基于 NTRUSign 的电子现金方案

汪 翔
(解放军信息工程大学 电子技术学院, 郑州 450004)

摘 要: 基于 NTRUSign 数字签名方案构建一个新的电子现金方案,该方案的安全性基于格上的最近向量问题,并对该方案进行了详细的安全性分析。结果表明该方案满足一个电子现金方案应具有的性质,且实现速度快、占用资源少以及产生密钥容易,具有更高的实用性和安全性。

关键词: NTRUSign; 电子现金; NTRU 格
中图分类号: TP391 **文献标志码**: A **文章编号**: 1001-3695(2010)01-0259-03
doi:10.3969/j.issn.1001-3695.2010.01.076

Electronic cash scheme based on NTRUSign

WANG Xiang
(*Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou* 450004, *China*)

Abstract: This paper proposed an electronic cash scheme based on the NTRUSign signature algorithm, and analyzed the security characters of this scheme. It shows that the scheme owns some essential character that an electronic cash system should have, and has the advantage of high implementation speed, saves computer resources and easy key creation. This scheme is applicable and secure.

Key words: NTRUSign; electronic cash; NTRU lattice

目前,电子商务已经广泛深入到各个经济活动和领域。它能够通过互联网实现快捷高效的信息交换、产品销售、广告等商务活动,并对交易活动进行计算机处理。电子支付手段是开展电子商务的核心内容,其安全性和效率成为广大学者的研究重点。作为电子支付手段之一的电子现金系统,由于具有保护支付者匿名性、保护支付者和接收者的个人隐私功能,相比基于账户的信用卡更具有优势。自从 D. Chaum[1] 提出电子现金的概念以来,科研人员致力于电子现金系统的研究并提出了许多电子现金支付方案[2~5],但这些方案所基于的公钥密码算法的基础安全性不高,且计算量较大。

NTRU[6] 是一种新型简单快速的公钥密码算法,现已被采用为 IEEE P1363 标准,其安全性基于多项式、不同模混合运算的相互作用,信赖于寻找格中最短向量的困难性。目前该公钥算法的良好性质已得到普遍公认,所以基于它的各种签名算法就具有非常好的实用价值。2003 年 Hoffstein 等人[7] 提出了一种基于 NTRU 的数字签名算法 NTRUSign,这个算法使用的困难问题是格上的最近向量问题。国内外许多专家对其进行了深入研究,并提出基于 NTRUSign 的其他特殊签名方案[8]。

本文利用 NTRUSign 数字签名方案,构造了一个新的电子现金方案,新方案满足一个电子现金方案应有的一些基本性质,且相对其他电子现金方案有着运算速度快、操作更简洁的优点。

1 NTRUSign 算法

NTRUSign 是在环 $R=Z[x]/(x^N-1)$ 上进行运算(N 是一个公开参数)。一个多项式 $a(x)\in R$ 可以用一个向量 a 来表示:$a=\sum_{i=0}^{N-1}a_ix^i=(a_0,\cdots,a_{N-1})$。两个多项式的积可以简单记为 $a\times b=c \bmod (x^N-1)$,$c$ 的第 k 个系数为 $c_k=\sum_{i=0}^{k}a_ib_{k-i}+\sum_{j=k+1}^{N}a_jb_{N+k-j}$。在 NTRUSign 中还使用了环 $R_q=Z_q[x]/(x^N-1)$,在这里多项式系数要取模数 q,q 为 2 的次幂,如 128。在 $R_q^*=\{R_q-0\}$ 中单位元记为 1,a 在 R_q^* 中的逆元记为 a^{-1}(可参见文献[7])。

L_h^{NT} 为 NTRU 格,它是以矩阵

$$\begin{bmatrix} 1 & 0 & \cdots & 0 & h_0 & h_1 & \cdots & h_{N-1} \\ 0 & 1 & \cdots & 0 & h_{N-1} & h_0 & \cdots & h_1 \\ \cdots & \cdots & & & \cdots & \cdots & & \cdots \\ 0 & 0 & \cdots & 1 & h_1 & h_2 & \cdots & h_0 \\ 0 & 0 & \cdots & 0 & q & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & q & \cdots & 0 \\ \cdots & \cdots & & & \cdots & \cdots & & \cdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & q \end{bmatrix}$$

的行向量为基构成的一个 $2N$ 维格。其中 h_i(i 为 $0\sim N-1$)为公钥 h 的第 i 个系数(具体定义可参见文献[7])。

定义 1 设 $a(x)$ 是环 $R=Z[x]/(x^N-1)$ 上的一个多项式,$a(x)$ 的中心范数定义为 $\|a(x)\|^2=\sum_{i=0}^{N-1}(a_i-\mu_a)^2=\sum_{i=0}^{N-1}a_i^2-(1/N)(\sum_{i=0}^{N-1}a_i)^2$,$\mu_a=\sum_{i=0}^{N-1}a_i$ 且有 $\|a*b\|\approx\|a\|\cdot\|b\|$。

公开参数:N 为维数,它是一个素数,如 251;q 为模数,通常为 2 的幂次;d_f、d_g 为密钥参数;NormBound 为验证时使用的限。

1.1 密钥的生成

a)选择两个多项式 f、g,它们分别有 d_f、d_g 个 1,其余为 0,并且要求 f、g 满足下面式子:

$$\|f\|,\|g\|=O(\sqrt{N})$$

计算公钥 $h=f^{-1}*g \bmod q$。

收稿日期: 2009-04-15; **修回日期**: 2009-05-25

作者简介:汪翔(1979-),男,博士研究生,主要研究方向为信息安全(dixonwx@163.com).

b)计算多项式(F,G)满足

$$f*G-F*g=q \tag{1}$$

且有$\|F\|\approx\|f\|\sqrt{N/12}$,$\|G\|\approx\|g\|\sqrt{N/12}$,$(F,G)$的生成方法可参见文献[7]。

1.2 签名

a)对消息D使用hash变换$H(D)$,得到多项式(m_1,m_2),m_1、m_2均为环$R_q=Z_q[x]/(x^N-1)$上的多项式。

b)计算多项式a、b、A、B,它们均属于环$R=Z[x]/(x^N-1)$:

$$G*m_1-F*m_2=A+q*B \tag{2}$$

$$-g*m_1+f*m_2=a+q*b \tag{3}$$

其中:a、A的系数均在$-q/2\sim q/2$。

c)计算多项式S如下:

$$S=f*B+F*b \bmod q \tag{4}$$

多项式S即为消息D的关于公钥h的签名。

1.3 验证

a)对消息D进行hash变换$H(D)$,得到多项式(m_1,m_2);

b)由S及h得到$T\equiv S*h \bmod q$;

c)验证$\|m_1-S\|+\|m_2-T\|\leqslant$NormBound是否成立,若成立则通过验证。

1.4 工作原理

由式(1)~(4)得$(S,T)=B*(f,g)+b*(F,G) \bmod q$,$(m_1,m_2)-(S,T)=(A/q,a/q)\begin{pmatrix}f & g\\ F & G\end{pmatrix}$。

所以有$m_1-S=\varepsilon_1*f+\varepsilon_2*F$,$m_2-T=\varepsilon_1*g+\varepsilon_2*G$;$\varepsilon_1=A/q$,$\varepsilon_2=a/q$,它们的系数均匀地分布在$-1/2\sim1/2$之间。可以认为它们的中心范数约为$\|\varepsilon_1\|$,$\|\varepsilon_2\|\approx\sqrt{N/12}$。

由上文可知$\|f\|$,$\|g\|\approx O(\sqrt{N})$,$\|F\|=\|f\|\sqrt{N/12}$,$\|G\|=\|g\|\sqrt{N/12}$,则可以估计(S,T)和(m_1,m_2)的距离:

$$\|(m_1-S),(m_2-T)\|^2=\|(\varepsilon_1 f,\varepsilon_2 F),(\varepsilon_1 g,\varepsilon_2 G)\|^2=\frac{c^2N^3}{72}\left(1+\frac{1}{N}\right)$$

它是一个较小的值。

在文献[7]中指出,在参数$(N,d_f,d_g,\text{NormBound})=(251,128,73,71,300)$的情况下,其安全性等同于RSA(1024)。

本文利用NTRUSign签名算法构造了一个电子现金方案。

2 基于NTRUSign的电子现金方案

方案包括六个阶段:系统初始化、成员加入、取款协议、支付协议、存款协议以及身份验证。具体内容如下:

假设系统参与者有银行B、成为群成员的消费者C、一个作为匿名性撤销者的作为群管理者(可信第三方)P、作为群签名验证者的商家S。消费者C和商家S在银行处有各自的账户,并可通过身份认证过程确认自己的身份。

1)系统初始化

(f_B,g_B),h_B分别为银行B的私钥和公钥。其中:f_B,g_B分别有d_{f_B}、d_{g_B}个1,$d_{f_B}=O(\sqrt{N})$,$d_{g_B}=O(\sqrt{N})$,其余为0;$h_B\equiv f_B^{-1}*g_B \pmod q$。

(f_C,g_C),h_C分别为消费者C的私钥和公钥。其中:f_C,g_C分别有d_{f_C}、d_{g_C}个1,$d_{f_C}\approx O(\sqrt{d_{f_B}})$,$d_{g_C}\approx O(\sqrt{d_{g_B}})$,其余为0;$h_C\equiv f_C^{-1}*g_C \pmod q$。

(f_P,g_P),h_P分别为可信第三方P的私钥和公钥。其中:f_P,g_P分别有d_{f_P}、d_{g_P}个1,$d_{f_P}=O(\sqrt{N})$,$d_{g_P}=O(\sqrt{N})$,其余为0;$h_P\equiv f_P^{-1}*g_P \pmod q$。

$K=\text{NTRSign}(a,D)$为用签名NTRUSign算法对消息D产生的数字签名。其中a为私钥,$\text{ver}(D,S,b)$为用NTRUSign验证算法对消息D的签名S进行验证,b为对应于a的公钥。

2)成员加入

消费者C向可信第三方(群管理者)P申请加入群,发送(ID_C,K_C)给银行B,ID_C为X_i身份消息,$K_C=\text{NTRUSign}((f_C,g_C),ID_C)$,群管理者P用$\text{ver}(ID_C,K_C,h_C)$验证签名的有效性,并查看$ID_C$是否符合要求。

若通过验证,可信第三方P将$h(ID_C)$签名后发给银行B,B验证通过后,用$h(ID_C)$开个账户W_C并发给可信第三方P,可信第三方P随机选取R上两个多项式ε_{i1}、ε_{i2},ε_{i1}、ε_{i2}分别有$d_{\varepsilon_{i1}}$、$d_{\varepsilon_{i2}}$个1,其余为0。群管理者P计算$h_{\varepsilon_C}=\varepsilon_{i1}^{-1}*\varepsilon_{i2}*f_P*g_P^{-1} \pmod q$,对不同的用户产生的$h_{\varepsilon_C}$是不同的,即是惟一的。$K_P=\text{NTRUSign}((f_P,g_P),z)$,$z=h(h_{\varepsilon_{X_i}},ID_C,W_C)$,把$((\varepsilon_{i1},\varepsilon_{i2}),h_{\varepsilon_{X_i}},h(ID_C),K_P,W_C)$秘密发送给C并将其与$ID_C$一起保存。

C收到$((\varepsilon_{i1},\varepsilon_{i2}),h_{\varepsilon_{X_i}},h(ID_C),K_P,W_C)$后,用$\text{ver}(z,K_P,h_P)$验证$K_P$的有效性,验证等式$\varepsilon_{i1}^{-1}*\varepsilon_{i2}=h_P*h_{\varepsilon_C} \pmod q$。若两条都满足,计算$f_i=f_C*\varepsilon_{i1}$,$g_i=g_C*\varepsilon_{i2}$,C以$(f_i,g_i)$为成员钥。

3)取款协议

取款的过程主要由银行B、消费者C、可信第三方P来完成。可信第三方P的参与主要是为了实现可匿名性。D表示取款的数目。

消费者C对D签名,计算$K_C=\text{NTRUSign}((f_i,g_i),D)$,将$(h_{\varepsilon_C},K_C,D,ID_C,W_C)$发送给可信第三方P。

可信第三方P用$\text{ver}(D,K_C,h_i)$验证K_C的有效性,并验证等式$\varepsilon_{i1}^{-1}*\varepsilon_{i2}=h_P*h_{\varepsilon_C} \pmod q$,其中$h_i=h_{\varepsilon_C}h_Ph_C$。若两个条件都满足,则在数据库中搜索确认与$h_{\varepsilon_C}$、$ID_C$对应的账户是否为$W_C$。若正确,则计算$K_P=\text{NTRUSign}((f_P,g_P),h(ID_C)*D*W_C)$,将$K_P$发送给C。

消费者C用$\text{ver}(h(ID_C)*D*W_C,K_P,h_P)$验证签名的有效性,通过则发送$(K_P,h(ID_C),W_C,D)$给银行B。B用同样的方法验证$K_P$的有效性。若通过验证,则搜索数据库查看与$h(ID_C)$对应的账户是否为$W_C$。用户和银行共享一个密钥对$(k_1,k_2)$($k_1$,$k_2$是两个对称密钥),用户从银行取款时,银行发送给他一对随机的信息(m_1,m_2),用户计算产生$(E_{k_1}(m_1),E_{k_2}(m_2))$并把它发送给银行。银行对其进行验证,如果结果正确,则同意用户从自己的账户上提取现金,扣除相应的钱,并计算$K_B=\text{NTRUSign}((f_B,g_B),D*L_1)$,$L_1$为取款的时间戳,把$(K_P,K_B,h(ID_C),W_C,D,L_1)$及余额发送给C。当用户遇到敲诈时,可以使用$(k_1,k'_2)$对$(m_1,m_2)$进行加密,再传递给银行,银行验证后可知这是被敲诈的现金,此时银行对用户将要提取的现金D进行标记(此标记只有银行才能识别),并且不从用户的账户扣除D。当敲诈者以后将钱存入银行时,银行将拒绝执行存款服务。

消费者C收到$(K_P,K_B,h(ID_C),W_C,D,L_1)$及余额后,首先核对余额是否正确;其次用$\text{ver}(D*L_1,K_B,h_B)$验证$K_B$的有效

性,若两个条件都满足,则接受该签名。

4)支付协议

支付协议就是消费者 C 向商家 S 出示一个群签名,证名自己在银行拥有合法账户,并有支付能力的过程。为了防止重复花费,在该过程中同样引入可信第三方,同时,同一个签名只能用一次,如果同一个签名用两次以上时就能被发现,以区分是消费者还是商家重复花费。

消费者 C 将从银行得到的签名(K_P,K_B,$h(ID_C)$,W_C,D,L_1)发给商家。

商家收到签名(K_P,K_B,$h(ID_C)$,W_C,D,L_1)后,首先用 ver($h(ID_C)*D*W_C$,K_P,h_P)验证可信第三方的签名,证明消费者是群里的成员;然后再用 ver($D*L_1$,K_B,h_B)验证银行签名,证明该签名得到银行的保证。若两个条件都满足,则将交易日期 L_2 签名后发给消费者 C。

C 收到 L_2 的签名,验证通过后,同样将 L_1、L_2 签名后发给可信第三方 P,P 将 L_2 签名 K'_P = NTRUSign((f_P,g_P),L_1*L_2)后发给 C,C 保留一个副本后将其发给商家 S,S 用 ver(L_1*L_2,K'_P,h_P)验证,通过后就接受签名,并将货物发给消费者 C。

5)存款协议

存款过程就是商家 S 将群签名交给银行 B,银行验证正确性并检查是否重复花费的过程。商家将在支付协议中得到 D 的群签名(K_P,K_B,K'_P,$h(ID_C)$,W_C,D,L_1,L_2)及自己的账户 W_S(商家获得账户的方法与消费者获得账户的方法相同)交给银行,银行首先用 ver($D*L_1$,K_B,h_B)、ver($h(ID_C)*D*W_C$,K_P,h_P)、ver(L_2,K'_P,h_P)验证 K_P、K_B、K'_P 的有效性,通过验证则用 $h(ID_C)$,W_C,D,L_1 核对是否有相同的存款记录:a)若有相同的记录,则说明消费者或者商家存在重复花费,这时再看相同的记录中的 L_2 是否相同,相同说明是商家重复花费,不同说明是消费者重复花费;b)若没有相同的记录,银行在商家的账户上增加相应的数额,并把账户上的金额数目通知商家。

6)身份恢复

当银行发现重复花费或是发生纠纷时,银行只需将自己保存的消费者账户信息(W_C,$h(ID_C)$)、商家信息(W_S,$h(ID_S)$)或账户信息交给可信第三方 P,由于 P 保存有群内人员的((ε_{i1},ε_{i2}),$h_{\varepsilon_{X_i}}$,$h(ID_C)$,K_P,W_C)等信息,可以很容易地恢复匿名者的身份 ID_C 或 ID_S。

3　新方案的安全性分析

1)不可伪造性　因为该方案是建立在一个基于 NTRUSign 的群签名上的,所以不可伪造性首先看的是群签名的不可伪造性。上文已经说明了群签名的不可伪造性,现在来看电子现金的不可伪造性。电子现金的最终签名(K_P,K_B,$h(ID_C)$,W_C,D,L_1)、(K'_P,L_2),因为 K_P,K_B,K'_P 中包含有 $h(ID_C)$,W_C,D,L_1,L_2 的信息,所以消费者不可能自己更改其中的任何一项,除非知道了银行 B 和可信第三方的私钥。由于电子现金方案是由群签名来建立的,它的签名也是不可伪造的。

2)匿名性　给定一个群签名后,除了可信第三方的任何人,要确定实际签名者的身份在计算上是不可行的。因为最终的电子现金签名(K_P,K_B,$h(ID_C)$,W_C,D,L_1)并不包含消费者的直接身份信息,而 $h(\,)$ 是单向哈希函数,要由 $h(ID_C)$ 求 ID_C 是困难的。

3)防敲诈　当敲诈发生时,用户在取款时使用特殊的密钥与银行进行交互,此时银行可知敲诈的发生,并对敲诈的金额进行标记,敲诈者无法识别该标记,而在其接受并将其存入银行的时候,银行将拒绝存款。

4)检测重复花费性　银行在每次存款时都会把信息记录下来。在商家交给银行的电子现金签名(K_P,K_B,$h(ID_C)$,W_C,D,L_1)、(K'_P,L_2)中,$h(ID_C)$,W_C,D,L_1 能有效地检测出是否重复花费,而 L_2 可以判断出是谁在重复花费。若 L_2 相同说明是商家重复花费,不同说明是消费者重复花费。

5)可跟踪性　在发生争论的情况下,可信第三方能根据银行提供的信息找到 $h(ID_C)$,W_C 对应 ID_C,确定实际签名者的身份。

6)关于银行的非法行为　首先,由于群签名的无陷害特性,即使银行与其他成员合谋,也不能以取款协议中的消费者名义进行群签名,故银行不能盗用用户的钱币;其次,可使银行不能诬陷消费者取过钱(类似实际从存折中取款过程,在取款时用户提交一个有自己签名的取款申请,说明取多少钱;取款之后银行将发给消费者一个有自己签名的余额记录,消费者检查正确性)。但银行的后一种行为将严重影响银行的信誉,因此一般情况下不会发生,这种签名交换过程是一种可选项。

4　结束语

电子现金系统在电子商务中起着重要作用,因此研究安全有效的电子现金方案有着重要意义。本文提出一个基于 NTRUSign 的电子现金方案,该方案的安全性依赖于 NTRU 格上寻找最近向量问题的困难性。经分析,该方案具有一个电子现金方案应有的性质,且具有实现速度快、占用资源少以及产生密钥容易等优点,具有较高的安全性和实用性。该方案还可与其他特殊的签名方案进行结合,以适用于不同的实际应用的需要,这也是本文进一步研究的思路。

参考文献:

[1] CHAUM D. Blind signatures for untraceable payments[C]//Proc of Cryptology Crypto'82. Berlin:Plenum Press,1983:199-203.

[2] HOU Xiao-song,TAN C H. A new electronic cash model[C]//Proc of International Conference on Information Technology:Coding and Computing. 2005:374-379.

[3] 雷超琴,王文钢,樊凯. 群签名在电子现金中的应用[J]. 电子科技,2007(4):79-82.

[4] 费雄伟,李乔良. 一个新的安全且高效的电子现金系统[J]. 计算机应用研究,2008,25(5):1543-1545.

[5] 蔡满春,赵海洋,马春光,等. 一个公平的离线电子现金方案[J]. 电子与信息学报,2006,28(5):78-82.

[6] HOFFSTEIN J,PIPHER J,SILVERMAN J. NTRU:a ring-based public key cryptosystem[C]//BUHLER J P. Proc of the 3rd Symposiumon Algorithm Number Theory. Berlin:Springer-Verlag,1998:267-288.

[7] HOFFSTEIN J,GRAHAM N,PIPHER J. NTRUSign:digital signatures using the NTRU lattice preliminary draft2[EB/OL]. (2002). http://www. ntru. com.

[8] 褚映红,胡予濮,胡新祥. 基于 NTRUSign 的代理签名方案[J]. 计算机工程与应用,2005,41(8):131-133.

[9] 徐国盛,谷立则,杨义先,等. 新的可转移电子现金方案[J]. 通信学报,2008,29(5): 1-5.

[10] 张建中,王洁,刘勤喜. 新的代理盲签名方案及其在电子现金中的应用[J]. 计算机应用研究,2009,26(1):347-349.