(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 109462481 A
(43)申请公布日 2019.03.12

(21)申请号 201811403997.X

(22)申请日 2018.11.23

(71)申请人 上海扈民区块链科技有限公司
地址 202156 上海市崇明区上海市新河镇新中路786号弄5号345室

(72)发明人 赵运磊 王红兵 黄兴忠

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 陈斌

(51)Int.Cl.
H04L 9/30(2006.01)
H04L 9/32(2006.01)
H04L 9/06(2006.01)
H04L 9/08(2006.01)
H04L 29/06(2006.01)

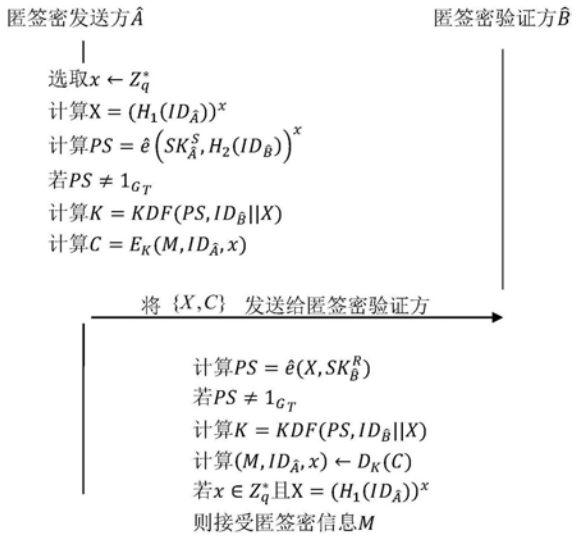
权利要求书2页 说明书5页 附图2页

(54)发明名称

一种基于非对称双线性对的匿签密方法

(57)摘要

本发明提供了一种非对称环境下高效的基于身份的匿签密方法，包括：私钥生成器生成系统主私钥$msk \leftarrow Z_q^*$；在非对称双线性对类型-1和类型-2下，身份为$ID_{\hat{A}}$的匿签密发送方的私钥为$SK_{\hat{A}} = (H(ID_{\hat{A}}))^{msk}$，身份为$ID_{\hat{B}}$的匿签密验证方的私钥为$SK_{\hat{B}} = (H(ID_{\hat{B}}))^{msk}$。$\hat{A}$选取$x \leftarrow Z_q^*$、计算$X = (H(ID_{\hat{A}}))^x$、$K = KDF(\hat{e}(SK_{\hat{A}}, \psi(H(ID_{\hat{B}})))^x, ID_{\hat{B}}||X)$、$C = E_K(M, ID_{\hat{A}}, x)$、并将{X,C}发送给$\hat{B}$，其中$\hat{e}$是双线性映射。$\hat{B}$计算$K = KDF(\hat{e}(X, \psi(SK_{\hat{B}})), ID_{\hat{B}}||X)$、$(M, ID_{\hat{A}}, x) \leftarrow D_K(C)$、$x \in Z_q^*$且$X = (H(ID_{\hat{A}}))^x$则接受匿签密信息M。在非对称双线性对类型-3下，身份为$ID_{\hat{A}}$的匿签密发送方的私钥为$SK_{\hat{A}}^S = (H_1(ID_{\hat{A}}))^{msk}, SK_{\hat{A}}^R = (H_2(ID_{\hat{A}}))^{msk}$；身份为$ID_{\hat{B}}$的匿签密验证方的私钥为$SK_{\hat{B}}^S = (H_1(ID_{\hat{B}}))^{msk}, SK_{\hat{B}}^R = (H_2(ID_{\hat{B}}))^{msk}$。$\hat{A}$选取$x \leftarrow Z_q^*$、计算$X = (H_1(ID_{\hat{A}}))^x$、$K = KDF(\hat{e}(SK_{\hat{A}}^S, H_2(ID_{\hat{B}}))^x, ID_{\hat{B}}||X)$、$C = E_K(M, ID_{\hat{A}}, x)$、并将{X,C}发送给$\hat{B}$，其中$\hat{e}$是双线性映射。$\hat{B}$计算$K = KDF(\hat{e}(X, SK_{\hat{B}}^R), ID_{\hat{B}}||X)$、$(M, ID_{\hat{A}}, x) \leftarrow D_K(C)$、$x \in Z_q^*$且$X = (H_1(ID_{\hat{A}}))^x$则接受匿签密信息M。



CN 109462481 A

1.一种高效的基于非对称双线性对的身份基匿签密方法,所述方法包括:

系统建立:生成系统公开参数,包括:一个安全参数n,双线性对$\hat{e}$:$G_1\times G_2\rightarrow G_T$,整数q,其中$G_1$、$G_2$和$G_T$是三个q阶循环群,q的二进制长度(记为|q|)为n的多项式;两个哈希函数:H_1:$\{0,1\}^*\rightarrow G_1$,H_2:$\{0,1\}^*\rightarrow G_2$,一个可有效计算的同构ψ:$G_1\rightarrow G_2$,一个密钥导出函数KDF:$\{0,1\}^*\rightarrow\{0,1\}^n$;令$g_1\in G_1$为$G_1$的生成元,$g_2\in G_2$为$G_2$的生成元,$1_{G_T}$为群$G_T$的单位元;E为一个对称加密函数;系统公开参数记为:

$$SysPar=\{n,\hat{e},G_1,G_2,G_T,q,H_1,H_2,\psi,KDF,g_1,g_2,1_{G_T},E\};$$

系统公开参数可以由系统内的用户协商决定,或由可信第三方给定;私钥生成器(Private Key Generator,简称为PKG)生成用户主密钥(Master Secret Key)$msk\leftarrow Z_q^*$(msk从Z_q^*中随机选取,其中Z_q^*的取值范围为1到q-1中的整数,且q为一个大素数);公开发布SysPar,保密保存msk。

用户私钥生成:具有身份ID∈$\{0,1\}^*$的用户在PKG注册,PKG根据主密钥msk和用户身份生成用户私钥:$SK_{ID}^S=(H_1(ID))^{msk}$,$SK_{ID}^R=(H_2(ID))^{msk}$,其中$SK_{ID}^S$用来签密,$SK_{ID}^R$用来验证签密。为了描述方便起见,下述的描述中签密生成方记为$\hat{A}$,签密和验证签密私钥分别为$SK_{\hat{A}}^S=(H_1(ID_{\hat{A}}))^{msk}$,$SK_{\hat{A}}^R=(H_2(ID_{\hat{A}}))^{msk}$;签密验证方记为$\hat{B}$,签密和验证签密私钥分别为$SK_{\hat{B}}^S=(H_1(ID_{\hat{B}}))^{msk}$,$SK_{\hat{B}}^R=(H_2(ID_{\hat{B}}))^{msk}$。

匿签密生成:令M∈$\{0,1\}^*$为匿签密的信息;

构造方法一(基于Type 1双线性对):用户$\hat{A}$选取$x\in Z_q^*$,计算$X=(H_1(ID_{\hat{A}}))^x$,计算$PS=\hat{e}\left(SK_{\hat{A}}^S,H_1(ID_{\hat{B}})\right)^x$;若$PS\neq 1_{G_T}$(否则重新选取x),计算K=KDF(PS,$aux_K$),$aux_K$或为空,或为$SysPar\cup aux_d\cup\{X,\hat{B},H_1(ID_{\hat{B}})\}$的一个子集,$aux_K$的具体形式或者双方事先约定或者是协议规范的一部分,aux_d可为空或包含一些不会泄露通信双方身份的附加信息;计算$C=E_K(M,ID_{\hat{A}},x,aux_M)$,即:将K作为对称加密函数E的密钥对$(M,ID_{\hat{A}},x,aux_M)$按照规定或约定编码方式进行加密,其中$aux_M$是可为空或包含一个时间戳信息的集合;最后,用户$\hat{A}$将{X,C}发送给用户$\hat{B}$;

构造方法二(基于Type 2双线性对):用户$\hat{A}$选取$x\in Z_q^*$,计算$X=(H_1(ID_{\hat{A}}))^x$,计算$PS=\hat{e}\left(SK_{\hat{A}}^S,\psi(H_1(ID_{\hat{B}}))\right)^x$;若$PS\neq 1_{G_T}$(否则重新选取x),计算K=KDF(PS,$aux_K$),$aux_K$或为空,或为$SysPar\cup aux_d\cup\{X,\hat{B},H_1(ID_{\hat{B}})\}$的一个子集,$aux_K$的具体形式或者双方事先约定或者是协议规范的一部分,aux_d可为空或包含一些不会泄露通信双方身份的附加信息;计算$C=E_K(M,ID_{\hat{A}},x,aux_M)$,即:将K作为对称加密函数E的密钥对$(M,ID_{\hat{A}},x,aux_M)$按照规定或约定编码方式进行加密,其中$aux_M$是可为空或包含一个时间戳信息的集合;最后,用户$\hat{A}$将{X,C}发送给用户$\hat{B}$;

构造方法三(基于Type 3双线性对):用户$\hat{A}$选取$x\in Z_q^*$,计算$X=(H_1(ID_{\hat{A}}))^x$,计算$PS=\hat{e}\left(SK_{\hat{A}}^S,H_2(ID_{\hat{B}})\right)^x$;若$PS\neq 1_{G_T}$(否则重新选取x),计算K=KDF(PS,$aux_K$),$aux_K$或为空,或为$SysPar\cup aux_d\cup\{X,\hat{B},H_1(ID_{\hat{B}})\}$的一个子集(这里,哈希函数$H_1$将$\hat{B}$的身份映射到群

G_1,哈希函数H_2将$\hat{B}$的身份映射到群G_2,且$SK_{\hat{B}}^{S}=(H_1(ID_{\hat{B}}))^{msk}$, $SK_{\hat{B}}^{R}=(H_2(ID_{\hat{B}}))^{msk}$),并且$aux_K$的具体形式或者双方事先约定或者是协议规范的一部分,aux_d可为空或包含一些不会泄露通信双方身份的附加信息;计算$C=E_K(M,ID_{\hat{A}},x,aux_M)$,即:将K作为对称加密函数E的密钥对$(M,ID_{\hat{A}},x,aux_M)$按照规定或约定编码方式进行加密,其中$aux_M$是可为空或包含一个时间戳信息的集合;最后,用户$\hat{A}$将{X,C}发送给用户$\hat{B}$;

匿签密验证:用户$\hat{B}$接收到{X,C}后,针对如上的三种匿签密算法分别做如下解密及验证:

验证方法一(基于Type 1双线性对):计算$PS=\hat{e}(X,SK_{\hat{B}}^{R})$,若$PS=1_{G_T}$,返回无效字符,表明匿签密无效;否则,计算K=KDF(PS,aux_K),利用K对C解密得到$(M,ID_{\hat{A}},x,aux_M)$;若$x\in Z_q^*$且$X=(H_1(ID_{\hat{A}}))^x$且aux_M有效,则接受匿签密信息M,否则拒绝接受。

验证方法二(基于Type 2双线性对):计算$PS=\hat{e}(X,\psi(SK_{\hat{B}}^{S}))$,若$PS=1_{G_T}$,返回无效字符,表明匿签密无效;否则,计算K=KDF(PS,auxK),利用K对C解密得到$(M,ID_{\hat{A}},x,aux_M)$;若$x\in Z_q^*$且$X=(H_1(ID_{\hat{A}}))^x$且aux_M有效,则接受匿签密信息M,否则拒绝接受。

验证方法三(基于Type 3双线性对):计算$PS=\hat{e}(X,SK_{\hat{B}}^{R})$,若$PS=1_{G_T}$,返回无效字符,表明匿签密无效;否则,计算K=KDF(PS,aux_K),利用K对C解密得到$(M,ID_{\hat{A}},x,aux_M)$;若$x\in Z_q^*$且$X=(H_1(ID_{\hat{A}}))^x$且aux_M有效,则接受匿签密信息M,否则拒绝接受。

2.如权利要求1所述的方法,其特征在于,

群G_1和G_2可以相等(记为G),即基于Type 1的双线性配对的构造(如构造方法一);q为素数或合数;从Z_q^*中随机选取,或在$Z_q\cap\{0,1\}^l$中随机选取,其中$l\leqslant|q|$;$aux_K=\{\hat{B},X\}$或$aux_K=\{H_1(ID_{\hat{B}}),H_2(ID_{\hat{B}}),X\}$;$aux_M$为空或包含一个时间戳信息;$aux_d$为空或包含不会泄露通信双方身份的附件信息;E是一个认证加密函数或者带有辅助输入的认证加密函数。

3.如权利要求书1～2中任一项所述的方法,其特征在于,对于Type 2和Type 3双线性对,$G_1\neq G_2$。

4.如权利要求书1～2中任一项所述的方法,其特征在于,对于Type 2双线性对,$H_1=H_2$:$\{0,1\}^*\rightarrow G_1$,记为H:$\{0,1\}^*\rightarrow G_1$,此时有$SK_{ID}=SK_{ID}^{S}=SK_{ID}^{R}=(H(ID))^{msk}$。

5.如权利要求书1～2中任一项所述的方法,其特征在于,对于Type 2双线性对,其构造方法不需要哈希函数H_2:$\{0,1\}^*\rightarrow G_2$。

6.如权利要求书1～2中任一项所述的方法,其特征在于,对于Type 3双线性对,其构造方法不需要一个可有效计算的同构ψ:$G_1\rightarrow G_2$。

7.如权利要求书1～2中任一项所述的方法,其特征在于,对于Type 3双线性对,$SK_{ID}^{S}=(H_1(ID))^{msk}$,$SK_{ID}^{R}=(H_2(ID))^{msk}$;其中$SK_{ID}^{S}$用来签密,$SK_{ID}^{R}$用来验证签密。

一种基于非对称双线性对的匿签密方法

技术领域

[0001] 本发明涉及密码技术领域，具体地说，涉及一种基于非对称双线性对的身份基匿签密方法。

背景技术

[0002] 数字签名和公钥加密是密码理论及应用的核心内容。签密是将数字签名和公钥加密的功能合二为一，既保证了加密内容的完整性和可验证性，又保证了加密消息的私密性，并且比简单地结合签名和加密的效率大为提升。与传统的公钥密码体制下相比，基于身份的签密将用户的身份作为公钥，可以简化公钥证书管理和发放的问题。但是，原有的基于身份签密方案均需公开传输用户的身份和公钥信息，并且效率较差。而在移动互联时代，设备的计算和存储能力受限，并且在很多应用中用户的身份信息往往属于敏感信息，需要保护。因此，发展高效的基于身份的身份匿藏签密方法(简记为“匿签密”)具有重要的理论及应用意义。

[0003] 令G_1、G_2和GT是三个q阶循环群(q可以是素数，也可以是合数，如RSA模数)。为了描述方便起见，我们记G_1、G_2和G_T为乘法群(所有本发明中描述的方案均在G_1、G_2和G_T记为加法群时同样工作)。一般而言，一个双线性对$\hat{e}$就是一个从$G_1\times G_2$到G_T的双线性映射，并满足下面性质:

[0004] (1)双线性性:设$g_1\in G_1$，$g_2\in G_2$，x，y$\in Z_q$，有$\hat{e}(g_1^x, g_2^y)=\hat{e}(g_1,g_2)^{xy}$;

[0005] (2)非退化性:对于每一个$g_1\in G_1/\{1_{G_1}\}$，总存在一个$g_2\in G_2$，使得$\hat{e}(g_1,g_2)\neq 1_{G_T}$，其中，$1_{G_1}$是$G_1$的单位元，$1_{G_T}$是$G_T$的单位元;

[0006] (3)双线性映射可以有效计算。

[0007] 双线性对有下面三种类型:

[0008] 类型1:$G_1\rightarrow G_2$有一个可有效计算的同构，这时一般记为$G_1=G_2$(通常用G表示)。这类双线性对一般可以用超奇异椭圆曲线或超椭圆曲线来实现。

[0009] 类型2:有一个有效计算群同态$G_2\rightarrow G_1$，但无从G_1到G_2的有效同态.这类双线性对一般用素数域上的一般椭圆曲线实现，G_1是基域上椭圆曲线群，G_2是扩域上椭圆曲线子群，$G_2\rightarrow G_1$的同态一般取迹映射。

[0010] 类型3:没有任何$G_2\rightarrow G_1$或$G_1\rightarrow G_2$的有效可计算的同态(同态甚至同构一定是存在的，这里是指没有有效计算的同构)。这类双线性对也是用素域上的一般曲线来构造，G_2一般取迹映射的核。

[0011] 本发明所描述的方法可以在上述三种类型双线性对任一类型上都可以工作，区别在于:对于类型1双线性对，$G_1=G_2$;对于类型2双线性对，系统公开参数中需要有一个可有效计算的同构ψ:$G_1\rightarrow G_2$，即ψ为将G_1中元素映射到G_2的可有效计算的同构;对于类型3双线性对，系统公开参数中不需要有一个可有效计算的同构ψ:$G_1\rightarrow G_2$，但每个用户的私钥由一个增加到两个，分别用于签密和验证签密。在下述的发明方案描述中，基于类型-2和类型-3来描

述，当应用到类型-1双线性对时则有$G_1=G_2$。

发明内容

[0012] 为解决上述问题，本发明提供了一种非对称环境下高效的基于身份的匿签密方法，包括：私钥生成器生成系统主私钥$msk \leftarrow Z_q^*$；在非对称双线性对类型-1和类型-2下，身份为$ID_{\hat{A}}$的匿签密发送方的私钥为$SK_{\hat{A}}=(H(ID_{\hat{A}}))^{msk}$，身份为$ID_{\hat{B}}$的匿签密验证方的私钥为$SK_{\hat{B}}=(H(ID_{\hat{B}}))^{msk}$。$\hat{A}$选取$x \leftarrow Z_q^*$、计算$X=(H(ID_{\hat{A}}))^x$、$K=KDF(\hat{e}(SK_{\hat{A}},\psi(H(ID_{\hat{B}})))^x,ID_{\hat{B}}||X)$、$C=E_K(M,ID_{\hat{A}},x)$、并将{X,C}发送给$\hat{B}$，其中$\hat{e}$是双线性映射。$\hat{B}$计算$K=KDF(\hat{e}(X,\psi(SK_{\hat{B}})),ID_{\hat{B}}||X)$、$(M,ID_{\hat{A}},x) \leftarrow D_K(C)$、$x \in Z_q^*$且$X=(H(ID_{\hat{A}}))^x$则接受匿签密信息M。在非对称双线性对类型-3下，身份为$ID_{\hat{A}}$的匿签密发送方的私钥为$SK_{\hat{A}}^S=(H_1(ID_{\hat{A}}))^{msk}, SK_{\hat{A}}^R=(H_2(ID_{\hat{A}}))^{msk}$；身份为$ID_{\hat{B}}$的匿签密验证方的私钥为$SK_{\hat{B}}^S=(H_1(ID_{\hat{B}}))^{msk}, SK_{\hat{B}}^R=(H_2(ID_{\hat{B}}))^{msk}$。$\hat{A}$选取$x \leftarrow Z_q^*$、计算$X=(H_1(ID_{\hat{A}}))^x$、$K=KDF(\hat{e}(SK_{\hat{A}}^S,H_2(ID_{\hat{B}}))^x,ID_{\hat{B}}||X)$、$C=E_K(M,ID_{\hat{A}},x)$、并将{X,C}发送给$\hat{B}$，其中$\hat{e}$是双线性映射。$\hat{B}$计算$K=KDF(\hat{e}(X,SK_{\hat{B}}^R),ID_{\hat{B}}||X)$、$(M,ID_{\hat{A}},x) \leftarrow D_K(C)$、$x \in Z_q^*$且$X=(H_1(ID_{\hat{A}}))^x$则接受匿签密信息M。

附图说明

[0013] 图1是发明方法一个实例(非对称双线性配对类型-2)实现的流程图。

[0014] 图2是发明方法一个实例(非对称双线性配对类型-3)实现的流程图。

具体实施方式

[0015] 图1是发明方法一个实例(非对称双线性配对类型-2)实现的流程图；其中，令$G_1 \neq G_2$，$aux_K=\{\hat{B},X\}$，aux_M为空，1_{G_T}为群G_T的单位元，$H:\{0,1\}^* \rightarrow G_1$是哈希函数，D是与加密函数E对应的解密函数，$(M,ID_{\hat{A}},x)$指的是利用密钥K对密文C进行解密得到$(M,ID_{\hat{A}},x)$；$x \leftarrow Z_q^*$表示的是x从$Z_q^*$中随机选取。

[0016] 图2是发明方法一个实例(非对称双线性配对类型-3)实现的流程图；其中，令$G_1 \neq G_2$，$aux_K=\{\hat{B},X\}$，aux_M为空，1_{G_T}为群G_T的单位元，$H_1:\{0,1\}^* \rightarrow G_1$，$H_2:\{0,1\}^* \rightarrow G_2$是两个哈希函数，D是与加密函数E对应的解密函数，$(M,ID_{\hat{A}},x)$指的是利用密钥K对密文C进行解密得到$(M,ID_{\hat{A}},x)$；$x \leftarrow Z_q^*$表示的是x从$Z_q^*$中随机选取。

[0017] 本发明提供了一种基于非对称双线性对的匿签密方法，现举例给出具体实施方式：

[0018] 系统建立：生成系统公开参数，一个安全参数n取128，双线性对$\hat{e}:G_1 \times G_2 \rightarrow G_T$，其中$G_1$、$G_2$和$G_T$是三个q阶循环群，整数q取

[0019] 359470774091272259258026482465924537458162000577212056614082739074 74

906182107327137762018291669211791046909853161708654033571280180531157052353650357569446667818402711513984860245089058190320664300428702940169973082320415710092390261998540583732271022110403965652301178012195981119983425075349972351920018 89，q的二进制长度(记为|q|)为n的多项式；两个哈希函数：H_1:{0,1}*→G_1，H_2:{0,1}*→G_2，分别采用MD5和SHA256函数；密钥导出函数KDF:{0,1}*→{0,1}n采用Openssl的AES算法内置KDF；g_1为G_1的生成元，取值

[0020] 7202675402793465149099591821252376624337100052597110133933469988532063654374607756348336406083955724437069422748791725240963819155056938902835938916497432385318002534623744576329342258385601402935259747917791032494193680752765137849500923534451690449027473197506307722961256236075464310225508989734814878069 0，g_2∈G_2为G_2的生成元，取值

[0021] 7770630256160844001061836831347865610850334358908951970056605558701855341430296855151671711550669833947364298147086882604244374180504428784666628945113362775136484322648378935033645108926505740862498256663673674475783544069662322035021962242666592157845457985347510761668809400733553694654934910109643234856 7，1_{G_T}为群G_T的单位元；E采用对称加密函数AES；系统公开参数包括：

[0022] $SysPar = \{n, \hat{e}, G_1, G_2, G_T, q, H_1, H_2, \psi, KDF, g_1, g_2, 1_{G_T}, E\}$；

[0023] 系统公开参数可以由系统内的用户协商决定，或由可信第三方给定；PKG生成系统主密钥$msk \leftarrow Z_q^*$，msk取64758132847809788388585681563710413213245356106 5；

[0024]

[0025] 用户私钥提取：具有身份ID∈{0,1}*的用户在PKG注册，PKG为其生成私钥：$SK_{ID}^S = (H_1(ID))^{msk}, SK_{ID}^R = (H_2(ID))^{msk}$；

[0026] 为了描述方便起见，下述的方法描述中签密的生成方的身份记为$\hat{A}$，令$ID_{\hat{A}}$ =IDaIDaIDa，计算签密和验证签密私钥分别$SK_{\hat{A}}^S = (H_1(ID_{\hat{A}}))^{msk}$=820778871199094917394789377997532061971159678259841684986687968395559176885964216347956687828413227364121358709794741000144579530928319369358213387144748347036558564248240229888609831842353736614838494315728704384389873801853963550030527631177702603421601018948318663644565307485443855420472827672714756627 7；$SK_{\hat{A}}^R = (H_2(ID_{\hat{A}}))^{msk}$=820778871199094917394789377997532061971159678259841684986687968395559176885964216347956687828413227364121358709794741000144579530928319369358213387144748347036558564248240229888609831842353736614838494315728704384389873801853963550030527631177702603421601018948318663644565307485443855420472827672714756627 7;签密验证方记为$\hat{B}$，令$ID_{\hat{B}}$ =IDbIDbIDb，签密和验证签密私钥分别为

$SK_{\hat{B}}^{S}=$

$(H_1(ID_{\hat{B}}))^{msk}$=16782924597672193751422100094413039632227089581396677576503818426

27591268378646377302965716466249571119375071819071857164654127768014957806058 82

86898206432282377806625522494471194414425668908119587998560436631746679216665 23

27392624829189074771604598901971873133030700552624111631933361468303247686826 6

677528; $SK_{\hat{B}}^{R}=$

$(H_2(ID_{\hat{B}}))^{msk}$=16782924597672193751422100094413039632227089581396677576503818426

27591268378646377302965716466249571119375071819071857164654127768014957806058 82

86898206432282377806625522494471194414425668908119587998560436631746679216665 23

27392624829189074771604598901971873133030700552624111631933361468303247686826 6

67752

[0027] 匿签密生成:令M∈{0,1}*为匿签密的信息,M取值

[0028] 2MMMMMMMMMMMMMMMMmmmmmmMMMMMMMMMMMMMMMMMMMM;用户$\hat{A}$选取x=34413595839 98071954583162253707631025877868091 62,计算$X=$

$(H_1(ID_{\hat{A}}))^{x}$=18175250936599843176749800420979716505292672018344748184312178041 15

35944954968982027582653905289819069368965634865635601593147659424294472591303 73

3759;若

70056658618029185500885218539434912172464121037934487535722434905065427975856 21

69428905500072623413595419635872501840888582153378604754766956816320333739410 27

采用类型-3双线性对,计算$PS=$

$\hat{e}\left(SK_{\hat{A}}^{S},H_2(ID_{\hat{B}})\right)^{x}$=12527106350117324855529040557630890510160128488831442808627 9

09176907497622555289365108012158096251571365866418900040122693318571969831065 91

10875987127611356383278972490347301753868237528692349681546164206590211344416 94

92243675828751574783773784666963819626881288872475444053149555298491483367825 36

08682703992;(若采用类型-2双线性对,计算$PS=\hat{e}\left(SK_{\hat{A}}^{S},\psi(H_1(ID_{\hat{B}}))\right)^{x}$;)若$PS\neq 1_{G_T}$(否则重新选取x,重新计算PS),计算K=KDF(PS,aux$_K$)=KDF(PS,aux$_K$)={rounds=10;rd_key=946168116 875979576 895575096 811676005 1969327858 1096281546 1949731314 1146599575 4252685724 3157080150},$aux_K=ID_{\hat{B}}||X$;计算$C=E_K(M,ID_{\hat{A}},x)$得

[0029] 667afc15fc776f81b5f74e9028723c7236f804cf40491f86cbcc70a1ef3b5976e134 3fe5cdedd30ad1da70fbfd61cf53a1a7ab57d004c56799351dd3afa32cdf13506dc5e10af7cd 39fc3ca426cb7b7fd091c5d70454517841a01412e48d2b43;最后,用户$\hat{A}$将{X,C}发送给用户$\hat{B}$;

[0030] 匿签密验证:用户$\hat{B}$接收到{X,C}后,若采用类型-3双线性对,计算$PS=$

$\hat{e}(X,SK_{\hat{B}}^{R})$=

12527106350117324855529040557630890510160128488831442808627909176907497622555289365108012158096251571365866418900040122693318571969831065911087598712761135638327897249034730175386823752869234968154616420659021134441694922436758287515747837737846669638196268812888724754440531495552984914833678253608682703992;(若采用类型-1双线性对,计算$PS=\hat{e}(X,SK_{\hat{B}}^{R})$),若采用类型-2双线性对,计算$PS=\hat{e}(X,\psi(SK_{\hat{B}}^{S}))$);若$PS\neq 1_{G_T}$,计算K=KDF(PS,aux$_K$)={rounds=10;rd_key=946168116 875979576 895575096 811676005 1969327858 1096281546 19497313141146599575 4252685724 3157080150},$aux_K=ID_{\hat{B}}||X$;利用K对C解密得到$(M,ID_{\hat{A}},x)$;

x= 344135958399807195458316225370763102587786809162∈ Z_q^*且$X=(H_1(ID_{\hat{A}}))^x$=

18175250936599843176749800420979716505292672018344748184312178041153594495496898202758265390528981906936896563486563560159314765942429447259130373700566586180291855008852185394349121724641210379344875357224349050654279758562169428905500072623413595419635872501840888582153378604754766956816320333739410273759,与传输密文相等,验证成功,接受匿签密信息M。

[0031] 本发明的其它特征和优点将在随后的说明书中阐述,并且,部分地从说明书中变得显而易见,或者通过实施本发明而了解。本发明的目的和其他优点可通过在说明书、权利要求书以及附图中所特别指出的结构来实现和获得。

[0032] 应该理解的是,本发明所公开的实施例不限于这里所公开的特定处理步骤,而应当延伸到相关领域的普通技术人员所理解的这些特征的等同替代。还应当理解的是,在此使用的术语仅用于描述特定实施例的目的,而并不意味着限制。

[0033] 说明书中提到的"两个实施例"或"实施例"意指结合实施例描述的特定特征、结构或特性包括在本发明的至少两个实施例中。因此,说明书通篇各个地方出现的短语"两个实施例"或"实施例"并不一定均指同一实施例。

[0034] 虽然上述示例用于说明本发明在一个或多个应用中的原理,但对于本领域的技术人员来说,在不背离本发明的原理和思想的情况下,明显可以在形式上、用法及实施的细节上作各种修改而不用付出创造性劳动。因此,本发明由所附的权利要求书来限定。

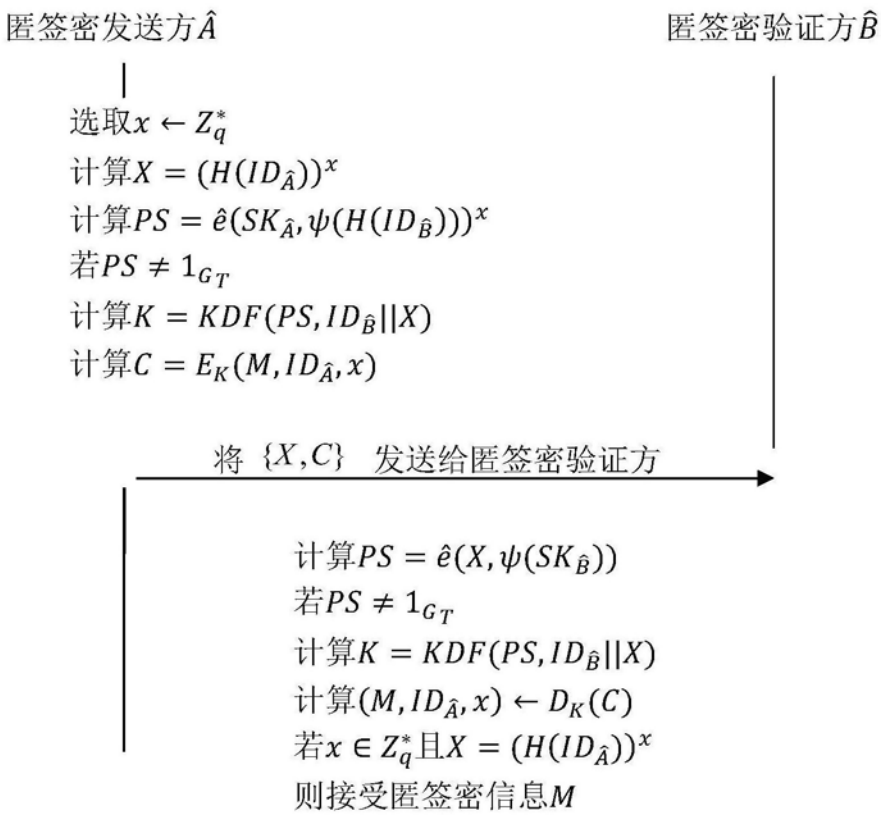

匿签密发送方$\hat{A}$
匿签密验证方$\hat{B}$
选取$x \leftarrow Z_q^*$
计算$X = (H(ID_{\hat{A}}))^x$
计算$PS = \hat{e}(SK_{\hat{A}}, \psi(H(ID_{\hat{B}})))^x$
若$PS \neq 1_{G_T}$
计算$K = KDF(PS, ID_{\hat{B}}||X)$
计算$C = E_K(M, ID_{\hat{A}}, x)$
将 $\{X, C\}$ 发送给匿签密验证方
计算$PS = \hat{e}(X, \psi(SK_{\hat{B}}))$
若$PS \neq 1_{G_T}$
计算$K = KDF(PS, ID_{\hat{B}}||X)$
计算$(M, ID_{\hat{A}}, x) \leftarrow D_K(C)$
若$x \in Z_q^*$且$X = (H(ID_{\hat{A}}))^x$
则接受匿签密信息M

图1

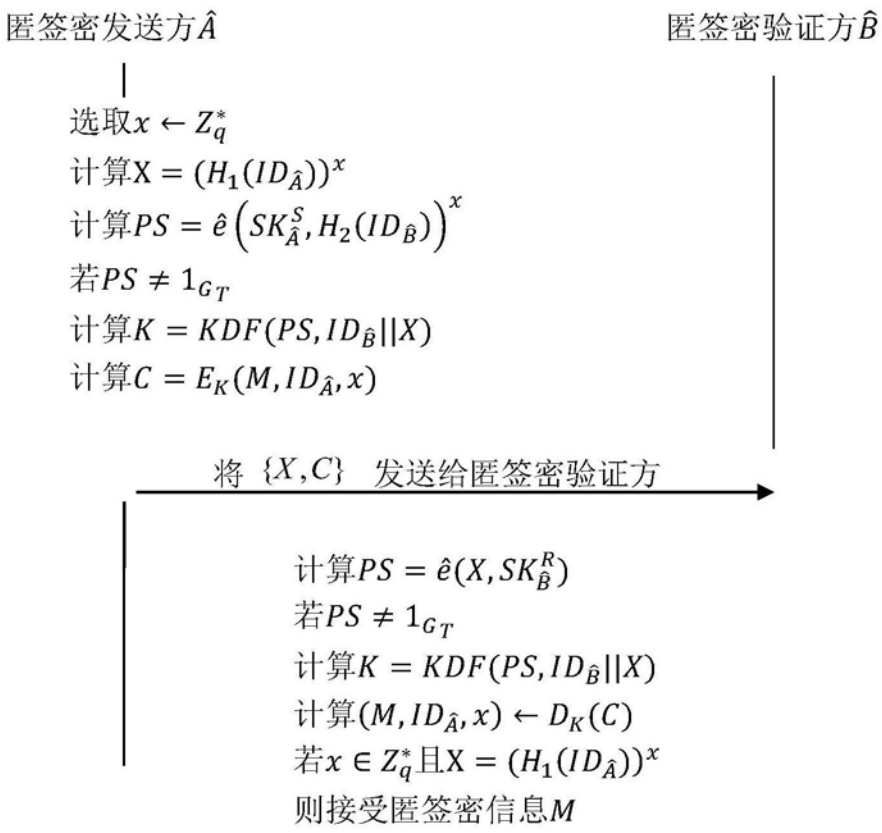

匿签密发送方$\hat{A}$
匿签密验证方$\hat{B}$
选取$x \leftarrow Z_q^*$
计算$X = (H_1(ID_{\hat{A}}))^x$
计算$PS = \hat{e}\left(SK_{\hat{A}}^S, H_2(ID_{\hat{B}})\right)^x$
若$PS \neq 1_{G_T}$
计算$K = KDF(PS, ID_{\hat{B}}||X)$
计算$C = E_K(M, ID_{\hat{A}}, x)$
将 $\{X, C\}$ 发送给匿签密验证方
计算$PS = \hat{e}(X, SK_{\hat{B}}^R)$
若$PS \neq 1_{G_T}$
计算$K = KDF(PS, ID_{\hat{B}}||X)$
计算$(M, ID_{\hat{A}}, x) \leftarrow D_K(C)$
若$x \in Z_q^*$且$X = (H_1(ID_{\hat{A}}))^x$
则接受匿签密信息M

图2