基于格构造非交互不可展承诺方案

孙微微 杨 波 杨德新 夏 峰
(华南农业大学信息学院 广州 510642)

摘 要 NTRU是基于格归约困难问题的公钥密码体制,目前主要用于公钥加密及数字签名。利用NTRU实现了一个非交互不可展承诺方案,其安全性基于格上CVP困难问题,实现了承诺者绑定性。它基于抗碰撞Hash函数的安全性对承诺合法性进行验证,通过随机映射扰动明文,使明文具有随机分布特性,以实现验证者隐藏性以及与揭示有关的不可展性质。本方案具有NTRU快速高效的特点,同时可抵抗信道窃听攻击、消息重放攻击及复制承诺攻击。

关键词 公钥密码,NTRU,格,承诺
中图法分类号 TP309 **文献标识码** A

Non-interactive and Non-malleable Commitment Scheme Based on Lattice

SUN Wei-wei YANG Bo YANG De-xin XIA Feng
(College of Informatics, South China Agricultural University, Guangzhou 510642, China)

Abstract NTRU is a well-known public-key cryptosystem based on the difficulty of lattice reduction problems, and is mainly applied in public-key encryption and digital signature. This paper constructed a non-interactive and non-malleable commitment scheme, which relies the security on the intractable CVP on lattice, and the binding property of committer is satisfied. The validity of commitment is verified by hash function's collision resistance. Perturbing the plaintext with randomized mapping, plaintext will be in random distribution, and this scheme satisfies the hiding property of verifier and is non-malleable with respect to decommitment. This scheme has high efficiency as well as NTRU, and can resist channel eavesdropping attack, message replay attack and copying commitment attack.

Keywords Public key cryptography, NTRU, Lattice, Commitment

1 引言

数字承诺是密码学中的一个基础模块,常用于安全多方计算、电子拍卖、电子选举、电子抽签、电子现金等场合。基本过程是参与方Alice希望向参与方Bob承诺一个值m,在承诺阶段,Alice将m的承诺值发送给Bob,Bob不知道m的真实值,猜测出m值的成功概率是可忽略的;在揭示阶段,Alice向Bob揭示m的值或求出m所必需的参数,Bob可以验证m确实是Alice所承诺的值,而Alice企图欺骗Bob的成功概率将是可忽略的。

已有的承诺方案所基于的密码学困难假设主要有离散对数问题、大整数因子分解问题、二次剩余问题、单向函数、伪随机数生成器等。文献[1]在公共参考串模型下,基于单向函数和强RSA困难假设构造了不可展承诺方案和通用可复合承诺方案。文献[2]在由可信第三方产生公共可用的RSA或离散对数参数的前提下,构造了仅需3轮交互的不可展承诺方案。文献[3]基于单向置换函数构造了完全隐藏计算绑定的承诺方案。但对于计算能力无限制的敌手或量子计算机,这些基于计算困难性的问题和协议都将被攻破,因此研究量子安全的承诺方案是一个有吸引力的课题。

基于格构建密码系统是近年来信息安全领域的研究热点。格上困难问题有最近向量问题(CVP, Closest Vector Problem)、最短向量问题(SVP, Shortest Vector Problem)以及它们的各种变型,这些问题目前尚无有效的多项式求解方法。研究表明,格上困难问题具有平均情况和最坏情况的等价性,因此基于格归约困难问题构建的密码系统可以抵抗量子计算攻击[4]。另外,由于在格上主要进行小整数的模乘和模加运算,故算法运算快速高效。文献[4]根据格归约问题的计算困难性,给出了一个新的单向陷门函数,并构造了基于格的公钥加密及数字签名方案。

NTRU是一种基于格归约困难问题的公钥密码体制[5],在加密解密速度、密钥生成速度方面优于RSA和ECC密码系统,是IEEE 1363.1标准。自NTRU提出后,人们主要将其用于公钥加密及各种特殊的数字签名。文献[6]基于NTRU格提出了NTRUSign数字签名方案。文献[7]根据NTRU类数字签名方案的一个缺陷,提出新的改进,使得攻击者不能由大量签名值得到私钥的线性组合式,从而防止私钥信息的泄漏。文献[8]基于NTRU格上的近似最近向量问题的

到稿日期:2011-05-09 返修日期:2011-07-29 本文受国家自然科学基金项目(60773175,60973134)资助。
孙微微(1971-),女,博士生,副教授,主要研究方向为格公钥密码和数字承诺,E-mail:sunvv@scau.edu.cn;杨 波(1963-),男,教授,博士生导师,主要研究方向为信息安全;杨德新(1966-),男,博士生,讲师,主要研究方向为生物特征和格公钥密码;夏 峰(1975-),男,博士生,讲师,主要研究方向为格公钥密码。

困难假设，通过构造短格基生成签名。NTRU 加密算法运算简单快速，因此适合于计算资源少的设备。文献[9]将 NTRU 用于 RFID 系统下的安全通信协议，文献[10]利用 NTRU 实现无线局域网下的密钥协商和身份认证。NTRU 近来被应用于除加密和签名以外的其它场合，如文献[11]利用 NTRU 算法和单向散列函数进行数据合法性验证，提出新的多秘密共享(t,n)门限方案。

本文利用 NTRU 实现了一个非交互不可展承诺方案，其安全性基于格上 CVP 困难问题，因此本文方案是量子安全的。通过随机化函数扰动明文及参与方 ID，使二者具有随机分布特性，然后利用 NTRU 进行加密，将密文作为承诺发送给验证者，以实现与揭示有关的不可展性质。利用抗碰撞 Hash 函数实现承诺合法性的验证。方案的安全性分析表明，本方案除实现承诺的绑定性和隐藏性之外，还可抵抗信道窃听攻击、消息重放攻击及复制承诺攻击。

2 预备知识

定义 1(可忽略函数) 称函数 $f(k)$是可忽略的，如果$\forall c>0,\exists K,\forall k>K:f(k)<k^{-c}$。记作 $f(k)<negl(k)$。

在下文中，符号 $x\in_R S$ 表示从集合 S 中均匀随机地选取 x；符号 $y\leftarrow f(n)$表示函数 $f(n)$的输出是 y；$Pr[R_1,\cdots,R_n:E]$ 表示执行完随机过程 $R_1,\cdots,R_n$ 后事件 E 发生的概率。

2.1 格

定义 2 设 $v_1,v_2,\cdots,v_n$ 是 R^n 上一组线性无关的向量，格 L 是由 $v_1,v_2,\cdots,v_n$ 张成的整数线性空间，表示为

$$L=\{\sum_{i=1}^{n}a_iv_i:a_i\in Z\}$$

$v_1,v_2,\cdots,v_n$ 称为 L 的基。

格上基本的困难问题之一是 CVP 问题。实际密码方案的安全性基础经常基于近似最近向量问题(apprCVP)。

定义 3(最近向量问题，CVP) 给定不在 L 中的向量$t\in R^n$，对任意向量 $w\in L$，找到向量 $v\in L$，使得 $\|v-t\|=\min\|w-t\|$。

定义 4(近似 CVP，apprCVP) 给定不在 L 中的向量 $t\in R^n$，对任意向量 $w\in L$，找到向量 $v\in L$，使得 $\|v-t\|=k\cdot\min\|w-t\|$，其中 k 是一个小常数。

2.2 NTRU 公钥加密体制

NTRU 公钥加密系统运行在多项式环 $R=Z[x]/(x^N-1)$上，其本质是卷积模格，NTRU 的安全性基础是在卷积模格中解决 CVP 的困难性。$h\in R$ 可表示成具有整数系数的多项式或向量形式：

$$h=\sum_{i=0}^{N-1}h_ix^i=[h_0,h_1,\cdots,h_{N-1}]$$

$h \bmod q$ 可使多项式系数被约简到$\left[-\frac{q}{2},\frac{q}{2}\right)$之间。

$h^{-1} \bmod q$ 满足$h\otimes h^{-1}\equiv 1 \bmod q$，其中$\otimes$表示卷积乘法运算。

与向量 h 及模数 q 有关的卷积模格 L_h 是 $2N$ 维的格，用向量集合可描述为

$$L_h=\{(a,b)\in Z^{2N}:a\otimes h\equiv b(\bmod q)\}$$

NTRU 方案可分为 3 个算法[5]。

KeyGen(N,p,q)：N 既是安全参数也是消息长度，$\gcd(p,q)=1$，$p<<q$。随机选取具有小整数系数的多项式 f，$g\in R$，计算 f 关于模数 q 和 p 的多项式逆：

$$F_q\equiv f^{-1} \bmod q$$

$$F_p\equiv f^{-1} \bmod p$$

如果 F_q 或 F_p 不存在，则重新选取 f。令 $h=g\otimes F_q(\bmod q)$，则公钥是 h，私钥是 f 及 F_p。

Enc(m,r,h,p,q)：明文 m 是一个具有 mod p 系数的多项式，随机选取具有小整数系数的多项式 r，密文 $e=p*r\otimes h+m(\bmod q)$。

Dec(e,f,F_p)：计算 $a=f\otimes e(\bmod q)$，适当选择 a 的系数，使得$-\frac{q}{2}\leqslant a_i<\frac{q}{2}$，则明文 $m=F_p\otimes a(\bmod p)$。

f,g,r 的系数中对$-1,0,1$ 的个数有一些额外要求，具体可参见文献[5]。解密时使 a 的所有系数都落在合适范围，则不会发生解密失败。在最高安全性要求下，(N,p,q)可取为$(503,3,256)$，则私钥长度为 1595bits，公钥长度为 4024 bits。而对于分解密文而实施的中间相遇攻击，密钥安全强度为 2^{285}，消息安全强度为 2^{170}。

对于适当的参数，在没有私钥的情况下，从密文 e 恢复明文 m 等价于在 L_h 中找到最靠近于向量$[0,e]$的向量，因此 NTRU 安全性可归约为 CVP 的困难假设。

2.3 数字承诺

通常承诺方案包含以下 3 个阶段，每个阶段的函数都是多项式时间算法。

在设置阶段，CRS$\leftarrow$Setup(1^k)。Setup(1^k)的输入是比特串 1^k，输出是一个所有用户可用的、多项式长度的公共参考串 CRS。CRS 可以是承诺者或验证者的公钥或随机数，也可以是由可信第三方产生并公开的随机数或某个 Z_p 子群的生成元等。

在承诺阶段，(com, dec)$\leftarrow$Commit(CRS, m, r)。m 是承诺者需要承诺的消息，可以是一个比特或比特串。为实现语义安全及不可展性，通常需要在承诺函数 Commit(CRS, m, r)中使用随机数 r。com 是承诺者对 m 做出的承诺，将发送给验证者。dec 是用于解承诺的信息，在揭示阶段，将 dec 发送给验证者，用于验证承诺的合法性或求出消息 m。

在揭示阶段，验证者执行 $m\leftarrow$Decommit(com, dec)和 valid$\leftarrow$Verify(CRS, com, dec)。如果验证函数 Verify(CRS, com, dec)认为 com 是承诺者对 m 做出的合法承诺，则 valid 为 1，否则为 0。解承诺函数 Decommit(com, dec)根据 dec 打开 com，得到 m。若 valid 为 1 则接受 m，否则拒绝。

一个不可展承诺方案需要满足的基本性质是：

1)正确性。对于消息空间 M 中的任何消息 m，有

Pr[CRS$\leftarrow$Setup(1^k)，

(com, dec)$\leftarrow$Commit(CRS, m, r)，

1=valid$\leftarrow$Verify(CRS, com, dec)：

$m\leftarrow$Decommit(com, dec)]$>1-$negl(k)

2)绑定性。承诺者发出承诺之后，不能修改所承诺的消息，即对于足够大的 k，有

Pr[CRS$\leftarrow$Setup(1^k)，$m_0\neq m_1$，

(com, dec$_0$, dec$_1$)$\leftarrow$Commit(CRS, m_0, m_1, r)，

1=valid$\leftarrow$Verify(CRS, com, dec$_0$, dec$_1$)：

$m_0\leftarrow$Decommit(com, dec$_0$) $\wedge$ $m_1\leftarrow$Decommit(com, dec$_1$)]$<$negl(k)

3)隐藏性。在揭示阶段之前，验证者不能区分 com 是承诺者对 m_0 还是 m_1 的承诺。即验证者运行一个分辨器 $b\leftarrow$ Distinguish(com_b)，使得

$\Pr[CRS\leftarrow Setup(1^k), b\leftarrow\{0,1\},$

$(com_b, dec_b)\leftarrow Commit(CRS, m_b, r):$

$b\leftarrow Distinguish(com_b)]<negl(k)$

4)与揭示有关的不可展[2]。如果敌手 $\mathcal{A}$ 得到承诺者的已有承诺 com 后，不能根据 com 运行 Commit*(com)，构造一个新承诺 com*，使得 $\mathcal{A}$ 看到原承诺 com 的揭示 dec 后，可以运行函数 Forge(dec)给出它的揭示 dec*，并用一个相关的消息 m^* 来正确打开它的承诺 com*，则称该承诺方案满足与揭示有关的不可展性质。即

$\Pr[CRS\leftarrow Setup(1^k),$

$(com, dec)\leftarrow Commit(CRS, m, r),$

$com^*\leftarrow Commit^*(com), dec^*\leftarrow Forge(dec):$

$1=valid\leftarrow Verify(CRS, com^*, dec^*)$

$\wedge m^*\leftarrow Decommit(com^*, dec^*)]<negl(k)$

不可展性质还有更强意义的“与承诺有关的不可展”[2]，但对大多数应用来说，“与揭示有关的不可展”已经足够。

3 新的基于 NTRU 的非交互不可展承诺方案

假设承诺者 Alice 和验证者 Bob 各有自己的身份信息 $id_A, id_B\in\{0,1\}^k$，且他们互相知道。例如在电子投标场合，id_B 可以是招标者的名称，id_A 可以是投标者在招标者处注册的名称或招标者给投标者的编号。敌手 $\mathcal{A}$ 对 Alice 和 Bob 间的信道进行窃听，企图利用 Alice 的承诺欺骗 Bob 或其它用户。

按照承诺方案的基本模型，本文构造的基于 NTRU 的非交互不可展承诺方案也分为 3 个阶段。

设置阶段：Bob 调用 NTRU 中的 KeyGen(N,p,q)算法，生成自己的公钥 h 以及私钥 f、F_p。输出的公共参考串 $CRS=(N,p,q,h)$。另外，还有一个双方可用的抗碰撞的哈希函数 $H(x):\{0,1\}^*\rightarrow\{0,1\}^t$，$H(x)$输出定长的 t 比特。

承诺阶段：Alice 要承诺的明文是 m，m 的长度为 $N-t$ 比特，Alice 执行以下运算：

1)计算 $s\leftarrow H(id_A\|m\|id_B)$，其中 $\cdot\|\cdot$ 表示比特串连接；

2)选取一次性的随机数 $u\in_R Z$，u 的长度为 N 比特；

3)$m'=(m\|s)\oplus u$，这里$\oplus$表示异或运算；

4)调用 NTRU 中的 Enc(m',r,h,p,q)，得到密文 $e=p*r\otimes h+m'(\bmod q)$；

5)将 e 发送给 Bob，作为对明文 m 的承诺。

这里，通过 $H(x)$和$\oplus u$ 运算对明文、承诺者及验证者 ID 进行扰动，使其具有随机分布特性，防止向不诚实参与方或敌手泄漏关于明文的信息。

揭示阶段：

1)Alice 将 u 发送给 Bob；

2)Bob 将 u 记入字典，并检查 u 是否已存在，是则拒绝并终止协议，否则继续以下步骤；

3)Bob 调用 NTRU 中的 $Dec(e,f,F_p)$，得到 m'；

4)Bob 执行 $m'\oplus u$，得到一个长度为 N 的比特串，取前面的 $N-t$ 比特作为 $\bar{m}$，后面的 t 比特作为 $\bar{s}$；

5)Bob 计算 $\hat{s}\leftarrow H(id_A\|\bar{m}\|id_B)$，如果 $\hat{s}=\bar{s}$，则验证通过，接受 $\bar{m}$ 是正确的明文 m，否则拒绝。

需要说明的是，某些已有承诺方案将 m 发送给验证者作为揭示，那么敌手通过窃听也可以得知 m，因此后验泄漏了明文。本文方案只将求出 m 所需的随机数 u 发送给验证者，敌手没有私钥将无法得知明文。

在方案的整个执行过程中，验证者公布 CRS 之后，不再与承诺者交互，承诺者单方向地向验证者发送承诺及解承诺信息，这种非交互性质除可以降低计算复杂性外，还可防止敌手实施中间人攻击。

4 新方案的安全性分析

新方案除执行 NTRU 的基本算法之外，额外增加了两次 $H(x)$执行及两次异或运算，因此时间复杂性与 NTRU 相同，在加密解密一个长度为 N 的消息块时所需的操作次数为 $O(N^2)$。

新方案所满足的正确性、绑定性、隐藏性、与揭示有关的不可展性以及对信道窃听攻击、消息重放攻击及复制承诺攻击的可抵抗性由下面定理证明。

定理 1 上述承诺方案满足正确性、计算绑定性、完全隐藏性要求。

证明：正确性：Bob 对 Alice 的承诺解密后得到 $m'=(m\|H(id_A\|m\|id_B))\oplus u$，执行 $m'\oplus u$ 得到 $m\|H(id_A\|m\|id_B)$。当 m 是正确明文并且 id_A, id_B 属于合法的承诺者和验证者时，显然 Bob 的验证可以通过，于是得到 m。

计算绑定性：对于具有多项式时间计算能力的承诺者 Alice* 来说，承诺部分不仅包含 m，还包含验证信息 $H(id_A\|m\|id_B)$，她无法找到 $H(x)$的一对碰撞，使得 $m\neq m^*$，但 $H(id_A\|m\|id_B)=H(id_A\|m^*\|id_B)$。这样当她企图以 m^* 打开承诺时，Bob 验证通过的概率是可忽略的，因此满足计算绑定性。

完全隐藏性：即使验证者 Bob* 具有无界的计算能力，他也不可能从承诺中得到被承诺值的任何信息。虽然 Bob* 可以利用他的私钥先行解密，得到 $m'=(m\|H(id_A\|m\|id_B))\oplus u$，但在 Alice 将均匀随机数 u 发给他之前，Bob* 不可能从 m'中得知 m 的任何信息。因为对于任何 m，每个 m'都存在一个 u'，使得 $m'=(m\|H(id_A\|m\|id_B))\oplus u'$成立，他猜测 m 的任一比特为 0 或 1 的概率都是$\frac{1}{2}$，因此满足完全隐藏性。

证毕。

定理 2 如果格上的 CVP 和 apprCVP 是难解的，则本文方案是与揭示有关的不可展承诺方案。

证明：敌手 $\mathcal{A}$ 得到了 Alice 对于 m 的承诺 e，假设他以有意义的可控方式通过修改承诺 e 得到 e^*，并能够正确揭示另外一个与 m 相关的消息 m^*，那么他除了需要给出 $e^*=p*r^*\otimes h+(m^*\|H(id_A\|m^*\|id_B))\oplus u^*(\bmod q)$，还必须知道 m^*，否则他无法计算出正确的 $H(id_A\|m^*\|id_B)$，也就无法通过验证者的验证。那么在没有私钥的情况下，从密文 e 恢复明文 m 等价于在 L_h 中找到最靠近于向量$[0,e]$的向量，于是敌手 $\mathcal{A}$ 可以求解格上的 CVP。这违背了 CVP 的困难性假设。

下面再用反证法证明。假设敌手 $\mathcal{A}$ 可以在多项式时间内，以不可忽略的成功概率修改承诺 e 得到 e^*，并正确揭示一个与 m 相关的消息 m^*，则构造敌手 $\mathcal{C}_{\mathcal{A}}$ 和 $\mathcal{C}_{\mathcal{B}}$，分别模拟承诺者和验证者执行本文承诺方案，并以 $\mathcal{A}$ 为子程序求解 aprCVP。假设挑战者 $\mathcal{C}_{\mathcal{B}}$ 从挑战预言机 $\mathcal{O}$ 处得到一个挑战实例 $\tilde{c}$，需要向 $\mathcal{O}$ 返回在格中靠近向量 $\tilde{c}$ 的向量 $\tilde{x}$，于是进行下面的游戏：

1）$\mathcal{C}_{\mathcal{B}}$ 通过秘密渠道将 $\tilde{c}$ 交给 $\mathcal{C}_{\mathcal{A}}$；

2）$\mathcal{C}_{\mathcal{A}}$ 开始执行承诺协议，将 $\tilde{c}$ 作为自己对任意消息 m 的承诺发送，且被 $\mathcal{A}$ 得到；

3）$\mathcal{A}$ 从 $\tilde{c}$ 中解出 m，并延展为一个与 m 有多项式因子关系的 m^*，生成承诺 e^* 发给 $\mathcal{C}_{\mathcal{B}}$；

4）揭示阶段结束后，$\mathcal{C}_{\mathcal{B}}$ 可得到 $\mathcal{A}$ 给出的 m^*；

5）$\mathcal{C}_{\mathcal{B}}$ 将 m^* 作为自己对挑战 $\tilde{c}$ 的响应 $\tilde{x}$ 发给 $\mathcal{O}$；

6）多次重复上述过程，直到 $\mathcal{O}$ 满意，即 $\mathcal{O}$ 认为向量 $\tilde{x}$ 在格中靠近向量 $\tilde{c}$。

由于 $\mathcal{A}$ 可对消息 m 延展得到 m^*，且成功概率不可忽略，因此如果 m 是最靠近于向量 $[0,\tilde{c}]$ 的向量，那么 m^* 与向量 $[0,\tilde{c}]$ 间的距离将是最近距离的多项式因子。重复多次，直到 $\mathcal{O}$ 认为多项式因子足够小，于是 $\mathcal{C}_{\mathcal{B}}$ 以不可忽略概率在 aprCVP 挑战游戏中胜出。

因此，本文方案是与揭示有关的不可展承诺方案。

证毕。

定理 3 上述承诺可以抵抗信道窃听攻击。

证明：假设有敌手 $\mathcal{A}$ 可以窃听 Alice 与 Bob 的所有通信，于是可得知 Alice 发送的密文 e，但他没有 Bob 的私钥，也不能求解 CVP 问题，于是无法从 e 得知明文 m。在揭示阶段，敌手 $\mathcal{A}$ 窃听到随机数 u，但对他获得 m 也毫无帮助，敌手 $\mathcal{A}$ 在整个协议运行过程中得不到关于 m 的任何信息。因此，该文方案可以抵抗信道窃听攻击。

证毕。

定理 4 上述承诺可以抵抗消息重放攻击。

证明：假设敌手 $\mathcal{A}$ 曾经窃听并记录了 Alice 与 Bob 的一次通信过程，在以后某个时间企图冒充 Alice 向 Bob 再次做出承诺。于是他将 m 的密文 e 及求出 m 所需的随机数 u 再次发给 Bob，显然 Bob 可以正确验证并解开这个承诺。但方案中使用的 u 是一次性随机数，因此 Bob 在验证之前就会发现这个 u 已经存在于他的字典中了。因此终止整个协议，敌手 $\mathcal{A}$ 的消息重放攻击失败。

证毕。

定理 5 上述承诺可以抵抗复制承诺攻击。

证明：假设敌手 $\mathcal{A}$ 曾经窃听并记录了 Alice 与 Bob 的一次通信过程，然后企图冒充 Carol 向 Bob 做出承诺，于是他将 m 的密文 e 及求出 m 所需的随机数 u 发给 Bob，他期望 Bob 解承诺后会认为 Carol 与 Alice 的承诺相同。但在 Bob 验证时发现 $H(id_A \| m \| id_B) \neq H(id_C \| m \| id_B)$，于是拒绝。复制承诺攻击失败。

证毕。

结束语 作为基于格的公钥加密系统的代表，NTRU 主要用于公钥加密及数字签名。本文在标准模型下，利用 NTRU 构建了一个非交互承诺方案，其不仅实现了绑定性和隐藏性，也实现了与揭示有关的不可展性，对于敌手的信道窃听攻击、消息重放攻击及复制承诺攻击有免疫能力。本文方案高效快速，可作为零知识证明及多方安全计算的基本模块。

参 考 文 献

[1] Damgard I, Groth J. Non-interactive and reusable non-malleable commitment schemes[C]// Proceedings of the Thirty-fifth Annual ACM Symposium on Theory of Computing (STOC'03). San Diego, California, USA, 2003: 426-437

[2] Fischlin M, Fischlin R. Efficient non-malleable commitment schemes[C]// Proceedings of Advances in Cryptology CRYPTO. LNCS, vol. 1880. New York: Springer Verlag, 2000: 413-431

[3] 唐春明，裴定一，姚正安. 基于单向函数的完全隐藏承诺方案的构造及应用 [J]. 应用数学学报，2008，31(4)：663-670

[4] Goldreich O, Goldwasser S, Halevi S. Public-key cryptosystems from lattice reduction problems[C]// Proceedings of Advances in Cryptology CRYPTO'97. LNCS, vol. 1294. Santa Barbara: Springer Verlag, 1997: 112-131

[5] Hoffstein J, Pipher J, Silverman J H. NTRU: A Ring-based Public Key Cryptosystem[C]// Third International Symposiun of Algorithmic Number Theory. 1998, LNCS 1423. Portland, Springer Verlag, 1998: 267-288

[6] Hoffstein J, Graham N H, Pipher J, et al. NTRUSign: Digital signatures using the NTRU lattice[C]// The Cryptographers' Track at the RSA Conference. LNCS 2612. Springer Verlag, 2003: 122-140

[7] 胡予濮. 一个新型的 NTRU 类数字签名方案 [J]. 计算机学报，2008，31(9)：1661-1666

[8] 张文芳，余位驰，何大可，等. 一种基于格理论的数字签名方案 [J]. 计算机科学，2006，33(3)：93-96

[9] 蔡庆玲，詹宜巨，余松森，等. 基于 NTRU 公钥密码系统的 RFID 通信安全协议的研究 [J]. 中山大学学报：自然科学版，2009，48(5)：6-11

[10] 张文芳，何大可，缪祥华，等. 基于 NTRU 公钥密码体制的无线局域网安全方案 [J]. 计算机科学，2006，33(1)：111-113

[11] 步山岳，王汝传. 一种可验证和高效的多秘密共享门限方案 [J]. 计算机科学，2011，38(1)：100-103

(上接第 45 页)

[7] Camenisch J, Kohlweiss M, Soriente C. Solving revocation with efficient update of anonymous credentials[C]// SCN2010. Berlin: Springer-Verlag, 2010: 454-471

[8] Bichsel P, Camenish J, Neven G, et al. Get shorty via group signatures without encryption[C]// Proc. of EUROCRYPT 2010. Berlin: Springer-Verlag, 2010: 381-398

[9] Camenisch J, Lysyanskaya A. Signature scheme and anonymous credentials from bilinear maps[C]// CRYPTO 2004. Berlin: Springer-Verlag, 2004: 56-72

[10] Camenisch J, Kohlweiss M, Soriente C. An Accumulator Based on Bilinear Maps and Efficient Revocation for Anonymous Credentials[C]// PKC2009. Berlin: Springer-Verlag, 2009: 481-500