单/多源网络编码同态签名方案

俞惠芳，李雯
（西安邮电大学网络空间安全学院，陕西 西安 710121）

摘 要：针对单源和多源网络编码污染问题，提出了 2 种网络编码同态签名方案。单源网络编码椭圆曲线同态签名在椭圆曲线上对消息的散列值进行签名，输出消息、散列值和散列值的签名，接收节点验证签名，该方案通过同态的椭圆曲线签名来抵御代内/间污染。基于双线性对的多源网络编码同态签名不仅能够抵抗污染攻击，而且引入时间戳来抵制网络中的重放攻击。通过随机预言模型下的证明，2 种方案在选择性攻击下都是安全的。通过效率分析发现，2 种方案都能有效提高验证效率。

关键词：单源网络编码；多源网络编码；同态签名；时间戳
中图分类号：TN918.4
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2019219

Homomorphic signature schemes for single-source and multi-source network coding

YU Huifang, LI Wen
School of Cyberspace Security, Xi’an University of Posts & Telecommunications, Xi’an 710121, China

Abstract: To solve the problems of pollution attacks of single-source and multi-source network coding, two homomorphic signature schemes for network coding were proposed. In homomorphic signature for single-source network, the message hash value was signed on the elliptic curve, then the message, hash value and the signature of hash value were output, and the receiving node could verify the signature, the elliptic curve signature based on homomorphism could resist intra/inter-generation pollution attacks. Homomorphic signature from pairings for multi-source network coding could resist pollution attacks, and the introduction of timestamp made it be capable to resist replay attacks. In the random oracle model, it proves that two schemes are all secure under the selective attacks. Analysis shows that two schemes can effectively improve the verification efficiency.

Key words: single-source network coding, multi-source network coding, homomorphic signature, timestamp

1 引言

网络编码[1]是一种新型的信息传输技术，在提升网络的吞吐量、增加网络的强壮性、减少网络宽带资源的消耗等方面比传统的路由技术都具有明显的优势。但是当节点受到恶意攻击或网络传输信道不稳定时，产生的污染信息将会随着编码传输与其他有效消息进行编码组合，进而将污染传染给其他消息，最终使信宿节点无法正确解码恢复出原始消息。

近年来，研究人员提出了一些抵抗污染攻击的方案，使网络编码污染问题在传统的签名方法中得到了很好解决。Yu 等[2]提出了基于同态签名的线性网络编码方案，可以检测出污染攻击的发生。但是

收稿日期：2019−04−15；修回日期：2019−07−23
基金项目：青海省基础研究计划基金资助项目（No.2016-ZJ-776）；西安邮电大学研究生创新基金资助项目（No.CXJJLY2018077）
Foundation Items: The Basic Research Plan Project of Qinghai Province (No.2016-ZJ-776), The Innovation Foundation of Post-graduate of Xi’an University of Posts & Telecommunications (No.CXJJLY2018077)

Yun 等[3]已证明了 Yu 等[2]提出的算法不满足同态性质，虽然能检测出污染攻击的发生，但是不能处理该节点。Boneh 等[4]提出了一种全局编码向量的签名方案，可以抵御代内/外污染，但是签名和验证的计算复杂度高，时延较长。Li 等[5]提出了分布式污染节点定位方案，每个节点都可运行算法，自行判断污染节点，缺点是算法精度不高，存在误判概率，并且需要运行多次才能确定污染处。Charles 等[6]利用椭圆曲线上的点设计了一种同态签名方案，缺点是存在漏洞，可以伪造通过验证[7]。He 等[8]提出了自适应网络编码方案，中间节点可根据网络污染情况自动调整策略进行验证，缺点是网络节点必须保证时间同步，这样会消耗大量网络资源。裴恒利等[9]使用时间戳生成网络编码的随机系数，利用 RSA 同态签名抵抗污染攻击和重放攻击，但是数据分组部分的正交分量计算复杂，增加了资源浪费。蒙云番等[10]构造了椭圆曲线密码体制（ECC, elliptic curve cryptography）下的同态签名方案，保障了无线体域网的通信安全，缺点是不能抵抗代间污染，计算开销大。Wu 等[11]提出了一种基于密钥预分发的标签编码方案，可以抵御污染攻击和标签污染攻击，但是不能检测出代间污染攻击。Cheng 等[12]提出了一种改进的同态子空间网络编码签名方案，将代间标识符结合到密钥生成过程中，不足之处是签名过程较复杂，网络负载大，易造成缓存溢出。

上述的抵抗污染攻击算法仅限于单源的网络编码，多源网络编码中的污染问题比单源网络编码复杂。Agrawal 等[13]针对多源网络编码构造了同态签名机制，当中间节点组合来自多个源的数据分组时，该机制能提供完整性，然而每个分组需要进行多次的签名验证，导致计算开销大。Yang 等[14]提出了能够保证数据完整性的无条件安全认证码的多源网络编码方案，不足之处是存在安全漏洞，容易受到重放攻击。Zhang 等[15]提出了一种实时签名方案以抵抗多源网络污染攻击，但在安全性方面存在一些缺陷。Le 等[16]提出了适用于多源网络编码的基于同态消息认证码的签名方案，缺点是中间节点不能将被污染的数据分组过滤掉。Li 等[17]为了解决网络编码认证问题，提出了一种多源线性同态网络编码签名方案，但节点的签名和验证运算中需要进行大量的模指数运算，增加了计算复杂度。俞惠芳等[18]采用 Schnorr 签名机制，提出了适用于多源网络编码的环签名方案，在环签名中引入时间概念，既能抵抗污染攻击又能抵抗重放攻击。彭勇等[19]为了预防多源网络的污染攻击和背叛攻击，提出了多源网络编码同态签名算法，改变了数据分组的组合方式，但是接收节点解码速度较慢。牛淑芬等[20]提出了一种多源网络编码数据完整性验证方案，利用私钥对散列值进行聚合签名，接收节点利用公钥验证线性编码消息的完整性，但需要在有限域中进行大量的指数运算，降低了验证效率。

针对单源网络编码中签名、验证计算复杂度高、效率低、资源浪费、不能有效地抵抗代间污染等不足，本文借鉴文献[10,21]的思想提出了一种单源网络编码体制下椭圆曲线同态签名方案，实现了确定污染节点和过滤污染信息的功能，从而可以抵抗代内/间的污染，仿真实验显示，所提方案比同类方案[22]提高了节点验证效率，减少了能源消耗。同时，针对所述多源网络编码方案中计算开销大、签名验证过程复杂、不能预防重放攻击等缺点，本文在文献[9,23]的理论基础上提出了基于双线性映射的多源网络编码同态签名方案，能有效抵抗污染攻击和重放攻击，分析表明，所提方案比同类方案降低了对节点计算能力的要求，减少了系统开销和节点的验证时间。

2　预备知识

2.1　单源线性网络编码模型

文献[24]将单源网络编码用 $<G,\tilde{V}>$ 来描述，其中 G、$\tilde{V}$ 分别是网络中边和节点的集合。适用于网络编码的单源传输网络模型如图 1 所示，其中 S 为源节点，$D=(d_1,d_2,\cdots,d_k)$ 为目的节点。

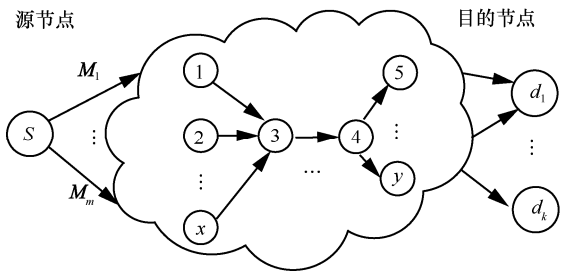


图 1　适用于网络编码的单源传输网络模型

源节点在发送数据 $\boldsymbol{M}$ 之前将其分为 m 个块，即 $\boldsymbol{M}_1,\boldsymbol{M}_2,\cdots,\boldsymbol{M}_m$，每块用 n 维向量来表示，即 $\boldsymbol{M}_i=(v_{i,1},v_{i,2},\cdots,v_{i,n})\in F_p^n\ (i=1,2,\cdots,m)$，$p$ 是一个大素数，同时将所有的文件块按照如下规则进行扩充

$$\boldsymbol{V}_i=(v_{i,1},v_{i,2},\cdots,v_{i,n},\overbrace{\underbrace{0,\cdots,0}_{i-1},1,0,\cdots,0}^{m})=(v_{i,1},v_{i,2},\cdots,v_{i,m+n}) \tag{1}$$

其中，$v_{i,j}\in F_p^{m+n}$ 是向量 $\boldsymbol{V}_i$ 中的元素，$j=1,2,\cdots,m+n$。

线性组合过程为源节点处随机选择向量 $\boldsymbol{a}=(a_1,a_2,\cdots,a_m\in F_p^{m+n})$，计算

$$\begin{aligned}\boldsymbol{w}&=\sum_{i=1}^{m}a_i\boldsymbol{V}_i=\\&\left(\sum_{i=1}^{m}a_iv_{i,1},\sum_{i=1}^{m}a_iv_{i,2},\cdots,\sum_{i=1}^{m}a_iv_{i,n},a_1,a_2,\cdots,a_m\right)=\\&(\overline{w}_1,\overline{w}_2,\cdots,\overline{w}_n,\overline{w}_{n+1},\overline{w}_{n+2},\cdots,\overline{w}_{n+m})=\\&(\overline{w}_1,\overline{w}_2,\cdots,\overline{w}_n,a_1,a_2,\cdots,a_m)\end{aligned} \tag{2}$$

其中，$\overline{w}_1,\overline{w}_2,\cdots,\overline{w}_n$ 是原始数据编码的部分，$\boldsymbol{a}=(a_1,a_2,\cdots,a_m)$ 为全局编码向量。设 $\boldsymbol{w}_1,\boldsymbol{w}_2,\cdots,\boldsymbol{w}_m$ 为目的节点收到的 m 个向量，$\boldsymbol{w}_i^{\mathrm{L}}$ 为向量中左边的 n 个元素，$\boldsymbol{w}_i^{\mathrm{R}}$ 为向量中右边的 m 个元素，计算 $m\times m$ 的矩阵 $\boldsymbol{H}$ 为

$$\boldsymbol{H}=\begin{bmatrix}\boldsymbol{w}_1^{\mathrm{R}}\\\boldsymbol{w}_2^{\mathrm{R}}\\\vdots\\\boldsymbol{w}_m^{\mathrm{R}}\end{bmatrix}^{-1}=\begin{bmatrix}w_{1,n+1},w_{1,n+2},\cdots,w_{1,n+m}\\w_{2,n+1},w_{2,n+2},\cdots,w_{2,n+m}\\\vdots\quad\vdots\quad\quad\vdots\quad\vdots\\w_{m,n+1},w_{m,n+2},\cdots,w_{m,n+m}\end{bmatrix}^{-1}=\begin{bmatrix}a_{1,1},a_{1,2},\cdots,a_{1,m}\\a_{2,1},a_{2,2},\cdots a_{2,m}\\\vdots\quad\vdots\quad\vdots\quad\vdots\\a_{m,1},a_{m,2},\cdots,a_{m,m}\end{bmatrix}^{-1} \tag{3}$$

将原始传输的文件设为 $\boldsymbol{M}_1,\boldsymbol{M}_2,\cdots,\boldsymbol{M}_m$，恢复原始文件时计算

$$\begin{bmatrix}\boldsymbol{M}_1\\\boldsymbol{M}_2\\\vdots\\\boldsymbol{M}_m\end{bmatrix}=\begin{bmatrix}v_{1,1},v_{1,2},\cdots,v_{1,n}\\v_{2,1},v_{2,2},\cdots,v_{2,n}\\\vdots\quad\vdots\quad\vdots\quad\vdots\\v_{m,1},v_{m,2},\cdots,v_{m,n}\end{bmatrix}=\boldsymbol{H}\begin{bmatrix}\boldsymbol{w}_1^{\mathrm{L}}\\\boldsymbol{w}_2^{\mathrm{L}}\\\vdots\\\boldsymbol{w}_m^{\mathrm{L}}\end{bmatrix}=\boldsymbol{H}\begin{bmatrix}w_{1,1},w_{1,2},\cdots,w_{1,n}\\w_{2,1},w_{2,2},\cdots,w_{2,n}\\\vdots\quad\vdots\quad\vdots\quad\vdots\\w_{m,1},w_{m,2},\cdots,w_{m,n}\end{bmatrix} \tag{4}$$

2.2 多源线性网络编码模型

文献[23]的多源网络编码模型中，每个源节点发送的每条消息都有统一分配的唯一的二维索引[25]，不同的源节点发送相同的多播消息有着相同的索引。将多播的多源网络编码用 $G=(V,E)$ 来描述，其中 V 和 E 分别是节点和边的集合，$S=\{s_1,s_2,\cdots,s_m\}\subset V$ 是源节点集，$D=\{d_1,d_2,\cdots,d_k\}\subset V$ 是目的节点集。D 接收 S 发送的 m 条多播消息，如图 2 所示。

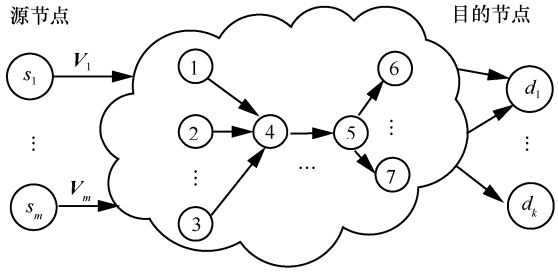


图 2 适用于网络编码的多源传输网络模型

将 m 条多播消息表示为 $\boldsymbol{V}_1,\cdots,\boldsymbol{V}_m$，将每条消息 $\boldsymbol{V}_i$ 看成是 n 维向量空间 V/F_p 中的一个向量，记为 $\boldsymbol{V}_i=(v_{i,1},\cdots,v_{i,n})\in F_p^n$，其中 $1\leqslant i\leqslant m$。

设 $\boldsymbol{W}=(\boldsymbol{W}_1,\boldsymbol{W}_2,\cdots,\boldsymbol{W}_l)$ 为多播网络中任意一条边上发送的消息，接收节点收到 l 条消息的线性组合，即

$$\boldsymbol{W}=\sum_{j=1}^{l}a_j\boldsymbol{W}_j \tag{5}$$

其中，$\boldsymbol{\alpha}=(a_1,a_2,\cdots,a_l)$ 称为局部编码向量。易知，任意一条边上发送的消息 $\boldsymbol{W}$ 也是原消息 $\boldsymbol{V}_j(1\leqslant j\leqslant m)$ 的线性组合，即

$$\boldsymbol{W}=\sum_{j=1}^{m}\beta_j\boldsymbol{V}_j \tag{6}$$

其中，$\boldsymbol{\beta}=(\beta_1,\beta_2,\cdots,\beta_m)$ 称为全局编码向量。

设接收节点 t_i 收到 m 个线性无关的编码消息 $\boldsymbol{W}_1,\boldsymbol{W}_2,\cdots,\boldsymbol{W}_m$，而且相关的全局编码向量用 $\boldsymbol{G}$ 表示，恢复原消息

$$\begin{bmatrix}\boldsymbol{W}_1\\\vdots\\\boldsymbol{W}_m\end{bmatrix}=\boldsymbol{G}\begin{bmatrix}\boldsymbol{V}_1\\\vdots\\\boldsymbol{V}_m\end{bmatrix}$$

其中，$\boldsymbol{G}=\begin{bmatrix}\beta_1\\\vdots\\\beta_m\end{bmatrix}$。

原消息 $\boldsymbol{V}_1,\cdots,\boldsymbol{V}_m$ 为

$$\begin{bmatrix}\boldsymbol{V}_1\\\vdots\\\boldsymbol{V}_m\end{bmatrix}=\boldsymbol{G}^{-1}\begin{bmatrix}\boldsymbol{W}_1\\\vdots\\\boldsymbol{W}_m\end{bmatrix} \tag{7}$$

消息后面附加全局编码向量 β_i 与消息一起传输，扩展的原消息可看成 $m+n$ 维的向量空间 V/F_p 中的一个向量，记作

$$\boldsymbol{V}_i=\left(v_{i,1},\cdots,v_{i,n},\underbrace{0,\cdots,0,1}_{i},\overbrace{0,\cdots,0}^{m}\right)\in F_p^{m+n},1\leqslant i\leqslant m$$

因为

$$\boldsymbol{W}=\sum_{i=1}^{m}\beta_i\boldsymbol{V}_i=$$
$$\beta_1\boldsymbol{V}_1+\beta_2\boldsymbol{V}_2+\cdots+\beta_m\boldsymbol{V}_m=$$
$$(\beta_1v_{1,1},\cdots,\beta_1v_{1,n},\beta_1,0,\cdots,0)+(\beta_2v_{2,1},\cdots,\beta_2v_{2,n},0,$$
$$\beta_2,\cdots,0)+\cdots+(\beta_mv_{m,1},\cdots,\beta_mv_{m,n},0,0,\cdots,\beta_m)=$$
$$(\beta_1v_{1,}+\beta_2v_{2,1}+\ldots+\beta_mv_{m,1},\ldots,\beta_1v_{1,n}+\beta_2v_{2,n}+$$
$$\cdots+\beta_mv_{m,n},\beta_1,\beta_2,\cdots,\beta_m)=$$
$$\left(\sum_{i=1}^{m}\beta_iv_{i,1},\cdots,\sum_{i=1}^{m}\beta_iv_{i,n},\beta_1,\beta_2,\cdots,\beta_m\right)=$$
$$\left(\sum_{i=1}^{m}w_{i,1},\cdots,\sum_{i=1}^{m}w_{i,n},\sum_{i=1}^{m}\beta_{i,1},\sum_{i=1}^{m}\beta_{i,2},\cdots,\sum_{i=1}^{m}\beta_{i,m}\right)$$

所以，编码消息可以表示为 $\boldsymbol{W}_i=(w_{i,1},\cdots,w_{i,n},\beta_{i,1},\beta_{i,2},\cdots,\beta_{i,m})$，为了方便，将编码消息表示成 $\boldsymbol{W}_i=(w_{i,1},\cdots,w_{i,m+n})$。

2.3　双线性对

令 a，$b\in Z_p$*；令 G_1 是阶为大素数 q 的加法循环群，生成元为 P；令 G_2 是阶为 q 的乘法循环群。若映射 $e:G_1\times G_1\to G_2$ 满足如下性质，则为双线性对[26]。

1) 双线性：对于任意的 $P,Q\in G_1$，都有 $e(aP,bQ)=e(P,Q)^{ab}$。

2) 非退化性：存在 $P,Q\in G_1$ 使 $e(P,Q)\neq 1$。

3) 可计算性：对于任意的 $P,Q\in G_1$，$e(aP,bQ)=e(P,Q)^{ab}=e(P,abQ)=e(abP,Q)$。

2.4　椭圆曲线密码简介

椭圆曲线密码体制（ECC）是基于椭圆曲线离散对数问题的公钥密码体制，椭圆曲线加法群的离散对数问题的求解比有限域乘法群的离散对数问题求解更难，它可用小密钥来保证高级别的安全性。选取椭圆曲线 $E(a,b)$：$y^2\equiv x^3+ax+b(\mathrm{mod}\,p)$。$E(a,b)$通过一组参数 (p,a,b,G,q,h) 唯一确定。在有限域 F_p 中，p 是一个大素数，表示域的大小；$a,b\in F_p$ 是椭圆曲线方程的参数，满足方程 $4a^3+27b^2(\mathrm{mod}\,p)\neq 0$，$G$ 是椭圆曲线上阶为大素数 q 的基点，$q\ll p$，且 $q>2^{160}$ 和 $q>4\sqrt{p}$，要满足 q 不能整除 p^k-1。

2.5　散列碰撞

输入　$P_1,\cdots,P_r$（r>1）是有限域 F_p 中阶为 q 的椭圆曲线上的点

输出　元组 $\boldsymbol{a}=(a_1,\cdots,a_r)$，$\boldsymbol{b}=(b_1,\cdots,b_r)\in F_p{}^r$，使 $\boldsymbol{a}\neq\boldsymbol{b}$ 且

$$\sum_{1\leqslant i\leqslant r}a_iP_i=\sum_{1\leqslant j\leqslant r}b_jP_j$$

椭圆曲线上 q 阶循环群上的离散对数到散列碰撞有一个多项式时间约简。

3　单源网络编码同态签名方案

3.1　方案实例

3.1.1　系统设置

H_G 是一个单向抗碰撞 hash 函数，$H_G:\{0,1\}^*\to Z_{p-1}{}^*$；$h$: $\{0,1\}^*\times G_1\to Z_{p-1}{}^*$。其中 G_1 是阶为大素数 q 的加法循环群，G 是椭圆曲线上的基点。密码学安全的散列函数 h_1：$\{0,1\}^*\times\{0,1\}^*\to Z_{p-1}{}^*$。选取秘密随机数 $\alpha\in Z_{p-1}{}^*$。假设源节点要发送 l 个代的消息，标识符 I 表示消息代。计算 $S_{\mathrm{PK}}=H_G(I)$，$S_{\mathrm{SK}}=\alpha S_{\mathrm{PK}}$，$S_{\mathrm{SK}}$ 是代对应的私钥。

1) 源节点处

选取秘密随机数 $\eta\in Z_{p-1}{}^*$，计算 $K=S_{\mathrm{SK}}\eta$，$P=KG$，其中 K 作为源节点每一代消息的签名私钥，P 作为公钥。选取 $K'\in Z_{p-1}{}^*$作为源节点的秘密随机数，随机选择椭圆曲线上的一组基点集 $R:(R_1,R_2,\cdots,R_{m+n})$，这里 $R_j(j=1,2,\cdots,m+n)$ 的阶均为 q。定义同态散列函数 δ，其中 δ 的定义采用了文献[6]中的定义，即

$$\delta=\sum_{j=1}^{m+n}R_jv_{i,j}\tag{8}$$

2) 中间节点处

选取秘密随机数 $\eta_{\mathrm{id}}\in Z_{p-1}{}^*$，$\mathrm{id}=(1,2,\cdots,e)$，$e$ 是中间节点的数量。计算 $K_{\mathrm{id}}=S_{\mathrm{SK}}\eta_{\mathrm{id}}$，$P_{\mathrm{id}}=K_{\mathrm{id}}G$，其中 K_{id} 作为中间节点每一代消息签名私钥，P_{id} 作为公钥。选取 $K_{\mathrm{id}}'\in Z_{p-1}{}^*$作为中间节点的秘密随机数，$\mathrm{id}=(1,2,\cdots,e)$，$e$ 是中间节点的数量。私钥 $\overline{S}=(K,K_{\mathrm{id}})$ 是签名私钥，$\overline{P}=(P,P_{\mathrm{id}})$ 是公钥。

3.1.2　签名算法

1) 源节点的签名过程

源节点处对原始消息计算散列函数

$\delta=\sum_{j=1}^{m+n}R_j v_{i,j}$。

计算签名 $h_1(\boldsymbol{V}_i,K')G=(x_1,y_1)$，令 $r=x_1 \bmod q$。若 $r=0$，则重新选 K' 的值。检验 $h(\delta)=rK$ 是否成立，若成立，则重新选 K' 的值。计算 $S=(h_1(\boldsymbol{V}_i,K')+r-h(\delta)K)\bmod q$，如果 $S=0$，则重新选 K' 的值。消息签名是 $(r,S,H_G(I))$。

2) 组合

组合后的向量为 $\boldsymbol{w}=\sum_{i=1}^{m}a_i\boldsymbol{V}_i$，$\boldsymbol{a}$=$(a_1,a_2,\cdots a_m)$ 是全局编码向量，$\boldsymbol{w}=(\boldsymbol{w}_1,\boldsymbol{w}_2,\cdots,\boldsymbol{w}_{m+n})$，则

$$\lambda=\sum_{j=1}^{m+n}R_j\boldsymbol{w}_j \tag{9}$$

3) 中间节点签名过程

计算签名 $h_1(\boldsymbol{w},K'_{\mathrm{id}})G=(x_{1\mathrm{id}},y_{1\mathrm{id}})$，令 $r_{\mathrm{id}}=x_{1\mathrm{id}} \bmod q$。若 $r_{\mathrm{id}}=0$，则重新选 K'_{id} 的值。检验 $h(\lambda)=r_{\mathrm{id}}K_{\mathrm{id}}$ 是否成立，若成立，则重新选 K'_{id} 的值。计算 $S_{\mathrm{id}}=(h_1(\boldsymbol{w},K'_{\mathrm{id}})+r_{\mathrm{id}}-h(\lambda)K_{\mathrm{id}})\bmod q$，若 $S_{\mathrm{id}}=0$，则重新选 K'_{id} 的值。签名是 $(r_{\mathrm{id}},S_{\mathrm{id}},H_G(I))$。

4) 验证

① 接收节点收到传递来的消息向量时，先对每一个接收到的签名 $(r_{\mathrm{id}},S_{\mathrm{id}},H_G(I))$ 进行验证，通过验证后再进行编码。

② 计算 $H'_G(I)$，若 $S_{\mathrm{PK}}=H'_G(I)$ 成立，则接受签名；否则，拒绝该签名。若 r_{id}, $S_{\mathrm{id}}\notin Z_{p-1}{}^*$，拒绝签名。

③ 计算

$$U_1=(S_{\mathrm{id}}-r_{\mathrm{id}})\bmod q \tag{10}$$

$$U_2=h\left(\sum_{i=1}^{m}a_i\delta\right)\bmod q \tag{11}$$

$$X=U_1G+U_2P_{\mathrm{id}}=(x'_{1\mathrm{id}},y'_{1\mathrm{id}}) \tag{12}$$

如果 $X=0$，则拒绝签名，否则，令 $V'=x'_{1\mathrm{id}} \bmod q$。若 $V'=r_{\mathrm{id}}$ 成立，则接受签名；否则，拒绝该签名。

④验证依据

散列函数同态性证明：组合后的向量为 $\boldsymbol{w}=\sum_{i=1}^{m}a_i\boldsymbol{V}_i$，其中 $\boldsymbol{a}$=$(a_1,a_2,\cdots a_m)$ 是全局编码向量，$\boldsymbol{w}=(\boldsymbol{w}_1,\boldsymbol{w}_2,\cdots,\boldsymbol{w}_{m+n})$，则

$$\lambda=\sum_{j=1}^{m+n}R_j\boldsymbol{w}_j=\sum_{j=1}^{m+n}R_j\left(\sum_{i=1}^{m}a_iv_{i,j}\right)=\sum_{i=1}^{m}a_i\left(\sum_{j=1}^{m+n}R_jv_{i,j}\right) \tag{13}$$

将式(8)代入式(13)，得到组合后消息的散列函数为

$$\lambda=\sum_{i=1}^{m}a_i\delta \tag{14}$$

由此说明了散列函数具有同态性质。

将式(10)和式(11)代入 $X=U_1G+U_2P_{\mathrm{id}}=(x_{1\mathrm{id}},y_{1\mathrm{id}})$ 中，可得

$$\begin{aligned}&X=U_1G+U_2P_{\mathrm{id}}=\\&(S_{\mathrm{id}}-r_{\mathrm{id}})G+h\left(\sum_{i=1}^{m}a_i\delta\right)K_{\mathrm{id}}G=\\&h_1(\boldsymbol{w},K'_{\mathrm{id}})G-h(\lambda)K_{\mathrm{id}}G+h\left(\sum_{i=1}^{m}a_i\delta\right)K_{\mathrm{id}}G\end{aligned} \tag{15}$$

由式(14)知 $\lambda=\sum_{i=1}^{m}a_i\delta$，代入式(15)可得到 $X=h_1(\boldsymbol{w},K'_{\mathrm{id}})G=(x'_{\mathrm{id}},y'_{\mathrm{id}})$，即可得 $x_{\mathrm{id}}=x'_{\mathrm{id}}$，所以 $V'=r_{\mathrm{id}}$ 成立。

3.2 安全性分析

在单源网络编码椭圆曲线同态签名中，为了防止污染攻击，在每个转发节点处进行一次签名验证和签名。在证明中利用了随机预言模型，假设某个节点被攻击者攻破，得到该节点的私有数据及所有公共参数，要伪造能通过验证的信息，必须破解椭圆曲线离散对数难题。攻击者 A 可以用这些参数来伪造签名，但是这相当于在求解椭圆曲线离散对数难题。

定理 1 当且仅当在多项式时间内求解椭圆曲线离散对数问题是困难的，单源网络编码椭圆曲线同态签名是安全的。

证明 令 B 是一个挑战者，B 的目标是利用攻击者 A 攻破椭圆曲线离散对数困难问题。A 和 B 进行的游戏如下。A 选择消息 $\boldsymbol{M}$=$(m_1,\cdots,m_{m+n})\in {F_p}^{m+n}$ 提交给 B。

系统设置。B 通过运行系统初始化算法得到 $(G,K_{\mathrm{id}},K',H_G(I),R)$，然后发送系统参数给 A。

h 询问。B 在任意时刻都可以询问 h 预言机，h-list 是一个起初为空的列表。如果表 h-list 有匹配的元组，则返回该值；否则，B 随机选择值 $h(\lambda')\in Z_{p-1}{}^*$返回，并将该值添加到表 h-list 中。

h_1 询问。B 在任意时刻都可以询问 h_1 预言机，h_1-list 是一个起初为空的列表。如果相应的值已经在表 h_1-list 中，则返回该值；否则，B 随机选择值 $h_1(\boldsymbol{M},K')\in Z_{p-1}{}^*$返回，然后添加该值到表 h_1-list 中。

签名询问。A 向 B 进行签名询问。B 将$(r_{\mathrm{id}}^{*},S_{\mathrm{id}}^{*})$发送给 A。

如果 A 能够赢得该游戏，则 $\mathrm{Ver}(r_{\mathrm{id}}^{*},S_{\mathrm{id}}^{*},H_G(I))=\mathrm{ture}$。然而，$X=U_1G+U_2P_{\mathrm{id}}=(x_{1\mathrm{id}}^{*},y_{1\mathrm{id}}^{*})$，$U_2P_{\mathrm{id}}=(x_{1\mathrm{id}}^{*},y_{1\mathrm{id}}^{*})-U_1G$，令 $L=(x_{1\mathrm{id}}^{*},y_{1\mathrm{id}}^{*})-U_1G$，则 $L=U_2P_{\mathrm{id}}$，求解 U_2 相当于多项式时间内解决椭圆曲线离散对数问题。但是，椭圆曲线上求解离散对数困难问题是不能在多项式时间内完成的。因此，所提方案是安全的。

证毕。

定理 2　当且仅当在多项式时间内散列函数是抗碰撞的，单源网络编码椭圆曲线同态签名是安全的。

证明　攻击者 A 伪造信息 $\boldsymbol{w}'$ $(\boldsymbol{w}'\neq\boldsymbol{w})$，使 $\lambda'=\lambda$。因为 $\lambda=\sum_{j=1}^{m+n}R_j\boldsymbol{w}$，可得 $\lambda'=\sum_{j=1}^{m+n}R_j\boldsymbol{w}'$，但是 A 的伪造过程等价于在有限域 F_p 上证明式(16)成立。

$$\sum_{j=1}^{m+n}R_j\boldsymbol{w}'=\sum_{j=1}^{m+n}R_j\boldsymbol{w},\quad \boldsymbol{w}'\neq\boldsymbol{w} \tag{16}$$

该问题可归于求解散列函数的碰撞问题。攻击者在不知道 $R_1\boldsymbol{w}_1,\cdots,R_m\boldsymbol{w}_m$ 和 $R_{m+1}\boldsymbol{w}_{m+1},\cdots,R_{m+n}\boldsymbol{w}_{m+n}$ 的情况下，可以对函数 $\lambda=\sum_{j=1}^{m+n}R_j\boldsymbol{w}$ 产生散列碰撞。散列函数碰撞在该方案中发生的概率小于 $\frac{1}{p}$（p 是一个很大的素数）。

证毕。

定理 3　当且仅当在多项式时间内能抵抗代间重放攻击，单源网络编码椭圆曲线同态签名是安全的。

证明　当 $I'\neq I$ 时，在随机预言模型下，散列函数 $H_G(I)$ 被看成是一个随机预言机，而攻击者不能在多项式时间内找到 $I'\neq I$ 使 $H_G(I')=H_G(I)$。因此，所提方案中代间重放攻击无法成功实施。

证毕。

3.3　实验结果与分析

本节利用 Matlab 工具对所提方案和 Cheng 等[22]方案进行计算开销对比，主要密码操作的计算成本定义如下。

执行一次指数运算的时间用 C_{me} 表示，C_{me}=0.83 ms。

执行一次椭圆曲线上标量乘运算的时间用 C_{mul} 表示，C_{mul}=0.75 ms。

执行一次散列运算的时间用 C_{mtp} 表示，C_{mtp}=1.18 ms。

执行一次双线性对运算的时间用 C_{par} 表示，C_{par}=2.75 ms。

所提方案和 Cheng 等方案的性能比较如表 1 所示。考虑到椭圆曲线上标量乘（160 位）比相同安全级别下的模指数运算（1 024 位）成本更低，因此所提方案平均具有最优的计算复杂度。具体来说，数据分组签名时，Cheng 等方案需要 $(m+n+2)C_{\mathrm{mul}}+(m+n+2)C_{\mathrm{me}}$，而所提方案需要 $(m+n+2)C_{\mathrm{mul}}+2C_{\mathrm{mtp}}$。为了验证数据分组，Cheng 等方案需要 $(3(m+n)+2)C_{\mathrm{mul}}+3(m+n+1)C_{\mathrm{me}}$，而所提方案需要 $(m+n+1)C_{\mathrm{mul}}+2C_{\mathrm{mtp}}$。很明显，所提方案效率优于 Cheng 等方案，因为所提方案中签名和验证也是基于椭圆曲线实现的，运算中用到椭圆曲线上的标量乘，没有模指数运算，从而减少了运算时间。

图 3 和图 4 分别表示所提方案和 Cheng 等[22]方案签名耗时和验证耗时的仿真曲线。本节选用椭圆曲线的安全参数 $q=2^{159}+2^{17}+1$，q 是 160 位的 Solinas 素数，p 是 512 位素数，令 m=50，消息向量维数 $m+n$ 分别为 100、200、300、400、500、600、700、800。由图 3 和图 4 可以看出，随着消息向量维数的增加，所提方案签名和验证的耗时低于 Cheng 等方案，因此得出所提方案优于 Cheng 等方案的结论。

4　多源网络编码同态签名方案

4.1　方案实例

1) 系统设置

G_1 是阶为大素数 q 的加法循环群，其中 G 为 G_1 的生成元，用户 u_d $(1\leqslant d\leqslant s)$ 随机选择 $s_k\in Z_{p-1}^{*}$

表 1　单源网络编码签名性能比较

方案	签名耗时	验证耗时
Cheng 等[22]方案	$(m+n+2)C_{\mathrm{mul}}+(m+n+2)C_{\mathrm{me}}$	$(3(m+n)+2)C_{\mathrm{mul}}+3(m+n+1)C_{\mathrm{me}}$
所提方案	$(m+n+2)C_{\mathrm{mul}}+2C_{\mathrm{mtp}}$	$(m+n+1)C_{\mathrm{mul}}+2C_{\mathrm{mtp}}$

$(1 \leqslant k \leqslant s)$ 作为私钥，计算 $p_k = s_k G$ 作为公钥。H_g 是一个单向抗碰撞 hash 函数，H_g:$\{0,1\}^* \to G_1$。T_i 为时间戳，且 $T_i \in Z_{p-1}{}^*$，T 为当前时刻。$T = (\beta_1 T_1 + \beta_2 T_2 + \cdots + \beta_m T_m) \bmod p$，其中 $\beta_1, \beta_2, \cdots, \beta_m$ 是随机系数，当前时刻 T 收到的 m 条消息组合中的时间戳为 $(T_1, T_2, \cdots, T_m)$。

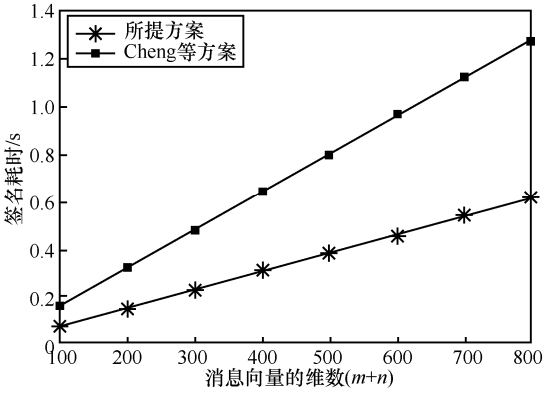


图 3 签名耗时比较

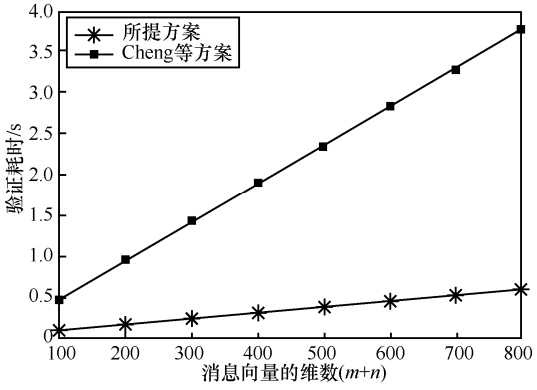


图 4 验证耗时比较

2) 签名算法

一个消息 $\boldsymbol{V}_j$ 的签名为 $\sigma_j(u_d)$，其中第 k 个数据分量的签名是

$$\sigma_{j,k}(u_d) = \left(\sum_{i=1}^{n} H_g(T) v_{j,i} s_k \right) \bmod p \tag{17}$$

输出用户 u_d 对 V_j $(1 \leqslant j \leqslant m)$ 的签名 $\sigma(u_d) = (\sigma_1(u_d), \sigma_2(u_d), \cdots, \sigma_s(u_d)) \in G_1^s$。当不涉及其他用户时，签名可以记为 $\boldsymbol{\sigma} = (\sigma_1, \sigma_2, \cdots, \sigma_s) \in G_1^s$。

3) 组合

$\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \cdots, \alpha_l)$ 为局部编码向量，$\sigma_1, \cdots, \sigma_l$ 分别为消息向量 $\boldsymbol{W}_1, \cdots, \boldsymbol{W}_l$ 的签名，其中组合后形成的向量为

$$\boldsymbol{W} = \sum_{j=1}^{l} \alpha_j \boldsymbol{W}_j$$

生成 $\boldsymbol{W}$ 的签名 $(\sigma_1, \sigma_2, \cdots, \sigma_s)$ 为

$$\sigma_k = \sum_{i=1}^{l} \alpha_i \sigma_{i,k}, \quad 1 \leqslant k \leqslant s \tag{18}$$

其中，$\sigma_{i,k} (1 \leqslant i \leqslant m, 1 \leqslant k \leqslant s)$ 是 σ_i 的第 k 个元素。

4) 签名验证算法

公钥为 $p_1, p_2, \cdots, p_s \in G_1$，消息向量 $\boldsymbol{W}$ 的全局编码向量是 $\boldsymbol{\beta} = (\beta_1, \beta_2, \cdots, \beta_m)$，签名为 σ，验证 $H_g(T) = H_g((\beta_1 T_1 + \beta_2 T_2 + \cdots + \beta_m T_m) \bmod p)$ 是否成立，若不成立，则拒绝验证；若成立，则验证等式

$$e(\sigma, G) = e\left(H_g(T), \sum_{k=1}^{s} \sum_{i=1}^{n} \boldsymbol{w}_i p_k \right) \tag{19}$$

是否成立，若成立，则验证成功。

4.2 正确性分析

1)由多源网络编码可得

$$\boldsymbol{W} = \sum_{j=1}^{m} \beta_j \boldsymbol{V}_j$$

为了区分不同用户的相同消息可组合在一起，设

$$\beta_j = \sum_{d=1}^{s} \beta_j(u_d) \tag{20}$$

在消息 $\boldsymbol{W}$ 的组合过程中，消息 $\boldsymbol{V}_j$ 来源于用户 $u_1, u_2, \cdots, u_s$，β_j 为消息 $\boldsymbol{V}_j$ 的全局组合系数。$\beta_j(u_1), \cdots, \beta_j(u_s)$ 分别是每个用户 $u_1, u_2, \cdots, u_s$ 对消息 V_j 赋予的组合系数，因此 $\boldsymbol{W}$ 可以表示为

$$\boldsymbol{W} = \boldsymbol{V}_1 \sum_{d=1}^{s} \beta_1(u_d) + \cdots + \boldsymbol{V}_m \sum_{d=1}^{s} \beta_m(u_d) = \sum_{j=1}^{m} \sum_{d=1}^{s} \beta_j(u_d) \boldsymbol{V}_j$$

组合的签名为

$$\sigma = \sum_{d=1}^{s} \beta_1(u_d) \sigma_1(u_d) \bmod p + \cdots +$$

$$\sum_{d=1}^{s} \beta_m(u_d) \sigma_m(u_d) \bmod p = \sum_{j=1}^{m} \sum_{d=1}^{s} \beta_j(u_d) \sigma_j(u_d) \bmod p \tag{21}$$

签名 σ 第 k 个分量 σ_k 为

$$\sigma_k = \left(\sum_{j=1}^{m} \sum_{d=1}^{s} \beta_j(u_d) \sigma_{j,k}(u_d) \right) \bmod p, \ 1 \leqslant k \leqslant s$$

其中，$\sigma_{j,k}(u_d)$ 是用户 u_d 对消息 $\boldsymbol{V}_j$ 签名 $\sigma_j(u_d)$ 的第 k 个分量。

2) 由于

$$e(\sigma,G)=e\left(\sum_{k=1}^{s}\sum_{j=1}^{m}\sum_{d=1}^{s}\beta_j(u_d)\sigma_{j,k}(u_d),G\right)=$$

$$e\left(H_g(T),\sum_{k=1}^{s}\sum_{i=1}^{n}\boldsymbol{w}_i p_k\right)=$$

$$e\left(H_g(T),\sum_{k=1}^{s}\sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{d=1}^{s}\beta_j(u_d)v_{j,i}s_k G\right)=$$

$$e\left(\sum_{k=1}^{s}\sum_{j=1}^{m}\sum_{d=1}^{s}\beta_j(u_d)\sum_{i=1}^{n}v_{j,i}s_k H_g(T),G\right)=$$

$$e\left(\sum_{k=1}^{s}\sum_{j=1}^{m}\sum_{d=1}^{s}\beta_j(u_d)\sigma_{j,k}(u_d),G\right)$$

因此，$e(\sigma,G)=e\left(H_g(T),\sum_{k=1}^{s}\sum_{i=1}^{n}\boldsymbol{w}_i p_k\right)$ 成立，显然签名方案组合前也成立。

4.3　安全性分析

定理 4　采用双线性对的多源网络编码签名能够抵抗污染攻击。

证明　挑战者 B 运行系统初始化算法，生成公开参数和系统私钥，然后将系统公开参数发送给攻击者 A，保存私钥。

询问。A 指定消息子空间，并且给定时间戳 $T_i\in {Z_{p-1}}^*$ 与之对应，通过签名算法生成每个消息向量的签名 σ_i，然后 B 将签名 σ_i 和时间戳 T_i 发给 A。

消息伪造。A 输出 $T_i\in {Z_{p\text{-}1}}^*$、非零消息向量 $\boldsymbol{m}^*$（$\boldsymbol{m}^*$ 不是 T_i 时刻的消息），以及签名 σ^*。验证 $\mathrm{Ver}(T_i,\boldsymbol{m}^*,\sigma^*)$ 合法，则说明 A 赢得了游戏。

当 $\boldsymbol{m}^*$ 不是时间戳 T_i 时刻的消息时，证明方式与文献[22]类似。在询问阶段，A 选择的消息子空间 $\boldsymbol{V}^\circ$ 是由向量 $(\boldsymbol{V}_1,\boldsymbol{V}_2,\cdots,\boldsymbol{V}_m)$ 张成的，并向 B 询问此消息子空间中各消息向量的签名。B 收到询问请求后，先选取 T_i 作为 $\boldsymbol{V}^\circ$ 的时间戳，然后生成各向量 $\boldsymbol{V}_i$ 的签名 σ_i，并将签名 σ_i 和时间戳 T_i 发送给 A。由此 A 可获得式(22)所示的方程组

$$\begin{bmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ v_{m1} & v_{m2} & \cdots & v_{mn} \end{bmatrix}\begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{bmatrix}=\begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_m \end{bmatrix} \tag{22}$$

其中，$f_i=H_g(T_i)s_i$。

A 输出一系列伪造消息 $(T_i,\boldsymbol{m}^*,\sigma^*)$，$\boldsymbol{m}^*\notin\boldsymbol{V}^\circ$，若伪造的消息量可通过验证，那么式(23)所示方程组成立

$$\begin{bmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ v_{m1} & v_{m2} & \cdots & v_{mn} \\ v_1^* & v_2^* & \cdots & v_n^* \end{bmatrix}\begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{bmatrix}=\begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_m \\ \sigma^* \end{bmatrix} \tag{23}$$

设在式(22)中，ζ 为系数矩阵与增广矩阵的秩，其解的个数为 $p^{n-\zeta}$，即式(23)的秩为 $\zeta+1$，解为 $p^{n-\zeta-1}$，易知式(22)中将有 p 个解满足式(23)。A 赢得游戏的概率为 $\frac{1}{P}$，可忽略不计（p 是一个很大的素数）。

签名伪造。由式(17)易知，签名 $\sigma_{j,k}(u_d)$ 是关于 n 个未知 $H_g(T)s_k$ 的一个线性方程。A 试图从传输的数据分组中推导出 $H_g(T)s_k$，而 $H_g(T)$ 是 m 个时间戳 T_i 线性组合的单向碰撞散列函数，A 不能通过解决单向碰撞散列函数问题得到 $H_g(T)s_k$，没有 $H_g(T)s_k$ 就不能伪造一个有效的签名，即签名不可伪造。

证毕。

定理 5　采用双线性映射的多源网络编码签名能够抵抗重放攻击。

证明　攻击者 A 截获 $(\boldsymbol{m},T,\sigma)$ 并将其重放到网络中，重放签名 $(\boldsymbol{m},T',\sigma')$ 在中间节点处重复发送，但因消息组合中的时间 T' $(T'\neq T)$，即 $H_g(T)\neq H_g(T')$，则可以断定该消息为重放消息签名并丢弃，所以攻击无效。

证毕。

4.4　实验结果与分析

本节中的主要密码操作的定义与 3.3 节中的一样，此处不再赘述，信源节点的个数用 s 表示，表 2 显示了不同方案的签名性能。

所提方案与 Li 等[17]方案、Zhang 等[15]方案的签名耗时仿真曲线如图 5 所示，三者的验证耗时仿真曲线如图 6 所示。通过 Matlab 仿真数据可以看出，随着消息向量维数的增加，不同方案的运行时间均线性增长，但是所提方案比 Li 等方案、Zhang 等方案增长缓慢，而且所提方案的签名和验证的耗时比同类方案低。

经过几组方案的对比可得出，所提方案效率优于同类方案是因为运算大多是标量乘，几乎不用指数运算，减少了运算时间的开销。

表 2　　多源网络编码签名性能比较

方案	签名	验证
Li 等方案	$2nC_{\text{mul}}+(2n+2)C_{\text{me}}$	$(m+n+s)C_{\text{mul}}+(m+n+1+s)C_{\text{me}}+(s+1)C_{\text{par}}$
Zhang 等方案	$(m+n)C_{\text{mul}}+(m+n+1)C_{\text{me}}$	$nC_{\text{mul}}+nC_{\text{me}}+(n+1)C_{\text{par}}$
所提方案	$nC_{\text{mul}}+1C_{\text{mtp}}$	$(n+s)C_{\text{mul}}+1C_{\text{mtp}}+2C_{\text{par}}$

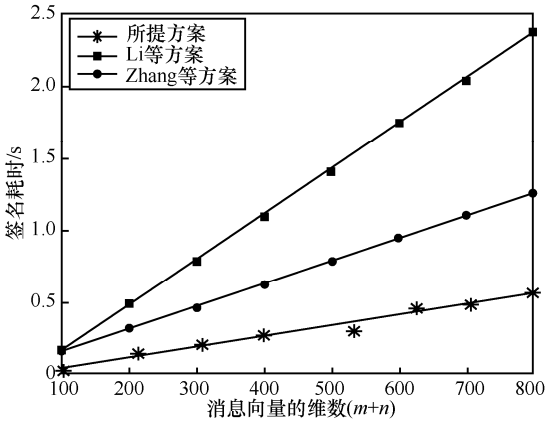


图 5　签名耗时比较

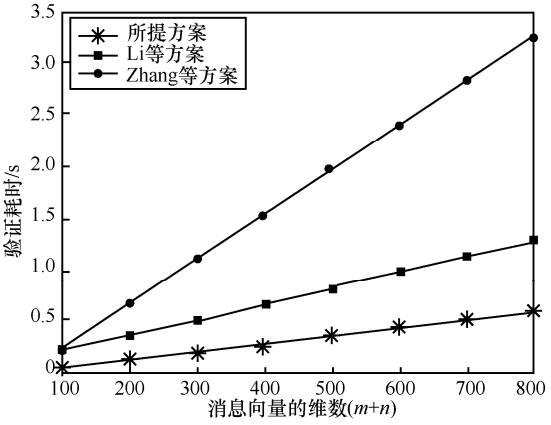


图 6　验证耗时比较

5　结束语

单源网络编码椭圆曲线同态签名是在 ECC 签名的基础上结合了同态散列函数和“代”的概念提出的，能够有效抵抗代内/代间污染。相比于同类方案，该方案的签名和验证计算时间短，能节约资源，减少通信开销。使用双线性对的多源网络编码同态签名是采用时间戳的同态签名方案，能够抵御污染攻击和重放攻击，该方案中的双线性对内部进行的是标量乘运算，与进行大量的指数运算的双线性对同类方案相比计算复杂度低，签名和验证效率更高；该方案在选择性攻击情况下是安全的。强安全性和更高签名验证效率的多源网络编码同态签名是本文下一步计划之一。

参考文献：

[1] AHLSWEDE R, AIN, LI S Y R, et al. Network information flow[J]. IEEE Transactions on Information Theory, 2000, 46(4): 1204-1216.

[2] YU Z, WEI Y, RAMKUMAR B, et al. An efficient signature-based scheme for securing network coding against pollution attacks[C]//IEEE INFOCOM 2008-The 27th Conference on Computer Communications. IEEE, 2008: 1409-1417.

[3] YUN A, CHEON J H, KIM Y. On homomorphic signatures for network coding[J]. IEEE Transactions on Computers, 2010, 59(9): 1295-1296.

[4] BONEH D, FREEMAN D, KATZ J, et al. Signing a linear subspace: signature schemes for network coding[C]//International Workshop on Public Key Cryptography. Springer, 2009: 68-87.

[5] LI Y, LUI J C S. Identifying pollution attackers in network-coding enabled wireless mesh networks[C]//International Conference on Computer Communications & Networks. IEEE, 2011.

[6] CHARLES D, JAIN K, LAUTER K. Signatures for network coding[J]. International Journal of Information and Coding Theory, 2009, 1(1): 3.

[7] WANG Y. Insecure provably secure network coding and homomorphic authentication schemes for network coding[J]. IACR Cryptology ePrint Archive, 2010: 1-9.

[8] HE M, CHEN L, WANG H, et al. Adapkeys: an adaptive security scheme for network coding[C]// IEEE Asia-pacific Services Computing Conference. IEEE Computer Society, 2012.

[9] 裴恒利, 尚涛, 刘建伟. 融合时间戳和同态签名的安全网络编码方法[J]. 通信学报, 2013, 34(4): 28-35.
PEI H L, SHANG T, LIU J W. A secure network coding method based on time stamp and homomorphic signature[J]. Journal on Communications, 2013, 34(4): 28-35.

[10] 蒙云番, 孙光昊, 邢杰, 等. 基于网络编码和 ECC 的无线体域网安全签名方案[J]. 电讯技术, 2015, 55(6): 605-610.
MENG Y F, SUN G B, XING J, et al. Wireless body area network security signature scheme based on network coding and ECC[J]. Telecommunications Technology, 2015, 55(6): 605-610.

[11] WU X, XU Y, YUEN C, et al. A tag encoding scheme against pollution attack to linear network coding[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(1): 33-42.

[12] CHENG C, LEE J, JIANG T, et al. Security analysis and improvements on two homomorphic authentication schemes for network coding[J]. IEEE Transactions on Information Forensics and Security, 2017, 11(5): 993-1002.

[13] AGRAWAL S, BONEH D, BOYEN X, et al. Preventing pollution attacks in multi-source network coding[C]//International Workshop on

Public Key Cryptography. Springer-Verlag, 2010.

[14] YANG H, YANG M. An unconditionally secure authentication code for multi-source network coding[J]. International Journal of Wireless and Microwave Technologies (IJWMT), 2012, 2(1): 45.

[15] ZHANG J, SHAO J, LING Y, et al. Efficient multiple sources network coding signature in the standard model[J]. Concurrency and Computation: Practice and Experience, 2015, 27(10): 2616-2636.

[16] LE A, MARKOPOULOU A. Cooperative defense against pollution attacks in network coding using spacemac[J]. IEEE Journal on Selected Areas in Communications, 2012, 30(2): 442-449.

[17] LI T, CHEN W, TANG Y, et al. A homomorphic network coding signature scheme for multiple sources and its application in IoT[J]. Security and Communication Networks, 2018, 2018: 1-6.

[18] 俞惠芳, 高新哲. 多源网络编码同态环签名方案研究[J]. 信息网络安全, 2019, 19(2): 36-42.
YU H F, GAO X Z. Homomorphic ring signature technology for multi-source network coding[J]. Netinfo Security, 2019, 19(2): 36-42.

[19] 彭勇, 严文杰, 陈俞强. 一种多源网络编码同态签名算法[J]. 合肥工业大学学报(自然科学版), 2014, 37(3): 310-313.
PENG Y, YAN W J, CHEN Y Q. A multi-source network coded homomorphic signature algorithm[J]. Journal of Hefei University of Technology (Natural Science), 2014, 37(3): 310-313.

[20] 牛淑芬, 王彩芬, 张玉磊, 等. 多源网络编码数据完整性验证方案[J]. 计算机工程, 2015, 41(3): 21-25.
NIU S F, WANG C F, ZHANG Y L, et al. Data integrity verification scheme for multi-source network coding[J]. Computer Engineering, 2015, 41(3): 21-25.

[21] 王起月. 基于椭圆曲线的数字签名算法研究[D]. 洛阳: 河南科技大学, 2018.
WANG Q Y. Research on digital signature algorithm based on elliptic curve[D]. Luoyang: Henan University of Science and Technology, 2018.

[22] CHEND C, JIANG T, LIU Y, et al. Security analysis of a homomorphic signature scheme for network coding[J]. Security and Communication Networks, 2015, 8(18): 4053-4060.

[23] 罗海, 王彩芬, 冯帆, 等. 多源网络编码同态签名方案[J]. 计算机应用研究, 2011, 28(4): 1465-1469.
LUO H,WANG C F,FENG F, et al. On homomorphic signature scheme for multi-source network coding[J]. Application Research of Computers, 2011, 28(4): 1465-1469.

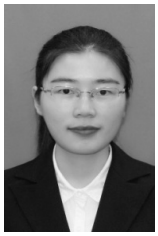
[24] 于志轩, 王彩芬. 改进的网络编码签名验证方案[J]. 计算机工程, 2012, 38(7): 122-124.
YU Z X, WANG C F. Improved verification scheme for network coding signature[J]. Computer Engineering, 2012, 38(7): 122-124.

[25] 杨铭熙, 罗蛟, 李腊元. 多源网络编码签名[J]. 中国通信, 2010, 7(1): 131-137.
YANG M X, LUO J, LI L Y. Signatures for multi-source network coding[J]. China Communications, 2010, 7(1): 131-137.

[26] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[C]//Annual International Cryptology Conference. Springer, 2001.

[作者简介]

俞惠芳（1972− ），女，青海乐都人，博士，西安邮电大学教授、硕士生导师，主要研究方向为密码学与信息安全。



李雯（1995− ），女，安徽全椒人，西安邮电大学硕士生，主要研究方向为密码学与信息安全。