命名数据网络中可追溯且轻量级的细粒度访问控制机制

雒江涛*② 何 宸①② 王俊霞①②

①(重庆邮电大学通信与信息工程学院 重庆 400065)

②(重庆邮电大学电子信息与网络工程研究院 重庆 400065)

摘 要：由于命名数据网络(NDN)具有网内缓存特点，任意用户可直接从中间路由节点获取数据，同时，内容提供商也无法得知用户的访问信息。针对这些问题，该文结合基于身份的组合公钥和Schnorr签名方法，提出了“三次握手”匿名安全认证协议，同时，采用改进的秘密共享方法来高效分发内容密钥，实现了一种可追溯且轻量级的细粒度访问控制机制(TLAC)，最后，通过实验验证了TLAC机制的高效性。

关键词：命名数据网络；内容缓存；访问控制；可追溯性

中图分类号：TP393 **文献标识码**：A **文章编号**：1009-5896(2019)10-2428-07

DOI: 10.11999/JEIT181160

Traceable Lightweight and Fine-grained Access Control in Named Data Networking

LUO Jiangtao② HE Chen①② WANG Junxia①②

①(*School of Communications and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing* 400065, *China*)

②(*Electronic Information and Networking Research Institute, Chongqing University of Posts and Telecommunications, Chongqing* 400065, *China*)

Abstract: Due to the feature of in-network caching in Named Data Networking (NDN), any consumer might fetch the cached contents from NDN routers, but the content producers have no idea about details of certain contents being accessed. Considering these problems, a fine-grained Traceable and Lightweight Access Control (TLAC) scheme is presented. In the TLAC scheme, an anonymous and secure “three-way handshake” authentication protocol is presented by collaboratively leveraging the combined public key and the Schnorr signature, and an improved secret sharing method is used to distribute the key efficiently. Finally, the experimental results prove the efficiency of TLAC scheme.

Key words: Named Data Networking (NDN); Content caching; Access control; Traceability

1 引言

随着互联网的普及，截止2016年底，网络视频流及下载量占互联网总流量的57%，预计在2021年会达到82%[1]。面对各类音视频业务的增加，人们对互联网的需求不再局限于端到端的传统通信，更多的是对海量内容的获取，因此传统的TCP/IP网络暴露出安全性差、内容分发效率低等弊端。为了更好地适应用户的需求，命名数据网络(Named Data Network, NDN)应运而生。

NDN中传输两类包：兴趣包和数据包。用户以pull方式向内容提供商(Content Providers, CP)请求内容，通过主动发送带有内容名的兴趣包来获取数据包，当兴趣包到达缓存了所请求数据包的路由器时，路由器将数据包以兴趣包传输的反向路径响应至用户。NDN将内容名代替IP地址作为包的唯一标识，并根据内容名实现包的转发路由[2]，并采用网内缓存机制来减少网络中冗余的请求数量，提高了网络资源的利用率。然而，任意用户可从网络节点中获取内容，同时，节点未向CP反馈访问信息，从而CP失去对内容的细粒度控制[3]，包括无法得知授权用户访问数据的信息。在商业模式中，

收稿日期：2018-12-18；改回日期：2019-06-14；网络出版：2019-06-24

*通信作者： 雒江涛 Luojt@cqupt.edu.cn

基金项目：教育部-中国移动科研基金(MCM20170203)，重庆市基础科学与前沿研究重点项目(cstc2015jcyjBX0009, CSTCK-JCXLJRC20)

Foundation Items: Ministry of Education-China Mobile Research Fund Project (MCM20170203), The Fundamental and Frontier Research Project of Chongqing (cstc2015jcyjBX0009, CSTCK-JCXLJRC20)

CP不会以免费的方式共享具有高价值的内容，同时，CP需要掌握用户的访问信息来完成内容的推荐或收费。因此，NDN的网内缓存特性导致NDN无法满足商业需求。为此，如何构建一种灵活高效且可对访问进行追溯的细粒度访问控制是提高NDN可用性的重要研究方向。

目前一些基于加密的方法被应用到NDN的访问控制中。文献[4,5]提出基于广播加密(Broadcast Encryption, BE)的访问控制机制，采用BE来分发内容的对称密钥，但未能有效解决用户共谋密钥的问题。文献[6]提出一种概率访问控制方法，采用公钥基础设施(Public Key Infrastructure, PKI)来分发内容密钥，并使边缘路由器通过布隆滤波器来过滤未授权的请求，但由于布隆滤波器具有假正例的误识别率，因而不能过滤掉所有未授权的请求。在文献[7]提出的代理重加密方案中，边缘路由器在响应数据前，会产生随机密钥来重加密数据，再将用CP公钥加密的随机密钥和重加密的数据响应给用户，然后用户向CP请求解密密钥，但重加密操作会占用边缘路由器过高的计算开销。文献[8]提出了一种可追溯的SEAF访问控制机制，该机制采用组签名在网络边缘实现匿名认证，并使用哈希链技术来降低用户连续请求时的开销，然而其采用的双线性对是已知最复杂的密码学操作[9]，导致SEAF机制不足够轻量级。

上述方案不能很好地满足NDN对访问控制的需求，包括高效的密钥分发和访问追溯。为解决这些问题，本文为NDN提出一种可追溯且轻量级的细粒度访问控制机制(Trackable and Lightweight Access Control, TLAC)。TLAC结合基于身份的组合公钥[10](IDentity-based Combined Public Key, ID-CPK)和高效安全的Schnorr签名[11]方法，在边缘路由器上对用户进行“三次握手”匿名安全认证，对非法用户的请求进行过滤，从而完成访问记录和追溯。TLAC在对合法用户完成“三次握手”认证后，基于共享的秘密并采用轻量级的单向散列函数[12]来减少后续认证开销。同时，TLAC结合基于身份密码学[13](Identity Based Cryptography, IBC)和改进的秘密共享[14](Shamir's Secret Sharing, SSS)方法来高效地分发密钥。

最后，本文进行了仿真实验，对标准的NDN和SEAF机制、TLAC机制进行了对比和分析，从而可知：在内容检索时，TLAC机制未引进明显的时延，验证了其高效性；同时，用户只需少量的计算开销来重构密钥，可以实现高效灵活的密钥分发。

2　TLAC原理

2.1　系统模型

首先，本文将NDN中的路由器分成两类：中间路由器和边缘路由器，两种路由器都会负责兴趣包和数据包的转发，并缓存转发过来且符合要求的数据包；而边缘路由器在将兴趣包传输进核心网前，还必须完成请求的认证。本文假设边缘路由器会如实地执行认证协议，并且不会泄露认证后和用户共享的秘密。其次，本文采用IBC方法为网络实体生成基于身份的密钥对，因此用户私钥(User's Secret Key, USK)与用户身份(User's IDentity, UID)构成密钥对。最后，本文将用户请求的数据分成3类，分别为不受访问限制的共享内容，受访问限制的内容以及受访问限制且要求对访问进行追溯的内容。TLAC机制采取加密的方式来保护后两类内容，并采用SSS方法分发内容密钥，同时，边缘路由器会协助CP完成第3类内容的访问追溯。为使边缘路由器有效区分用户所请求的内容类别，第3类内容的名字后缀会额外地增加“/EOF”。

2.2　“三次握手”匿名安全认证协议

当用户请求第3类内容时，必须向边缘路由器发起身份认证的请求，同时，边缘路由器新增一个认证状态表(Authentication State Table, AST)。AST中的条目可以表示为{UID和注册时间戳的散列值，CPK，最新请求时间戳，秘密值，标识位}，其中，当标识位为1时，表明该用户已成功完成“三次握手”；当标识位为0时，表明路由器处于等待用户完成“三次握手”最后确认的状态中。

在TLAC中，CP的初始化步骤如下所示。

(1) CP根据ID-CPK为授权用户生成访问内容的匿名公私钥：

(a) 选择一个大素数P，并在P阶有限域GF(P)上构建椭圆曲线$E(a,b): y^2 \equiv x^3+ax+b \bmod P, a,b,x,y \in \mathrm{GF}(P)$，其中，$4a^3+27b^2 \neq 0 \bmod P$；

(b) 在$E(a,b)$上选择基点G，其阶为大素数n。然后，CP产生$m \times q$的私钥矩阵$\boldsymbol{X}_{\mathrm{PR}}$

$$\boldsymbol{X}_{\mathrm{PR}}=\begin{bmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,q} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,q} \\ \vdots & \vdots & \ddots & \vdots \\ x_{m,1} & x_{m,2} & \cdots & x_{m,q} \end{bmatrix} \tag{1}$$

其中，$x_{i,j}<n, 1\le i\le m, 1\le j\le q$，且$x_{i,j}$互不相等。由$\boldsymbol{X}_{\mathrm{PR}}$派生得公钥矩阵$\boldsymbol{Y}_{\mathrm{PU}}$: $x_{i,j}\cdot G=y_{i,j}$，有

$$\boldsymbol{Y}_{\mathrm{PU}}=\begin{bmatrix} y_{1,1} & y_{1,2} & \cdots & y_{1,q} \\ y_{2,1} & y_{2,2} & \cdots & y_{2,q} \\ \vdots & \vdots & \ddots & \vdots \\ y_{m,1} & y_{m,2} & \cdots & y_{m,q} \end{bmatrix} \tag{2}$$

(c) 选择单向散列函数$H_1:\{0,1\}^*\to\{0,1\}^l$, $H_2:\{0,1\}^*\to Z_n^*$;

(d) 当CP对身份为UID的用户进行授权时，首先通过$H_1(\text{UID})=h_1h_2\cdots h_i\cdots h_l$计算得二进制定长为$l$的序列，并按每$x$ bit分割序列得$w_1w_2\cdots w_i\cdots w_q$，其中$m=2^x, w_i\in[0,m), l=x\times q$。然后，CP以$n$阶有限域$F(n)$上的倍数加法计算用户的标识私钥$\text{isk}=\sum_{i=1}^{q}x_{(w_i+1),i}\text{mod}n$，并以椭圆曲线$E(a,b)$上的倍点加法计算用户的标识公钥$\text{IPK}=\sum_{i=1}^{q}y_{(w_i+1),i}$;

(e) CP产生一个由N_2个公私钥对$(\text{ssk}_i,\text{SPK}_i)$组成的分割密钥序列，其中，$\text{ssk}_i$为分割私钥且$\text{ssk}_i<n$，$\text{SPK}_i$为分割公钥且$\text{SPK}_i=\text{ssk}_i\cdot G$, $N_2=m\times m$, $i=0,1,\cdots,N_2-1$。CP首先基于用户注册的时间戳T_s和UID生成分割参数$\text{KP}=\{\text{UID}||T_\text{s}\}$，再按上一步骤的方法通过$H_1(\text{KP})=h_1h_2\cdots h_i\cdots h_l$计算得$w_1'w_2'\cdots w_i'\cdots w_q'$，从而根据$w_{q-1}'$, w_q'得到$t=w_{q-1}'\times m+w_q'$，最后从分割密钥序列中选取用户的分割密钥$(\text{ssk}_t,\text{SPK}_t)$;

(f) CP基于标识密钥和分割密钥计算用户公钥CPK和用户私钥upk

$$\left.\begin{aligned}&\text{upk}=(\text{ssk}_t+\text{isk})\text{mod}n\\&\text{CPK}=\text{SPK}_t+\text{IPK}\end{aligned}\right\}\tag{3}$$

(2) CP根据Schnorr签名方法为授权用户生成签名证书$\sigma_u=\{U_\text{pub},E_u\}$。CP随机选择一个数$C_\text{pri}\in Z_n^*$，并计算$C_\text{pub}=C_\text{pri}\cdot G$。为隐藏用户的真实信息，CP基于$h_\text{uid}=H_2(\text{UID}||T_\text{s})$和CPK生成签名证书，并通过证书里的$T_\text{s}$来限制用户的访问时间，具体算法如下：

(a) 随机选择一个数$U_\text{pri}\in Z_n^*$，计算$U_\text{pub}=U_\text{pri}\cdot G$;

(b) 计算$E_u=U_\text{pri}+C_\text{Pri}H_2(h_\text{uid}||\text{CPK}||T_\text{s})\text{mod}n$。

(3) CP将$\{\text{CPK},\text{upk},\sigma_u,T_\text{s}\}$安全地分发给授权用户，并向全网络公开参数$\{E(a,b),G,P,n,H_2,C_\text{pub},T_\text{a}\}$，其中，$T_\text{a}$为授权用户证书的有效截止时间。

为请求第3类内容，用户将和边缘路由器进行“三次握手”身份认证，从而与边缘路由器建立虚连接，如图1所示。

(1) 第1次握手：此时，边缘路由器处于LISTEN状态，即等待用户的连接请求。为防止攻击者截取签名证书，用户需要隐藏证书，得到$\{W,E_u'\}$。首先，用户获取当前时间戳T_1和$h_\text{uid}=H_2(\text{UID}||T_\text{s})$，再选择两个随机数$u_1,r_u\in Z_n^*$，并计算

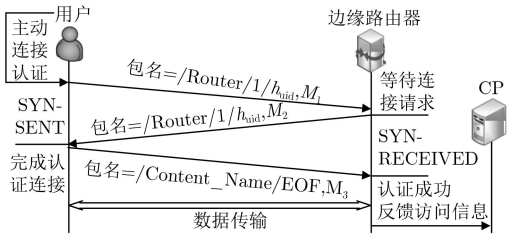

图 1 “三次握手”身份认证

$$\left.\begin{aligned}&R_1=u_1\cdot G, R_u=r_u\cdot G\\&h_{T_1}=H_2(T_1)\\&W=h_{T_1}\cdot U_\text{pub}+R_u\\&E_u'=(h_{T_1}E_u)\cdot G+R_u\\&h_1=H_2(\text{CPK}||R_1||T_1)\\&Z_1=u_1+h_1\times\text{upk}\text{mod}n\end{aligned}\right\}\tag{4}$$

然后，将$M_1=\{T_1,T_\text{s},R_1,Z_1,W,E_u',\text{CPK}\}$添加至以“/Router/1/$h_\text{uid}$”为名的兴趣包中，再将兴趣包发送至边缘路由器。此时，用户处于SYN-SENT状态，即等待匹配的连接响应。

(2) 第2次握手：边缘路由器收到连接请求的兴趣包后，首先验证T_1是否在有效范围内。若T_1未在有效时间范围内，就丢掉该兴趣包，否则检查是否缓存对应CP的公开参数。若未缓存参数，则向CP或中间节点请求。然后，边缘路由器验证T_s是否小于T_a，并验证等式$E_u'=W+[H_2(h_\text{uid}||\text{CPK}||T_\text{s})\cdot H_2(T_1)]\cdot C_\text{pub}$。若成立，则用CPK进一步验证等式$Z_1\cdot G=R_1+H_2(\text{CPK}||R_1||T_1)\cdot\text{CPK}$。若验证成功，则选择一个随机数$u_2\in Z_n^*$，并计算

$$\left.\begin{aligned}&R_2=u_2\cdot G\\&K_\text{ur}=u_2\cdot R_1\\&h_2=H_2(\text{CPK}||R_1||T_2)\end{aligned}\right\}\tag{5}$$

其中，T_2是当前时间戳。最后，边缘路由器在AST中新建条目$\{h_\text{uid},\text{CPK},T_1,K_\text{ur},0\}$，并将$M_2=\{T_2,R_2,h_2\}$响应给用户。此时边缘路由器处于SYN-RECEIVED状态，即等待用户最后的连接确认，若在一定时间范围内，未收到确认信息，则会删除AST中的对应条目。

(3) 第3次握手：用户收到M_2后，验证T_2是否在有效范围内，并验证等式$h_2=H_2(\text{CPK}||R_1||T_2)$。若验证成功，则计算

$$\left.\begin{aligned}&K_\text{ur}=u_1\cdot R_2\\&h_3=H_2(\text{CPK}||K_\text{ur}||T_3)\end{aligned}\right\}\tag{6}$$

再将$M_3=\{T_3,h_\text{uid},\text{CPK},h_3\}$添加至以“/Content_Name/EOF”为名的兴趣包中，并将兴趣包发送至边缘路由器。此时，用户处于ESTABLISHED状态，即完成认证连接并开始请求内容

“Content_Name”。当边缘路由器收到确认信息时，检查T_3是否大于AST对应条目中的时间戳，并验证等式$h_3 = H_2(\mathrm{CPK}||K_{\mathrm{ur}}||T_3)$。若验证成功，则连接成功，边缘路由器将兴趣包传输进核心网里，并将AST中的对应条目更新为$\{h_{\mathrm{uid}}, \mathrm{CPK}, T_3, K_{\mathrm{ur}}, 1\}$，同时开始记录访问信息。若用户长时间未请求数据，边缘路由器则会释放连接，清除AST中的对应条目。

(4) 在“三次握手”后，用户将会直接基于单向散列函数和K_{ur}来请求第3类内容。用户计算$h_0 = H_2(\mathrm{CPK}||K_{\mathrm{ur}}||T_0)$，其中$T_0$是当前时间戳，并将$M_0 = \{T_0, h_{\mathrm{uid}}, \mathrm{CPK}, h_0\}$添加至兴趣包中。当边缘路由器收到兴趣包后，首先验证T_0是否大于AST中对应条目里的时间戳。若时间戳满足要求且$h_0 = H_2(\mathrm{CPK}||K_{\mathrm{ur}}||T_0)$，则边缘路由器将AST中对应条目里的时间戳更新为$T_0$，同时将兴趣包传输进核心网里。

为实现访问可追溯性，边缘路由器向CP定期地反馈访问信息。对于AST条目中标识位为1的请求，边缘路由器在更新AST里的时间戳时，会保存访问信息，然后将这些信息和h_{uid}, CPK等认证信息发送给CP。由于CP存有UID与$(h_{\mathrm{uid}}, \mathrm{CPK})$的映射关系，当CP对身份为UID的用户进行访问追溯时，便通过映射关系找到$(h_{\mathrm{uid}}, \mathrm{CPK})$，再在路由器反馈的访问信息中进行查询。

2.3 密钥分发

TLAC机制通过对称加密的方式来保护内容，并采用SSS方法来高效分发密钥。在Shamir方法中，假定多项式次数为k–1，当用户数达到k时，秘密值便可被还原，因此多项式次数与用户数相互关联，通过限制用户数来避免合谋攻击，同时在更新多项式时，用户持有的秘密份额也会得到更新。受文献[15]的启发，在改进的秘密共享方法中，本文先定义两个基本概念：

(1) 用户份额US：它是由CP计算得到的一个数值，会被安全地分发给授权用户。

(2) 互补份额CS：它是由CP为授权用户计算得到的两个数值，是一个与用户和内容相关的参数。

一个用户可以基于US和CS重构对称密钥DK。对于一个复杂且过长的DK, CP可将其划分成更小的子串$\lambda : \mathrm{DK} = \lambda_1||\lambda_2||\cdots||\lambda_\mu$。SSS算法包括以下5个步骤：

步骤1　CP输入安全参数P, Q, k，其中，P, Q是大素数，并满足P=rQ+1, r是一个正整数，k为多项式次数且k<Q。然后CP随机生成一个k次多项式$q(x) = s + a_1x + a_2x^2 + \cdots + a_kx^k$，其中，$s, a_1, a_2, \cdots, a_k \in Z_Q^*$, Z_Q^*是Q阶整数乘法群。

步骤2　CP随机选取k个点$(x_1, q(x_1)), (x_2, q(x_2)), \cdots, (x_k, q(x_k))$，其中，$x_j$($j$=1, 2, ⋯, k)互不相等。

步骤3　CP为某个授权用户随机选取一个点$(u_i, q(u_i))$，其中，u_i与步骤2中的x_j均不等。然后，CP计算$\mathrm{US}_i = \prod_{j=1}^{k} x_j/(x_j - u_i)$。

步骤4　CP计算并存储中间参数值$w(u_i) = \sum_{j=1}^{k} q(x_j)u_i/(u_i - x_j)\prod_{l=1,l\neq j}^{k} x_l/(x_l - x_j)$。

步骤5　CP产生$\tau \in Z_Q^*$，并计算$\xi_\eta = \lambda_\eta g^{\tau s}$和$\mathrm{CS}_i$，包括$\mathrm{CS}_{i0} = g^{q(u_i)\tau}, \mathrm{CS}_{i1} = g^{w(u_i)\tau}$，其中，$\lambda_\eta \in Z_Q^*$, $\eta = (1, 2, \cdots, \mu)$, g是G_P的Q阶子群的生成元，G_P是P阶循环群。

CP将US代替$(u_i, q(u_i))$分发给授权用户，使用UID加密US_i，并将加密后的信息US'_i分发至授权用户。用户收到US'_i后，使用USK来解密获得US_i。一旦授权用户获得US，便可请求不同内容的CS。在步骤5中，τ随着不同内容而改变，当用户访问不同内容时，CP会基于中间参数$w(u_i)$快速计算CS_i，并直接分发未被加密的ξ_η, CS_i，而用户基于$\xi_\eta, \mathrm{CS}_i, \mathrm{US}_i$计算$\mathrm{DK} = \lambda_1||\lambda_2||\cdots||\lambda_\mu$

$$\lambda_\eta = \frac{\xi_\eta}{\mathrm{CS}_{i1}\mathrm{CS}_{i0}^{\mathrm{US}_i}} = \frac{\lambda_\eta g^{\tau s}}{g^{\tau s}}, \eta \in [1, \mu] \tag{7}$$

其中，s是通过拉格朗日插值多项式计算而得。

3　安全性分析

(1) 数据保密性。TLAC机制通过加密方式防止恶意用户读取数据明文，并通过边缘路由器的认证来有效过滤未授权的请求。同时，SSS方法可以防止共谋威胁。在Shamir秘密共享方法里，合谋用户总数达到门限值时，就可以由插值定理重构s。而在SSS方法中，授权用户拥有一个不完整的特定份额US，虽然用户可由$\mathrm{CS}_i, \mathrm{US}_i$求得$g^{\tau s} = \mathrm{CS}_{i0}^{\mathrm{US}_i}\mathrm{CS}_{i1} = g^{\tau q(u_i)\mathrm{US}_i}g^{\tau w(u_i)}$，但$\tau, s$的计算存在求解离散对数的数学难题，因此用户无法合谋重构s。当添加一个新用户时，CP不受多项式次数的限制，可在当前多项式中选取一个未被使用的u_i，并计算US。同时，当CP更新秘密值s和多项式时，CP仅需更新$w(u_i)$，$q(x_j)$和$q(u_i)$，而无需更新授权用户持有的US。故SSS方法改善了可扩展性。

(2) 不可伪造性。椭圆曲线上存在离散对数问题：由Q和P很难计算$x \cdot P = Q$中的x。因此，已知$C_{\mathrm{pub}} = C_{\mathrm{pri}} \cdot G$, $U_{\mathrm{pub}} = U_{\mathrm{pri}} \cdot G$和$G$，用户很难计算得$C_{\mathrm{pri}}$，$U_{\mathrm{pri}}$，从而无法由$E_u = U_{\mathrm{pri}} + C_{\mathrm{Pri}}H_2 \cdot (h_{\mathrm{uid}}||\mathrm{CPK}||T_5)$得到$C_{\mathrm{pri}}$。在授权用户向边缘路由器进行认证时，由于证书被隐藏，攻击者很难从

$E_u' = (h_{T_i}E_u)\cdot G + R_u$ 和 $W = h_{T_i}\cdot U_{\text{pub}} + R_u$ 中计算得$\{U_{\text{pub}}, E_u\}$。因此，签名证书是不可伪造的。

(3) 防重放攻击。在第1次握手中，所传送的信息带有时间戳，可以在一定程度上防止被攻击者再次利用。当边缘路由器的时间不同步且网络存在不可预测的延迟时，所截取的第1次握手信息里的时间戳可能仍有效，因此攻击者成功骗取到边缘路由器的响应，但由于不知道u_1，攻击者也无法完成第3次握手。

(4) 匿名性。由于请求不包含真实的身份信息，因此用户的请求隐私在非安全信道上将不会被泄露。

4 实验分析

本文通过对算法的执行和网络仿真来证明TLAC机制的性能。所有的实验是在具有2 GB内存和4核CPU的Ubuntu 16.04系统环境下完成，并使用GMP库和PBC库中的Type A椭圆曲线完成程序设计。

4.1 “三次握手”协议的性能分析

本文将所提TLAC机制与SEAF机制进行了对比，表1为边缘路由器对用户进行认证时的理论开销对比，其中，U和R分别表示用户和边缘路由器，p, e, m_0, h分别表示双线性对运算、双线性对的指数运算、群中点乘运算以及Hash运算。在TLAC机制中，用户对R_1, R_u预计算后，共需进行3次点乘运算，而边缘路由器对R_2预计算后，需进行4次点乘运算。在无预计算时，TLAC机制在用户和边缘路由器上的计算量都明显低于SEAF机制。而通过预计算后，虽然TLAC机制在用户端的计算量高于SEAF机制，但TLAC机制在边缘路由器上的计算量更明显低于SEAF机制，能有效减小边缘路由器的计算压力。

在TLAC机制中，最为耗时的是椭圆曲线上的点乘运算。如图2所示，当$x\cdot G$中的x越大时，所需的计算开销越多。而预计算后认证所需的时间开销如表2所示，TLAC机制在边缘路由器上的时间开销低于SEAF机制，更适用于边缘路由器，其中，TLAC机制的计算开销是所需的最大时间开销，SEAF机制的计算开销是在随机生成中间参数时所需的平均时间开销。

表 1 认证时的计算开销对比

对比项目	TLAC机制	SEAF机制
U(无预计算)	$5m_0$+$5h$	$3p$+$3e$+$9m_0$+h
U(预计算后)	$3m_0$+$4h$	h
R(无预计算)	$5m_0$+$4h$	$5p$+$4e$+$8m_0$+h
R(预计算后)	$4m_0$+$4h$	/

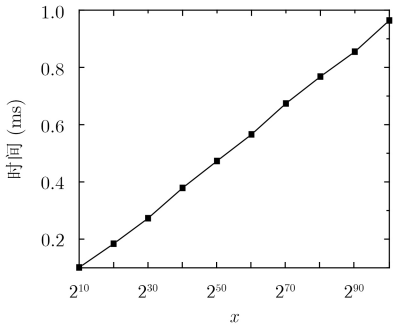

图 2 $x\cdot G$的计算开销

表 2 预计算后的时间开销对比(ms)

对比项目	TLAC机制	SEAF机制
U	5.15	0.05
R	6.67	13.75

本文进一步通过ndnSIM比较NDN原型和SEAF, TLAC机制的内容检索总时延T_u。实验采用一端为用户、另一端为CP的单瓶颈链路拓扑，并且包含4个路由器，与用户和CP直接相连的为边缘路由器，用户数量N_u分别为50, 100, 200，以100/s个兴趣包的速率请求不同内容。路由器间的链路传播时延和带宽分别为10 ms和10 MB/s，数据包的大小为2 kB。

图3为不同用户数下检索10 KB内容的总时延，当用户规模越大时，TLAC机制的内容检索总时延相对SEAF机制更少。图4为100个用户分别检索100 kB, 300 kB, 500 kB, 700 kB, 1 MB内容的总时延，由于“三次握手”认证完成后，后续请求的认证是基于单向散列函数来完成，相对标准的NDN而言，当请求文件增大时，TLAC机制未引进明显的时延。

4.2 SSS方法的性能分析

本文通过执行SSS算法来测量计算份额和DK的时间开销，其中，SSS算法中的P是260位的大素数，r=2，且多项式次数k从50增加至400，用户数m从1000增加至5000。

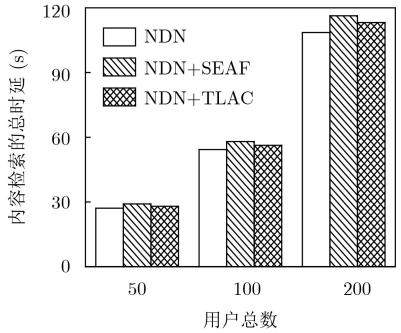

图 3 不同用户数量规模下的内容检索时延对比

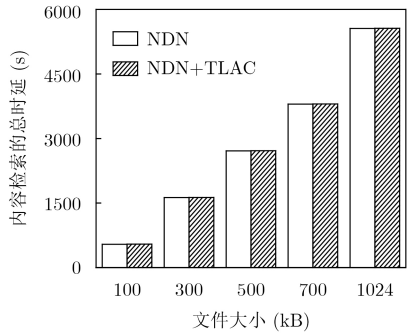

图 4 不同文件大小的内容检索时延对比

图5为CP计算US和CS的时间开销，该计算开销随k和m增加而增加，尤其是当k越大时，m的增加对计算开销的影响越大。虽然CS和US的计算开销很大，但它能在离线状态完成。此外，SSS方法解决了扩展性问题，因此，CP可以选择一个大小适中的k来减小计算开销。当CP为用户计算内容密钥时，只需执行SSS算法中的步骤5，便可为用户生成对应的CS，其计算开销约为0.36 ms。当用户端获取内容密钥时，SEAF机制所采用的广播解密需进行两次双线性对运算，时间开销约为2.59 ms，而在TLAC机制中，用户基于CS和US进行少量的计算得到DK，时间开销约为0.21 ms，大大降低了用户端的时间开销。

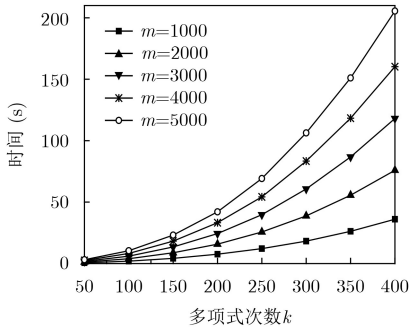

图 5 US, CS的计算开销

NDN的PKI机制采用非对称加密算法来分发内容或密钥[6]。相比NDN的PKI机制，TLAC机制基于US，CS和签名证书实现了细粒度访问控制，具有以下优势：结合IBC和SSS方法来分发密钥，通过SSS方法减少了非对称加密算法的较高计算开销，实现了高效的密钥分发；边缘路由器通过用户签名证书中的有效截止时间来限制用户的访问时间，并通过认证及时过滤非法的请求。

5　结束语

本文为NDN构建了一种可追溯且轻量级的细粒度访问控制机制，结合基于身份的组合公钥和Schnorr签名方法，用户在与边缘路由器完成“三次握手”匿名安全认证后，再基于共享的秘密值和单向散列函数来高效完成后续请求的认证，同时采用改进的秘密共享方法来高效地分发内容密钥。最后，本文通过实验仿真证明了该机制的高执行效率。本文所做的工作仍有许多不足，未来将从以下2个方面展开研究：(1)在NDN实验网中验证方案在真实环境下的可行性；(2)研究NDN中即时撤销以及密钥泄露后叛徒追踪问题。

参 考 文 献

[1] CISCO. Cisco visual networking index: Forecast and methodology, 2016–2021 white paper[EB/OL]. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html, 2018.

[2] GASTI P and TSUDIK G. Content-centric and named-data networking security: The good, the bad and the rest[C]. 2018 IEEE International Symposium on Local and Metropolitan Area Networks, Washington, USA, 2018: 1–6. doi: 10.1109/LANMAN.2018.8475052.

[3] TOURANI R, MISRA S, MICK T, *et al*. Security, privacy, and access control in information-centric networking: A survey[J]. *IEEE Communications Surveys & Tutorials*, 2018, 20(1): 566–600. doi: 10.1109/COMST.2017.2749508.

[4] MISRA S, TOURANI R, and MAJD N E. Secure content delivery in information-centric networks: Design, implementation, and analyses[C]. The 3rd ACM SIGCOMM Workshop on Information-centric Networking, Hong Kong, China, 2013: 73–78. doi: 10.1145/2491224.2491228.

[5] MISRA S, TOURANI R, NATIVIDAD F, *et al*. AccConF: An access control framework for leveraging in-network cached data in the ICN-enabled wireless edge[J]. *IEEE Transactions on Dependable and Secure Computing*, 2019, 16(1): 5–17. doi: 10.1109/TDSC.2017.2672991.

[6] CHEN Tao, LEI Kai, and XU Kuai. An encryption and probability based access control model for named data networking[C]. The 33rd IEEE International Performance Computing and Communications Conference, Austin, USA, 2014: 1–8. doi: 10.1109/PCCC.2014.7017100.

[7] ZHENG Qingji, WANG Guoqiang, RAVINDRAN R, *et al*. Achieving secure and scalable data access control in information-centric networking[C]. 2015 IEEE International Conference on Communications, London, UK, 2015: 5367–5373. doi: 10.1109/ICC.2015.7249177.

[8] XUE Kaiping, ZHANG Xiang, XIA Qiudong, *et al*. SEAF: A secure, efficient and accountable access control framework for information centric networking[C]. The IEEE INFOCOM 2018 - IEEE Conference on Computer Communications, Honolulu, USA, 2018: 2213–2221. doi:

10.1109/INFOCOM.2018.8486407.

[9] CHEN Liqun, CHENG Z, and SMART N P. Identity-based key agreement protocols from pairings[J]. *International Journal of Information Security*, 2007, 6(4): 213–241. doi: 10.1007/s10207-006-0011-9.

[10] 南湘浩. 组合公钥(CPK)体制标准(V5.0)[J]. 计算机安全, 2010(10): 1–2, 5. doi: 10.3969/j.issn.1671-0428.2010.10.001.
NAN Xianghao. Combined public key(CPK)cryptosystem standard(V5.0)[J]. *Computer Security*, 2010(10): 1–2, 5. doi: 10.3969/j.issn.1671-0428.2010.10.001.

[11] SCHNORR C P. Efficient signature generation by smart cards[J]. *Journal of Cryptology*, 1991, 4(3): 161–174. doi: 10.1007/bf00196725.

[12] NAOR M and YUNG M. Universal one-way hash functions and their cryptographic applications[C]. The 21st Annual ACM Symposium on Theory of Computing, Seattle, USA, 1989: 33–43. doi: 10.1145/73007.73011.

[13] SHAMIR A. Identity-based cryptosystems and signature schemes[C]. The Workshop on the Theory and Application of Cryptographic Techniques, Berlin, Germany, 1984: 47–53. doi: 10.1007/3-540-39568-7_5.

[14] SHAMIR A. How to share a secret[J]. *Communications of the ACM*, 1979, 22(11): 612–613. doi: 10.1145/359168.359176.

[15] IMINE Y, LOUNIS A, and BOUABDALLAH A. ABR: A new efficient attribute based revocation on access control system[C]. The 13th International Wireless Communications and Mobile Computing Conference, Valencia, Spain, 2017: 735–740. doi: 10.1109/IWCMC.2017.7986376.

雒江涛：男，1971年生，教授，研究方向为新一代网络技术、通信网络测试与优化、移动大数据等.

何 宸：男，1994年生，硕士生，研究方向为新一代网络技术.

王俊霞：女，1992年生，博士生，研究方向为新一代网络技术.