辫群上群签名方案的安全性分析及改进

隗 云[1] 熊国华[2] 张兴凯[3] 鲍皖苏[1]
(信息工程大学电子技术学院 郑州 450004)[1]
(电子技术研究所 北京 100195)[2] (96610部队 北京 102208)[3]

摘 要 量子计算的快速发展给传统密码体制带来严重威胁,使得基于非交换代数的密码体制成为研究热点。辫指数大于2的辫群具有非交换性,因此成为了构造密码协议的新平台。分析了一个基于辫群的群签名方案的安全性,指出该方案不满足不关联性,即同一群成员的多次签名能够被关联,且公布多个签名将泄露群私钥的信息。采用引入随机因子的方法对方案进行改进,既消除了原方案的可关联性,又保护了群私钥。安全性分析表明,改进后的方案满足群签名的各种安全性质。

关键词 辫群,群签名,共轭搜索,多重共轭搜索
中图法分类号 TP309 **文献标识码** A

Security Analysis and Improvement of a Group Signature Scheme Based on the Braid Groups

WEI Yun[1] XIONG Guo-hua[2] ZHANG Xing-kai[3] BAO Wan-su[1]
(Institute of Electronic Technology, Information Engineering University, Zhengzhou 450004, China)[1]
(Institute of Electronic Technology, Beijing 100195, China)[2] (Unit 96610, Beijing 102208, China)[3]

Abstract The rapid development of quantum computing makes public key cryptosystems based on noncommutative algebraic systems hot topic. Because of the non-commutativity property, the braid groups with braid index more than two become a new candidate for constructing cryptographic protocols. The security vulnerabilities of a group signature scheme based on the braid groups were pointed out that it does not satisfy the unlinkability, which means the signatures generated by the same group member can be linked, and the publication of several signatures will induce information leakage of the private key of the group. An improved scheme was proposed using random factor, which not only ensures the unlinkability of the scheme but also protects the group's private key. Security analysis shows that the improved scheme satisfies the security requirements of group signature.

Keywords Braid group, Group signature, Conjugacy search, Multiple conjugacy search

1 引言

众所周知,目前公钥密码体制最典型的两类安全性假设为整数分解和离散对数的难解性。量子计算[1,2]的快速发展使得目前的公钥密码体制面临严重威胁。为了抵抗已知量子算法的攻击,大量学者开始设计非基于数论的、基于非交换代数的公钥密码体制,如基于一般非交换群的密码[3]、基于有限非交换群的MOR密码[4]等。辫群的概念由Artin于1947年首次提出[5],由于其复杂的非交换结构,运算所需的时间和空间很小的特点,它也被用于构造公钥密码系统[6],基于辫群的密钥交换协议[7,8]、认证方案[9,10]、加密方案[11]及签名方案[12-18]相继被提出。

群签名的概念是Chaum等[19]于1991年提出的。在群签名中,群中任何成员都可代表群进行签名,且除群管理员外,任何人都无法判断一个群签名由哪个群成员产生,也无法判断两个不同的群签名是否是同一群成员所为。当发生争议时,群管理员可以打开签名以便揭示签名人的身份。群签名在电子选举、电子拍卖及电子现金系统等方面有广泛应用,是签名领域的研究热点之一[20-24]。但是,基于辫群的群签名研究还是一个比较新的课题,目前公开文献中的相关成果只有Thomas T和Lal A K构造的群签名方案[13]。

本文对Thomas T和Lal A K的群签名方案进行了安全性分析,指出了其安全缺陷,并利用随机因子提出了改进方案,新方案能满足群签名的各种安全需求。

2 预备知识

本节主要介绍辫群、辫群上的难解问题及群签名的安全性质。

2.1 辫群

定义1[6] 辫群 B_n($n\geqslant 2$为自然数)是由生成元 $\sigma_1,\sigma_2,\cdots,\sigma_{n-1}$ 生成的有限表示的无限群。其生成元满足

$$\sigma_i\sigma_j=\sigma_j\sigma_i \quad (|i-j|\geqslant 2)$$

到稿日期:2009-10-20 返修日期:2009-12-28 本文受国家自然科学基金(10501053)资助。

隗 云 博士生,CCF会员,主要研究方向为密码协议的设计与分析,E-mail:weiyun456@sohu.com;熊国华 博士后,高级工程师,主要研究方向为密码与编码;张兴凯 硕士,主要研究方向为密码协议的设计与分析;鲍皖苏 博士,教授,主要研究方向为密码学与网络安全。

$\sigma_i\sigma_{i+1}\sigma_i=\sigma_{i+1}\sigma_i\sigma_{i+1}$ $(1\leqslant i\leqslant n-2)$

因此辫群 B_n 可表示为

$$B_n=\langle\sigma_1,\sigma_2,\cdots,\sigma_{n-1}\mid\begin{matrix}\sigma_i\sigma_{i+1}\sigma_i=\sigma_{i+1}\sigma_i\sigma_{i+1}, & 1\leqslant i\leqslant n-2\\ \sigma_i\sigma_j=\sigma_j\sigma_i, & |i-j|\geqslant 2\end{matrix}\rangle$$

辫群中的元素称为一个 n 辫或辫元。当 $n=2$ 时，B_n 为无限循环群，本文不予考虑。

在 B_n 上定义偏序关系"$\leqslant$"如下：对 $(v,w)\in B_n\times B_n$，$v\leqslant w$ 当且仅当存在 $\alpha,\beta\in B_n^+$ 使得 $w=\alpha v\beta$。满足 $\varepsilon\leqslant\alpha\leqslant\Delta$ 的辫元 $\alpha\in B_n$ 称为正规因子。对正辫子 $\gamma=\alpha\beta$，α 为正规因子，如果 α 在所有的分解中根据偏序关系长度最长，则称这种分解是左加权的。任意辫元 $w\in B_n$ 都可以唯一表示成 $w=\Delta^r\alpha_1\cdots\alpha_q$，其中 $\alpha_1,\cdots,\alpha_q$ 为正规因子，$\alpha_i\alpha_{i+1}$ $(1\leqslant i<q)$ 是左加权的。q 称为 w 的正规长度，r 称为 w 的下确界，记作 $inf(w)$，$r+q$ 称为 w 的上确界，记为 $sup(w)$。

定义 2[6] 在辫群 B_n 中，由生成元 $\sigma_1,\sigma_2,\cdots,\sigma_{\lfloor n/2\rfloor-1}$ 生成的群叫 B_n 的左子群，记作 LB_n；由 $\sigma_{\lfloor n/2\rfloor+1},\cdots,\sigma_{n-1}$ 生成的群叫 B_n 的右子群，记作 RB_n。

显然，对任意 $(a,b)\in LB_n\times RB_n$，均有 $ab=ba$。

定义 3[6] 对于辫元 $x,y\in B_n$，若存在一个辫元 $a\in B_n$ 使得 $y=a^{-1}xa$，则称辫元 x,y 共轭，记作 $x\sim y$。

定义 4[6] 给定 $(x,y)\in B_n\times B_n$，判断 $x\sim y$ 是否成立，称之为共轭判断问题(Conjugacy Decision Problem，CDP)。

定义 5[6] 给定共轭辫元对 $(x,y)\in B_n\times B_n$，找到满足 $y=a^{-1}xa$ 的辫元 $a\in B_n$，称之为共轭搜索问题(Conjugacy Search Problem，CSP)。

定义 6[6] 给定 $(x_1,a^{-1}x_1a),\cdots,(x_N,a^{-1}x_Na)\in B_n\times B_n$，求辫元 $b\in B_n$，满足

$$b^{-1}x_1b=a^{-1}x_1a,\cdots,b^{-1}x_Nb=a^{-1}x_Na$$

称之为多重共轭搜索问题(Multiple Conjugacy Search Problem，MCSP)。

辫群内元素的乘法和求逆运算都存在快速算法，可以用计算机编程来实现。对辫群上的共轭判断问题，Ko 等人提出了一种多项式时间算法[6]。但是，尚未有算法能证明可在多项式时间内求解 CSP 或 MSCP。

2.2 群签名

定义 7[19] 一个群签名方案是包含以下过程的数字签名方案：

(1)创建。用以产生群公钥和私钥的多项式概率算法。

(2)加入。一个用户和群管理员之间的交互协议，使得用户成为群成员。执行该协议可产生群成员的私钥和成员证书。

(3)签名。一个概率算法，输入待签名的消息和某个群成员的私钥，输出对消息的群签名。

(4)验证。一个在输入对消息的签名及群公钥后确定签名是否有效的算法。

(5)打开。一个在给定某个签名和群私钥条件下确定签名人身份的算法。

群签名方案应满足以下安全性质[19]：

(1)正确性。一个群成员使用签名算法生成的签名可以被验证算法所接受。

(2)不可伪造性。只有群成员才能产生有效的群签名。

(3)匿名性。给定一个群签名，除群管理员外的任何人在计算上确定签名人身份是不可行的。

(4)不可关联性。在不打开签名的情况下，在计算上确定两个不同的签名是否为同一群成员所为是困难的。

本文中，$a\in_R A$ 表示从集合 A 中随机均匀地选择元素 a。对二进制串 $m_1,m_2\in\{0,1\}^*$，$m_1||m_2$ 表示 m_1 和 m_2 的级联。

3 Thomas-Lal 群签名方案及安全性分析

3.1 签名方案

假设群管理员与所有群成员之间都存在一条秘密信道。系统参数 n 和 l 都是足够大的正整数，令

$B_n(l)=\{b\in B_n\mid 0\leqslant\inf b\leqslant\sup b\leqslant l\}$

$LB_n(l)=\{b\in LB_n\mid 0\leqslant\inf b\leqslant\sup b\leqslant l\}$

$RB_n(l)=\{b\in RB_n\mid 0\leqslant\inf b\leqslant\sup b\leqslant l\}$

则有 $|B_n(l)|\leqslant l(n!)^l$，且 $B_n(l)$，$LB_n(l)$，$RB_n(l)$ 都是有限集合[13]。$H_1:B_n(l)\to\{0,1\}^*$，$H_2:\{0,1\}^*\to B_n(l)$ 为抗碰撞的单向函数，$m\in\{0,1\}^*$ 为待签名的消息。

建立

群管理员 T 选择 $s\in_R LB_n(l)$，$k_1,k_2\in_R RB_n(l)$ 及 $\alpha\in_R B_n(l)$，公开 $x=s^{-1}\alpha s$ 为群公钥。

加入

用户 P 与 T 执行以下协议后成为群成员。

(1)T 发送 (s,α) 至 P；

(2)P 选择 $u\in_R B_n(l)$，$a\in_R LB_n(l)$，并计算 $v=u^{-1}\alpha u$，$w=a^{-1}ua$，将 (v,w) 发送至 T；

(3)T 计算 $z_1=k_1^{-1}wk_1$，$z_2=k_2^{-1}wk_2$，并将 (z_1,z_2) 发送至 P；

(4)P 计算 $\beta_1=az_1a^{-1}$，$\beta_2=az_2a^{-1}$。

完成加入协议后，T 保存 v 作为 P 的公钥。

签名

签名用户 P 计算

$S_1=s^{-1}ys$，$S_2=s^{-1}\beta_1^{-1}y\beta_2s$

其中 $y=H_2(m)$，则关于消息 m 的群签名为 $\sigma_m=(S_1,S_2)$。

验证

签名接收人验证 $S_1\sim y$ 及 $S_1x\sim y\alpha$ 是否成立，若都成立，接受 $\sigma_m=(S_1,S_2)$ 为消息 m 的有效群签名。

打开

出现争议时，群管理员计算 $S_3=k_1sS_2s^{-1}k_2^{-1}$，验证 $S_3v\sim k_1yk_2^{-1}\alpha$ 是否成立，若成立，则签名成员为 v 对应的成员。

3.2 安全性分析

Thomas 和 Lal 称上述签名方案满足不关联性，其实不然。

假设同一群成员对两个消息 m_1 和 m_2 进行签名。令 $y_1=H(m_1)$，$y_2=H(m_2)$，$\sigma_{m_1}=(S_1^1,S_2^1)$，$\sigma_{m_2}=(S_1^2,S_2^2)$，则有

$S_2^1=s^{-1}\beta_1^{-1}y_1\beta_2s$，$S_2^2=s^{-1}\beta_1^{-1}y_2\beta_2s$

$S_2^1(S_2^2)^{-1}=s^{-1}\beta_1^{-1}y_1\beta_2ss^{-1}\beta_2^{-1}y_2^{-1}\beta_1s=s^{-1}\beta_1^{-1}y_1y_2^{-1}\beta_1s$

即 $S_2^1(S_2^2)^{-1}\sim y_1y_2^{-1}$ 成立。

若不同的群成员 P 和 P' 对消息 m_1,m_2 进行签名，则有

$S_2^1=s^{-1}\beta_1^{-1}y_1\beta_2s$，$S_2^2=s^{-1}(\beta_1')^{-1}y_2\beta_2's$

$S_2^1(S_2^2)^{-1}=s^{-1}\beta_1^{-1}y_1\beta_2ss^{-1}(\beta_2')^{-1}y_2^{-1}\beta_1's=s^{-1}\beta_1^{-1}y_1\beta_2(\beta_2')^{-1}y_2^{-1}\beta_1's$

由于 $\beta_1\neq\beta_1'$，$\beta_2\neq\beta_2'$，$S_2^1(S_2^2)^{-1}\sim y_1y_2^{-1}$ 不成立，因此任

何人都可以通过判断 $S_2^1(S_2^2)^{-1}\sim y_1y_2^{-1}$ 是否成立来判断两个签名是否为同一群成员所为，故该方案不满足不关联性。

此外，该方案的安全性建立在多重共轭搜索问题的难解性基础之上，每次签名中的 $S_1=s^{-1}ys$ 与 y 都成共轭关系，且共轭子均为群私钥 s，当多个签名公开时，必将泄露 s 的信息。下一节的改进方案将采用随机因子的方法，既消除了原方案的可关联性，又避免出现多个以 s 为共轭子的共轭辫元对，保护了群私钥 s。

4 新的群签名方案及安全性分析

4.1 签名方案

方案的建立、加入过程同原方案。

签名

签名用户 P 选择 $s_m\in_R LB_n(l)$，计算

$S_0=s^{-1}s_m^{-1}vs_ms$

$y=H_2(m||H_1(S_0))$

$S_1=s_m^{-1}s^{-1}yss_m$

$S_2=s^{-1}s_m^{-1}\beta_1^{-1}y\beta_2s_ms$

$S_3=s_m^{-1}xs_m$

则关于消息 m 的群签名为 $\sigma_m=(S_0,S_1,S_2,S_3)$。

验证

签名接收人计算 $y=H_2(m||H_1(S_0))$，验证 $S_1\sim y$ 及 $S_1S_3\sim y\alpha$ 是否成立，若都成立，接受 $\sigma_m=(S_0,S_1,S_2,S_3)$ 为消息 m 的有效群签名。

打开

出现争议时，群管理员计算

$\overline{S}_0=sS_0s^{-1}$，$\overline{S}_2=k_1sS_2s^{-1}k_2^{-1}$

首先判断 $\overline{S}_2\overline{S}_0\sim k_1yk_2^{-1}\alpha$ 是否成立，若成立，说明签名用户为群中成员。然后验证 $\overline{S}_0\sim v$ 是否成立，若成立，签名用户为 v 对应的成员。

4.2 安全性分析

由于随机因子 s_m 的引入，不同签名采用的随机因子不同，当多个签名公布时，虽然每个 $S_1=s_m^{-1}s^{-1}yss_m$ 仍与 y 共轭，但每次的共轭子 s_ms 因包含的随机因子 s_m 不同而不同，隐藏了群私钥 s 的信息，避免了秘密信息的泄露。方案的正确性、不可伪造性和不关联性如下。

(1)正确性

正确性可由下列式子获得。

$S_1=s_m^{-1}s^{-1}yss_m\sim y$

$S_1S_3=s_m^{-1}s^{-1}yss_ms_m^{-1}xs_m=s_m^{-1}s^{-1}yss^{-1}\alpha ss_m\sim y\alpha$

$\overline{S}_0=sS_0s^{-1}=s_m^{-1}vs_m\sim v$

$$\begin{aligned}\overline{S}_2&=k_1ss^{-1}s_m^{-1}\beta_1^{-1}y\beta_2s_mss^{-1}k_2^{-1}\\&=k_1s_m^{-1}(k_1^{-1}u^{-1}k_1)y(k_2^{-1}uk_2)s_mk_2^{-1}\\&=s_m^{-1}k_1(k_1^{-1}u^{-1}k_1)y(k_2^{-1}uk_2)k_2^{-1}s_m\\&=s_m^{-1}u^{-1}k_1yk_2^{-1}us_m\end{aligned}$$

$$\begin{aligned}\overline{S}_2\overline{S}_0&=s_m^{-1}u^{-1}k_1yk_2^{-1}us_ms_m^{-1}vs_m\\&=s_m^{-1}u^{-1}k_1yk_2^{-1}uu^{-1}\alpha us_m\\&=s_m^{-1}u^{-1}k_1yk_2^{-1}\alpha us_m\sim k_1yk_2^{-1}\alpha\end{aligned}$$

(2)不可伪造性

签名信息 S_0，S_1，S_2 都包含了群私钥 s 的信息，非群成员可以产生与 y 共轭的 S_1，但由于不知道 s，因此无法产生满足 $S_1S_3\sim y\alpha$ 的 S_1。计算 S_2 所需的 β_1 和 β_2 包含群成员的秘密信息 u，故任何群成员都无法假冒其他群成员进行签名。

(3)不关联性

假设同一群成员对两个消息 m_1，m_2 签名得到 $\sigma_{m_1}=(S_0^1,S_1^1,S_2^1,S_3^1)$ 和 $\sigma_{m_2}=(S_0^2,S_1^2,S_2^2,S_3^2)$，则对 $i=1,2$，有

$S_0^i=s^{-1}s_{m_i}^{-1}vs_{m_i}s$

$y_i=H_2(m_i||H_1(S_0^i))$

$S_1^i=s_{m_i}^{-1}s^{-1}y_iss_{m_i}$

$S_2^i=s^{-1}s_{m_i}^{-1}\beta_1^{-1}y_i\beta_2s_{m_i}s$

$S_3^i=s_{m_i}^{-1}xs_{m_i}$

$$\begin{aligned}S_2^1(S_2^2)^{-1}&=s^{-1}s_{m_1}^{-1}\beta_1^{-1}y_1\beta_2s_{m_1}ss^{-1}s_{m_2}^{-1}\beta_2^{-1}y_2^{-1}\beta_1s_{m_2}s\\&=s^{-1}s_{m_1}^{-1}\beta_1^{-1}y_1\beta_2s_{m_1}s_{m_2}^{-1}\beta_2^{-1}y_2^{-1}\beta_1s_{m_2}s\end{aligned}$$

若不同的群成员 P 和 P' 对消息 m_1，m_2 进行签名，有

$$\begin{aligned}S_2^1(S_2^2)^{-1}&=s^{-1}s_{m_1}^{-1}\beta_1^{-1}y_1\beta_2s_{m_1}ss^{-1}s_{m_2}^{-1}\beta'^{-1}_2y_2^{-1}\beta'_1s_{m_2}s\\&=s^{-1}s_{m_1}^{-1}\beta_1^{-1}y_1\beta_2s_{m_1}s_{m_2}^{-1}\beta'^{-1}_2y_2^{-1}\beta'_1s_{m_2}s\end{aligned}$$

两种情况下，$S_2^1(S_2^2)^{-1}$ 均未与某些公开信息成共轭关系，因此，方案满足不关联性。

结束语 由于非交换性，辫群成为了构造公钥密码体制的新平台。本文对辫群上的群签名进行了研究，指出 Thomas 和 Lal 的群签名方案存在两个安全缺陷：可关联性和群私钥的信息泄露，并利用随机因子对方案进行了改进。研究辫群上群签名方案的群成员删除问题是下一步的工作。

参 考 文 献

[1] Shor P W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer[J]. SIAM J. Comput, 1997, 5: 1484-1509

[2] Kitaev A. Quantum Measurements and the Abelian Stabilizer Problem [DB/OL]. http://arxiv.org/quant-ph/9511026

[3] Anshel I, Anshel M, Goldfeld D. An Algebraic Method for Public Key Cryptography[J]. Math. Research Letters, 1999, 6: 287-291

[4] Paeng S H, Kwon D, Ha K C, et al. Improved Public Key Cryptosystem Using Finite Non-Abelian Groups[DB/OL]. http://eprint.iacr.org/2001/066

[5] Artin E. Theory of Braids[J]. Annals of Math, 1947, 48(1): 101-126

[6] Ko K H, Lee S J, Cheon J H, et al. New Public Key Cryptosystem Using Braid Groups[A]// Proceedings of Crypto-2000, Lecture Notes in Computer Science[C]. Benlin: Springer-Verlag, 2000, 1880: 166-183

[7] Anshel I, Anshel M, Fisher B, et al. New Key Agreement Protocol in Braid Group Cryptography[A]// Topics in Cryptology-CT-RSA 2001, Lectures in Computer Science [C]. Benlin: Springer Verlag, 2001, 2020: 1-15

[8] Cha J C, Ko K H, Lee S J, et al. An Efficient Implementation of Braid Groups [A] // Advances in Cryptology: Proceedings of ASIACRYPT 2001, Lecture Notes in Computer Science [C]. Springer-Verlag, 2001, 2248: 144-156

[9] Sibert H, Dehornoy P, Girault M. Entity Authentication Schemes Using Braid Word Reduction[DB/OL]. http://eprint.iacr.org/2002/187

[10] Lal S, Chaturvedi A. Authentication Schemes Using Braid Groups[DB/OL]. http://arXiv.org/cs.CR/0507066

[11] 汤学明，洪帆，崔国华. 辫子群上的公钥加密算法[J]. 软件学报，2007, 18(3): 722-729

[12] Ko K H, Choi D H, Cho M S, et al. New Signature Scheme Using Conjugacy Problem [DB/OL]. http://eprint.iacr.org/

2002/168
[13] Thomas T, Lal A K. Group Signature Scheme Using Braid Groups[DB/OL]. http://arXiv.org/cs.CR/0602063
[14] Zou S H, Zeng J W, Quan J J. Designated Verifier Signature Scheme Based on Braid Groups[DB/OL]. http://eprint.iacr.org/2006/329
[15] Verma G K. Blind Signature Schemes over Braid Groups[DB/OL]. http://eprint.iacr.org/2008/027
[16] Verma G K. A Proxy Signature Scheme over Braid Groups[DB/OL]. http://eprint.iacr.org/2008/160
[17] Zhang L L, Zeng J W. Proxy Signature Based on Braid Group [J]. Journal of Mathematical Study, 2008, 41(1): 56-64
[18] Lal S, Verma V. Some Proxy Signature and Designated Verifier Signature Schemes over Braid Groups[DB/OL]. http://arXiv.org/cs.CR/09043422
[19] Chaum D, Van E H. Group Signatures[A]// Proceedings of Europcrypt'91, Lecture Notes in Computer Science[C]. Springer-Verlag, 1991, 547: 257-265
[20] 刘文远,宋高效. 高效可撤销成员的不可链接的群盲签名方案[J]. 计算机科学,2008,35(11):60-62
[21] 全俊杰,曾吉文,邹时华. 基于 MSP 秘密共享的(t,n)门限群签名方案[J]. 数学研究,2008,41(1):65-71
[22] 于宝证,徐枞巍. 对一类群签名方案的伪造攻击[J]. 电子与信息学报,2009,31(1):246-249
[23] 禹勇,许春香,周敏,等. 对两个提名代理签名方案的密码学分析[J]. 电子与信息学报,2009,31(5):1218-1220
[24] 蔡永泉,刘岩. 一种基于身份信息无可信中心无随机预言的群签名方案[J]. 电子学报,2009,37(4A):87-91

(上接第 39 页)

时,则在 Hash(16),Hash(32),Hash(48)及 Hash(64)中,修改前缀 P 的子前缀 $P_s(P,16)$,$P_s(P,32)$,$P_s(P,48)$,$P_s(P,64)$表项的 C_Total 及 C_Zone。如果 VP_Flag=1 且 C_Total=0,则将该表项置为无效。

(2)如果 *len* 不能被 16 整除,则首先在 Hash(16),Hash(32)及 Hash(48)中,修改前缀 P 的子前缀 $P_s(P,16)$,$P_s(P,32)$,$P_s(P,48)$表项的 C_Total 及 C_Zone。如果 VP_Flag=1 且 C_Total=0,则将该表项置为无效,然后通过树位图的入口地址,在其对应的树位图中执行相应的修改和删除操作。

3 实验及性能分析

3.1 虚拟前缀数量

在基于 Hash 表和树位图的两级 IPv6 地址查找算法中,由于前缀之间大量存在覆盖关系,较长前缀可以借助 Hash 表中的前缀表项来表示该前缀 P 中能被 16 整除的部分,因此会在 Hash 表中引入一定数量的虚拟前缀 VP。实验中采用的路由表信息来自网络 potaroo[9]上的统计信息,其中长度为 16,32,48,64 比特的实际前缀总数为 1734,引入虚拟前缀之后,长度为 16,32,48 及 64 比特的前缀总数为 1841,增加的前缀数目为 107 个,所占的比例为 6.17%。同时,由于前缀之间的覆盖关系密切,相对于总前缀数目而言,引入的虚拟前缀的比例为 107/1917,约为 5%左右,如图 6 所示。

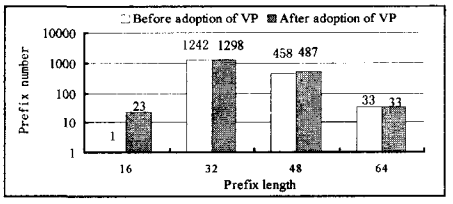

图 6 算法引入的虚拟前缀数目

3.2 两级地址查找的效率

为了评估本文 IP 地址查找算法的效率,本文使用随机和非随机两种策略产生 IPv6 测试地址,生成脚本采用了 ipv6gen[10]。表 4 中列出了采用 4 种 IP 测试数据所得到的地址查找次数和平均查找次数。可以看出,本文算法的平均查找次数介于 1～2 之间。尤其是当 IPv6 地址的分布规律与路由表分布规律类似时,算法的平均查找性能接近于 1。

表 4 平均查找次数

路由前缀数目	IP 地址数目	总查找次数	平均查找次数
1917	1917(随机)	3836	2.001
1917	19021(随机)	36369	1.912
1917	33124(随机)	61250	1.849
1917	43737(非随机)	55065	1.259

结束语 本文将按前缀长度二分查找与树位图查找的方法结合起来,将 IPv6 的地址查找分成两个阶段,第一个阶段直接使用 Hash 查找,第二阶段使用树位图查找。本文算法的主要优点为:1)由于采用两级查找,增加了查找算法的灵活性,两级算法可以相对独立,便于算法的升级;2)相对于按前缀二分查找算法来说,本算法引入的虚拟前缀数量较少,可以节约存储空间,提高了平均查找性能;相对于 Tree bitmap 算法而言,大大降低了树的高度,提高了查找效率;3)本算法平均查找次数为 1～2 次,最差查找次数为 7,查找效率较高。进一步的研究将采用并行的处理方法,同时对各个 Hash 表进行查找,从而进一步提高地址查找的效率。

参 考 文 献

[1] Fuller V, Li T, Yu J, et al. Classless Inter-domain Routing(CIDR): an address assignment and aggregation strategy (RFC 1519)[EB/OL]. ftp://ds.internic.net/rfc/rfc1519.txt, 1993
[2] Deering S, Hinden R. Rfc1883: Internet protocol, version 6 (ipv6) specification [EB/OL]. ftp://ds.internic.net/rfc/rfc1883.txt, 1995
[3] Sánchez M, Biersack E W, Dabbous W. Survey and taxonomy of IP address lookup algorithms[J]. IEEE Network, 2001, 15(2): 8-23
[4] Li Y K, Pao D. Address lookup algorithms for IPv6[J]. IEE Proceedings-Communications, 2006, 153(6): 909-918
[5] Waldvogel M, Varghese G, Turner J, et al. Scalable high speed IP routing lookups[C]// Proceedings of the ACM SIGCOMM'97 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication. ACM, 1997
[6] Eatherton W. Hardware-based internet protocol prefix lookups [D]. St. Louis: Washington University, 1999
[7] Eatherton W, Varghese G, Dittia Z. Tree bitmap: hardware/software IP lookups with incremental updates[J]. ACM SIGCOMM Computer Communication Review, 2004, 34(2): 97-122
[8] Huston G. Analyzing the Internet's BGP routing table[J]. The Internet Protocol Journal, 2001, 4(1): 2-15
[9] AS2-IPv6 BGP Table Statistics[EB/OL]. http://bgp.potaroo.net/v6/as2.0/index.html. 2009-06-18
[10] ipv6gen-IPv6 prefix generator[EB/OL]. http://techie.dev-null.cz/ipv6/ipv6gen. 2009-06-18