text{POS}}) = \{\text{Cert}^1(\text{BANK}_{\text{POS}}), \text{Cert}^2(\text{BANK}_{\text{POS}}), \dots, \text{Cert}^m(\text{BANK}_{\text{POS}})\};$$

$$\text{Cert}(\text{BANK}_{\text{Wallet}}) = \{\text{Cert}^1(\text{BANK}_{\text{Wallet}}), \text{Cert}^2(\text{BANK}_{\text{Wallet}}), \dots, \text{Cert}^m(\text{BANK}_{\text{Wallet}})\}; m \geq 3;$$

其中,消费POS终端的信用签证证书与其金融签证证书为一一对应关系,移动钱包的信用签证证书与其金融签证证书为一一对应关系;所述消费POS结算终端金融签证证书集合中的各金融签证证书以及所述移动钱包金融签证证书集合中的各金融签证证书遵循遍历使用规则且均限制使用一次;

(3) 消费POS结算终端生成第一随机数和第一随机数的有效时间值,获取消费POS结算终端当前位置、当前位置的噪声和空气湿度数据,并存储该第一随机数和有效时间值,然后将包括消费POS结算终端自身签名的付款请求信息发送给移动钱包,并发送消费POS结算终端当前位置及当前位置的噪声和空气湿度数据给认证机构;其中:

所述付款请求信息包括消费POS结算终端生成的第一随机数RP₁、该第一随机数RP₁的有效时间值TP、付款请求ReqW、消费POS结算终端选取的金融签证证书Cert^t(BANK_{POS})、消费POS结算终端选取的信用签证证书Cert^t(TSM_{POS})、消费POS结算终端的自身签名Sig_{POS}以及消费POS结算终端的私钥sk(POS);其中,该付款请求信息标记为Message_{P-W},付款请求信息Message_{P-W}由公式标记如下:

$$Message_{P-W} = \left\{ \begin{array}{l} POS, Wallet, RP_1, TP, Cert^t(BANK_{POS}), Cert^t(TSM_{POS}), ReqW, \\ Sig_{POS}, sk(POS) \end{array} \right\}; \quad t \in [1, m];$$

(4) 移动钱包在预设时间周期内实时采集其合法拥有者施加在键盘上各按键的摁压力数值及摁压力方向, 构建移动钱包合法拥有者利用左手和右手分别针对各按键的左手摁压力数据库和右手摁压力数据库, 并分别计算各按键左手摁压力数据库和右手摁压力数据库的方差; 其中:

所述移动钱包上第*i*个按键标记为Button*i*, 针对按键Button*i*所构建的移动钱包合法拥有者的左手摁压力数据库标记为 $F_{Button_i}^{Left}$, $F_{Button_i}^{Left} = \{F_{Button_i}^{Left}(n)\}$, 移动钱包合法拥有者的右手摁压力数据库标记为 $F_{Button_i}^{Right}$, $F_{Button_i}^{Right} = \{F_{Button_i}^{Right}(n)\}$, $n \in N$, N 为左手摁压力数据库以及摁压力数据库中分别存储的摁压力数据个数; $F_{Button_i}^{Left}(n)$ 表示针对按键Button*i*采集的移动钱包合法拥有者左手的第*n*个摁压力数据, $F_{Button_i}^{Right}(n)$ 表示针对按键Button*i*采集的移动钱包合法拥有者右手的第*n*个摁压力数据; 所述按键Button*i*所受移动钱包合法拥有者左手摁压力的方差标记为 $\sigma_{Left}^2(Button_i)$, 移动钱包合法拥有者右手摁压力的方差标记为 $\sigma_{Right}^2(Button_i)$; 其中, 方差 $\sigma_{Left}^2(Button_i)$ 和 $\sigma_{Right}^2(Button_i)$ 的计算公式分别如下:

$$\sigma_{Left}^2(Button_i) = \sum_{n=1}^N \frac{(F_{Button_i}^{Left}(n) - \overline{F}_{Button_i}^{Left})^2}{N}, \quad \overline{F}_{Button_i}^{Left} = \sum_{n=1}^N \frac{F_{Button_i}^{Left}(n)}{N};$$

$$\sigma_{Right}^2(Button_i) = \sum_{n=1}^N \frac{(F_{Button_i}^{Right}(n) - \overline{F}_{Button_i}^{Right})^2}{N}, \quad \overline{F}_{Button_i}^{Right} = \sum_{n=1}^N \frac{F_{Button_i}^{Right}(n)}{N};$$

(5) 移动钱包接收消费POS结算终端发送的付款请求信息, 生成防窃密的第一随机数, 获取移动钱包当前位置、当前位置的噪声和空气湿度数据, 并发送包括消费POS结算终端付款请求信息的认证请求信息以及移动钱包当前位置、当前位置的噪声和空气湿度数据给认证机构; 其中:

所述移动钱包发送的认证请求信息包括消费POS结算终端的付款请求信息Message_{P-W}、移动钱包生成的防窃密的第一随机数RW₁、认证请求ReqT、其与消费POS结算终端会话请求ReqSession以及移动钱包与认证机构间通信的公钥k(Wallet, TSM); 其中, 移动钱包的该认证请求信息标记为Message_{W-T}, Message_{W-T}由公式标记如下:

$$Message_{W-T} = \{Message_{P-W}, TSM, RW_1, ReqT, ReqSession, k(Wallet, TSM)\};$$

(6) 认证机构接收、提取移动钱包发送的认证请求信息以及移动钱包当前位置、当前位置的噪声和空气湿度数据, 记录接收移动钱包认证请求的时间, 并根据所提取的移动钱包的认证请求信息、移动钱包当前位置及当前位置噪声和空气湿度数据、消费POS结算终端当前位置及当前位置噪声和空气湿度数据对移动钱包做出交易反馈; 其中, 该步骤依次包括步骤(6-1)至步骤(6-3):

(6-1) 当认证机构判断提取的认证请求信息中的消费POS结算终端信用签证证书存在于认证机构已存储的信用签证证书数据库中且认证机构接收移动钱包认证请求时间位于第一随机数的有效时间值内时, 表明该信用签证证书有效且对应的消费POS终端为安全NFC

终端,认证机构生成移动钱包与消费POS终端之间的交易秘钥,并执行步骤(6-2);否则,认证机构发送拒绝交易信息给移动钱包;

(6-2)认证机构根据提取的消费POS结算终端当前位置噪声数据和移动钱包当前位置噪声数据,判断消费POS结算终端与移动钱包所分别对应的当前位置噪声之差位于预设的差值范围内,且消费POS结算终端与移动钱包所分别对应的当前位置之差位于预设的距离差值范围之内时,执行步骤(6-3);否则,认证机构发送拒绝交易信息给移动钱包;则认证机构发送确认交易信息给移动钱包;

(6-3)认证机构根据提取的消费POS结算终端当前位置空气湿度数据和移动钱包当前位置空气湿度数据,判断消费POS结算终端与移动钱包所分别对应的当前位置空气湿度之差位于预设的差值范围内时,则认证机构发送确认交易信息给移动钱包;否则,认证机构发送拒绝交易信息给移动钱包;其中:

所述认证机构发送的确认交易信息标记为Message_{T-W-Confirm},认证机构发送的拒绝交易信息标记为Message_{T-W-Reject};Message_{T-W-Confirm}和Message_{T-W-Reject}分别由公式标记如下:

$$\text{Message}_{T-W-Confirm} = \{TSM, Wallet, POS, RP_1, RW_1, TP, \text{Cert}^t(TSM_{POS}), K, k(Wallet, TSM)\};$$

$$\text{Message}_{T-W-Reject} = \{TSM, Wallet, POS, RP_1, RW_1, \text{RejectP}, k(Wallet, TSM)\};$$

(7)移动钱包接收认证机构发送的确认交易信息,并将包括移动钱包签名的交易交互信息发送给消费POS结算终端;其中:

所述交易交互信息包括移动钱包的签名Sig_{Wallet}、移动钱包生成的防窃密的第一随机数RW₁、移动钱包与消费POS终端之间的交易秘钥K、移动钱包选取的金融签证证书Cert^s(BANK_{Wallet})、移动钱包选取的信用签证证书Cert^s(TSM_{Wallet})以及消费POS结算终端的信用签证证书Cert^t(TSM_{POS});其中,所述移动钱包发送的交易交互信息标记为Message_{W-P},Message_{W-P}由公式标记如下:

$$\text{Message}_{W-P} = \left\{ \begin{array}{l} Wallet, POS, TSM, RW_1, \text{Cert}^s(BANK_{Wallet}), \text{Cert}^s(TSM_{Wallet}), K, \\ \text{Sig}_{Wallet}, \text{Cert}^t(TSM_{POS}) \end{array} \right\}; \quad s \in [1, m];$$

(8)消费POS结算终端接收、提取移动钱包发送的交易交互信息,并根据在交易交互信息中提取的信息做出判断:

当消费POS结算终端在交易交互信息中提取到的消费POS结算终端信用签证证书已经存储于其存储的信用签证证书数据库中时,则执行步骤(9);否则,消费POS结算终端拒绝与移动钱包进行支付交易;

(9)消费POS结算终端生成第二随机数,并发送包括生成的第二随机数、第一随机数、移动钱包防窃密的第一随机数、移动钱包所需支付款项数据的支付款项信息给移动钱包;其中,所述支付款项信息记为Message_{P-W-Payment},Message_{P-W-Payment}由公式标记如下:

$$\text{Message}_{P-W-Payment} = \{POS, Wallet, RP_2, RW_1, RP_1, Payment, K\};$$

其中,RP₂表示消费POS结算终端生成的第二随机数,Payment表示移动钱包所需支付款项,K为消费POS结算终端与移动钱包之间的交易秘钥;

(10)移动钱包接收消费POS结算终端发送的支付款项信息,并生成防窃密的第二随机数,由移动钱包将包括所接收支付款项信息以及新生成第二随机数的支付交易记录信息发送给签证机构存储;其中,所述支付交易记录信息标记为S_{W-T-Payment},支付交易记录信息

$S_{W-T-Payment}$ 由公式标记如下：

$$S_{W-T-Payment} = \{Wallet, TSM, POS, RW_2, k(Wallet, TSM)\};$$

其中， RW_2 表示移动钱包生成的防窃密的第二随机数；

(11)移动钱包接收外部通过各按键输入的支付密码，由移动钱包根据各按键所受摁压力方向判断摁压各按键的为左手或右手，并将各摁键所受摁压力添加到判断结果所对应的左手摁压力数据库或右手摁压力数据库中，重新计算此时各按键对应摁压力数据库的方差；

(12)移动钱包根据步骤(11)中各按键重新所得摁压力数据库方差与步骤(4)中所对应摁压力数据库方差之间的差值，对是否执行支付操作做出判断：

(12-1)当各按键所得差值均小于或等于预设阈值时，表示该支付密码为移动钱包合法拥有者所输入，移动钱包发送包括该支付密码、其金融签证证书和信用签证证书的支付命令给银行账户管理平台，由银行账户管理平台判断支付密码与预设支付密码一致时，将移动钱包付款账户的款项转移至消费POS结算终端在银行账户管理平台的收款账户内，并由银行账户管理平台存储移动钱包发送的支付命令；

(12-2)当各按键所得差值中出现大于预设阈值时，表示该支付密码不是移动钱包合法拥有者输入，移动钱包拒绝执行支付操作。

基于近场通信的移动钱包安全支付方法

技术领域

[0001] 本发明涉及移动支付领域,尤其涉及一种基于近场通信的移动钱包安全支付方法。

背景技术

[0002] 移动支付也称手机支付,就是允许用户使用其移动终端(通常是手机)对所消费的商品或服务进行账务支付的一种服务方式。单位或个人通过移动设备、互联网或者近距离传感直接或间接向银行金融机构发送支付指令产生货币支付与资金转移行为,从而实现移动支付功能。移动支付将终端设备、互联网、应用提供商以及金融机构相融合,为用户提供货币支付、缴费等金融业务。移动支付主要分为近场支付和远程支付两种,所谓近场支付,就是用手机刷卡方式坐车、买东西等;远程支付是指,通过发送支付指令(如网银、电话银行、手机支付等)或借助支付工具(如通过邮寄、汇款)进行的支付方式,如掌中付推出的掌中电商,掌中充值,掌中视频等属于远程支付。

[0003] 在人们日常生活中,近场支付在移动支付中占据了更大的使用比例。作为近场支付的关键实现形式,基于近场通信(Near Field Communication,简称NFC)的NFC支付技术迅速兴起。内置有NFC功能模块的智能终端具有了NFC支付功能,而具有NFC支付功能的智能终端又被称为NFC移动钱包。

[0004] 随着具有NFC功能的消费POS结算终端在商场、停车场等场所的大量布局设置,NFC支付在方便人们日常生活的同时,也带来了严重的信息安全问题:当消费者处于商场中,由于人群密集,使得现有的NFC支付仍然存在信息泄漏或者恶意第三方伺机窥探支付信息,从而给消费者的经济利益带来严重威胁的问题;另外,一旦移动钱包丢失,非法用户通过破解方式获得支付密码后,也会给移动钱包合法拥有者经济利益造成威胁。

发明内容

[0005] 本发明所要解决的技术问题是针对上述现有技术提供一种既能够防止信息泄露,又可避免因移动钱包丢失而对其合法拥有者经济利益造成威胁的基于近场通信的移动钱包安全支付方法。

[0006] 本发明解决上述技术问题所采用的技术方案为:基于近场通信的移动钱包安全支付方法,用于具有NFC功能的移动钱包、具有NFC功能的消费POS结算终端、认证机构以及银行账户管理平台组成的支付系统,其特征在于,依次包括如下步骤(1)至步骤(12):

[0007] (1)消费POS结算终端和移动钱包分别发送信用签证请求给认证机构,由认证机构分别生成消费POS结算终端和移动钱包的信用签证证书集合,并将信用签证证书集合分别发送给消费POS结算终端和移动钱包;其中:

[0008] 所述消费POS结算终端标记为POS,移动钱包标记为Wallet,认证机构标记为TSM,消费POS结算终端的信用签证证书集合标记为Cert(TSM_{POS}),移动钱包的信用签证证书标记为Cert(TSM_{Wallet});消费POS结算终端信用签证证书集合Cert(TSM_{POS})和移动钱包信用签证

证书集合 $\text{Cert}(\text{TSM}_{\text{Wallet}})$ 分别由如下公式表示：

[0009] $\text{Cert}(\text{TSM}_{\text{POS}}) = \{\text{Cert}^1(\text{TSM}_{\text{POS}}), \text{Cert}^2(\text{TSM}_{\text{POS}}), \dots, \text{Cert}^m(\text{TSM}_{\text{POS}})\};$

[0010] $\text{Cert}(\text{TSM}_{\text{Wallet}}) = \{\text{Cert}^1(\text{TSM}_{\text{Wallet}}), \text{Cert}^2(\text{TSM}_{\text{Wallet}}), \dots, \text{Cert}^m(\text{TSM}_{\text{Wallet}})\}; m \geq 3;$

[0011] 其中， m 表示消费POS结算终端以及移动钱包可用的信用签证证书个数，所述消费POS结算终端信用签证证书集合中的各信用签证证书以及所述移动钱包信用签证证书集合中的各信用签证证书遵循遍历使用规则且均限制使用一次；

[0012] (2)消费POS结算终端在银行账户管理平台注册收款账户和账户密码，移动钱包在银行账户管理平台注册付款账户和支付密码，并由消费POS结算终端和移动钱包分别发送金融签证请求给银行账户管理平台，由银行账户管理平台分别生成消费POS结算终端和移动钱包的金融签证证书集合，并将金融签证证书集合分别发送给消费POS结算终端和移动钱包；其中：

[0013] 所述银行账户管理平台标记为BANK，消费POS结算终端的金融签证证书集合标记为 $\text{Cert}(\text{BANK}_{\text{POS}})$ ，移动钱包的金融签证证书集合标记为 $\text{Cert}(\text{BANK}_{\text{Wallet}})$ ，消费POS结算终端金融签证证书集合 $\text{Cert}(\text{BANK}_{\text{POS}})$ 和移动钱包信用签证证书集合 $\text{Cert}(\text{TSM}_{\text{Wallet}})$ 分别由如下公式表示：

[0014] $\text{Cert}(\text{BANK}_{\text{POS}}) = \{\text{Cert}^1(\text{BANK}_{\text{POS}}), \text{Cert}^2(\text{BANK}_{\text{POS}}), \dots, \text{Cert}^m(\text{BANK}_{\text{POS}})\};$

[0015] $\text{Cert}(\text{BANK}_{\text{Wallet}}) = \{\text{Cert}^1(\text{BANK}_{\text{Wallet}}), \text{Cert}^2(\text{BANK}_{\text{Wallet}}), \dots, \text{Cert}^m(\text{BANK}_{\text{Wallet}})\}; m \geq 3;$

[0016] 其中，消费POS终端的信用签证证书与其金融签证证书为一一对应关系，移动钱包的信用签证证书与其金融签证证书为一一对应关系；所述消费POS结算终端金融签证证书集合中的各金融签证证书以及所述移动钱包金融签证证书集合中的各金融签证证书遵循遍历使用规则且均限制使用一次；

[0017] (3)消费POS结算终端生成第一随机数和第一随机数的有效时间值，获取消费POS结算终端当前位置、当前位置的噪声和空气湿度数据，并存储该第一随机数和有效时间值，然后将包括消费POS结算终端自身签名的付款请求信息发送给移动钱包，并发送消费POS结算终端当前位置及当前位置的噪声和空气湿度数据给认证机构；其中：

[0018] 所述付款请求信息包括消费POS结算终端生成的第一随机数 RP_1 、该第一随机数 RP_1 的有效时间值 TP 、付款请求 $ReqW$ 、消费POS结算终端选取的金融签证证书 $\text{Cert}^t(\text{BANK}_{\text{POS}})$ 、消费POS结算终端选取的信用签证证书 $\text{Cert}^t(\text{TSM}_{\text{POS}})$ 、消费POS结算终端的自身签名 Sig_{POS} 以及消费POS结算终端的私钥 $sk(POS)$ ；其中，该付款请求信息标记为 $Message_{P-W}$ ，付款请求信息 $Message_{P-W}$ 由公式标记如下：

[0019]

$$\text{Message}_{P-W} = \left\{ POS, Wallet, RP_1, TP, \text{Cert}^t(BANK_{POS}), \text{Cert}^t(TSM_{POS}), ReqW, \right. \\ \left. Sig_{POS}, sk(POS) \right\}; \quad t \in [1, m];$$

[0020] (4)移动钱包在预设时间周期内实时采集其合法拥有者施加在键盘上各按键的摁压力数值及摁压力方向，构建移动钱包合法拥有者利用左手和右手分别针对各按键的左手摁压力数据库和右手摁压力数据库，并分别计算各按键左手摁压力数据库和右手摁压力数据库的方差；其中：

[0021] 所述移动钱包上第*i*个按键标记为 $Button_i$ ，针对按键 $Button_i$ 所构建的移动钱包合

法拥有者的左手摁压力数据库标记为 $F_{Button_i}^{Left}$ ， $F_{Button_i}^{Left} = \{F_{Button_i}^{Left}(n)\}$ ，移动钱包合法拥有者的右手摁压力数据库标记为 $F_{Button_i}^{Right}$ ， $F_{Button_i}^{Right} = \{F_{Button_i}^{Right}(n)\}$ ， $n \in N$ ， N 为左手摁压力数据库以及摁压力数据库中分别存储的摁压力数据个数； $F_{Button_i}^{Left}(n)$ 表示针对按键 $Button_i$ 采集的移动钱包合法拥有者左手的第 n 个摁压力数据， $F_{Button_i}^{Right}(n)$ 表示针对按键 $Button_i$ 采集的移动钱包合法拥有者右手的第 n 个摁压力数据；所述按键 $Button_i$ 所受移动钱包合法拥有者左手摁压力的方差标记为 $\sigma_{Left}^2(Button_i)$ ，移动钱包合法拥有者右手摁压力的方差标记为 $\sigma_{Right}^2(Button_i)$ ；其中，方差 $\sigma_{Left}^2(Button_i)$ 和 $\sigma_{Right}^2(Button_i)$ 的计算公式分别如下：

$$[0022] \quad \sigma_{Left}^2(Button_i) = \sum_{n=1}^N \frac{(F_{Button_i}^{Left}(n) - \bar{F}_{Button_i}^{Left})^2}{N}, \quad \bar{F}_{Button_i}^{Left} = \sum_{n=1}^N \frac{F_{Button_i}^{Left}(n)}{N};$$

$$[0023] \quad \sigma_{Right}^2(Button_i) = \sum_{n=1}^N \frac{(F_{Button_i}^{Right}(n) - \bar{F}_{Button_i}^{Right})^2}{N}, \quad \bar{F}_{Button_i}^{Right} = \sum_{n=1}^N \frac{F_{Button_i}^{Right}(n)}{N};$$

[0024] (5)移动钱包接收消费POS结算终端发送的付款请求信息，生成防窃密的第一随机数，获取移动钱包当前位置、当前位置的噪声和空气湿度数据，并发送包括消费POS结算终端付款请求信息的认证请求信息以及移动钱包当前位置、当前位置的噪声和空气湿度数据给认证机构；其中：

[0025] 所述移动钱包发送的认证请求信息包括消费POS结算终端的付款请求信息 $Message_{P-W}$ 、移动钱包生成的防窃密的第一随机数 RW_1 、认证请求 $ReqT$ 、其与消费POS结算终端会话请求 $ReqSession$ 以及移动钱包与认证机构间通信的公钥 $k(Wallet, TSM)$ ；其中，移动钱包的该认证请求信息标记为 $Message_{W-T}$ ， $Message_{W-T}$ 由公式标记如下：

[0026] $Message_{W-T} = \{Message_{P-W}, TSM, RW_1, ReqT, ReqSession, k(Wallet, TSM)\}$ ；

[0027] (6)认证机构接收、提取移动钱包发送的认证请求信息以及移动钱包当前位置、当前位置的噪声和空气湿度数据，记录接收移动钱包认证请求的时间，并根据所提取的移动钱包的认证请求信息、移动钱包当前位置及当前位置噪声和空气湿度数据、消费POS结算终端当前位置及当前位置噪声和空气湿度数据对移动钱包做出交易反馈；其中，该步骤依次包括步骤(6-1)至步骤(6-3)：

[0028] (6-1)当认证机构判断提取的认证请求信息中的消费POS结算终端信用签证证书存在于认证机构已存储的信用签证证书数据库中且认证机构接收移动钱包认证请求时间位于第一随机数的有效时间值内时，表明该信用签证证书有效且对应的消费POS终端为安全NFC终端，认证机构生成移动钱包与消费POS终端之间的交易秘钥，并执行步骤(6-2)；否则，认证机构发送拒绝交易信息给移动钱包；

[0029] (6-2)认证机构根据提取的消费POS结算终端当前位置噪声数据和移动钱包当前位置噪声数据，判断消费POS结算终端与移动钱包所分别对应的当前位置噪声之差位于预设的差值范围内，且消费POS结算终端与移动钱包所分别对应的当前位置之差位于预设的距离差值范围之内时，执行步骤(6-3)；否则，认证机构发送拒绝交易信息给移动钱包；则认证机构发送确认交易信息给移动钱包；

[0030] (6-3)认证机构根据提取的消费POS结算终端当前位置空气湿度数据和移动钱包当前位置空气湿度数据,判断消费POS结算终端与移动钱包所分别对应的当前位置空气湿度之差位于预设的差值范围内时,则认证机构发送确认交易信息给移动钱包;否则,认证机构发送拒绝交易信息给移动钱包;其中:

[0031] 所述认证机构发送的确认交易信息标记为Message_{T-W-Confirm},认证机构发送的拒绝交易信息标记为Message_{T-W-Reject};Message_{T-W-Confirm}和Message_{T-W-Reject}分别由公式标记如下:

[0032] $Message_{T-W-Confirm} = \{TSM, Wallet, POS, RP_1, RW_1, TP, Cert^t(TSM_{POS}), K, k(Wallet, TSM)\};$

[0033] $Message_{T-W-Reject} = \{TSM, Wallet, POS, RP_1, RW_1, RejectP, k(Wallet, TSM)\};$

[0034] (7)移动钱包接收认证机构发送的确认交易信息,并将包括移动钱包签名的交易交互信息发送给消费POS结算终端;其中:

[0035] 所述交易交互信息包括移动钱包的签名Sig_{Wallet}、移动钱包生成的防窃密的第一随机数RW₁、移动钱包与消费POS终端之间的交易秘钥K、移动钱包选取的金融签证证书Cert^s(BANK_{Wallet})、移动钱包选取的信用签证证书Cert^s(TSM_{Wallet})以及消费POS结算终端的信用签证证书Cert^t(TSM_{POS});其中,所述移动钱包发送的交易交互信息标记为Message_{W-P},Message_{W-P}由公式标记如下:

[0036]

$$Message_{W-P} = \left\{ \begin{array}{l} Wallet, POS, TSM, RW_1, Cert^s(BANK_{Wallet}), Cert^s(TSM_{Wallet}), K, \\ \{Sig_{Wallet}, Cert^t(TSM_{POS})\} \end{array} \right\}; \quad s \in [1, m];$$

[0037] (8)消费POS结算终端接收、提取移动钱包发送的交易交互信息,并根据在交易交互信息中提取的信息做出判断:

[0038] 当消费POS结算终端在交易交互信息中提取到的消费POS结算终端信用签证证书已经存储于其存储的信用签证证书数据库中时,则执行步骤(9);否则,消费POS结算终端拒绝与移动钱包进行支付交易;

[0039] (9)消费POS结算终端生成第二随机数,并发送包括生成的第二随机数、第一随机数、移动钱包防窃密的第一随机数、移动钱包所需支付款项数据的支付款项信息给移动钱包;其中,所述支付款项信息记为Message_{P-W-Payment},Message_{P-W-Payment}由公式标记如下:

[0040] $Message_{P-W-Payment} = \{POS, Wallet, RP_2, RW_1, RP_1, Payment, K\};$

[0041] 其中,RP₂表示消费POS结算终端生成的第二随机数,Payment表示移动钱包所需支付款项,K为消费POS结算终端与移动钱包之间的交易秘钥;

[0042] (10)移动钱包接收消费POS结算终端发送的支付款项信息,并生成防窃密的第二随机数,由移动钱包将包括所接收支付款项信息以及新生成第二随机数的支付交易记录信息发送给签证机构存储;其中,所述支付交易记录信息标记为S_{W-T-Payment},支付交易记录信息S_{W-T-Payment}由公式标记如下:

[0043] $S_{W-T-Payment} = \{Wallet, TSM, POS, RW_2, k(Wallet, TSM)\};$

[0044] 其中,RW₂表示移动钱包生成的防窃密的第二随机数;

[0045] (11)移动钱包接收外部通过各按键输入的支付密码,由移动钱包根据各按键所受

摁压力方向判断摁压各按键的为左手或右手，并将各摁键所受摁压力添加到判断结果所对应的左手摁压力数据库或右手摁压力数据库中，重新计算此时各按键对应摁压力数据库的方差；

[0046] (12)移动钱包根据步骤(11)中各按键重新所得摁压力数据库方差与步骤(4)中所对应摁压力数据库方差之间的差值，对是否执行支付操作做出判断；

[0047] (12-1)当各按键所得差值均小于或等于预设阈值时，表示该支付密码为移动钱包合法拥有者所输入，移动钱包发送包括该支付密码、其金融签证证书和信用签证证书的支付命令给银行账户管理平台，由银行账户管理平台判断支付密码与预设支付密码一致时，将移动钱包付款账户的款项转移至消费POS结算终端在银行账户管理平台的收款账户内，并由银行账户管理平台存储移动钱包发送的支付命令；

[0048] (12-2)当各按键所得差值中出现大于预设阈值时，表示该支付密码不是移动钱包合法拥有者输入，移动钱包拒绝执行支付操作。

[0049] 与现有技术相比，本发明的优点在于：

[0050] 首先，消费POS结算和移动钱包分别在认证机构、银行账户管理平台处获得各自对应的信用签证证书集合和金融签证证书集合，消费POS结算终端以其防窃密的第一随机数和有效时间值作为保证交易安全的条件，并将仅限单次使用有效的信用签证证书添加到付款请求信息中，以防止信用签证证书被恶意第三方重复使用，造成信息泄漏；

[0051] 其次，消费POS结算终端和移动钱包均分别发送其当前位置、当前位置噪声和空气湿度数据给认证机构，由认证机构判断消费POS结算终端与移动钱包交易双方处于安全交易的同一个位置环境时，则分别发送交易秘钥给消费POS结算终端和移动钱包，即利用同一位置同一环境参数值相同的特点以及两者的位置距离，来共同实现对消费POS结算终端和移动钱包所处交易位置的准确判断，以保证两者间的支付交易安全；

[0052] 再次，利用人体行为特征的唯一性，移动钱包通过构建其合法拥有者支付时，施加在各按键的左手摁压力数据库和右手摁压力数据库对合法拥有者的身份信息再次认证，并在移动钱包进行支付操作时，进行关于各按键所受摁压力数值及方法的匹配，以防止非法用户单纯依靠破解移动钱包支付密码即可威胁移动钱合法拥有者的经济利益，从而在完成移动钱包支付的同时，也保证了支付信息不被泄露，同样避免了因移动钱包丢失而对其合法拥有者经济利益造成威胁的问题。

附图说明

[0053] 图1为本发明实施例中支付系统的结构示意图；

[0054] 图2为本发明中基于近场通信的移动钱包安全支付方法的流程示意图。

具体实施方式

[0055] 以下结合附图实施例对本发明作进一步详细描述。

[0056] 本实施例中基于近场通信的移动钱包安全支付方法，用于具有NFC功能的移动钱包、具有NFC功能的消费POS结算终端、认证机构以及银行账户管理平台组成的支付系统，该支付系统参见图1所示。其中，参见图2所示，本实施例中基于近场通信的移动钱包安全支付方法依次包括如下步骤：

[0057] 步骤1,消费POS结算终端和移动钱包分别发送信用签证请求给认证机构,由认证机构分别生成消费POS结算终端和移动钱包的信用签证证书集合,并将信用签证证书集合分别发送给消费POS结算终端和移动钱包;信用签证证书集合中包含有多个供选择使用的信用签证证书,信用签证证书作为消费POS结算终端或移动钱包的可信凭证,用以核准支付交易双方的合法身份,以保证支付交易的安全;消费POS结算终端和移动钱包可以根据需要,在各自对应的信用签证证书集合中遍历地选择信用签证证书;其中:

[0058] 消费POS结算终端标记为POS,移动钱包标记为Wallet,认证机构标记为TSM,消费POS结算终端的信用签证证书集合标记为Cert(TSM_{POS}),移动钱包的信用签证证书标记为Cert(TSM_{Wallet});消费POS结算终端信用签证证书集合Cert(TSM_{POS})和移动钱包信用签证证书集合Cert(TSM_{Wallet})分别由如下公式表示:

$$[0059] \text{Cert}(\text{TSM}_{\text{POS}}) = \{\text{Cert}^1(\text{TSM}_{\text{POS}}), \text{Cert}^2(\text{TSM}_{\text{POS}}), \dots, \text{Cert}^m(\text{TSM}_{\text{POS}})\};$$

$$[0060] \text{Cert}(\text{TSM}_{\text{Wallet}}) = \{\text{Cert}^1(\text{TSM}_{\text{Wallet}}), \text{Cert}^2(\text{TSM}_{\text{Wallet}}), \dots, \text{Cert}^m(\text{TSM}_{\text{Wallet}})\}; m \geq 3;$$

[0061] 其中,m表示消费POS结算终端以及移动钱包可用的信用签证证书个数;消费POS结算终端需要使用其信用签证证书时,则在信用签证证书集合的m个信用签证证书中依次遍历地进行选择使用,同一个信用签证证书不会被重复使用,以此防止恶意第三方在窥探到消费POS结算终端已使用的信用签证证书后,再次对该信用签证证书使用,威胁消费POS结算终端交易安全;同样地,移动钱包也遵循与消费POS结算终端相同的使用规则,依次遍历选择使用其信用签证证书集合中的信用签证证书,且同一个信用签证证书不会被重复使用,即各信用签证证书遵循遍历使用规则且仅限制使用一次,信用签证证书被重复使用即为作废;

[0062] 步骤2,消费POS结算终端在银行账户管理平台注册收款账户和账户密码,移动钱包在银行账户管理平台注册付款账户和支付密码,并由消费POS结算终端和移动钱包分别发送金融签证请求给银行账户管理平台,由银行账户管理平台分别生成消费POS结算终端和移动钱包的金融签证证书集合,并将金融签证证书集合分别发送给消费POS结算终端和移动钱包;

[0063] 金融签证证书集合中包含有多个供选择使用的金融签证证书,金融签证证书用以表明消费POS结算终端或移动钱包对支付交易信息的确认,使消费POS结算终端或移动钱包对各自已经确认的支付交易不具有抵赖性,从而保证支付交易的正常进行;金融签证证书集合中的各金融签证证书也遵循同金融签证证书相同的使用规则;其中:银行账户管理平台记为BANK,消费POS结算终端的金融签证证书集合记为Cert(BANK_{POS}),移动钱包的金融签证证书集合记为Cert(BANK_{Wallet}),消费POS结算终端金融签证证书集合Cert(BANK_{POS})和移动钱包信用签证证书集合Cert(TSM_{Wallet})分别由如下公式表示:

$$[0064] \text{Cert}(\text{BANK}_{\text{POS}}) = \{\text{Cert}^1(\text{BANK}_{\text{POS}}), \text{Cert}^2(\text{BANK}_{\text{POS}}), \dots, \text{Cert}^m(\text{BANK}_{\text{POS}})\};$$

$$[0065] \text{Cert}(\text{BANK}_{\text{Wallet}}) = \{\text{Cert}^1(\text{BANK}_{\text{Wallet}}), \text{Cert}^2(\text{BANK}_{\text{Wallet}}), \dots, \text{Cert}^m(\text{BANK}_{\text{Wallet}})\}; m \geq 3;$$

[0066] 其中,消费POS终端的信用签证证书与其金融签证证书为一一对应关系,移动钱包的信用签证证书与其金融签证证书为一一对应关系;也就是说,当消费POS结算终端使用其信用签证证书集合中的第三个信用签证证书Cert³(TSM_{POS})时,消费POS结算终端则对应的使用其金融签证证书集合中的第三个金融签证证书Cert³(BANK_{POS});当移动钱包使用其信

用签证证书集合中的第四个信用签证证书Cert⁴(TSM_{Wallet})时,消费POS结算终端则对应的使用其金融签证证书集合中的第四个金融签证证书Cert⁴(BANK_{Wallet})；

[0067] 步骤3,消费POS结算终端生成第一随机数和第一随机数的有效时间值,获取消费POS结算终端当前位置、当前位置的噪声和空气湿度数据,并存储该第一随机数和有效时间值,然后将包括消费POS结算终端自身签名的付款请求信息发送给移动钱包,并发送消费POS结算终端当前位置、当前位置噪声和空气湿度数据给认证机构；

[0068] 第一随机数作为防恶意第三方窃密的数据,通过设置第一随机数的有效时间值,以限定该随机数有效的时间,进一步保证消费POS结算终端所发送付款请求信息的有效时间,例如设定第一随机数的有效时间为10s,则第一随机数在消费POS结算终端发送付款请求信息起的10s内有效,超过10秒,该第一随机数失效,则消费POS结算终端发送的付款请求信息也随之失效；

[0069] 消费POS结算终端获取的当前位置数据即为当前支付交易地点的位置;当前位置噪声数据,作为所处位置环境的特征之一,可以对一个位置进行表征;当前位置空气湿度数据,表征了消费POS结算终端当前所处环境中的空气环境情况,在同一位置的空气湿度具有相同性,即在NFC通信的距离内,消费POS结算终端与移动钱包两者获取的当前位置空气湿度数据位于预设的误差范围之内,因此可以利用空气湿度的不可伪装性,即利用同一位置的环境参数的共性来对消费POS结算终端和移动钱包当前是否处于同一位置进行判断;其中：

[0070] 付款请求信息包括消费POS结算终端生成的第一随机数RP₁、该第一随机数RP₁的有效时间值TP、付款请求ReqW、消费POS结算终端选取的金融签证证书Cert^t(BANK_{POS})、消费POS结算终端选取的信用签证证书Cert^t(TSM_{POS})、消费POS结算终端的自身签名Sig_{POS}以及消费POS结算终端的私钥sk(POS);其中,该付款请求信息标记为Message_{P-W},付款请求信息Message_{P-W}由公式标记如下:

[0071]

$$\text{Message}_{P-W} = \left\{ \begin{array}{l} POS, Wallet, RP_1, TP, Cert^t(BANK_{POS}), Cert^t(TSM_{POS}), ReqW, \\ Sig_{POS}, sk(POS) \end{array} \right\}; \quad t \in [1, m];$$

[0072] 步骤4,移动钱包在预设时间周期内实时采集其合法拥有者施加在键盘上各按键的摁压力数值及摁压力方向,构建移动钱包合法拥有者利用左手和右手分别针对各按键的左手摁压力数据库和右手摁压力数据库,并分别计算各按键左手摁压力数据库和右手摁压力数据库的方差；

[0073] 由于移动钱包的合法拥有者每次利用左手或者右手通过键盘上按键输入密码时,其拥有者在每个键盘上施加的摁压力大小及方向是不同的,因此可以通过采集一段时间内各键盘上所受摁压力数值及对应的摁压力方向情况,以构建移动钱包其合法拥有者针对支付时的左手摁压力数据库和右手摁压力数据库,从而可以利用构建的左手摁压力数据库或右手摁压力数据库作为表征移动钱包合法拥有者的身份认证信息,以确保支付交易的安全;其中,键盘上某个按键的左手摁压力数据库中包含了在支付状态下,其合法拥有者利用左手摁压该按键时的摁压力数值及摁压力方向;同样地,键盘上某个按键的右手摁压力数据库中包含了在支付状态时,其合法拥有者的右手摁压该按键时的摁压力数值及摁压力方向；

[0074] 其中,移动钱包上第i个按键标记为Button_i,针对按键Button_i所构建的移动钱包合法拥有者的左手摁压力数据库标记为F_{Button_i}^{Left}, F_{Button_i}^{Left}={F_{Button_i}^{Left}(n)},移动钱包合法拥有者的右手摁压力数据库标记为F_{Button_i}^{Right}, F_{Button_i}^{Right}={F_{Button_i}^{Right}(n)},n∈N,N为左手摁压力数据库以及摁压力数据库中分别存储的摁压力数据个数;F_{Button_i}^{Left}(n)表示针对按键Button_i采集的移动钱包合法拥有者左手的第n个摁压力数据,F_{Button_i}^{Right}(n)表示针对按键Button_i采集的移动钱包合法拥有者右手的第n个摁压力数据;按键Button_i所受移动钱包合法拥有者左手摁压力的方差标记为σ_{Left}²(Button_i),移动钱包合法拥有者右手摁压力的方差标记为σ_{Right}²(Button_i);其中,方差σ_{Left}²(Button_i)和σ_{Right}²(Button_i)的计算公式分别如下:

$$[0075] \sigma_{Left}^2(Button_i) = \sum_{n=1}^N \frac{(F_{Button_i}^{Left}(n) - \overline{F_{Button_i}^{Left}})^2}{N}, \quad \overline{F_{Button_i}^{Left}} = \sum_{n=1}^N \frac{F_{Button_i}^{Left}(n)}{N};$$

$$[0076] \sigma_{Right}^2(Button_i) = \sum_{n=1}^N \frac{(F_{Button_i}^{Right}(n) - \overline{F_{Button_i}^{Right}})^2}{N}, \quad \overline{F_{Button_i}^{Right}} = \sum_{n=1}^N \frac{F_{Button_i}^{Right}(n)}{N};$$

[0077] 步骤5,移动钱包接收消费POS结算终端发送的付款请求信息,生成防窃密的第一随机数,获取移动钱包当前位置及当前位置噪声和空气湿度数据,并发送包括消费POS结算终端付款请求信息的认证请求信息以及移动钱包当前位置、当前位置噪声和空气湿度数据给认证机构;其中:

[0078] 移动钱包发送的认证请求信息包括消费POS结算终端的付款请求信息Message_{P-W}、移动钱包生成的防窃密的第一随机数RW₁、认证请求ReqT、其与消费POS结算终端会话请求ReqSession以及移动钱包与认证机构之间通信的公钥k(Wallet,TSM);移动钱包的该认证请求信息标记为Message_{W-T},Message_{W-T}由公式标记如下:

$$[0079] Message_{W-T} = \{Message_{P-W}, TSM, RW_1, ReqT, ReqSession, k(Wallet, TSM)\};$$

[0080] 步骤6,认证机构接收、提取移动钱包发送的认证请求信息以及移动钱包当前位置噪声和空气湿度数据,记录接收移动钱包认证请求的时间,并根据所提取的移动钱包的认证请求信息、移动钱包当前位置及当前位置噪声和空气湿度数据、消费POS结算终端当前位置及当前位置噪声和空气湿度数据对移动钱包做出交易反馈;其中,该步骤依次包括步骤6-1至步骤6-3:

[0081] 步骤6-1,当认证机构判断提取的认证请求信息中的消费POS结算终端信用签证证书存在于认证机构已存储的信用签证证书数据库中且认证机构接收移动钱包认证请求时间位于第一随机数的有效时间值内时,表明该信用签证证书有效且对应的消费POS终端为安全终端,该交易行为可信,认证机构生成移动钱包与消费POS终端之间的交易秘钥,并执行步骤6-2;否则,表明该信用签证证书对应的终端不可信,此时的交易行为不可信,认证机构发送拒绝交易信息给移动钱包;

[0082] 步骤6-2,认证机构根据提取的消费POS结算终端当前位置噪声数据和移动钱包当前位置噪声数据,判断消费POS结算终端与移动钱包所分别对应的当前位置噪声之差位于预设的差值范围内,且消费POS结算终端与移动钱包所分别对应的当前位置之差位于预设

的距离差值范围之内时,说明初步确定消费POS结算终端和移动钱包处于同一位置,则执行步骤6-3,以作进一步确定;否则,认证机构发送拒绝交易信息给移动钱包;

[0083] 步骤6-3,认证机构根据提取的消费POS结算终端当前位置空气湿度数据和移动钱包当前位置空气湿度数据,判断消费POS结算终端与移动钱包所分别对应的当前位置空气湿度之差位于预设的差值范围内时,表明消费POS结算终端和移动钱包当前处于安全的同一个位置的交易环境内,则认证机构发送确认交易信息给移动钱包;否则,认证机构发送拒绝交易信息给移动钱包;其中:

[0084] 认证机构发送的确认交易信息标记为Message_{T-W-Confirm},认证机构发送的拒绝交易信息标记为Message_{T-W-Reject};确认交易信息Message_{T-W-Confirm}和拒绝交易信息Message_{T-W-Reject}分别由公式标记如下:

[0085] $\text{Message}_{T-W-Confirm} = \{\text{TSM}, \text{Wallet}, \text{POS}, \text{RP}_1, \text{RW}_1, \text{TP}, \text{Cert}^t(\text{TSM}_{\text{POS}}), \text{K}, \text{k}(\text{Wallet}, \text{TSM})\};$

[0086] $\text{Message}_{T-W-Reject} = \{\text{TSM}, \text{Wallet}, \text{POS}, \text{RP}_1, \text{RW}_1, \text{RejectP}, \text{k}(\text{Wallet}, \text{TSM})\};$

[0087] 步骤7,移动钱包接收认证机构发送的确认交易信息,并将包括移动钱包签名的交易交互信息发送给消费POS结算终端;其中:

[0088] 交易交互信息包括移动钱包的签名Sig_{Wallet}、移动钱包生成的防窃密的第一随机数RW₁、移动钱包与消费POS终端之间的交易秘钥K、移动钱包选取的金融签证证书Cert^s(BANK_{Wallet})、移动钱包选取的信用签证证书Cert^s(TSM_{Wallet})及消费POS结算终端的信用签证证书Cert^t(TSM_{POS});移动钱包与消费POS终端之间利用交易秘钥K作为进行交易的凭证;移动钱包发送的交易交互信息记为Message_{W-P},Message_{W-P}由公式标记如下:

[0089]

$$\text{Message}_{W-P} = \left\{ \begin{array}{l} \text{Wallet}, \text{POS}, \text{TSM}, \text{RW}_1, \text{Cert}^s(\text{BANK}_{\text{Wallet}}), \text{Cert}^s(\text{TSM}_{\text{Wallet}}), \text{K}, \\ \text{Sig}_{\text{Wallet}}, \text{Cert}^t(\text{TSM}_{\text{POS}}) \end{array} \right\}; \quad s \in [1, m];$$

[0090] 步骤8,消费POS结算终端接收、提取移动钱包发送的交易交互信息,并根据在交易交互信息中提取的信息做出判断:

[0091] 当消费POS结算终端在交易交互信息中提取到的消费POS结算终端信用签证证书已经存储于其存储的信用签证证书数据库中时,说明消费POS结算终端发起的支付交易请求已经得到了移动钱包的确认,即移动钱包同意消费POS结算终端发起的该笔支付交易行为,则执行步骤9;否则,表明移动钱包不同意该笔支付交易行为,消费POS结算终端拒绝与移动钱包进行支付交易;

[0092] 步骤9,消费POS结算终端生成第二随机数,并发送包括生成的第二随机数、第一随机数、移动钱包防窃密的第一随机数、移动钱包所需支付款项数据的支付款项信息给移动钱包;其中,支付款项信息标记为Message_{P-W-Payment},Message_{P-W-Payment}由公式标记如下:

[0093] $\text{Message}_{P-W-Payment} = \{\text{POS}, \text{Wallet}, \text{RP}_2, \text{RW}_1, \text{RP}_1, \text{Payment}, \text{K}\};$

[0094] 其中,RP₂表示消费POS结算终端生成的第二随机数,Payment表示移动钱包所需支付款项,K为消费POS结算终端与移动钱包之间的交易秘钥;

[0095] 步骤10,移动钱包接收消费POS结算终端发送的支付款项信息,并生成防窃密的第二随机数,由移动钱包将包括所接收支付款项信息以及新生成第二随机数的支付交易记录

信息发送给签证机构存储；其中，支付交易记录信息标记为 $S_{W-T-Payment}$ ，支付交易记录信息 $S_{W-T-Payment}$ 由公式标记如下：

[0096] $S_{W-T-Payment} = \{Wallet, TSM, POS, RW_2, k(Wallet, TSM)\}$ ； RW_2 表示移动钱包生成的防窃密的第二随机数；

[0097] 步骤11，移动钱包接收外部通过各按键输入的支付密码，由移动钱包根据各按键所受摁压力方向判断摁压各按键的为左手或右手，并将各摁键所受摁压力添加到判断结果所对应的左手摁压力数据库或右手摁压力数据库中，重新计算此时各按键对应摁压力数据库的方差；

[0098] 步骤12，移动钱包根据步骤11中各按键重新所得摁压力数据库方差与步骤4中所对应摁压力数据库方差之间的差值，对是否执行支付操作做出判断；

[0099] 步骤12-1，当各按键所得差值均小于或等于预设阈值时，表示该支付密码为移动钱包合法拥有者所输入，移动钱包发送包括该支付密码、其金融签证证书和信用签证证书的支付命令给银行账户管理平台，由银行账户管理平台判断支付密码与预设支付密码一致时，将移动钱包付款账户的款项转移至消费POS结算终端在银行账户管理平台的收款账户内，并由银行账户管理平台存储移动钱包发送的支付命令；

[0100] 步骤12-2，当各按键所得差值中出现大于预设阈值时，说明此时各按键所受的摁压力数值出现了较大的波动，表示该支付密码不是移动钱包合法拥有者输入，移动钱包拒绝执行支付操作，以防止非法用户对移动钱包合法拥有者的账户安全造成威胁。

[0101] 在本发明的移动钱包安全支付方法中，首先，消费POS结算和移动钱包分别在认证机构、银行账户管理平台处获得各自对应的信用签证证书集合和金融签证证书集合，消费POS结算终端以其防窃密的第一随机数和有效时间值作为保证交易安全的条件，并将仅限单次使用有效的信用签证证书添加到付款请求信息中，以防止信用签证证书被恶意第三方重复使用，造成信息泄漏；

[0102] 其次，消费POS结算终端和移动钱包均分别发送其当前位置、当前位置噪声和空气湿度数据给认证机构，由认证机构判断消费POS结算终端与移动钱包交易双方处于安全交易的同一个位置环境时，则分别发送交易秘钥给消费POS结算终端和移动钱包，即利用同一位置同一环境参数值相同的特点以及两者的位置距离，来共同实现对消费POS结算终端和移动钱包所处交易位置的准确判断，以保证两者间的支付交易安全；

[0103] 再次，利用人体行为特征的唯一性，移动钱包通过构建其合法拥有者支付时，施加在各按键的左手摁压力数据库和右手摁压力数据库对合法拥有者的身份信息再次认证，并在移动钱包进行支付操作时，进行关于各按键所受摁压力数值及方法的匹配，以防止非法用户单纯依靠破解移动钱包支付密码即可威胁移动钱合法拥有者的经济利益，从而在完成移动钱包支付的同时，也保证了支付信息不被泄露，同样避免了因移动钱包丢失而对其合法拥有者经济利益造成威胁的问题。

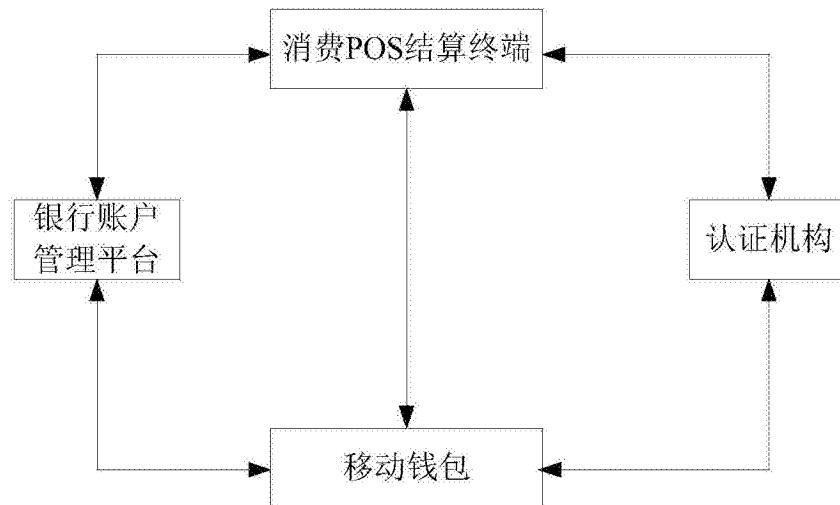


图1

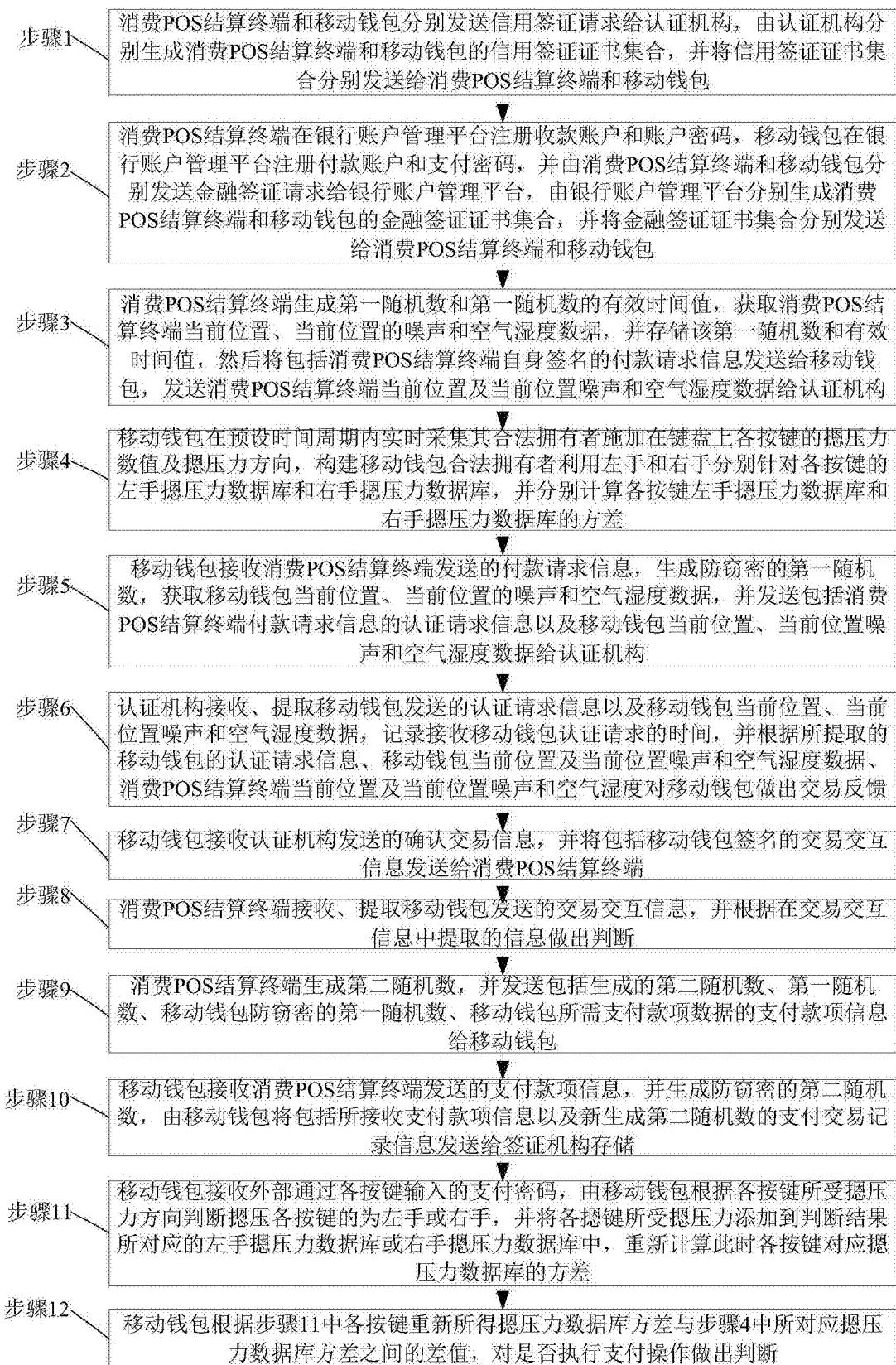


图2