基于格的可验证定时签名与应用

陈辉焱，王庆楠，王克，谭舜聪，辛红彩
（北京电子科技学院密码科学与技术系，北京 100070）

摘　要：针对目前的可验证定时签名（VTS）方案无法有效抵抗量子计算攻击的威胁问题，基于格上困难问题，提出了一种基于格的可验证定时签名（LVTS）方案。该方案不仅符合可验证定时签名不可伪造性和隐私性的基本要求，同时能够在随机预言机模型下实现高度的强不可伪造性，以及在混合实验环境中保障隐私性的有效实施，从而展现出卓越的安全性能。此外，LVTS 可被应用在电子拍卖协议（LVTS-EA）中，实现拍卖过程的高效性、安全性以及公平性，为电子拍卖领域提供了一种创新且实用的解决方案。

关键词：可验证定时签名；格；电子拍卖
中图分类号：TP309.7
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2024185

Lattice-based verifiable timed signature and application

CHEN Huiyan, WANG Qingnan, WANG Ke, TAN Shuncong, XIN Hongcai
Department of Cryptology Science and Technology, Beijing Electronic Science and Technology Institute, Beijing 100070, China

Abstract: Aiming at the problem that current verifiable timed signature (VTS) schemes cannot effectively resist the threat of quantum computing attacks, a lattice-based verifiable timed signature (LVTS) scheme was proposed, founded on challenging problems over lattices. This scheme not only fulfilled the fundamental criteria of unforgeability and privacy for verifiable timed signatures but also attained a heightened level of existential unforgeability in the random oracle model while ensuring the effective enforcement of privacy in hybrid argument. As a result, it exhibited exemplary security performance. Moreover, LVTS could be seamlessly integrated into electronic auction protocols (LVTS-EA) to enhance efficiency, security, and fairness in auction proceedings, offering an innovative and pragmatic solution for the electronic auction domain.

Keywords: verifiable timed signature, lattice, electronic auction

0　引言

定时密码学是一种设计用于在多项式时间内保持安全性的密码学原语，在预定时间 T 之后，任何人都能访问秘密信息。在这一领域，时间锁谜题（TLP, time-lock puzzle）[1-3]、定时释放签名[4-5]、定时承诺[6-7]等多种方案相继被提出和研究，既丰富了理论体系，也为实际应用提供了新的选择。

定时签名是定时密码学中的关键概念，分为前向定时签名[8]和后向定时签名 2 种类型，如图 1 所示。前向定时签名在特定时间前有效，过时失效；后向定时签名在指定时间段后生效，通过时间约束和延迟计算机制确保签名的安全性和不可抵赖性。Thyagarajan 等[9]提出了可验证定时签名（VTS, verifiable timed signature）的概念，并基于 BLS（Boneh-Lynn-Shacham）、Schnorr 和椭圆曲线数字签名算法（ECDSA, elliptic curve digital signa-

收稿日期：2024–07–11；修回日期：2024–10–08
通信作者：陈辉焱，hychen2001@126.com
基金项目：中央高校基本科研业务费资金资助项目（No.3282024048）
Foundation Item：The Fundamental Research Funds for the Central Universities (No.3282024048)

ture algorithm）构建了具体方案。VTS作为一种后向定时签名，允许发送方生成签名承诺，任何人都能验证签名承诺中是否包含消息的合理签名，可应用于支付通道网络[10]、多重签名交易[11]、公平多方计算[12]等领域。在区块链中，VTS可以替代传统的时间锁定功能，如比特币中的检查锁定时间验证（CLTV），在电子投票、身份验证、电子拍卖等领域也展现出了巨大潜力。Thyagarajan等[13]提出了可验证定时环签名，构建了与门罗币交易方案兼容的安全支付通道协议。Zhou等[14]改进了VTS，通过优化签名和公钥中的秘密共享降低了计算开销。此外，侯慧莹等[15]提出了可验证的属性基定时签名，Bao等[16]基于比特币投票协议提出了可验证定时签名。然而，目前的VTS方案仍是基于传统数论的困难假设构造的，无法有效抵抗量子计算攻击的威胁。

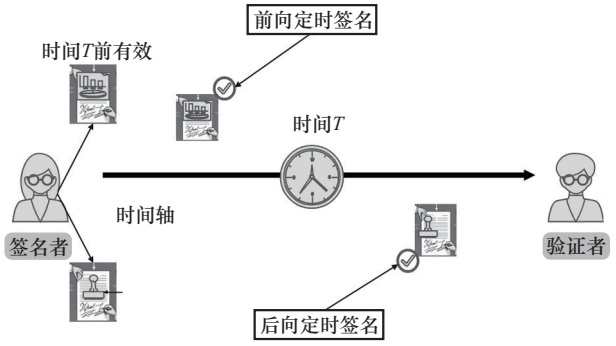

图1　定时签名

量子计算结合了量子力学和计算机科学，利用量子比特的叠加和纠缠特性，可以高效解决一些在经典计算模式下非常困难的问题。量子比特可以同时表示0和1的叠加状态，使得量子计算机在某些问题上比经典计算机快很多。在量子比特中，叠加特性允许它们同时存在于多个状态，而纠缠特性则使得一个量子比特的状态可以直接影响另一个无论多远的量子比特。这2个特性是量子计算能够在解决复杂问题上表现出色的原因[17-19]。

格密码的安全性基于格上困难问题，这些问题目前没有高效的量子求解算法，被认为是一种可以抵抗量子计算攻击的公钥密码体制[20-21]。此外，格密码系统还具有算法效率高、高并行性等优点，使其在后量子密码学领域具有广泛的应用[22]。Goldreich等[21]首次提出了基于格的数字签名方案。格签名在数字签名领域一直是一个重要的研究方向，特别是在美国NIST（National Institute of Standards and Technology）公布的首批后量子签名标准算法中[23]，基于格的数字签名方案占比三分之二。因此，本文设计一种能够抵抗量子计算攻击的可验证定时签名方案尤为关键。

为了实现后量子安全的VTS，本文提出了一种基于格的可验证定时签名（LVTS, lattice-based VTS）方案。本文主要贡献如下。

1) 通过将格密码与可验证定时签名相结合，提出了一种基于格的可验证定时签名方案（LVTS），并建立了LVTS的不可伪造性和隐私性安全模型，证明了该方案在随机预言机模型下具有强不可伪造性，并基于混合实验环境证明了该方案的隐私性。

2) 通过结合具有抗量子特性的非交互式门限秘密共享、伪链时间锁谜题（PCTLP, pseuelo-chain TLP）和简洁非交互式零知识证明这些抗量子组件，并将其与抗量子基础签名方案巧妙结合，有效解决了现有VTS方案在后量子安全性上的缺陷，增强了LVTS的可验证性和整体安全性。

3) 设计了一个基于LVTS的电子拍卖协议LVTS-EA，进一步论证了本文方案在区块链上应用的实用性和安全性。最后，通过仿真实验展示了LTVS的实际应用性能。

1　基础知识

1.1　符号含义

$\mathbb{R}$表示实数集合，$\mathbb{Z}$表示整数集合；加粗大写字母表示矩阵，如$\boldsymbol{A}$；加粗小写字母表示向量，如$\boldsymbol{a}$；$\boldsymbol{a}^{\mathrm{T}}$表示向量的转置；$\sum$表示求和；$\|\cdot\|$表示欧几里得范数，$\|\cdot\|_\infty$表示无穷范数；$s_1(\boldsymbol{a})$表示向量$\boldsymbol{a}$的最大奇异值；$d\sim D$表示$d$服从分布$D$；$\mathrm{negl}(n)$表示关于$n$的可忽略函数；$\xleftarrow{\$}$表示从某个分布中随机选取一个元素；$[N]$表示集合$1,2,\cdots,N$。

1.2　格

定义1　设$\boldsymbol{B}=\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n$是向量空间$\mathbb{R}^m$上$n$个线性无关的向量，则由$\boldsymbol{B}$生成的格$\Lambda$定义为$\Lambda=\mathcal{L}(\boldsymbol{B})=\left\{\sum_{i=1}^{n}x_i\boldsymbol{b}_i : x_i\in\mathbb{Z}\right\}$。其中，$\boldsymbol{B}$为格$\Lambda$的一组基。

定义2　设$\mathbb{Z}[x]$是由全体整系数多项式构成的多项式环，给定次数为n的分圆多项式$f(x)\in\mathbb{Z}[x]$，

定义分圆多项式环 $R=\dfrac{\mathbb{Z}[x]}{f(x)}$。给定素数 $q=1\bmod 2n$，定义 $R_q=\dfrac{R}{qR}=\dfrac{\mathbb{Z}_q[x]}{f(x)}$ 是模 $f(x)$ 和素数 q 的整数多项式环。

本文所采用的多项式环均为 $R=\dfrac{\mathbb{Z}[x]}{x^n+1}$，其中 n 取 2 的幂次。

定义 3 设 q 是一个素数，$\boldsymbol{a}\in R_q^m$，$u\in R_q$，定义多项式环上 q 模格为

$$\Lambda_q(\boldsymbol{a})=\left\{\boldsymbol{e}\in R^m,\text{s.t. }\exists s\in R_q,\boldsymbol{a}s=\boldsymbol{e}\left(\bmod q\right)\right\} \tag{1}$$

$$\Lambda_q^{\perp}(\boldsymbol{a})=\left\{\boldsymbol{e}\in R^m,\text{s.t. }\boldsymbol{a}^{\mathrm{T}}\boldsymbol{e}=0\left(\bmod q\right)\right\} \tag{2}$$

$$\Lambda_q^{u}(\boldsymbol{a})=\left\{\boldsymbol{e}\in R^m,\text{s.t. }\boldsymbol{a}^{\mathrm{T}}\boldsymbol{e}=u\left(\bmod q\right)\right\} \tag{3}$$

定义 4 对任意向量 $\boldsymbol{c}\in\mathbb{R}^n$，实数 $s>0$，n 维高斯函数定义为

$$\rho(x)=\exp\left(-\pi\left(\frac{\|x-c\|}{s}\right)^2\right),\forall\boldsymbol{x}\in\Lambda \tag{4}$$

定义 5 对任意向量 $\boldsymbol{c}\in\mathbb{R}^n$，实数 $s>0$，n 维格 Λ 上的离散高斯分布定义为

$$D_{\Lambda,s,c}(\boldsymbol{x})=\frac{\rho_{(s,c)}(\boldsymbol{x})}{\rho_{(s,c)}(\Lambda)},\forall\boldsymbol{x}\in\Lambda \tag{5}$$

引理 1 尾切。为了使一维高斯分布的尾部小于 $2^{-\lambda}$，本文使用以下事实。对于 $x\leftarrow D_{\mathbb{Z},\sigma}$，有 $\Pr_{x\leftarrow D_{\mathbb{Z},\sigma}}[|x|>t\sigma]\leqslant\operatorname{erfc}\left(\dfrac{t}{\sqrt{2}}\right)$，其中有 $\operatorname{erfc}(x)=1-\dfrac{2}{\sqrt{\pi}}\displaystyle\int_0^x\exp(-t^2)\mathrm{d}t$。例如，当 $\lambda=100$ 时，取 $t=12$，那么，一个从 $D_{\mathbb{Z}^m,\sigma}$ 采样的向量 x 的范数 $\|x\|\leqslant t\sigma\sqrt{m}$ 会以压倒性的概率成立。

1.3 格上困难问题

定义 6 小整数解（SIS, small integer solution）问题。给定一个整数矩阵 $\boldsymbol{A}\in\mathbb{Z}^{m\times n}$ 和一个整数 q，寻找一个非零向量 $\boldsymbol{x}\in\mathbb{Z}^n$，并且 $\boldsymbol{x}$ 的范数比较小，使得 $\boldsymbol{A}\boldsymbol{x}\equiv 0\,(\bmod q)$。

SIS 问题被认为在大多数情况下是难以解决的，特别是当矩阵 $\boldsymbol{A}$ 和模数 q 选择合适时，寻找满足条件的小范数解具有很高的计算复杂性。

定义 7 环上小整数解（Ring-$\mathrm{SIS}_{q,m,\beta}$, ring shortest intger solution）问题[24-25]。给定正整数 q 和 m，向量 $\boldsymbol{a}=\left(a_1,a_2,\cdots,a_m\right)^{\mathrm{T}}\in R_q^m$ 和实数 β，找到一个小系数的非零多项式向量 $\boldsymbol{x}=\left(x_1,x_2,\cdots,x_m\right)^{\mathrm{T}}\in R^m$，满足式(6)。

$$\begin{cases}\boldsymbol{a}^{\mathrm{T}}\boldsymbol{x}=\displaystyle\sum_{i=1}^{m}a_ix_i=0\bmod q\\ 0<\|\boldsymbol{x}\|_{\infty}\leqslant\beta\end{cases} \tag{6}$$

相较于 SIS 问题，Ring-SIS 问题主要通过引入环结构提升计算效率和存储优化，在实际应用中具有更好的性能，而安全性并未因此降低。Ring-SIS 问题仍然保持与 SIS 问题相同的安全级别。虽然它在计算效率上进行了优化，但从理论上讲，Ring-SIS 问题仍然是基于格的困难问题，因此与抗量子计算攻击的 SIS 问题一样安全。

1.4 陷门函数及相关算法

定义 8[22] 给定向量 $\boldsymbol{a}\in R_q^m$，本原向量 $\boldsymbol{g}=\left(1,2,4,\cdots,2^{k-1}\right)^{\mathrm{T}}\in R_q^k$ 和可逆 $h\in R_q$，其中 $k=\lceil\log q\rceil$，$m>k$。若存在向量 $\boldsymbol{R}\in R^{(m-k)\times k}$ 满足 $\boldsymbol{a}^{\mathrm{T}}\begin{pmatrix}\boldsymbol{R}\\ \boldsymbol{I}_k\end{pmatrix}=h\boldsymbol{g}^{\mathrm{T}}$，则称 $\boldsymbol{R}$ 为 $\boldsymbol{a}$ 的 $\boldsymbol{g}$ −陷门，h 为 $\boldsymbol{R}$ 的标签多项式。

根据文献[26]，分别给出陷门生成算法 TrapGen 和原像抽样算法 SamplePre，如算法 1 和算法 2 所示。

算法 1 $\mathrm{TrapGen}\left(q,\sigma,\boldsymbol{a}',h\right)$

输入 随机选择 $\boldsymbol{a}'\in R_q^{m-k}$，可逆 $h\in R_q$，模数 q，高斯参数 σ

输出 $\boldsymbol{a}\in R_q^m$ 和 $\boldsymbol{a}$ 的 $\boldsymbol{g}$ − 陷门 $\boldsymbol{R}\in R^{(m-k)\times k}$，$\|\boldsymbol{R}\|\leqslant t\sigma\sqrt{(m-k)n}$

1) 根据 $D_{R^{(m-k)\times k},\sigma}$ 采样得到一组线性无关的环元素的向量 $\boldsymbol{R}$

2) 输出 $\boldsymbol{a}=\left(a'^{\mathrm{T}}\middle|h\boldsymbol{g}^{\mathrm{T}}-a'^{\mathrm{T}}\boldsymbol{R}\right)^{\mathrm{T}}\in R_q^m$，以及陷门 $\boldsymbol{R}\in R^{(m-k)\times k}$

算法 2 $\mathrm{SamplePre}\left(\boldsymbol{a},\boldsymbol{R},h,\zeta,\sigma,\alpha,u\right)$

输入 $\boldsymbol{a}\in R_q^m$，$\boldsymbol{a}$ 的 $\boldsymbol{g}$ −陷门 $\boldsymbol{R}\in R^{(m-k)\times k}$，可逆 $h\in R_q$，$u\in R_q$，高斯参数 ζ,σ,α

输出 原像 $\boldsymbol{x}\in R_q^m$，满足 $\boldsymbol{a}^{\mathrm{T}}\boldsymbol{x}=u\in R_q$

1) 选择一个新的扰动向量 $\boldsymbol{p}\leftarrow\mathrm{SampleP}\left(q,\zeta,\alpha,\boldsymbol{R}\right)$，令 $v\leftarrow h^{-1}\left(u-\boldsymbol{a}^{\mathrm{T}}\boldsymbol{p}\right)$

2) 选择 $\boldsymbol{z}\leftarrow\mathrm{SamplePolyG}\left(\sigma,v\right)$，计算 $\boldsymbol{x}\leftarrow\boldsymbol{p}+\begin{pmatrix}\boldsymbol{R}\\ \boldsymbol{I}_k\end{pmatrix}\boldsymbol{z}$

3) 输出 $\boldsymbol{x}$

定理 1[26]　存在多项式时间算法 SamplePolyG $(\sigma,v)\to z$，输入高斯参数 σ 和目标多项式 $v\in R_q$，输出 $z\leftarrow D_{\Lambda_q^{\perp}(\boldsymbol{g}^{\mathrm{T}}),\alpha,v}$，其中 $\alpha=\sqrt{5}\,\sigma$。

定理 2[26]　存在多项式时间算法 SampleP $(q,\zeta,\alpha,\boldsymbol{R})\to\boldsymbol{p}$，输入模数 q，高斯参数 ζ 和 α，$\boldsymbol{R}\in R^{(m-k)\times k}$，输出 $\boldsymbol{p}\leftarrow D_{R^m,\sqrt{\sum_p}}$，其中 $\sum_p=\zeta^2\boldsymbol{I}_m-\alpha^2\begin{pmatrix}\boldsymbol{R}\\ \boldsymbol{I}_k\end{pmatrix}(\boldsymbol{R}^{\mathrm{T}}\quad\boldsymbol{I}_k),\zeta>s_1(\boldsymbol{R})\alpha$。

1.5　非交互式门限秘密共享

非交互式门限秘密共享[27]用于将一个秘密分割成多个份额，并分发给一组参与者。“非交互式”意味着一旦秘密被分割并分发，参与者之间不需要进一步的交互就能重建秘密。非交互式门限秘密共享机制确保只有当足够数量的份额（达到或超过预设的门限值）被集合起来时，秘密才能被重建。

设用户集合 $\boldsymbol{U}=\{U_1,\cdots,U_n\}$，$t$ 为秘密份额的个数，在集合 A、B 上分别定义 +、∗ 的二元运算。令 H_1 表示 $A\to B$ 的具有同态性的抗碰撞哈希函数族，均匀随机选取 $F\in H_1$。本文随机选择一个秘密 s 并编码为 a_0，使得 $s=a_0\in A$，均匀随机选取 $a_1,\cdots,a_{t-1}\in A$，构造伪随机函数 $f(x)=a_0+a_1x+\cdots+a_{t-1}x^{t-1}$，并公布 $F(a_0),F(a_1),\cdots,F(a_{t-1})$。非交互式门限秘密共享方案由以下 3 种算法组成。

1) 份额生成算法。计算 $f(i)$ 和 $F(a_{t-1})$，秘密发送 $f(i)$ 给对应用户 U_i 作为其份额，公开 $F(f(i))$。

2) 验证算法。对于 $1\leqslant i\leqslant N$，验证 $f(i)\in A$ 和 $F(f(i))=F(a_0)(F(a_1))^{i}\cdots(F(a_{t-1}))^{i^{t-1}}$ 是否成立，若成立则输出 1，否则输出 0。

3) 秘密重构算法。如果有 t 个或更多个用户提供其拥有的份额，则可以使用拉格朗日插值公式重构 F 的所有系数，从而获得秘密 $s=a_0$。

1.6　伪链时间锁谜题

伪链时间锁谜题[28]允许发送者创建一个谜题，这个谜题只能在经过特定的时间后被接收者解开，而且解锁过程不能通过增加计算资源来显著加速，即谜题生成器 Gen(S) 输入谜底 S，输出谜题 P，解谜器 Solve(P) 输入谜题 P，输出谜底 S。伪链时间锁谜题通常由以下 3 种算法组成。

1) PSetup$(1^{\lambda},T)\to$ pp：输入安全参数 λ 和时间 T，输出公开参数 pp。

2) Gen$(\mathrm{pp},s,r)\to Z$：输入参数 pp、秘密 s 和随机数 r，输出谜题 Z。

3) Solve$(\mathrm{pp},Z)\to s$：输入参数 pp 和谜题 Z，输出秘密 s。

改进的伪链时间锁谜题[28]定义如下。令随机预言机 H_2: $\{0,1\}^{\kappa}\to\{0,1\}^{\kappa}$，输入安全参数 κ 和整数 $q\geqslant 0$，执行以下操作。

1) 采样 $x_0,x_1,\cdots,x_{q+1}\xleftarrow{\$}\{0,1\}^{\kappa}$。

2) 对随机预言机进行（一轮）查询 $(x_0,\cdots,x_q)$，得到 $(H_2(x_0),\cdots,H_2(x_q))$。

3) 令 $P=(x_0,H_2(x_0)\oplus x_1,\cdots,H_2(x_q)\oplus x_{q+1})$，$s=(x_0,x_1,\cdots,x_{q+1})$，$\oplus$ 表示异或。

4) 发送 P 给（解谜器）算法 $\mathcal{A}$。

5) 算法 $\mathcal{A}$ 向 H_1 查询后，输出 s'。

用 $<\mathcal{C},\mathcal{A}>$ 表示在伪链时间锁谜题实验中挑战者 $\mathcal{C}$ 和算法 $\mathcal{A}$ 之间的交互。本文定义当且仅当 $s=s'$ 时 $<\mathcal{C},\mathcal{A}>=1$，否则置 0。易得，如果 $\mathcal{A}$ 能进行至少 $(q+1)$ 轮查询，那么 $\mathcal{A}$ 总能找到 s。

伪链时间锁谜题具有完美正确性和自适应线性差距[25]，这种伪链时间锁谜题在经典模型下的算法 Gen 和 Solve，需要一轮 $q+1$ 次查询来生成，且不能通过 q 轮的量子查询来解决。

1.7　简洁非交互式零知识证明

简洁非交互式零知识证明（zkSNARK, zero-knowledge succinct non-interactive argument of knowledge）[29]允许证明者向验证者证明某个陈述是正确的，而不需要透露任何其他信息，且在这个过程中不需要双方进行交互。以下给出 zkSNARK 的算法组成。

1) $\mathrm{zk}_{\mathrm{setup}}(1^{\lambda})\to$ crs：输入安全参数 λ，输出公共参考字符串 crs。

2) $\mathrm{zk}_{\mathrm{prove}}(\mathrm{crs},x,\omega)\to\pi$：输入 crs，声明 x 和证据 ω，输出证明 π。

3) $\mathrm{zk}_{\mathrm{verify}}(\mathrm{crs},x,\pi)\to 0/1$：输入 crs，声明 x 和证明 π，如果证明是正确的，则输出 1，否则输出 0。

2　基于格的可验证定时签名

2.1　方案定义

定义 9　基于格的可验证定时签名（LVTS）。

LVTS 由以下 8 个算法构成。

1) 初始化 $\mathrm{Setup}(1^{\lambda}) \to \mathrm{crs}$：输入安全参数 λ，输出公共参考字符串 crs。

2) 密钥生成 $\prod.\mathrm{KeyGen}(1^{n})$：输入安全参数 n，生成用户公私钥 $(\mathrm{pk},\mathrm{sk})$。

3) 签名 $\prod.\mathrm{Sign}(\mathrm{sk},\mu)$：输入用户私钥 sk 和消息 μ，生成签名 $\boldsymbol{s}$。

4) 承诺 $\mathrm{Commit}(\mathrm{pk},\boldsymbol{s},T,\mathrm{crs}) \to (C,\pi)$：输入公钥 pk、$\prod.\mathrm{Sign}$ 生成的签名 $\boldsymbol{s}$、解谜时间 T 和公共参考字符串 crs，输出承诺 C 和对应证明 π。

5) 验证 $\mathrm{Verify}(\mathrm{pk},C,\pi) \to 0/1$：输入承诺 C 和对应证明 π，输出判定结果 0/1。

6) 打开承诺 $\mathrm{Open}(C) \to (\boldsymbol{s},r)$：输入承诺 C，输出签名 $\boldsymbol{s}$ 和伴随 C 的随机数 r。

7) 签名验证 $\prod.\mathrm{Verify}(\mathrm{pk},\mu,\boldsymbol{s}) \to 0/1$：输入公钥 pk、消息 μ 和签名 $\boldsymbol{s}$，若签名有效输出 1，否则输出 0。

8) 强制打开承诺 $\mathrm{ForceOpen}(C) \to \boldsymbol{s}$：输入承诺 C，输出签名 $\boldsymbol{s}$。

定义 10 正确性。如果对于所有消息 m，$(\mathrm{pk},\mathrm{sk}) \leftarrow \mathrm{KeyGen}(1^{\lambda})$，$\mathrm{Verify}(\mathrm{pk},m,\mathrm{Sign}(1^{\lambda},\mathrm{sk},m))=1$ 以压倒性的概率成立，则称 $\prod(\mathrm{KeyGen},\mathrm{Sign},\mathrm{Verify})$ 满足正确性。

定义 11 选择消息攻击不可伪造性。选择消息攻击不可伪造性（SU-CMA, selective unforgeability against chosen message attack）安全模型由以下游戏描述。

1) Init：假设敌手 $\mathcal{A}$ 选择挑战消息 μ^{*}。

2) Setup：挑战者运行 $\mathrm{KeyGen}(1^{\lambda})$ 并将公钥 pk 提供给敌手 $\mathcal{A}$。

3) Queries：敌手 $\mathcal{A}$ 选择消息 $\mu \neq \mu^{*}$ 进行询问，挑战者运行 $\boldsymbol{s} \leftarrow \mathrm{Sign}(1^{\lambda},\mathrm{sk},\mu)$。

4) Forgery：敌手 $\mathcal{A}$ 输出伪造签名 $\boldsymbol{s}^{*}$，如果 $\mathrm{Verify}(1^{\lambda},\mathrm{pk},\mu^{*},\boldsymbol{s}^{*})=1$，则敌手获胜。

敌手 $\mathcal{A}$ 赢得上面游戏的概率为

$$\mathrm{Adv}(\mathcal{A})_{\mathrm{sig}}^{\text{SU-CMA}}=\left|\Pr\left[\mathrm{Verify}(1^{\lambda},\mathrm{pk},\mu^{*},\boldsymbol{s}^{*})=1\right]-\frac{1}{2}\right| \tag{7}$$

如果对于所有多项式时间敌手 $\mathcal{A}$，其优势 $\mathrm{Adv}(\mathcal{A})_{\mathrm{sig}}^{\text{SU-CMA}}$ 可以忽略不计，则签名方案是 SU-CMA 安全的。

定义 12 隐私性。在多项式时间内，如果存在一个模拟器 $\mathcal{S}$ 和一个可忽略函数 negl，所有具备并行计算能力的敌手 $\mathcal{A}$ 的最大运行时间 $t < T$，并且满足不等式(8)。

$$\begin{aligned}&\left|\Pr\left[(\mathrm{pk},\mathrm{sk}) \leftarrow \prod.\mathrm{KeyGen}(1^{\lambda}),\boldsymbol{s} \leftarrow \prod.\mathrm{Sign}(\mathrm{sk},\mu),\right.\right.\\&\left.(C,\pi) \leftarrow \mathrm{Commit}(\boldsymbol{s},T):\mathcal{A}(\mathrm{pk},\mu,C,\pi)=1\right]-\\&\Pr\left[(\mathrm{pk},\mathrm{sk}) \leftarrow \prod.\mathrm{KeyGen}(1^{\lambda}),(C,\pi,\mu) \leftarrow\right.\\&\left.\left.\mathcal{S}(\mathrm{pk},T):\mathcal{A}(\mathrm{pk},\mu,C,\pi)=1\right]\right| \leqslant \mathrm{negl}(\lambda)\end{aligned} \tag{8}$$

定义 13 合理性。在多项式时间内，对于任意敌手 $\mathcal{A}$ 以下概率是可忽略的，则称该签名方案满足合理性。

$$\begin{aligned}&\Pr\left[(\mathrm{pk},\mu,C,\pi,T) \leftarrow \mathcal{A}(1^{\lambda}),(\boldsymbol{s},r) \leftarrow \mathrm{ForceOpen}(C):\right.\\&\left.\mathrm{Verify}(\mathrm{pk},\mu,C,\pi)=1\ ;\ \prod.\mathrm{Verify}(\mathrm{pk},\mu,\boldsymbol{s})=0\right] \leqslant\\&\mathrm{negl}(\lambda)\end{aligned} \tag{9}$$

2.2 方案构造

LVTS 具体构造如下。

1) $\mathrm{Setup}(1^{\lambda})$：输入安全参数 λ。

① 调用算法 $\mathrm{crs}_{\mathrm{rng}} \leftarrow \mathrm{ZKsetup}(1^{\lambda})$。

② 调用算法 $\mathrm{pp} \leftarrow \mathrm{PCTLP.PSetup}(1^{\lambda},T)$。

③ 输出 $\mathrm{crs}=(\mathrm{crs}_{\mathrm{rng}},\mathrm{pp})$。

2) $\prod.\mathrm{KeyGen}(1^{n})$：输入安全参数 n。

① 调用 $(\boldsymbol{a},\boldsymbol{R}) \leftarrow \mathrm{TrapGen}(q,\sigma,\boldsymbol{a}',h=0)$ 算法。

② 输出用户公钥 $\mathrm{pk}=\boldsymbol{a} \in R^{m}$，用户私钥 $\mathrm{sk}=\boldsymbol{R} \in R^{(m-k)\times k}$。

3) $\prod.\mathrm{Sign}(\boldsymbol{a},\boldsymbol{R},\mu)$：输入用户公钥 $\mathrm{pk}=\boldsymbol{a}$，用户私钥 $\mathrm{sk}=\boldsymbol{R}$ 和消息 $\mu \in R_2$。

① 计算 $h_{\mu}=H_3(\mu)$，其中 $\mu \in R_2$，$H_3:R_2 \to R_q$（由于 1.3 节中要求 h 是可逆的，因此这里 H_3 的输出也必须保证是可逆的）。

② 计算 $\boldsymbol{a}_{\mu}=\boldsymbol{a}+(0|h_{\mu}\boldsymbol{g}^{\mathrm{T}})^{\mathrm{T}}=(\boldsymbol{a}'^{\mathrm{T}}|h_{\mu}\boldsymbol{g}^{\mathrm{T}}-\boldsymbol{a}'^{\mathrm{T}}\boldsymbol{R})^{\mathrm{T}}$。

③ 调用算法 $\boldsymbol{s} \leftarrow \mathrm{SamplePre}(\boldsymbol{R},\boldsymbol{a}_{\mu},h_{\mu},\zeta,\sigma,\alpha,0)$。

④ 输出签名 $\boldsymbol{s} \in R^{m}$。

4) $\mathrm{Commit}(\boldsymbol{a},\boldsymbol{s},T,\mathrm{crs})$：输入签名 $\boldsymbol{s}$，时间 T，公共参考字符串 crs。

① 设置集合 $\boldsymbol{U}=\{U_1,U_2,\cdots,U_n\}$。

② 设置 $[\boldsymbol{s}_0]=\boldsymbol{s}$，均匀随机选取 $[\boldsymbol{s}_1],\cdots,[\boldsymbol{s}_{t-1}] \in R^{m}$。

③ 对所有 $i \in [n]$，计算 $f(U_i)$，其中伪随机函数 $f:\mathbb{Z}_p \to R^{m}$，$f(x)=[\boldsymbol{s}_0]+[\boldsymbol{s}_1]x+\cdots+[\boldsymbol{s}_{t-1}]x^{t-1}$。

④ 对所有 $j \in \{0,\cdots,t-1\}$，计算 $F([\boldsymbol{s}_0]),\cdots,F([\boldsymbol{s}_{t-1}])$，$F:R^{m} \to R$ 是一个单向函数，这里的具体定义形式是 $F(\boldsymbol{X}=(X_1,X_2,\cdots,X_m))=<\boldsymbol{X},\boldsymbol{a}>$

$\sum_{i=1}^{m} X_i a_i$，其中$\boldsymbol{X}=(X_1,X_2,\cdots,X_m)$。

⑤ 对所有$i\in[n]$，计算$F(f(U_i))$。

⑥ 对所有$i\in[n]$，分别调用算法$Z_i\leftarrow$ PCTLP.PGen(pp,$f(U_i)$; r_i) 和 $\pi_{\mathrm{rng},i}\leftarrow \mathrm{zk}_{\mathrm{prove}}(\mathrm{crs}_{\mathrm{rng}},(Z_i,0,2^{\lambda},T),(f(U_i),r_i))$，其中，$r_i\xleftarrow{\$}\{0,1\}^{\lambda}$。

⑦ 计算$I\leftarrow H'(\mathrm{pk},(Z_1,\pi_{\mathrm{rng},1}),\cdots,(Z_n,\pi_{\mathrm{rng},n}))$。其中，$H'\colon\{0,1\}^{*}\rightarrow I\subset[n],|I|=t-1$。

⑧ 输出承诺$C=(Z_1,\cdots,Z_n,T)$和证明$\pi=(\{\pi_{\mathrm{rng},i}\}_{i\in[n]},I,\{f(U_i),r_i\}_{i\in I})$。

5) Verify(C,π)：输入承诺$C=(Z_1,\cdots,Z_n,T)$和证明$\pi=(\{\pi_{\mathrm{rng},i}\}_{i\in[n]},I,\{f(U_i),r_i\}_{i\in I})$。如果满足以下任意一种情况则输出0，否则输出1。

① 存在$i\in[n]$，满足$\mathrm{zk}_{\mathrm{verify}}(\mathrm{crs}_{\mathrm{rng}},(Z_i,0,2^{\lambda},T),\pi_{\mathrm{rng},i})\neq 1$。

② 存在$i\in I$，满足$Z_i\neq$ PCTLP.PGen(pp, $f(U_i)$; r_i)或$F(f(U_i))\neq\sum_{j=0}^{t-1}F([\boldsymbol{s}_j])U_i^{j}$。

③ $I\neq H'(\mathrm{pk},(Z_1,\pi_{\mathrm{rng},1}),\cdots,(Z_n,\pi_{\mathrm{rng},n}))$。

6) Open(C)：输入承诺$C=(Z_1,\cdots,Z_n,T)$，输出签名$\boldsymbol{s}$和随机数集合$\{r_i\}_{i\in[n]}$。

7) $\prod$.Verify($\boldsymbol{a},\mu,\boldsymbol{s}$)：输入公钥$\boldsymbol{a}$，消息$\mu$和签名$\boldsymbol{s}$。

① 计算h_{μ}和$\boldsymbol{a}_{\mu}$。

② 验证$\boldsymbol{a}_{\mu}^{\mathrm{T}}\boldsymbol{s}=0\bmod q$是否成立，并且满足$0<\|\boldsymbol{s}\|\leqslant t\zeta\sqrt{mn}$，若成立输出1，否则输出0。

8) ForceOpen(C)：输入承诺$C=(Z_1,\cdots,Z_n,T)$。

① 对所有$i\in[n]$，调用算法$f(U_i)\leftarrow$ PCTLP.Solve(pp,Z_i)。

② 输出签名$\boldsymbol{s}=\sum_{j\in[t]}f(U_j)\mathcal{L}_j(0)$，其中$\mathcal{L}_j(\cdot)$表示第$j$个拉格朗日多项式基。

2.3　安全性分析

本节从签名方案$\prod$的正确性、选择消息攻击不可伪造性（SU-CMA）、隐私性和合理性4个方面分析本文方案的安全性。

定理3　正确性。基于定义11对本文方案模型正确性证明的描述，再根据引理1的高斯尾切可知，$\prod$(KeyGen,Sign,Verify)中算法SamplePre生成签名的范数大概率被$t\zeta\sqrt{nm}$限制（因为其签名大小为nm的整数向量，且具有高斯参数ζ），所以本文方案的正确性可以得证。

定理4　SU-CMA。如果Ring-$\mathrm{SIS}_{q,m-k,\beta}$假设成立，其中$\beta=(1+t\sigma\sqrt{(m-k)n})t\zeta\sqrt{mn}$)，则签名方案$\prod$(KeyGen,Sign,Verify)在随机预言机模型下满足SU-CMA安全。

证明　假设敌手$\mathcal{A}$通过SU-CMA攻击签名方案$\prod$(KeyGen,Sign,Verify)，构造一个模拟器$\mathcal{B}$用于攻击Ring-SIS问题。

1) Init。模拟器$\mathcal{B}$在R_q中独立均匀随机采样得到$\boldsymbol{a}'=(a_1,\cdots,a_{m-k})^{\mathrm{T}}\in R_q^{m-k}$，敌手$\mathcal{A}$给出挑战消息$M^{*}$。$\mathcal{B}$运行TrapGen($q,\sigma,\boldsymbol{a}',-h_{\mu^{*}}$)，得到$\boldsymbol{a}=(\boldsymbol{a}'^{\mathrm{T}}|-h_{\mu^{*}}\boldsymbol{g}-\boldsymbol{a}'^{\mathrm{T}}\boldsymbol{R})^{\mathrm{T}}$和$\boldsymbol{R}\leftarrow D_{R^{(m-k)\times k},\sigma}$。模拟器将pk$=\boldsymbol{a}$给敌手$\mathcal{A}$。

2) Queries。敌手$\mathcal{A}$询问$\mathcal{B}$关于消息$m\neq m^{*}$的签名。为了回答$\mathcal{A}$的询问，模拟器计算$\boldsymbol{a}_{\mu}=\boldsymbol{a}^{\mathrm{T}}+(0|h_{\mu}\boldsymbol{g})=(\boldsymbol{a}'^{\mathrm{T}}|(h_{\mu}-h_{\mu^{*}})\boldsymbol{g}-\boldsymbol{a}'^{\mathrm{T}}\boldsymbol{R})^{\mathrm{T}}$，运行SamplePre($\boldsymbol{R},\boldsymbol{a}_{\mu},h_{\mu}-h_{\mu^{*}},\zeta,\sigma,\alpha,0$)生成签名$\boldsymbol{s}\in R^{m}$。

3) Forgery。敌手$\mathcal{A}$输出关于消息μ^{*}的伪造签名$\boldsymbol{s}^{*}$，满足$\boldsymbol{a}_{\mu^{*}}^{\mathrm{T}}\boldsymbol{s}^{*}=0\bmod q$，即$\boldsymbol{a}'^{\mathrm{T}}(I_{m-k}|-\boldsymbol{R})\boldsymbol{s}^{*}=0\bmod q$。

由于$\|\boldsymbol{R}\|\leqslant t\sigma\sqrt{(m-k)n}$，因此敌手$\mathcal{A}$能够找到关于Ring-SIS问题的解$\|(I_{m-k}|-\boldsymbol{R})\boldsymbol{s}^{*}\|\leqslant\beta=\left(1+t\sigma\sqrt{(m-k)n}\right)t\zeta\sqrt{mn}$。证毕。

定理5　隐私性。假设PCTLP是满足完美正确性，LVTS满足定义12中的隐私性。

证明　假设敌手$\mathcal{A}$具有有限深度T^{ϵ}，其中ϵ为非负数，签名方案$\prod$(KeyGen,Sign,Verify)满足正确性和选择消息攻击不可伪造性（SU-CMA），TLP满足正确性，非交互式零知识（NIZK, non-interactive zero-knowledge）具有零知识性，则LVTS满足隐私性。下面通过一系列混合实验证明。

1) Hybrid$\mathcal{H}_0$。执行原始算法LVTS。

2) Hybrid$\mathcal{H}_1$。在这个实验中，将随机预言机变为惰性抽样模拟，提前采样一个随机集合I^{*}（其中$|I^{*}|=t-1$），并将随机预言机在剪切选择实例上的输出设置为I^{*}。相比于$\mathcal{H}_0$，$\mathcal{H}_1$仅是语法上的变化，因此是不可区分的。

3) Hybrid$\mathcal{H}_2$。在这个实验中，模拟$\mathrm{crs}_{\mathrm{rng}}$。相比于$\mathcal{H}_1$，由于($\mathrm{zk}_{\mathrm{setup}},\mathrm{zk}_{\mathrm{prove}},\mathrm{zk}_{\mathrm{verify}}$)的零知识性，这

种变化在计算上是不可区分的。

4) Hybrid$\mathcal{H}_3 \cdots \mathcal{H}_{3+n}$。在这个实验中，对所有的$i \in [n]$通过底层zkSNARK证明提供的模拟器计算$\pi_{\mathrm{rng},i}$。由于$(\mathrm{zk}_{\mathrm{setup}},\mathrm{zk}_{\mathrm{prove}},\mathrm{zk}_{\mathrm{verify}})$的零知识性，任意2个相邻混合实验之间的$\pi_{\mathrm{rng},i}$是不可区分的。

5) Hybrid$\mathcal{H}_{3+n} \cdots \mathcal{H}_{3+2n-t+1}$。在第$i$个混合实验$\mathcal{H}_{3+i}$中，对所有的$i \in [n-(t-1)]$，集合$\bar{I}^*$的第$i$个元素的谜题由PCTLP.PGen$(\mathrm{pp},0^{\lambda};r_i)$计算得到，其中$\bar{I}^*$是$I^*$的补集。由于区分器是深度有限的，不可区分性来源于对伪链时间锁谜题PCTLP的安全性。

6)模拟器$\mathcal{S}$: 模拟器定义为与最后一个混合实验相同。值得注意的是，计算证明不使用关于证据的任何信息。证毕。

定理6 合理性。假设PCTLP是一个安全的时间锁谜题，则LVTS满足定义13中的合理性。

证明 首先分析协议的交互特点，由于Fiat-Shamir转换针对恒定轮次协议，因此非交互式协议的正确性可以得证。其次，假设敌手$\mathcal{A}$能够攻破方案的合理性，这意味着敌手生成承诺$(Z_1,\cdots,Z_n)$，使得对所有$Z_i \notin I$，都满足PCTLP.Solve$(\mathrm{pp},Z_i)=\tilde{f}(U_i)$，且

$$F(\tilde{f}(U_i)) \neq \sum_{j=0}^{t-1} F([s_i]U_i^j) \tag{10}$$

否则，可以通过插值定理$\tilde{f}(U_i)$与$\{f(U_i)\}_{i\in I}$恢复关于消息μ的有效签名。进一步，对于所有谜题$(Z_1,\cdots,Z_n)$是正确的，即解算法总是输出某一明确定义的值，除了一个可以忽略的概率。

因此，给定$(Z_1,\cdots,Z_n)$，本文可以恢复某个集合$I'=I$，这意味着证明者正确猜测了一个从恰好含$\frac{n}{2}$个0的字符串集合中均匀选择的随机n比特字符串，发生的概率是$\frac{\left(\frac{n}{2}!\right)^2}{n!}$。证毕。

3 基于比特币的链上电子拍卖协议

本节基于LVTS提出了一种基于比特币的链上电子拍卖协议[30]LVTS-EA，相比于目前基于时间释放的电子拍卖协议，LVTS-EA构建了链上隐私保护的惩罚机制，用于惩罚未及时投标的竞拍人。该协议的核心思想是竞拍人需要先做出投标承诺，然后在指定时间T内宣布投标结果，否则判定违约，其他人（即随机选择的竞拍人）可以使用LVTS获得惩罚交易T_{x_t}的最终签名，并生成惩罚交易获得补偿金。

3.1 区块链中的电子拍卖

电子拍卖流程如图2所示，本文方案中使用的系统参数如表1所示。

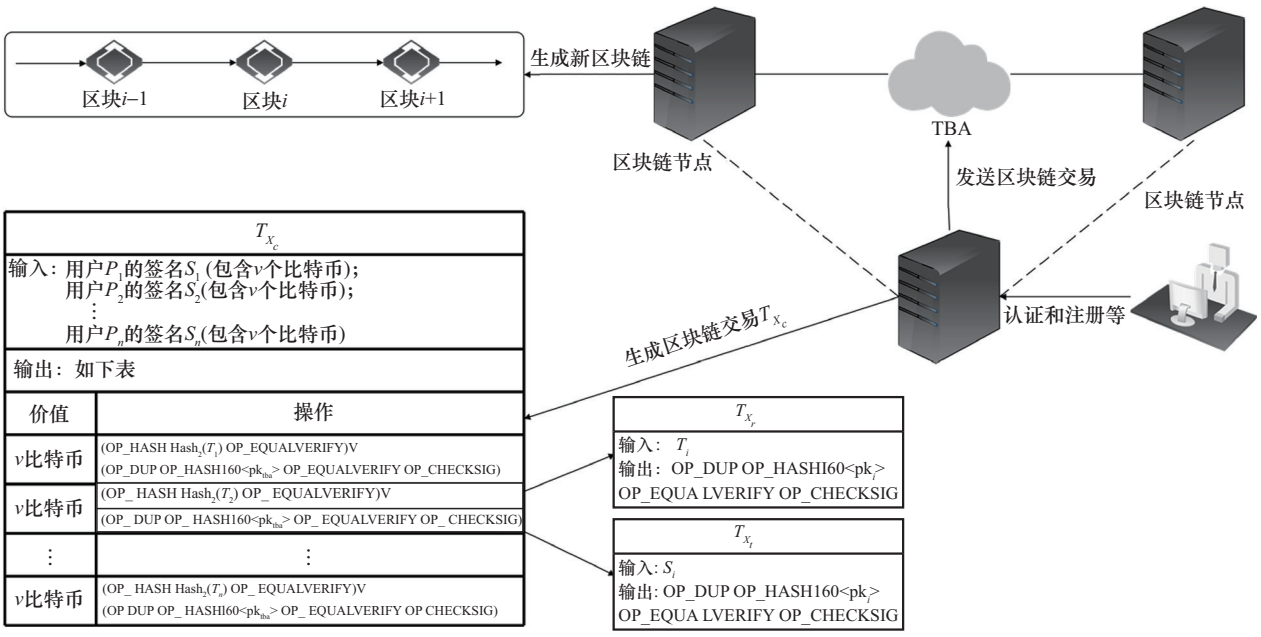

图2 电子拍卖流程

表1　　系统参数

符号	含义
P_i	竞拍人
T_{x_c}	担保交易
T_1	注册截止时间
OP_DUP	将堆栈顶部的元素复制到堆栈顶部
T_3	竞拍截止时间
OP_CHECKSIG	验证交易签名
cert_i	证书
TBA	可信拍卖中心
Hash_2	哈希函数$\{0,1\}^* \to \{0,1\}^{256}$
T_{x_r}	赎回交易
OP_HASH160	将栈顶元素散列到HASH160
OP_EQUALVERIFY	检查堆栈顶部的2个元素是否相等
T_2	承诺截止时间
T	解谜时间
T_{x_t}	惩罚交易
Obj	拍卖物

3.2　协议构造

1) 初始化。TBA生成crs_{rng},pp和比特币公私钥地址$(\text{pk}_{\text{TBA}},\text{sk}_{\text{TBA}})$。每个竞拍人$P_i$生成比特币地址$(\text{pk}_i,\text{sk}_i)$。TBA运行VTS.KeyGen生成密钥对$(\text{pk},\text{sk})$。

2) 注册。P_i需要在T_1前完成注册。每个竞拍人P_i发送身份信息ID给TBA，TBA检查竞拍人身份是否合格，若合格则颁发证书cert_i，并广播到公告栏上。

3) 承诺。对于每个拍卖物Obj，P_i需要在T_2前完成竞拍。每个竞拍人P_i给出竞拍价格p，并用私钥sk_i对p进行签名得到$\boldsymbol{s}_i$，上传承诺$\text{Hash}_2(\boldsymbol{s}_i)$到公告栏上。所有竞拍人共同发起交易$T_{x_c}$，$T_{x_c}$的输入是$n$个持有$v$个比特币的竞拍人，输出是$v$个比特币对应的$n$个输出，不考虑交易过程中产生的手续费。

每个输出需要满足以下2个条件：① 输出$\text{Hash}_2(\boldsymbol{s})$的原像；② 有与TBA公钥$\text{pk}_{\text{TBA}}$对应的签名。TBA将竞拍人列表$P_i(i\in[1,n])$打乱得到$P_{\hat{i}}(\hat{i}\in[1,n])$。TBA计算不含最终签名的惩罚交易$\{\tilde{T}_{x_t}\}_{\hat{i}}(\hat{i}\in[1,n])$，其输入是$T_{x_c}$的输出（条件②），输出是竞拍人的公钥$\text{pk}_{\hat{i}}$。

TBA计算$\boldsymbol{s}_{\hat{i}}=\text{Sign}(\text{sk},\text{Hash}_2(\{\tilde{T}_{x_t}\}_{\hat{i}}))(\hat{i}\in[1,n])$，可以得到$(C_{\hat{i}},\pi_{\hat{i}})\leftarrow\text{Commit}(\text{pk},\boldsymbol{s}_{\hat{i}},T,\text{crs})$，将$(C_{\hat{i}},\pi_{\hat{i}})$发送给每位竞拍人$P_{\hat{i}}$。每位竞拍人可以通过算法$\text{Verify}(C_{\hat{i}},\pi_{\hat{i}})$检验真伪。

4) 竞拍。P_i在T_3之前完成竞拍后，通过上传$\boldsymbol{s}_i$到公告栏发起交易T_{x_r}来赎回v个比特币。

5) 公布。如果竞拍人未在时间T之前发布竞拍结果，那么其他竞拍人可以通过计算$\text{ForceOpen}(C)$来获得签名$\boldsymbol{s}_{\hat{i}}$，并使用sk_{TBA}与TBA进行交互获得关于$\{\tilde{T}_{x_t}\}_{\hat{i}}$的最终签名$\boldsymbol{s}_{\hat{i}}'$从而获得$\{T_{x_t}\}_{\hat{i}}$，竞拍人上传$\{T_{x_t}\}_{\hat{i}}$和$\boldsymbol{s}_{\hat{i}}'$可以提取得到$v$个比特币。

6) 拍卖结算。对每一件Obj，TBA比较每一位竞拍人出价后，给出最高出价人的cert并授予购买资格。

3.3　方案分析

隐私保护。LVTS-EA采用零知识证明来确保竞拍的合法性，从而防止竞拍人隐私的泄露。

通用可验证性。LVTS-EA通过使用比特币存储投票信息，将竞拍人的承诺和拍卖结果公开记录在比特币网络上，与其他电子拍卖协议相比，任何人都可以验证和访问这些信息。

公平性。在LVTS-EA方案中，承诺和竞拍等关键操作都在区块链上进行，使得整个投票过程透明化，并可供任何人审计。这一机制有效防止了恶意TBA对竞拍结果的操纵，并通过链上证据识别竞拍中的任何不正当行为，因为区块链系统仅允许每个竞拍人对拍卖物进行一次出价。

链上隐私保护。LVTS-EA通过将传统的CLTV要求转换为标准的P2PKH交易，实现了部分链上隐私安全，避免了可能的隐私泄露问题。

4　性能评估

本节本文通过仿真实验分析了LVTS的时间效率，实验环境为Intel(R) Core(TM) i9-12900H@ 2.50 GHz处理器、16 GB运行内存、Ubuntu 20.04操作系统，基于NFLlib库用C++语言实现。

本文设计了一种基于格的可验证定时签名LVTS，并对该方案各个步骤的性能进行了详细的描述和呈现。由于目前没有其他同类型的方案，而本文方案在签名部分是抗量子的，因此在安全性方面具有一定的优势，但是不可避免地也会导致签名

时间和尺寸略长。

4.1 签名算法时间开销

表2给出了签名算法$\prod$(KeyGen,Sign,Verify)时间开销。通过改变与签名计算效率密切相关的安全参数n和高斯参数σ，签名时间和验证时间也随之改变。具体来说，随着n和σ变大，签名时间和验证时间随之增加。这是因为随着安全参数和高斯参数的增大，生成格签名所需的密钥也会变得更加复杂。密钥生成通常涉及复杂的数学运算和格结构的构建，因此会消耗更多的时间。其次，格签名的生成过程通常包括向量的加密、向量的线性变换和哈希等操作，这些操作的复杂度会随着安全和高斯参数的增大而增加，导致签名算法的时间开销增大。

表2 签名算法时间开销

安全参数n	高斯参数σ	生成密钥时间/ms	签名时间/ms	验证时间/ms
64	3	3	35.63	51.19
	5	1	34.39	50.72
	7	1	32.39	49.49
128	3	1	46.73	96.24
	5	1	73.55	96.16
	7	1	49.31	97.26
256	3	2	98.24	179.02
	5	2	128.84	188.12
	7	8	98.91	195.23
512	3	10	183.27	385.22
	5	4	189.35	395.73
	7	4	200.76	393.95
1 024	3	4	374.98	750.87
	5	8	359.67	769.54
	7	4	374.27	760.40
2 048	3	18	767.87	1 510.49
	5	10	153.83	1 520.57
	7	7	740.35	1 508.71

4.2 LVTS时间开销

图3展示了LVTS中Commit和ForceOpen算法的时间开销。设时间$T=2^k$，随着时间参数k值增大，时间开销也相应增加。分析表明，Commit和ForceOpen算法中涉及伪链时间锁谜题PCLTP和简洁非交互式零知识证明zkSNARK，伪链时间锁谜题通过增加计算量来延长解题时间。当时间T增加时，解题所需时间变长，需要更多计算操作才能找到解决方案，从而增加了计算开销。在简洁非交互式零知识证明中，生成证明是最耗时的环节，随着时间T的提升，证明者需要更多计算步骤来确保安全性和正确性，导致时间开销增加。

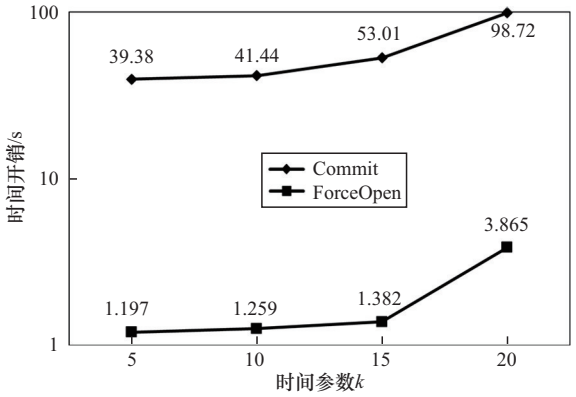

图3 LVTS时间开销

5 结束语

通过结合具有抗量子特性的非交互式门限秘密共享、伪链时间锁谜题和简洁非交互式零知识证明这些抗量子组件，并将其与抗量子基础签名方案巧妙结合，本文提出了一种基于格的可验证定时签名方案LVTS，该方案有效解决了现有VTS方案在后量子安全性上的缺陷，增强了LVTS的可验证性和整体安全性。本文给出了LVTS的方案定义、具体构造和安全模型，对该方案的安全性进行了完整的分析和证明。同时，本文还将LVTS与电子拍卖协议结合提出了一个实用的电子拍卖协议LVTS-EA，并通过仿真实验展示了LVTS在个人电脑上的实际应用性能。今后将继续优化LVTS方案，使其具备更好的性能和适用性。

参考文献：

[1] RIVEST R L, SHAMIR A, WAGNER D A. Time-lock puzzles and timed-release crypto[R]. 1996.

[2] MALAVOLTA G, THYAGARAJAN S A K. Homomorphic time-lock puzzles and applications[C]//Annual International Cryptology Conference. Berlin: Springer, 2019: 620-649.

[3] LIU Y, WANG Q, YIU S M. Towards practical homomorphic time-lock puzzles: applicability and verifiability[C]//European Symposium on Research in Computer Security. Berlin: Springer, 2022: 424-443.

[4] CHVOJKA P, JAGER T, SLAMANIG D, et al. Versatile and sustainable timed-release encryption and sequential time-lock puzzles (extended abstract) [C]//European Symposium on Research in Computer Security. Berlin: Springer, 2021: 64-85.

[5] LOE A, MEDLEY L, O'CONNELL C, et al. Applications of timed-release encryption with implicit authentication[C]//International Conference on Cryptology in Africa. Berlin: Springer, 2023: 490-515.

[6] BONEH D, NAOR M. Timed commitments[C]//Annual International Cryptology Conference. Berlin: Springer, 2000: 236-254.

[7] KATZ J, LOSS J, XU J Y. On the security of time-lock puzzles and timed commitments[C]//Theory of Cryptography. Berlin: Springer, 2020: 390-413.

[8] ARUN A, BONNEAU J, CLARK J. Short-lived zero-knowledge proofs and signatures[C]//International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2022: 487-516.

[9] THYAGARAJAN S A K, BHAT A, MALAVOLTA G, et al. Verifiable timed signatures made practical[C]//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2020: 1733-1750.

[10] MALAVOLTA G, MORENO-SANCHEZ P, KATE A, et al. Concurrency and privacy with payment-channel networks[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2017: 455-471.

[11] BONEH D, DRIJVERS M, NEVEN G. Compact multi-signatures for smaller blockchains[C]//International Conference on the Theory and Application of Cryptology and Information Securit. Berlin: Springer, 2018: 435-464.

[12] BENTOV I, KUMARESAN R. How to use bitcoin to design fair protocols[C]//Annual International Cryptology Conference. Berlin: Springer, 2014: 421-439.

[13] THYAGARAJAN S A, MALAVOLTA G, SCHMID F, et al. Verifiable timed linkable ring signatures for scalable payments for monero[C]//European Symposium on Research in Computer Security. Berlin: Springer, 2022: 467-486.

[14] ZHOU X T, HE D B, NING J T, et al. Efficient construction of verifiable timed signatures and its application in scalable payments[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 5345-5358.

[15] 侯慧莹, 宁建廷, 黄欣沂, 等. 可验证的属性基定时签名方案及其应用[J]. 软件学报, 2023, 34(5): 2465-2481.
HOU H Y, NING J T, HUANG X Y, et al. Verifiable attribute-based timed signatures and its applications[J]. Journal of Software, 2023, 34(5): 2465-2481.

[16] BAO Z J, HE D B, FENG Q, et al. Constant-size verifiable timed signatures from RSA group for bitcoin-based voting protocols[J]. IEEE Transactions on Services Computing, 2024, 17(4): 1414-1425.

[17] NIELSEN M A, CHUANG I L. Quantum computation and quantum information: 10th anniversary edition[M]. Cambridge: Cambridge University Press, 2010.

[18] SHOR P W. Algorithms for quantum computation: discrete logarithms and factoring[C]//Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS). Piscataway: IEEE Press, 1994: 124-134.

[19] ARUTE F, ARYA K, BABBUSH R, et al. Quantum supremacy using a programmable superconducting processor[J]. Nature, 2019, 574(7779): 505-510.

[20] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[C]//Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2009: 84-93.

[21] GOLDREICH O, GOLDWASSER S, HALEVI S. Public-key cryptosystems from lattice reduction problems[C]//Annual International Cryptology Conference. Berlin: Springer, 1997: 112-131.

[22] MICCIANCIO D, PEIKERT C. Trapdoors for lattices: simpler, tighter, faster, smaller[C]//European Cryptology Conference. Berlin: Springer, 2012: 700-718.

[23] NIST. NIST announces first four quantum-resistant cryptographic algorithms[R]. 2022.

[24] LYUBASHEVSKY V, MICCIANCIO D. Generalized compact knapsacks are collision resistant[C]//International Colloquium on Automata, Languages, and Programmin. Berlin: Springer, 2006: 144-155.

[25] PEIKERT C, ROSEN A. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices[C]//Theory of Cryptography. Berlin: Springer, 2006: 145-166.

[26] LAI R W F, CHEUNG H K F, CHOW S S M. Trapdoors for ideal lattices with applications[C]//International Conference on Information Security and Cryptology. Berlin: Springer, 2015: 239-256.

[27] RAJABI B, ESLAMI Z. A verifiable threshold secret sharing scheme based on lattices[J]. Information Sciences, 2019, 501: 655-661.

[28] AFSHAR A, CHUNG K M, HSIEH Y C, et al. On the (Im)possibility of time-lock puzzles in the quantum random oracle model[C]//International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2023: 339-368.

[29] ISHAI Y, SU H, WU D J. Shorter and faster post-quantum designated-verifier zkSNARKs from lattices[C]//Proceedings of the 2021 ACM

SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2021: 212-234.

[30] XIONG J, WANG Q. Anonymous auction protocol based on time-released encryption atop consortium blockchain[J]. International Journal of Advanced Information Technology, 2019, 9(1): 1-16.

[作者简介]

陈辉焱（1968– ），男，山东菏泽人，北京电子科技学院正高级工程师、博士生导师，主要研究方向为后量子密码、公钥密码等。

王庆楠（2000– ），男，广东汕头人，北京电子科技学院硕士生，主要研究方向为格密码理论应用与分析。

王克（1992– ），男，河南南阳人，博士，北京电子科技学院讲师，主要研究方向为基于格的密码方案的设计与分析。

谭舜聪（2000– ），男，重庆人，北京电子科技学院硕士生，主要研究方向为格密码理论应用与分析。

辛红彩（1991– ），女，河北邯郸人，博士，北京电子科技学院讲师，主要研究方向为信息处理与信息安全中的数学方法。