doi:10.3969/j.issn.1000-436x.2013.z1.035

面向移动 IPv6 层次化网络的快速接入认证方案

宋姗姗，尚涛，刘建伟
(北京航空航天大学 电子信息工程学院，北京 100191)

摘 要：提出了一个面向移动 IPv6 层次化网络的快速接入认证方案，从效率和安全性 2 个方面提高移动 IPv6 层次化网络接入认证的性能。首先，利用向量网络地址编码方法实现网络数据传输，提高家乡注册性能；其次，提出一种基于格的层次化签名方案，在接入认证过程中实现双向认证，提高认证过程的安全性。方案分析表明，所提出的接入认证方案具有强不可伪造性并可以抵御网络中的重放攻击，同时可以减少整个接入认证过程的延迟时间。
关键词：移动 IPv6；层次化；接入认证；格签名
中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2013)Z1-0263-05

Fast access authentication scheme for mobile IPv6 hierarchical network

SONG Shan-shan, SHANG Tao, LIU Jian-wei
(School of Electronic and Information Engineering, Beihang University, Beijing 100191, China)

Abstract: A fast access authentication scheme for mobile IPv6 hierarchical network was proposed, which improves the performance of access authentication of mobile IPv6 hierarchical network from two aspects, efficiency and security. Firstly, the scheme used the vector network address coding method to improve the home registration performance. Secondly, a hierarchical lattice-based signature scheme was designed to implement the two-way authentication and improve the security of the authentication process. The analysis of the scheme shows that it is strongly unforgeable, and meanwhile it can defend replay attacks and reduce the delay time of the entire authentication process.
Key words: mobile IPv6; hierarchical; access authentication; lattice signature

1 引言

移动 IPv6(MIPv6, mobile IPv6)网络为用户随时随地接入网络提供了可能性，也给用户的接入控制和管理提出了新的挑战。其中如何实现安全快速的接入认证是移动 IPv6 网络的一个关键问题。

对于复杂的网络环境，层次化结构可以将网络问题分解为较小的、比较简单的部分处理，减轻网络复杂性，优化网络性能。在认证系统中，签名者使用私钥对信息进行签名，验证者使用签名和身份进行验证，层次化身份签名(HIBS, hierarchical identity-based signature)机制简化了私钥的管理并支持大规模的层次化网络结构，更适用于移动 IPv6 网络环境中的认证。目前基于 HIBS 的移动 IPv6 认证协议 2-IBS-HAMIPv6[1]、结合 IBS 和移动 IPv6 的快速认证方法[2,3]都一定程度上优化了认证性能，但是 TIAN[1]的方案只可为 2 层用户提供服务，ZHANG[2]和 TIAN[3]的方案则需要更多的交互过程获取相关参数。因此，需要设计一种层次化身份签名方案，提高认证效率。

通过结合向量网络地址编码方法和格签名，本文提出了一个面向移动 IPv6 层次化网络的快速接入认证方案，具体从 2 个方面展开，一是采用向量网络地址编码方法实现注册过程中的数据传输，提

收稿日期：2013-07-02
基金项目：国家重点基础研究发展规划项目计划（“973”计划）基金资助项目（2012CB315905）；国家自然科学基金资助项目（61272501）；北京市自然科学基金资助项目（4132056）
Foundation Items: The National Key Basic Research Program (NKBRP) (973 program) (2012CB315905); The National Natural Science Foundation of China (61272501); The Beijing Natural Science Foundation (4132056)

高家乡注册效率；二是在认证过程中采用一种基于格的层次化身份签名方案，它具有更短的参数和签名长度，可以提高接入认证的安全性和效率。

2 相关工作

2.1 向量网络地址编码方法

向量网络地址编码方法(vector network address coding)是依据数据传输路径方向上的信源设备和转发设备的输出端口名进行地址编码的一种编码方法，每个输出端口名作为分量地址，依路径方向次序组成一个序列，即为编码结果。向量网络地址编码方法支持以向量地址 VA(vector address)为交换地址的向量网络结构[4,5]。向量地址中携带路由交换信息，易于转发数据，因此采用向量交换 VS(vector switching)的方法进行数据传输可以极大地提高数据传输效率。为了适用于大规模网络，使用层次化网络结构，提高向量交换效率。

2.2 格签名

格是 N 维空间中规则排列的离散点集合，格上任意实例的安全度都相同，并且至今没有可行的量子算法能够破解格上的困难问题，而 SHOR[6]已经指出可以使用量子算法解决离散对数问题，因此基于格的签名方案对于认证系统的安全性具有重要意义。

格签名相关算法如下。

1) 定理 1[7]：$q \geqslant 3$ 且为奇数，$m := \lceil 6n\log q \rceil$；存在一个算法 TrapGen$(q,n)$ 输出一对矩阵 $A \in Z_q^{n\times m}$，$S \in Z^{m\times m}$，S 是格 $\Lambda_q^{\perp}(A)$ 的基并且满足 $\|\tilde{S}\| \leqslant o(\sqrt{n\log q})$，$\|S\| \leqslant o(n\log q)$。

2) AGRAWAL[8]提供了算法在格 $\Lambda_q^{u}(F)(F = (A|AR+B))$ 中抽取短向量 e。

算法 SampleLeft(A, M_1, T_A, u, σ)：输入秩为 n 的矩阵 $A \in Z_q^{n\times m}$ 和矩阵 $M_1 \in Z_q^{n\times m_1}$，格 $\Lambda_q^{\perp}(A)$ 的基 T_A，向量 $u \in Z_q^n$，高斯参数 $\sigma > \|\tilde{T}_A\| \cdot \omega(\sqrt{\log(m+m_1)})$；令 $F_1 := (A|M_1)$，输出向量 $e \in Z^{m+m_1}$，其分布在统计学上接近于 $D_{\Lambda_q^u(F_1),\sigma}$，$e \in \Lambda_q^u(F_1)$。

算法 SampleRight$(A, B, R, T_B, u, \sigma)$：输入矩阵 $A, B \in Z_q^{n\times m}$ 且矩阵 B 的秩为 n，随机矩阵 $R \in \{-1,1\}^{m\times m}$，格 $\Lambda_q^{\perp}(B)$ 的基 T_B，向量 $u \in Z_q^n$，高斯参数 $\sigma > \|\tilde{T}_B\| \cdot \sqrt{m} \cdot \omega(\log m)$；令 $F_2 = (A|AR+B)$，输出向量 $e \in Z^{2m}$ 其分布在统计学上接近于 $D_{\Lambda_q^u(F_2),\sigma}$，$e \in \Lambda_q^u(F_2)$。

根据适当的参数，以上2个算法得到的短向量 e 的分布在统计学上是不可区分的。

3）在格签名方案中，将用户身份和消息作为一个整体计算，可以减少公共参数长度，提高签名效率。使用编码功能 $H: Z_q^n \to Z_q^{n\times n}$ 将用户的身份和消息（属于集合 Z_q^n）映射到矩阵（属于集合 $Z_q^{n\times n}$），基于安全性要求映射H满足内射性，即对任意2个不同的输入 u 和 v，输出 $H(u)$ 和 $H(v)$ 的差异性不单一，$\det(H(u) - H(v)) \neq 0$ [8]。

3 接入认证方案

3.1 网络结构

家乡注册是影响认证效率的重要因素之一，为了提高数据传输效率，引入向量网络地址编码方法层次化网络结构。在网络结构中，ID (identifier)代表网络节点的身份，Locator 代表网络节点当前的位置，PG(peer group)由网络结构中的实体构成，每个 PG 中有一个 PGL(peer group leader)，这些 PG 形成树状结构 PGT(peer group tree)，ID-PGL 负责用户的分配及从 *ID* 到 *Locator* 的映射，Loc-PGL 控制拓扑的集合和路由路径的建立，ID_{MN} 即用户的身份通过 MN 在家乡网络中的 HPGL 确定，$Locator_{\mathrm{MN}}$ 根据当前的节点位置由各种接入路由确定，ID_{MN} 和 $Locator_{\mathrm{MN}}$ 相互独立，共同支持节点的移动性。网络节点中初始位置的 PG 或者 PGL 称为 HPGL(home PGL)，相当于移动 IPv6 中的家乡代理 HA(home agent)，在网络中利用 *VA* 传输数据，将转发设备的输入输出端口从 1 开始用数字编号，称为端口号，*VA* 以端口号为编码基础，描述传送数据的通信路径。*VA* 由接入路由的 Loc-PGL 计算获得，在切换发生前存储于 MN 中，包括接入网络和 HPGL 之间的往返路径。*ID*、*Locator*、*VA* 3 者之间的映射关系如下图 1 所示。

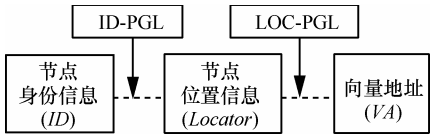


图 1 3 者映射关系

3.2 基于格的层次化身份签名方案

1) 困难假设

本文签名方案的安全性依赖于格中经典的SIS问题的困难性，SIS问题的定义如下。

SIS问题：设q为整数，$\beta(n)$是任意的多项式有界函数，矩阵$A\in Z_q^{n\times m}(m>n)$，则以$(q,m,\beta)$为参数的SIS问题是：求一个非零向量$e\in\{v\in Z_q^m:\|v\|\leqslant\beta\}$，满足$Ae=0(\mathrm{mod}\,q)$。

SIS假设：如果对某些以n为自变量的有界多项式函数$q(n),m(n)$和$\beta(n)$，在不知陷门的情况下，任意多项式时间敌手攻破SIS问题的概率是可忽略的，则称SIS假设成立。

2) 抽样短基算法

在HIBS中需要考虑一个简单的授权机制使矩阵的维数不变[9]，根据抽样算法扩展得到以下算法以获取格的一个短基。

SampleLeftBasis(A,M_1,T_A,σ)：输入秩为n的矩阵$A\in Z_q^{n\times m}$和一个矩阵$M_1\in Z_q^{n\times m_1}$，格$\Lambda_q^{\perp}(A)$的基T_A，高斯参数$\sigma>\|\tilde{T}_A\|\cdot\omega(\sqrt{\log(m+m_1)})$，得到格$\Lambda_q^{\perp}(F_1)$的基$T_{F_1}'$；进行格基的随机化运算，输出最终结果格$\Lambda_q^{\perp}(F_1)$的基$T_{F_1}$，且$\|\tilde{T}_{F_1}\|=\|\tilde{T}_A\|,F_1=(A|M_1)$。

SampleRightBasis(A,B,R,T_B,σ)：输入矩阵A、秩为n的矩阵$B\in Z_q^{n\times m}$，随机矩阵$R\in\{-1,1\}^{m\times m}$，格$\Lambda_q^{\perp}(B)$的基，高斯参数$\sigma>\|\tilde{T}_B\|\cdot\sqrt{m}\cdot\omega(\log m)$，得到格$\Lambda_q^{\perp}(F_2)$的基$T_{F_2}'$；进行格基的随机化运算，输出格$\Lambda_q^{\perp}(F_2)$的基$T_{F_2}$，且$\|\tilde{T}_{F_2}\|\leqslant\|\tilde{T}_B\|\cdot\sqrt{m}\cdot\omega(\sqrt{\log m})$，$F_2=(A|AR+B)$。

3) 基于格的层次化签名方案

根据基于格的身份加密方案[8]，本文设计一种层次化身份签名方案，它具有强不可伪造性[10]及更短的参数和签名，适用于层次化网络，可提高接入认证的安全性和效率。

在向量网络中，根PKG即相当于最顶部的PGL，将签名机制的最大层（包括根PKG）设为$d+1$，用户的身份为向量$id=\{id_0,\cdots,id_i,\cdots\}$，其中$id_i\in Z_q^n(0)$，签名方案包括以下4个部分。

系统建立：输入安全参数ε，设置参数n,m,q,σ；选择$d+3$个随机$n\times m$矩阵$A_1,\cdots,A_d,A_{d+1}$和$B,C\in Z_q^{n\times m}$和一个随机n维向量$u\in Z_q^n$，使用算法TrapGen(q,n)生成矩阵$A_0\in Z_q^{n\times m}$及格$\Lambda_q^{\perp}(A_0)$的基$T_{A_0}(\|\tilde{T}_{A_0}\|\leqslant o(\sqrt{n\log q}))$，输出公共参数和主密钥分别为$PP=(A_1,\cdots,A_d,A_{d+1},B,C,u)$，$MK=T_{A_0}\in Z^{m\times m}$。

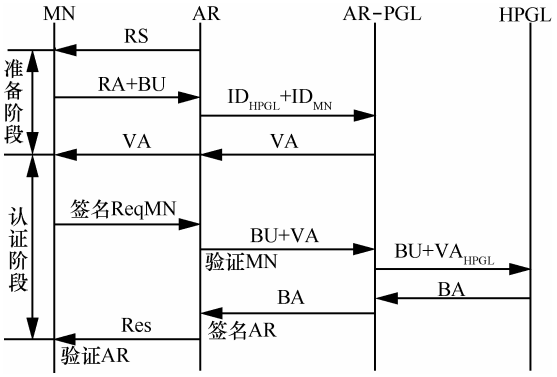
参数生成：l–1层用户身份$id|l-1=\{id_0,\cdots,id_{l-1}\}$的私钥为$SK_{id|l-1}$（格$\Lambda_q^{\perp}(F_{id|l-1})$的基），输入公共参数$PP$，定义$F_{id|l-1}=A_0|(A_1+\mathrm{H}(id_1)B)|\cdots|(A_{l-1}+\mathrm{H}(id_{l-1})B)\in Z_q^{n\times lm}$，则$F_{id|l}=F_{id|l-1}|(A_l+\mathrm{H}(id_l)B)$，通过算法SampleLeftBasis $(F_{id|l-1},A_l+\mathrm{H}(id_l)B,SK_{id|l-1},\sigma)$，输出格$\Lambda_q^{\perp}(F_{id|l})$的基$T_{id|l}$，即$l$层用户的私钥$SK_{id|l}$。

签名：l层用户身份$id|l=\{id_0,\cdots,id_l\}$，输入消息$M\in Z_q^{n-1}$和私钥$SK_{id|l}$，选择随机数$r\in Z_q$，通过算法SampleLeft $(F_{id|l},A_{d+1}+\mathrm{H}(M|r)C,SK_{id|l},u,\sigma)$计算签名$\delta$，$F_{id|l}=A_0|(A_1+\mathrm{H}(id_1)B)|\cdots|(A_l+\mathrm{H}(id_l)B)$，输出签名$(\delta,r)$。

验证：输入公共参数PP，签名(δ,r)和消息M，l层用户身份$id|l=\{id_0,\cdots,id_l\}$，当且仅当$0<\|\delta\|\leqslant\sigma\cdot\sqrt{(l+2)m}$和$F_{id|l,M,r}\cdot\delta=u$时，算法输出为1，$F_{id|l,M,r}=F_{id|l}|(A_{d+1}+\mathrm{H}(M|r)C)=A_0|(A_1+\mathrm{H}(id_1)B)\cdots|(A_l+\mathrm{H}(id_l)B)|(A_{d+1}+\mathrm{H}(M|r)C)$。

3.3 移动 IPv6 网络接入认证协议

在移动IPv6网络环境中，当MN发生移动后，整个接入认证过程包括接入认证和家乡注册2部分，具体如下。



RS/RA: router solicitations/router advertisement
BU/BA: binding update/acknowledgement
Req/Res: registration request packet/registration response packet

图 2　移动 IPv6 网络接入认证协议流程

1) 准备阶段：获取往返传输路径。

MN进入到外地网络后，生成响应消息RA及绑定更新消息BU，连同时戳T_1发送给AR作为响应，AR-PGL从AR收到消息后，首先在自己的数据列表中寻找VA，若存在则直接发送给AR；若不存在则通过ID_{MN}和ID_{HPGL}寻找AR和HPGL之间的传输路径：AR-PGL将ID_{HPGL}映射到$Locator_{\mathrm{HPGL}}$上，通过相关的Loc-PGL得到AR和HPGL之间的往返传输路径地址（即向量地址VA），并发送给AR。AR存储VA后将其发送给MN。

2) 认证阶段：双向认证和家乡注册。

MN收到VA后，生成消息M_1=(BU,T_1,ID_{MN},ID_{AR},VA)并对其签名，组成消息Req=(BU,ID_{MN},ID_{AR},T_1,$HVAP$,M_1,δ_{MN})发送给AR，其中T_1必须与准备阶段中的T_1同步保证此步骤与准备阶段同时进行。

AR收到BU消息后首先将其发送给AR-PGL，然后验证签名（两步分开可以实现家乡注册和用户认证的独立）。验证成功后，检查时戳T_1，以保证签名的新鲜性。

AR-PGL 收到注册信息后，从 VA 中提取 VA_{HPGL} (从接入网络到 HPGL 的传输路径)，将 BU 信息通过 VA_{HPGL} 发送给 HPGL，完成家乡注册。

HPGL收到BU信息后，更新$Locator_{\mathrm{MN}}$以获得ID_{MN}和$Locator_{\mathrm{MN}}$的同步，同时生成BA消息通过VA_{MN}发送给AR-PGL。VA_{MN}直接从VA中获得，减少HPGL的计算量。

AR-PG接着将BA消息发送给AR。

AR收到BA消息后，生成消息M_2=(BU,T_2,ID_{MN},ID_{AR},ID_{HPGL})并对其签名，组成消息Res=(BU,T_2,ID_{MN}, ID_{AR}, ID_{HPGL}, M_2,δ_{AR})发送给MN。MN验证AR的签名，实现MN与接入网络的双向认证。其中时戳T_2可以有效地防止重放攻击。

4 安全性分析

4.1 强不可伪造性的安全性分析

本文所提签名方案在适应性选择消息攻击下具有强不可伪造性。

证明 假设对于签名机制存在伪造者A及相关参数(t,ε,q_e,q_s)，则存在一个算法C，使A以至少ε'的概率在至多t'时间内解决SIS问题。

1) 系统建立：设整个签名机制为d+1层，敌手A的目标身份设为l层用户id。选择一个随机n维向量$u \leftarrow Z_q^n$和随机矩阵A_0，d+3个随机矩阵$A_1,\cdots,A_d,A_{d+1},B,C \in Z_q^{n\times m}$生成公共参数,其中$T_B$，$T_C$为$\Lambda_q^{\perp}(B),\Lambda_q^{\perp}(C)$的门限，2个随机矩阵$R \in \{-1,1\}^{m\times m}$ $R_1 \in \{-1,1\}^{2m\times m}$，设置$A_1 = A_0R - \mathrm{H}(id_l)B$和$A_{d+1} = (A_0 \mid A_0R)R_1 - \mathrm{H}(id_l)C$。

2) 签名询问：对消息M'及身份id'的签名询问。

如果$id' \neq id$，挑战者无法得到主密钥T_{A_0}，但可以使用门限T_B建立私钥,运行算法SampleRightBasisA_0, B_1,R,T_B, σ) 得到$T_{id'}$对敌手响应私钥询问，其中$F_{id'} = F_{id'|l-1} \mid (A_l + \mathrm{H}(id_l')B) = F_{id'|l-1} \mid (A_{l-1}R + (\mathrm{H}(id_l') - \mathrm{H}(id_l))B)$。通过计算，$T_B$也是格$\Lambda_q^{\perp}(B_1)(B_1 = (\mathrm{H}(id_l') - \mathrm{H}(id_l))B)$的门限，因此$B$与$B_1$是秩为$n$的矩阵。然后根据签名算法生成消息$M'$的签名。

如果$id' = id$，挑战者试图在提取问询中使用门限T_B用相似的方法创建一个签名。为了响应签名询问，挑战者选择随机数$r' \in Z_q$，抽取短向量$e \in \Lambda_q^{\perp}(F_{id',M',r'})$，运行算法SampleRight($(A_0 \mid A_0\ R)$, C_1,R_1,T_C,u,σ) 生成e响应签名询问，其中$F_{id',M',r'} = F_{id'} \mid (A_{d+1} + \mathrm{H}(M' \mid r')C) = F_{id'} \mid ((A_0 \mid A_0\ R)R_1 + (\mathrm{H}(M' \mid r') - \mathrm{H}(id_l'))C)$，如果$\mathrm{H}(M' \mid r') - \mathrm{H}(id_l')$是单一的，挑战者在重新选择随机数$r' \in Z_q$生成结果不单一的$\mathrm{H}(M' \mid r') - \mathrm{H}(id_l')$，计算出新的$F_{id',M',r'}$，因此$T_C$也是格$\Lambda_q^{\perp}(T_{C_1})$的门限，其中$C_1 = (\mathrm{H}(M' \mid r') - \mathrm{H}(id_l'))C$。然后将签名发送给敌手A。

3）伪造：敌手A生成一个对目标身份有效的伪造$(M,\delta \neq 0,r)$，此时在签名询问中已经有一元组(M_i,δ_i,r_i)，且对于$i \in (1,\cdots,q_s), M = M_i, \delta \neq \delta_i, r = r_i$。挑战者输出向量$v = \delta - \delta' \in \Lambda_q^{\perp}(F_{id,M,r})$，挑战者输出向量$v$作为困难问题SIS的解答。

由证明可知，如果假设成立，则存在算法可以在时间t'内以不可忽略的概率ε'解决格上SIS的一个困难问题，这与SIS假设矛盾，因此该方案具有强不可伪造性。

4.2 重放攻击的安全性分析

本方案采用时戳阻止重放攻击。在整个认证流程中，MN与AR的签名信息中都添加了时戳T_1、T_2。在协议的认证阶段，时戳T_1是签名消息M_1中的一部分，时戳T_2包含在签名消息M_2中。当攻击者有权进行重放攻击时，接受者会检验时戳的正确性，如果时戳无效，请求会被拒绝，对时戳的有效性确认应该在对签名的验证之后。因此，该协议方案可以防止重放攻击。

5 性能分析

接入认证的效率主要体现在网络数据传输和签名验证算法2个环节。

5.1 传输性能

为达到快速注册，使用基于端口的向量地址代替路由表查询。对于不同的路由表的大小需要考虑带宽和跳数，对于不同的路由器则只需要考虑VS的工作过程。因此家乡注册延迟包括注册延迟、跳

数、数据传输机制（VS或者IP）等几个因素。

VS传输机制由于不需要查询大量的传输表而减少了操作时间和路由器数据包的存储量，其时间延迟随着背景流量的增加而改变。而对于传统路由机制，路由表越大，传输时间将会越长；同时，在实际环境中，当MN离HA较远时，传输路径中会有更多的跳数，路由表也会增大，因此使用VS传输机制将会大大减少时间延迟。

5.2　签名性能

RUCKERT[11]在2010年提出了一个基于格的层次化身份签名机制，它具有更高的安全性——强不可为造性，但是由于其签名长度和私钥长度随着层次结构的增多而增大，并不适用于大的网络系统。对于本文提出的格签名机制与其之间签名效率的对比如表1所示，其中包括公共参数的长度、签名长度、密钥长度。假设签名机制的最大层为$d+1$，在每个层次子身份的长度为k，消息的长度为λ，每个子矩阵$\in Z_q^{n\times m}$，l代表身份的层次即第l层的身份$id=\{id_0,\cdots,id_l\}$。

表 1　　签名方案对比

签名机制	公共参数长度/bit	私钥长度/bit	签名长度/bit
文献[11]	$(nm(2dk+2\lambda+1)+n)\mathrm{lb}q$	$(lk+1)^2m^2\mathrm{lb}q$	$(lk+\lambda+1)m\mathrm{lb}q+n$
本文签名方案	$(nm(d+4)+n)\mathrm{lb}q$	$m^2\mathrm{lb}q$	$(2m+1)\mathrm{lb}q$

由表1中可以看出本文所提出的方案更适用于层次化网络，从公共参数的长度来说将用户身份和消息作为一个整体映射到矩阵而不是按比特进行计算，公共参数会更短，可以有效提高签名效率；同时，由于私钥与签名长度更短且不随层次化的增加而改变，更适用于大型层次化网络的接入认证。

6　结束语

本文提出了一个面向移动 IPv6 层次化网络的快速接入认证方案，该方案采用向量网络地址编码方法实现网络数据传输，解决了接入认证过程中家乡注册的性能问题，并在协议设计过程中，采取并行方式，将向量地址的获取和认证过程同时进行，简化了协议流程。而且本文设计了一种基于格的层次化签名方案，具有更高的安全性，同时对于层次化网络的接入认证来说，它具有更短的参数和签名长度，可以提高签名效率。

本文从效率和安全性 2 个方面提高接入认证的性能，但并未实现接入认证的层次化，当移动节点距离家乡代理较远时，认证的层次化会进一步减少与家乡代理的交互过程，从而提高协议的效率，同时层次之间的交互也会增加，如何实现认证的层次化并结合具体协议简化协议流程，是下一步需要解决的问题。

参考文献：

[1] TIAN Y, ZHANG Y, ZHANG H. Identity-based hierarchical access authentication in mobile IPv6 networks[A]. IEEE ICC[C]. Istanbul, 2006. 1953-1958.

[2] ZHANG J, ZHANG Y, ZHANG H. Trust-based fast authentication for mobile IPv6 networks[A]. IEEE Globecom[C]. New Orleans, LO, 2008. 1-5.

[3] TIAN Y, ZHANG Y, LIU Y. A fast authentication mechanism using identity based signature in mobile IPv6 network[J]. Chinese Journal of Computers, 2007, 17(9): 1980-1988.

[4] LIANG M. A Method for Vector Network Address Coding[P]. WO2007147328A1, 2007.

[5] ZHAO A Q, LIANG M G. A new forwarding address for next generation networks[J]. Journal of Zhejiang University Science C, 2012, 13(1): 1-10.

[6] SHOR P. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM Journal on Computing, 1997, 26(5):1484-1509.

[7] ALWEN J, PEIKERT C. Generating shorter bases for hard random lattices[J]. Theory of Computing Systems, 2011, 48(3):535-553.

[8] AGRAWAL S, BONEH D, BOYEN X. Efficient lattice (H)IBE in the standard model[A]. Advances in Cryptology-Eurocrypt[C]. Riviera, French, 2010. 553-572.

[9] CASH D, HOFHEINZ D, KILTZ E, *et al*. Bonsai trees, or how to delegate a lattice basis[J]. Journal of Cryptology, 2012, 25(4): 523-552.

[10] LI F, MUHAYA F T B, KHAN M K, *et al*. Lattice-based signcryption. http://onlinelibrary.wiloy.com/doi/10.1002cpe.2826/pdf.

[11] RUCKERT M. Strongly unforgeable signatures and Hierarchical identity based signatures from lattices without random oracles[A]. Post-Quantum Cryptography[C]. Darmstadt, Germany, 2010. 182-200.

作者简介：

宋姗姗（1989-），女，河南省遂平人，北京航空航天大学硕士生，主要研究方向为移动 IPv6、信息安全等。

尚涛（1976-），男，辽宁营口人，博士，北京航空航天大学讲师、硕士生导师，主要研究方向为无线网络通信、网络编码、网络安全等。

刘建伟（1964-），男，山东莱州人，博士，北京航空航天大学教授、博士生导师，主要研究方向为密码学、信息安全、网络安全等。