中国科学: 信息科学 2023 年 第 53 卷 第 12 期: 2472–2492
SCIENTIA SINICA Informationis
论文

多方 ARX 系统的协作安全辨识 —— 一种基于门限 Paillier 密码体制的最小二乘辨识方法

谭建伟[1,2], 王继民[3*], 张纪峰[1,2]

1. 中国科学院数学与系统科学研究院, 北京 100190
2. 中国科学院大学数学科学学院, 北京 100049
3. 北京科技大学自动化学院, 北京 100083
* 通信作者. E-mail: jimwang@ustb.edu.cn

收稿日期: 2023–05–14; 修回日期: 2023–07–04; 接受日期: 2023–08–02; 网络出版日期: 2023–12–11

国家重点研发计划 "变革性技术关键科学问题" 重点专项 (批准号: 2018YFA0703800) 和国家自然科学基金 (批准号: 62203045, T2293770) 资助项目

摘要 本文研究了多方参与的随机线性系统的协作安全参数辨识问题, 提出了一种基于门限 Paillier 密码体制的安全多方最小二乘辨识算法. 具体地, 通过对正负整数的合理编码, 将 (门限) Paillier 密码体制的加密对象及同态特性由非负整数扩展到了整数. 利用门限 Paillier 密码体制和将数据沿时间轴切分的方法, 设计了相应的安全多方参数辨识算法. 给出了算法正确加解密所需的明文空间大小条件、保证隐私安全性的时间切分长度条件以及一定条件下估计误差与加密量化误差之间的定量关系. 证明了, 只要选取的时间切分长度合适, 对于任意一个参与者, 即使其他所有参与者联合起来仍然无法得到其具体的隐私信息. 最后, 通过数值仿真验证了算法的有效性.

关键词 多方参与的 ARX 系统, 隐私安全, 系统辨识, 门限 Paillier 加密体制, 最小二乘方法

1 引言

随着计算机技术的不断发展及各种网络化系统, 如信息物理系统、传感器网络等大量涌现, 控制系统与信息网络的结合越来越紧密. 因此, 控制系统面临的安全风险也随之增加. 比如, 2010 年, "震网" 病毒 (Stuxnet) 利用工业控制系统漏洞入侵伊朗布尔什核电站, 通过获取历史运行信息进行重放攻击, 导致 1/5 的离心机报废, 核反应堆长时间无法运营 [1,2]. 这表明对控制系统的安全应该提出更高的要求, 即不仅要保证系统的正常运行, 也要保证系统的信息安全.

传统的信息安全主要是指保护信息及信息系统免受未经授权的进入、使用、破坏、修改、检视、记录等, 即经典的 CIA 三合体 (保密性、完整性、可用性). 经典的控制理论, 如鲁棒控制、适应控制

引用格式: 谭建伟, 王继民, 张纪峰. 多方 ARX 系统的协作安全辨识 —— 一种基于门限 Paillier 密码体制的最小二乘辨识方法. 中国科学: 信息科学, 2023, 53: 2472–2492, doi: 10.1360/SSI-2023-0140
Tan J W, Wang J M, Zhang J F. Cooperative secure parameter identification of multi-participant ARX systems — a threshold Paillier cryptosystem-based least-squares identification algorithm (in Chinese). Sci Sin Inform, 2023, 53: 2472–2492, doi: 10.1360/SSI-2023-0140

等 [3,4], 是以设计算法抵抗某种故障、扰动并保证系统的物理稳定运行来作为系统安全的考量的, 未充分考虑控制系统本身对信息安全的需要. 现阶段很多研究也主要集中于系统在遭受完整性攻击 (如拒绝服务攻击、重放攻击、欺骗攻击或者隐蔽攻击等) 时的检测和应对策略. 针对系统参数辨识过程中的隐私安全 (保密性) 的研究还相对较少. 事实上, 信息隐私安全至关重要 [5]. 对于控制系统而言, 系统的输入、状态和测量输出很可能蕴含输入者和被测量者的隐私或者机密信息, 该信息的泄露将对被泄露者造成恶劣影响. 如智能电网中, 家庭的用电量蕴含了家庭成员的日常活动信息; 多智能体系统中个体的位置、速度信息; 社交网络中, 参与者的观点信息等.

控制系统中的隐私保护问题已引起控制界的关注, 常用的方法有差分隐私、同态加密和基于安全系统结构的技术等 [6]. 比如, 利用差分隐私方法, 隐私保护下的 Kalman 滤波算法 [7] 和分布式参数估计算法 [8] 分别得到了研究. 但该方法需要引入额外噪声用于数据扰动, 往往在保护隐私的同时降低了系统的性能. 从系统的能观性出发 [9], 利用系统状态和输入信息构造扰动信号加到原来系统的状态和输出上, 在保持原来系统可控的条件下, 使得系统不可观, 从而防止攻击者由输出确定系统的输入及初始状态. 但该方法要求系统各节点相互信任, 且会导致系统结构上的改变. 密码学在隐私保护问题中得到了充分的研究 [10~15]. 作为一种特殊的密码学技术, 同态加密支持密文层面的加法或者乘法运算, 从而实现数据的 “可算不可见”. 同态加密得到的密文计算结果在进行对应的同态解密后的明文等同于对明文数据直接进行相同的计算, 现已被用来研究控制系统中的隐私保护问题. 比如, 利用同态加密方法, 常值输入量化输出情形下的随机线性系统的安全参数辨识问题 [16,17], 分布式趋同控制 [18,19] 和分布式优化 [20] 的隐私保护问题分别得到了研究. 需要指出的是, 存在的 Paillier 密码体制只能对非负整数进行加密 [18~20]. 实际中控制系统的输入输出信息往往是用实数表示的, 甚至可能为负数, 所以有必要将 Paillier 密码体制的明文空间扩展到实数 (包括负整数).

最小二乘方法作为数据分析和系统辨识的最基本方法之一, 已经取得了一系列的理论成果, 并且已经应用于众多领域, 如工程系统、社会系统、生物系统、经济系统等 [21~25]. 随着数据时代智能化的发展, 相当多的系统辨识问题中会涉及隐私数据, 因此需要考虑同时实现系统辨识和隐私保护的方法. 受到关于安全求解线性方程组应用的工作 [14] 及关于固定输入下集值系统的辨识算法 [16] 启发, 我们将门限 Paillier 同态密码体制应用于多方参与的随机线性系统的协作安全辨识问题中, 提出了基于门限 Paillier 密码体制的安全多方最小二乘辨识算法. 该算法能保证每个参与者在不泄露自己输入的情况下, 与其他参与者协作辨识出系统参数, 具有密码学意义下的安全性. 本文的主要贡献如下:

(i) 针对多方参与的随机线性系统, 本文提出了基于门限 Paillier 密码体制的隐私安全多方最小二乘参数辨识方法. 利用正负整数的合理编码, 使得门限 Paillier 密码体制能够适用于负整数并保持其同态特性; 利用门限 Paillier 加密体制和将数据在时间上切分的思想, 设计了相应的安全多方辨识算法. 与现有相关文献相比 [18~20], 本文详细地说明了 Paillier 密码体制如何能够适用于负整数并保持其同态特性. 与 Xu 等 [16] 的工作相比, 问题模型中的输入不再是常值输入, 而是可以在某一有界范围内自由选取.

(ii) 针对所提的隐私保护算法, 本文给出了正确加密解密所需要的明文空间大小条件, 保证隐私安全性下的沿时间轴切分的长度条件, 以及在几乎处处意义下算法估计误差与加密带来的量化误差之间的定量关系, 由此表明了可通过选取合适的量化误差使得估计误差任意小.

本文其余部分结构安排如下: 第 2 节介绍问题模型和相关基础知识, 第 3 节将详细叙述安全算法的设计, 第 4 节分析算法的正确加解密条件、安全性和收敛误差; 第 5 节给出算法的仿真验证; 最后, 第 6 节将对本文作出总结.

符号说明. 本文使用符号 $\mathbb{R}$, $\mathbb{Z}$ 和 $\mathbb{N}$ 分别表示实数集, 整数集和非负整数集. $\mathbb{R}^n$ 表示 n 维欧氏

空间或 n 维实数列向量的集合. $\mathbb{Z}_n$ 和 $\mathbb{Z}_n^*$ 分别表示集合 $\{0,1,\ldots,n-1\}$ 和 $\{z\in\mathbb{Z}_n|\gcd(z,n)=1\}$. $a\equiv_n b$ 表示 a 和 b 在模 n 意义下同余. $\gcd(a,b)$ 表示整数 a 和 b 的最大公约数. mod 表示模运算, 即 $a \mod n = a - n*\lfloor\frac{a}{n}\rfloor$. 对于任意的 $x\in\mathbb{R}$, $\lfloor x\rfloor=\max\{z\in\mathbb{Z}|z\leqslant x\}$ 和 $\lceil x\rceil=\min\{z\in\mathbb{Z}|z\geqslant x\}$. $[v]_i$ 和 $[M]_{i,j}$ 分别表示向量 v 的第 i 个分量和矩阵 M 的第 i 行第 j 列的分量. $\|v\|$ 表示向量 v 的 2-范数. $\|M\|$ 表示矩阵 M 的 2- 范数, 若 $M\in\mathbb{R}^{m\times n}$, 则 $\|M\|=\sup_{\|x\|=1}\|Mx\|$. $\lambda_{\max}(M)$ 和 $\lambda_{\min}(M)$ 分别表示矩阵 M 的最大特征值和最小特征值.

2 问题描述及相关基础知识

2.1 问题描述及目标

考虑如下多参与者的安全多方参数辨识模型:

$$\begin{aligned}y_{k+1}=&\,a_1y_k+a_2y_{k-1}+\cdots+a_{n_0}y_{k-n_0+1}\\&+b_{1,1}u_{1,k}+b_{1,2}u_{1,k-1}+\cdots+b_{1,n_1}u_{1,k-n_1+1}\\&+b_{2,1}u_{2,k}+b_{2,2}u_{2,k-1}+\cdots+b_{2,n_2}u_{2,k-n_2+1}\\&\vdots\\&+b_{m_0,1}u_{m_0,k}+b_{m_0,2}u_{m_0,k-1}+\cdots+b_{m_0,n_{m_0}}u_{m_0,k-n_{m_0}+1}\\&+\omega_{k+1},\quad\forall k\in\mathbb{N},\end{aligned}\tag{1}$$

其中 m_0 为输入参与者总数; $n_i, i=0,1,\ldots,m_0$ 为已知的系统阶数; $y_k\in\mathbb{R}$, $u_{i,k}\in\mathbb{R}$ 和 $\omega_k\in\mathbb{R}$ 分别为 k 时刻系统的输出、第 i 个参与者 $\mathcal{P}_i$ 的输入和系统噪声; $a_1,\ldots,a_{n_0}$ 和 $b_{i,1},\ldots,b_{i,n_i}, i=1,2,\ldots,m_0$ 为系统的未知参数. 我们称如式 (1) 描述的多方参与的 ARX 模型 [25] 为 MP-ARX (ARX model with multi-participants) 系统.

记待估参数个数为 $d_1=\sum_{i=0}^{m_0}n_i$, 相应的参数向量和回归向量为

$$\begin{aligned}\theta&=[a_1,\ldots,a_{n_0},b_{1,1},\ldots,b_{1,n_1},\ldots,b_{m_0,1},\ldots,b_{m_0,n_{m_0}}]^{\mathrm{T}},\\\varphi_k&=[y_k,\ldots,y_{k-n_0+1},u_{1,k},\ldots,u_{1,k-n_1+1},\ldots,u_{m_0,k},\ldots,u_{m_0,k-n_{m_0}+1}]^{\mathrm{T}},\end{aligned}$$

则系统 (1) 可简写为

$$y_{k+1}=\theta^{\mathrm{T}}\varphi_k+\omega_{k+1},\quad\forall k\in\mathbb{N}.\tag{2}$$

为叙述方便, 我们假定系统输出 y_k 由参与者 $\mathcal{P}_0$ 所有. 我们的目标是设计一种算法使得所有 m_0+1 个参与者能够协作地辨识出系统参数 θ, 同时保证在辨识过程中或者辨识完成后, 每个参与者都不能获得其他参与者拥有的具体隐私数据, 即 y_k 或者 $u_{i,k}$, 实现安全多方参数辨识.

注释1 这里的攻击者是对其他参与者隐私信息感兴趣的某个或者某些参与者, 且此攻击者会严格执行相应的协议, 仅根据在交互过程中得到的信息去推测其他参与者的隐私信息. 这类参与者被称为被动攻击者; 而其他参与算法协议的非攻击者被称为诚实参与者. 事实上, 本文所说的安全性结论可以自然地扩展到其他被动攻击者类型, 如能够获取参与者间通信信息的窃听类攻击者. 另外, 攻击者的能力还可以进一步加强, 如某些参与者还可能相互联合, 共享更多的中间信息来推测剩余参与者的信息, 这会在稍后的安全性相关结论中予以更明确的说明.

2.2 最小二乘估计

记 k 时刻系统的参数估计为 θ_k, 系统 "累积预报误差" 定义为

$$J_k(\theta) \triangleq \sum_{i=1}^{k}(y_i - \theta^{\mathrm{T}}\varphi_{i-1})^2.$$

注意到上式为关于 θ 的二次型, 我们通过对 θ 求导并令其等于 0, 可得到使 $J_k(\theta)$ 取极小值的 θ_k, 即相应的最小二乘估计:

$$\theta_k = \left(\sum_{i=0}^{k-1}\varphi_i\varphi_i^{\mathrm{T}}\right)^{\dagger}\left(\sum_{i=0}^{k-1}\varphi_i y_{i+1}\right), \tag{3}$$

其中 $A^{\dagger}$ 表示矩阵 A 的伪逆. 进一步, 当 $\sum_{i=0}^{k-1}\varphi_i\varphi_i^{\mathrm{T}}$ 可逆时, 式 (3) 中 $(\sum_{i=0}^{k-1}\varphi_i\varphi_i^{\mathrm{T}})^{\dagger}$ 变成 $(\sum_{i=0}^{k-1}\varphi_i\varphi_i^{\mathrm{T}})^{-1}$.

2.3 (m_0+1, m_0+1)- 门限 Paillier 密码体制

为解决隐私保护的问题, 我们引入 Paillier 密码体制 [11]. 由于有 m_0+1 个参与者共同辨识参数, 我们希望即使有 m_0 个参与者联合起来仍然无法得到最后一个参与者的隐私信息, 故采用门限化的 Paillier 密码体制 [12, 13]. 下面给出 (m_0+1, m_0+1)- 门限 Paillier 密码体制 [14], 即该密码体制有 m_0+1 个子密钥且只有当 m_0+1 个子密钥所有者都同意解密时才能进行正确解密.

具体算法描述如下:

• **密钥生成.** 生成器选取大整数 $N = pq$, 其中 $p = 2p'+1$, $q = 2q'+1$, p', q', p, q 均为素数, 且 $\gcd(N, \phi(N)) = \gcd(pq, (p-1)(q-1)) = 1$. 令 $M = p'q'$, 选择 $k_{\mathcal{P}}$ 和 e 满足 $k_{\mathcal{P}} \equiv_M 0$, $k_{\mathcal{P}}e \equiv_N 1$. 随机选择 $b \in \mathbb{Z}_N^*$, 令 $g = (1+N)^e b^N \mod N^2$, 则公钥为 (N, g), 私钥为 $k_{\mathcal{P}}$.

• **私钥分配.** 生成器随机选取 $k_{\mathcal{P}_0}, k_{\mathcal{P}_1}, \ldots, k_{\mathcal{P}_{m_0}}$ 使得 $k_{\mathcal{P}} \equiv_{NM} k_{\mathcal{P}_0} + k_{\mathcal{P}_1} + \cdots + k_{\mathcal{P}_{m_0}}$, 将 $k_{\mathcal{P}_i}$ 传递给参与者 $\mathcal{P}_i$ 作为其私钥, $i = 0, 1, \ldots, m_0$.

• **加密.** 对于任意的明文 $m \in \mathbb{Z}_N$, 加密者在 $\mathbb{Z}_N^*$ 中随机选取 $h \in \mathbb{Z}_N^*$, 密文

$$c = \mathcal{E}(m) \triangleq g^m h^N \mod N^2. \tag{4}$$

• **解密.** 对于 $i = 0, 1, \ldots, m_0$, 参与者 $\mathcal{P}_i$ 计算 $c_i = c^{2k_{p_i}} \mod N^2$, 则

$$m = \mathcal{D}(c) \triangleq \frac{(\prod_{i=0}^{m_0} c_i \mod N^2) - 1}{N} \cdot \frac{N+1}{2} \mod N. \tag{5}$$

注释2 该门限密码体制与 Paillier 密码体制一样, 明文空间为 $\mathbb{Z}_N$, 密文空间为 $\mathbb{Z}_{N^2}^*$. 其加密安全性建立在 "判定复合剩余类是困难的" 的假设上, 能够抵御选择密文攻击 (一种针对加密体制的强攻击方式) [10~12].

注释3 密钥生成阶段所用到的素数 p' 和 q' 满足 $2p'+1$ 和 $2q'+1$ 也是素数, 这样的 p' 和 q' 称为 Sophie Germain 素数; 相应的 $p = 2p'+1$ 和 $q = 2q'+1$ 称为安全素数. 此外, 当 p' 和 q' 以二进制表示且具有相同的表示长度时, 密钥生成阶段所需的要求 $\gcd(N, \phi(N)) = 1$ 会自动满足 (见 [10], 492 页).

注释4 (m_0+1, m_0+1)- 门限 Paillier 密码体制继承了 Paillier 密码体制的良好特性. 对任意的明文 $m_1, m_2 \in \mathbb{Z}_N$, 有

• 加法同态性: $\mathcal{D}(\mathcal{E}(m_1)\cdot\mathcal{E}(m_2))=m_1+m_2 \mod N$, 即

$$\mathcal{E}(m_1+m_2)=\mathcal{E}(m_1)\cdot\mathcal{E}(m_2) \mod N^2; \tag{6}$$

• 密文隐藏性: 设 $c=\mathcal{E}(m)$, 对任意 $h'\in\mathbb{Z}_N^*$, 有 $\mathcal{D}(ch'^N \mod N^2)=m$, 即 $ch'^N \mod N^2$ 也是 m 的密文. 这意味着我们可以对密文进行随机修改但能保证解密结果不变. 这是由 Paillier 密码体制密文的不惟一性决定的[11].

注释5 利用整数加法和整数乘法的关系, 以及式 (6), 可以得到 Paillier 密码体制的如下伪乘法同态性: 设 m_1 和 m_2 为两个明文, 则

$$\begin{aligned}\mathcal{E}(m_1\cdot m_2)&=[\mathcal{E}(m_1)]^{m_2} \mod N^2\\&=[\mathcal{E}(m_2)]^{m_1} \mod N^2.\end{aligned} \tag{7}$$

注意, 上式中 $\mathcal{E}(m_1\cdot m_2)$ 并非完全由密文计算得出的, 所以式 (7) 并不是真正的乘法同态特性.

注释6 为下文叙述方便, 对矩阵 $M\in\mathbb{Z}_N^{k\times l}$, 我们用 $\mathcal{E}(M)$ 表示对矩阵 M 中元素加密后得到的加密矩阵, 即 $[\mathcal{E}(M)]_{i,j}=\mathcal{E}([M]_{i,j})$, $\forall 1\leqslant i\leqslant k$, $1\leqslant j\leqslant l$.

3 算法设计

观察式 (3) 可知, 想要保护的隐私信息出现在 $\varphi_k\varphi_k^{\mathrm{T}}$ 和 $\varphi_k y_{k+1}$ 中. 要实现最小二乘估计的安全计算, 一个简单的想法是: 首先, 将时间轴以某个长度, 比如说 T_0, 分段; 然后, 安全计算出前述两项在每个时间段的累加和; 最后, 将累加所得结果代入式 (3) 即可. 如此, 算法设计的难点变成了如何实现 $\varphi_k\varphi_k^{\mathrm{T}}$ 和 $\varphi_k y_{k+1}$ 在每个时间段内的计算, 同时还不泄露每个诚实参与者的隐私数据. 我们引入门限 Paillier 密码体制来解决这个问题. 具体的设计过程及关键点如下.

3.1 输入输出的整数化

首先注意到, Paillier 密码体制的明文空间是 $\mathbb{Z}_N$, 即其加密对象为 $\mathbb{Z}_N$ 中的整数, 而实际中我们遇到的输入输出信息往往是用实数表示的. 故需要在加密前将输入输出信息转化为整数. 我们采用将原有数据扩大 τ 倍后再截取整数部分的方法来实现.

扩大取整后的回归向量和输出分别为

$$\bar{\varphi}_k=[\lceil\tau y_k\rceil,\ldots,\lceil\tau y_{k-n_0+1}\rceil,\lceil\tau u_{1,k}\rceil,\ldots,\lceil\tau u_{1,k-n_1+1}\rceil,\ldots,\lceil\tau u_{m_0,k}\rceil,\ldots,\lceil\tau u_{m_0,k-n_{m_0}+1}\rceil]^{\mathrm{T}}, \tag{8}$$

$$\bar{y}_k=\lceil\tau y_k\rceil, \tag{9}$$

此即为真正的加密对象. 自然地, 我们也可以将式 (8) 和 (9) 恢复, 有

$$\hat{\varphi}_k=\frac{1}{\tau}\bar{\varphi}_k,$$
$$\hat{y}_k=\frac{1}{\tau}\bar{y}_k.$$

显然, 此时有 $|\hat{y}_k-y_k|\leqslant\frac{1}{\tau}$, $|[\hat{\varphi}_k]_i-[\varphi_k]_i|\leqslant\frac{1}{\tau}$, $i=1,2,\ldots,d_1$. 于是我们定义这个过程的整数化误差 δ 为

$$\delta\triangleq\frac{1}{\tau},\ \tau\geqslant 1.$$

注释7 我们以引入整数化误差 δ 来换取 Paillier 密码体制在实数数据上的应用. 这里为方便, 取整函数采用向上取整形式, 实际应用中还可以采用向中间取整的方法来得到更小的量化误差, 从而使估计误差更小. 具体来说, 整数化误差 δ, 或者说参数 τ 的选取依赖于应用中对估计误差的容忍度, 越小的 δ 意味着越精确的参数估计, 详见后面的误差分析定理.

3.2 加密对象及同态运算的扩展

注意到实际问题中, 系统输入及输出可能为负数, 而 2.3 小节中的门限密码体制只能对非负整数进行加密, 所以需要将 Paillier 密码体制的明文空间扩展到负整数. 其次, 式 (6) 和 (7) 的同态性只针对 $\mathbb{Z}_N$ 上的整数成立, 也需要扩展到负整数.

受计算机中的补码运算 (见 [26], 2.2 小节) 启发, 可以将 $\mathbb{Z}_N$ 视为模 N 下的整数环, 对给定的正整数 N, 定义如下模 N 意义下的正整数和负整数:

定义1 给定正整数 $N>0$, 定义整数 m 在模 N 意义下的表示为 $m^{(N)} \triangleq m \mod N$.

为叙述方便, 我们用 $v^{(N)}$ 表示向量 v 中分量转化为其在模 N 下表示后所得的向量, 即 $[v^{(N)}]_i = ([v]_i)^{(N)}$; 用 $M^{(N)}$ 表示矩阵 M 中元素转化为其在模 N 下表示后所得的矩阵, 即 $[M^{(N)}]_{i,j} = ([M]_{i,j})^{(N)}$.

注释8 当 N 为前述 Paillier 密码体制所用模数时, 记 $\mathscr{M}^{(N)} = \{-\frac{N-1}{2}, -\frac{N-3}{2}, \ldots, \frac{N-1}{2}\}$. 若限制 $m \in \mathscr{M}^{(N)}$, 则定义 1 给出了 $\mathscr{M}^{(N)}$ 到 $\mathbb{Z}_N$ 的一一对应, 即对于由 m 得到 $m^{(N)}$ 这样的编码过程, 等价地有

$$m^{(N)} = \begin{cases} m, & \text{当 } m = 0, 1, \ldots, \frac{N-1}{2} \text{ 时}, \\ N+m, & \text{当 } m = -\frac{N-1}{2}, -\frac{N-3}{2}, \ldots, -1 \text{ 时}. \end{cases}$$

对应地, 由 $m^{(N)}$ 得到 m 的解码过程为

$$m = \begin{cases} m^{(N)}, & \text{当 } m^{(N)} = 0, 1, \ldots, \frac{N-1}{2} \text{ 时}, \\ m^{(N)} - N, & \text{当 } m^{(N)} = \frac{N+1}{2}, \frac{N+3}{2}, \ldots, N-1 \text{ 时}. \end{cases} \tag{10}$$

例如, 当给定 $N=11$ 时, $2^{(N)}=2$, $-2^{(N)}=9$; 数字 8 实际表示负整数 $-3=8-11$, 即 $(-3)^{(N)}=8$.

注释9 在定义 1 下, 由模运算性质知, 对任意整数 m_1 和 m_2 有

$$(m_1+m_2)^{(N)} = m_1^{(N)} + m_2^{(N)} \mod N, \tag{11}$$

$$(m_1-m_2)^{(N)} = m_1^{(N)} + (-m_2)^{(N)} \mod N, \tag{12}$$

$$(m_1 m_2)^{(N)} = m_1^{(N)} m_2^{(N)} \mod N. \tag{13}$$

于是, 利用定义 1, 我们构建了含负整数的集合 $\mathscr{M}^{(N)}$ 到 Paillier 密码体制明文空间 $\mathbb{Z}_N$ 的同态映射, 其满足加法与乘法同态. 这样就在 $\mathbb{Z}_N$ 中解决了 $\mathscr{M}^{(N)}$ 中的两个问题: (1) 正负整数的表示问题; (2) 加、减和乘运算的定义及计算问题. 从而, 对负整数 m 的加密及计算就可以转化为对 $m^{(N)}$ 的加密与计算.

对于上述模 N 意义下的整数, 所给出的门限 Paillier 密码体制 (包括传统 Paillier 密码体制) 具有以下性质:

命题1 在所给出的门限 Paillier 密码体制中, 对任意整数 m_1, m_2, 有

$$\mathcal{E}((m_1+m_2)^{(N)}) = \mathcal{E}(m_1^{(N)})\mathcal{E}(m_2^{(N)}) \mod N^2, \tag{14}$$

$$\mathcal{E}((-m_1)^{(N)}) = [\mathcal{E}(m_1^{(N)})]^{-1} \mod N^2, \tag{15}$$

$$\mathcal{E}((m_1 m_2)^{(N)}) = [\mathcal{E}(m_1^{(N)})]^{m_2^{(N)}} \mod N^2. \tag{16}$$

证明 由式 (4) 和 (11) 可知, 存在 $h_0 \in \mathbb{Z}_N^*$ 使得

$$\begin{aligned}\mathcal{E}((m_1+m_2)^{(N)}) &= \mathcal{E}(m_1^{(N)} + m_2^{(N)} \mod N)\\ &= g^{m_1^{(N)}+m_2^{(N)} \mod N} h_0^N \mod N^2\\ &= g^{m_1^{(N)}} 1^N g^{m_2^{(N)}} h_0^N \mod N^2\\ &= \mathcal{E}(m_1^{(N)})\mathcal{E}(m_2^{(N)}) \mod N^2,\end{aligned}$$

从而式 (14) 成立.

设 $\mathcal{E}(m_1^{(N)}) = g^{m_1^{(N)}} h_1^N \mod N^2$. 由 $\gcd(1+N, N^2) = 1$, $b \in \mathbb{Z}_N^*$, $h_1 \in \mathbb{Z}_N^*$ 和 g 的取法 (见密钥生成阶段), 知 g, h_1 在模 N^2 下可逆. 设 $\gamma = g^{-1}h_1^{-1} \mod N^2$, 则存在 $k \in \mathbb{Z}$ 使得 $g^{-1}h_1^{-1} = kN + \gamma$, $0 \leqslant \gamma < N$. 考虑二项展开式 $(g^{-1}h_1^{-1})^N = (kN+\gamma)^N = \gamma^N + \binom{N}{1}\gamma^{N-1}kN + \cdots$, 可知 $(g^{-1}h_1^{-1})^N \equiv_{N^2} (g^{-1}h_1^{-1} \mod N)^N$. 同理, 有 $(h_1^{-1})^N \equiv_{N^2} (h_1^{-1} \mod N)^N$. 进而, 由

$$\begin{aligned}[\mathcal{E}(m_1^{(N)})]^{-1} \mod N^2 &= (g^{m_1^{(N)}} h_1^N)^{-1} \mod N^2\\ &= (g^{-1})^{m_1^{(N)}} (h_1^{-1})^N \mod N^2\\ &= \begin{cases} g^{-m_1+N}(g^{-1}h_1^{-1})^N \mod N^2 & \text{若} \quad m_1 \geqslant 0\\ g^{-m_1}(h_1^{-1})^N \mod N^2 & \text{若} \quad m_1 < 0 \end{cases}\\ &= \begin{cases} g^{(-m_1)^{(N)}}(g^{-1}h_1^{-1} \mod N)^N \mod N^2 & \text{若} \quad m_1 \geqslant 0\\ g^{(-m_1)^{(N)}}(h_1^{-1} \mod N)^N \mod N^2 & \text{若} \quad m_1 < 0 \end{cases}\\ &= \mathcal{E}((-m_1)^{(N)}),\end{aligned}$$

因此式 (15) 成立.

设 $\gamma' = m_1^{(N)} m_2^{(N)} \mod N$, 则存在 $k' \in \mathbb{Z}$ 使得 $m_1^{(N)} m_2^{(N)} = k'N + \gamma'$. 于是

$$\begin{aligned}g^{m_1^{(N)} m_2^{(N)}} &\equiv_{N^2} (1+N)^{e(k'N+\gamma')} b^{N(k'N+\gamma')}\\ &\equiv_{N^2} [(1+N)^e b^N]^{\gamma'} [(1+N)^{ek'} b^{k'N}]^N\\ &\equiv_{N^2} g^{m_1^{(N)} m_2^{(N)} \mod N} [(1+N)^{ek'} b^{k'N}]^N.\end{aligned}$$

类似前面对 $g^{-1}h_1^{-1}$ 的讨论, 可知 $[(1+N)^{ek'} b^{k'N} h_1^{m_2^{(N)}}]^N \equiv_{N^2} [(1+N)^{ek'} b^{k'N} h_1^{m_2^{(N)}} \mod N]^N$, 其中 $(1+N)^{ek'} b^{k'N} h_1^{m_2^{(N)}} \mod N \in \mathbb{Z}_N^*$. 从而根据式 (13) 有

$$\begin{aligned}[\mathcal{E}(m_1^{(N)})]^{m_2^{(N)}} \mod N^2 &= [g^{m_1^{(N)}} h_1^N \mod N^2]^{m_2^{(N)}} \mod N^2\\ &= [g^{m_1^{(N)} m_2^{(N)}} h_1^{m_2^{(N)} N}] \mod N^2\\ &= g^{m_1^{(N)} m_2^{(N)} \mod N} [(1+N)^{ek'} b^{k'N} h_1^{m_2^{(N)}} \mod N]^N \mod N^2\\ &= \mathcal{E}((m_1 m_2)^{(N)}),\end{aligned}$$

故式 (16) 成立.

注释10 式 (14) 给出了模 N 表示下 Paillier 密码体制的加法同态特性, 式 (16) 给出了模 N 表示下 Paillier 密码体制的伪乘法同态特性, 此二式可以看作是对原来同态特性的拓展, 将同态特性从只包含正整数的 $\mathbb{Z}_N$ 上拓展到了包含正负整数的 $\mathscr{M}^{(N)}$ 上. 形式上, 它们与未拓展前的式 (6) 和 (7) 非常相似. 这是由于 Paillier 密码体制是从 $\mathbb{Z}_N\times\mathbb{Z}_N^*\to\mathbb{Z}_{N^2}^*$ 上的同构映射 [11], 明文空间 $\mathbb{Z}_N$ 本身构成了一个加法交换群; 同时, $\mathbb{Z}_N^*$ 中不同元都可以与 $\mathbb{Z}_N$ 中的同一个明文联系得到形式不同但解密结果相同的密文, 即加密过程式 (4) 中 h 的选择对于一个完整的加密、解密过程的正确性无影响, 只起到进一步混淆密文的目的.

注释11 在命题 1 条件下, 当 $m_2<0$ 时, 由定义 1 知 $m_2^{(N)}>|m_2|$. 因此, 利用式 (16) 计算 $\mathcal{E}((m_1m_2)^{(N)})$ 时会涉及较多的求幂运算. 利用式 (15) 可以减少这部分运算. 事实上, 注意到 $(m_1m_2)^{(N)}=(-m_1|m_2|)^{(N)}$ 和 $|m_2|^{(N)}=|m_2|$, 由式 (15) 和 (16) 有

$$\begin{aligned}\mathcal{E}((m_1m_2)^{(N)})&=\mathcal{E}((-m_1|m_2|)^{(N)})\\&=[\mathcal{E}((-m_1)^{(N)})]^{|m_2|}\mod N^2\\&=\{[\mathcal{E}((m_1)^{(N)})]^{-1}\}^{|m_2|}\mod N^2.\end{aligned}$$

从而通过求取 $\mathcal{E}((m_1)^{(N)})$ 在模 N^2 下的逆, 将幂运算次数从 $m_2^{(N)}$ 降到了 $|m_2|$.

3.3 安全多方最小二乘辨识算法

利用最小二乘估计式 (3)、门限 Paillier 密码体制及其扩展的同态特性, 我们设计如下安全多方辨识算法.

为方便产生密钥并将其安全地分发给所有参与者, 我们假定在算法准备阶段有一个可信第三方 (如某个参与者) 存在. 在算法执行阶段此第三方将不再需要.

算法准备阶段. 可信第三方选取整数化误差 δ (等价地说, 整数化参数 τ)、时间分段长度 T_0 和 $d_1\times d_1$ 常数正定矩阵 $\bar{P}_0$. 然后, 其按照前述的 (m_0+1,m_0+1)- 门限 Paillier 密码体制的密钥生成方法, 生成公钥 (N,g) 和私钥 $(k_{\mathcal{P}_0},k_{\mathcal{P}_1},\dots,k_{\mathcal{P}_{m_0}})$. 可信第三方将公钥 (N,g)、整数化参数 τ 和常数正定矩阵 $\bar{P}_0$ 广播给所有参与者; 将私钥 $k_{\mathcal{P}_i}$ 秘密地发送给参与者 $\mathcal{P}_i$.

在此准备阶段, 所有参与者都掌握公钥 (N,g), 整数化误差参数 $\delta=\frac{1}{\tau}$ 和常数正定矩阵 $\bar{P}_0$. 对 $i=0,1,\dots,m_0$, 参与者 $\mathcal{P}_i$ 单独掌握的信息有

- 隐私信息 y_k ($i=0$ 时) 或者 $u_{i,k}$ ($i=1,2,\dots,m_0$ 时);
- 私钥 $k_{\mathcal{P}_i}$.

算法执行阶段. 记 $\tau_k=\lfloor\frac{k}{T_0}\rfloor$, $\bar{S}_{\tau_k}=\sum_{i=0}^{T_0-1}\bar{\varphi}_{\tau_kT_0+i}\bar{\varphi}_{\tau_kT_0+i}^{\mathrm{T}}$, $\bar{R}_{\tau_k}=\sum_{i=0}^{T_0-1}\bar{\varphi}_{\tau_kT_0+i}\bar{y}_{\tau_kT_0+i+1}$. 对每一个时刻 $k\geqslant 1$, 参与者执行如下步骤.

步骤 1. 计算 $\mathcal{E}(\bar{\varphi}_{k-1}^{(N)})$. 具体过程为: 参与者 $\mathcal{P}_i$ 先按照式 (8) 和 (9) 整数化自己的隐私信息, 再按照定义 1 将整数化结果转化为模 N 意义下的表示, 最后按式 (4) 加密转化后的结果并将加密结果广播给所有参与者.

步骤 2. 计算 $\mathcal{E}((\bar{\varphi}_{k-1}\bar{\varphi}_{k-1}^{\mathrm{T}})^{(N)})$ 和 $\mathcal{E}((\bar{\varphi}_{k-1}\bar{y}_k)^{(N)})$. 具体过程为: 对 $j_1=0,1,\dots,n_0$, $j_2=1,2,\dots,n_0$, 参与者 $\mathcal{P}_0$ 加密 $(\bar{y}_{k-j_1}\bar{y}_{k-j_2})^{(N)}$; 再利用 $\mathcal{E}(\bar{\varphi}_{k-1}^{(N)})$ 和命题 1, 对 $i=1,2,\dots,m_0,j_1=0,1,\dots,n_0,j_2=1,2,\dots,n_i$ 计算 $\mathcal{E}((\bar{y}_{k-j_1}\bar{u}_{i,k-j_2})^{(N)})$; 如此得到 $\mathcal{E}((\bar{y}_{k-j}\bar{\varphi}_{k-1})^{(N)})$, 其中 $j=0,1,\dots,n_0$. 同理, 当 $i=1,2,\dots,m_0$ 时, 对 $j_1,j_2=1,2,\dots,n_i$, 参与者 $\mathcal{P}_i$ 加密 $(\bar{u}_{i,k-j_1}\bar{u}_{i,k-j_2})^{(N)}$; 再利用 $\mathcal{E}(\bar{\varphi}_{k-1}^{(N)})$ 和命题 1, 对 $j\in\{1,2,\dots,m_0\}\setminus\{i\},j_1=1,2,\dots,n_i,j_2=1,2,\dots,n_0$ 和 $j_3=1,2,\dots,n_j$, 计算

$\mathcal{E}((\bar{u}_{i,k-j_1}\bar{y}_{k-j_2})^{(N)})$ 和 $\mathcal{E}((\bar{u}_{i,k-j_1}\bar{u}_{j,k-j_3})^{(N)})$; 如此得到 $\mathcal{E}((\bar{u}_{i,k-j}\bar{\varphi}_{k-1})^{(N)})$, 其中 $j=1,2,\ldots,n_i$. 每个参与者将自己的计算密文结果广播给其他所有参与者.

步骤 3. 当 $k \mod T_0 \neq 0$ 时, 输出系统参数估计 $\bar{\theta}_k=\bar{\theta}_{\tau_k}$ 并返回步骤 1; 否则, 即当 $k \mod T_0=0$ 时, 每个参与者利用前 T_0 个历史结果和式 (14) 计算 $\mathcal{E}(\bar{S}^{(N)}_{\tau_k-1})$ 和 $\mathcal{E}(\bar{R}^{(N)}_{\tau_k-1})$.

步骤 4. 参与者联合解密 $\mathcal{E}(\bar{S}^{(N)}_{\tau_k-1})$ 和 $\mathcal{E}(\bar{R}^{(N)}_{\tau_k-1})$ 并将结果还原为 $\bar{S}_{\tau_k-1}$ 和 $\bar{R}_{\tau_k-1}$. 具体过程为: 对 $\mathcal{E}(\bar{S}^{(N)}_{\tau_k-1})$ 和 $\mathcal{E}(\bar{R}^{(N)}_{\tau_k-1})$ 中的每个密文元素 c, 参与者 $\mathcal{P}_0$ 计算 $c^{2k_{\mathcal{P}_0}} \mod N^2$ 后将结果传给 $\mathcal{P}_1$, $\mathcal{P}_1$ 计算 $c^{2k_{\mathcal{P}_0}}c^{2k_{\mathcal{P}_1}} \mod N^2$ 后将结果传给 $\mathcal{P}_2$, 依此类推, $\mathcal{P}_{m_0}$ 计算 $c^{2(k_{\mathcal{P}_0}+\cdots+k_{\mathcal{P}_{m_0}})} \mod N^2$ 后按照式 (5) 解密再按式 (10) 还原后广播给所有人.

步骤 5. 所有参与者均可计算 $\bar{\theta}_k=(\bar{P}_0^{-1}+\sum_{i=0}^{\tau_k-1}\bar{S}_i)^{-1}\sum_{i=0}^{\tau_k-1}\bar{R}_i$ 得到 k 时刻的系统参数估计.

上述的安全多方最小二乘辨识算法可简单描述为算法 1.

算法 1 基于门限 Paillier 密码体制的安全多方最小二乘辨识算法

初始化: 可信第三方选取整数化参数 τ, 时间分段长度 T_0, 初始正定矩阵 $\bar{P}_0$, 根据门限 Paillier 密码体制生成公钥 (N,g), 私钥 $(k_{\mathcal{P}_0},k_{\mathcal{P}_1},\ldots,k_{\mathcal{P}_{m_0}})$ 并完成相应的分发工作; 参与者总数 m_0+1, 初始估计 $\bar{\theta}_0$;

while $k\geqslant 1$ **do**
  根据步骤 1 计算 $\mathcal{E}(\bar{\varphi}^{(N)}_{k-1})$;
  根据步骤 2 计算 $\mathcal{E}((\bar{\varphi}_{k-1}\bar{\varphi}^{\mathrm{T}}_{k-1})^{(N)})$ 和 $\mathcal{E}((\bar{\varphi}_{k-1}\bar{y}_k)^{(N)})$;
  if $k \mod T_0 \neq 0$ **then**
    $\bar{\theta}_k=\bar{\theta}_{\tau_k}$;
  else $\{k \mod T_0=0\}$
    利用前 T_0 个历史结果和式 (14) 计算 $\mathcal{E}(\bar{S}^{(N)}_{\tau_k-1})$ 和 $\mathcal{E}(\bar{R}^{(N)}_{\tau_k-1})$;
    根据步骤 4 解密 $\mathcal{E}(\bar{S}^{(N)}_{\tau_k-1})$ 和 $\mathcal{E}(\bar{R}^{(N)}_{\tau_k-1})$ 并将结果还原为 $\bar{S}_{\tau_k-1}$ 和 $\bar{R}_{\tau_k-1}$;
    $\bar{\theta}_k=(\bar{P}_0^{-1}+\sum_{i=0}^{\tau_k-1}\bar{S}_i)^{-1}\sum_{i=0}^{\tau_k-1}\bar{R}_i$;
  end if
end while

输出: $\bar{\theta}_k, k\geqslant 1$.

注释12 由算法的执行过程可知, 最终产生的参数估计结果是每隔 T_0 时间更新一次, 满足

$$\bar{\theta}_k=\left(\bar{P}_0^{-1}+\sum_{i=0}^{\tau_kT_0-1}\bar{\varphi}_i\bar{\varphi}_i^{\mathrm{T}}\right)^{-1}\left(\sum_{i=0}^{\tau_kT_0-1}\bar{\varphi}_i\bar{y}_{i+1}\right). \tag{17}$$

与最初的最小二乘估计式 (3) 不同点在于这里所用的回归向量和输出均变成了整数化后的形式 $\bar{\varphi}_i$ 和 $\bar{y}_i$, 同时引入了常数正定矩阵 $\bar{P}_0$ 来保证式 (17) 右边第一个括号内的矩阵可逆. 4.3 小节的收敛性分析将指出, 在满足正确加解密条件和一般收敛性条件下, $\bar{P}_0$ 的选取对于 $\bar{\theta}_k$ 收敛的一致性及速度无本质影响.

4 算法分析

4.1 算法的正确加密和解密条件

安全多方最小二乘辨识算法应用了门限化的 Paillier 密码体制, 该密码体制的明文空间为 $\mathbb{Z}_N$, 当明文超出这个范围时, 算法将无法正确解密得到原始明文. 所以, 要求算法执行步骤 3 中的 $\bar{S}^{(N)}_{\tau_k-1}$ 和 $\bar{R}^{(N)}_{\tau_k-1}$ 中的元素不能超出明文空间 $\mathbb{Z}_N$, 即 $\bar{S}_{\tau_k-1}$ 和 $\bar{R}_{\tau_k-1}$ 中的元素不能超出 $\mathscr{M}^{(N)}$ 的范围. 从而, 我们有如下结论.

定理1 对安全多方最小二乘辨识算法的步骤 1∼5, 若系统输入输出的最大绝对值 c_1, 整数化误差参数 τ, 时间分段长度 T_0 和所用门限 Paillier 加密体制的模数 N 满足

$$N \geqslant 2T_0\lceil \tau c_1\rceil^2+1, \tag{18}$$

则采用的门限 Paillier 密码体制可以正确加密和解密.

证明 由 $\bar{S}_{\tau_k}$ 和 $\bar{R}_{\tau_k}$ 的定义及定理条件知, $\bar{S}_{\tau_k}$ 和 $\bar{R}_{\tau_k}$ 中任一元素的绝对值均小于等于 $T_0\lceil \tau c_1\rceil^2$. 要想让 $\bar{S}_{\tau_k}$ 和 $\bar{R}_{\tau_k}$ 中元素均在 $\mathscr{M}^{(N)}$ 内, 只需要 $\frac{N-1}{2}\geqslant T_0\lceil \tau c_1\rceil^2$, 即 $N\geqslant 2T_0\lceil \tau c_1\rceil^2+1$. 此时算法可以正确加密和解密, 从而定理得证.

注释13 式 (18) 描述了在给定整数化参数 τ、时间分段长度 T_0 和系统输入输出的绝对值上界 c_1 后, 所用门限 Paillier 加密体制中模数 N 的取法. 另一方面, 从式 (18) 也可导出

$$c_1\leqslant \frac{1}{\tau}\sqrt{\frac{N-1}{2T_0}},$$

此式描述了给定整数化参数 τ 和所用门限 Paillier 加密体制中模数 N 后, 系统输入输出的容许取值范围, 即输入输出的绝对值上界 c_1.

4.2 安全性分析

定理2 对系统 (1) 和安全多方最小二乘算法的步骤 1∼5, 即在所有人遵守算法协议的前提下, 若算法中时间分段长度 $T_0>\frac{d_1(d_1+3)}{2}$, 则任意 l ($l\leqslant m_0$) 个参与者联合起来, 都无法得到其他参与者的具体输入信息.

证明 根据算法描述, 除了准备阶段的公共信息外, 在算法运行阶段攻击者能够拿到的有效信息包括: 自己的真实信息, 算法执行过程的所有加密信息, $\bar{S}_{\tau_k}$ 和 $\bar{R}_{\tau_k}$ (或者等价地, 它们在模 N 意义下的表示).

加密信息的安全性由 Paillier 加密体制及门限 Paillier 加密体制的安全性保证 [10∼12]. 因此, 我们只需要证明攻击者在已知自己真实信息及算法运行过程产生的中间信息 ($\bar{S}_{\tau_k}$ 和 $\bar{R}_{\tau_k}$) 的情况下仍然无法得到其他参与者的具体隐私信息即可.

记 $\mathscr{T}_i=\{k\in\mathbb{N}|\lfloor\frac{k}{T_0}\rfloor=i\}$, 则 $\bar{S}_i=\sum_{j\in\mathscr{T}_i}\bar{\varphi}_j\bar{\varphi}_j^{\mathrm{T}}, \bar{R}_i=\sum_{j\in\mathscr{T}_i}\bar{\varphi}_j\bar{y}_{j+1}$. 进而, 到任一时刻 k 为止, 攻击者已知的信息为

$$\sum_{j\in\mathscr{T}_i}\bar{\varphi}_j\bar{\varphi}_j^{\mathrm{T}}=\bar{S}_i,\quad i=0,1,2,\ldots,\tau_k-1, \tag{19}$$

$$\sum_{j\in\mathscr{T}_i}\bar{\varphi}_j\bar{y}_{j+1}=\bar{R}_i,\quad i=0,1,2,\ldots,\tau_k-1. \tag{20}$$

攻击者利用如上两式求解其他参与者的隐私信息. 在式 (19) 刻画的方程中, 考虑对称性后, 方程的约束数为 $\frac{\tau_k(1+d_1)d_1}{2}$; 在式 (20) 刻画的方程中, 方程的约束数为 $\tau_k d_1$. 另一方面, 除去输入输出初值外, 式 (19) 和 (20) 含有的未知变量数 (即其他参与者的隐私数据数) 为 $(1+m_0-l)T_0\tau_k$ 个. 要想让攻击者无法求解出其他参与者隐私信息, 只需要在任何时刻 k 总有未知量数大于方程约束数, 即

$$(1+m_0-l)T_0\tau_k>\tau_k\frac{(1+d_1)d_1}{2}+\tau_k d_1$$

对任意 k 成立. 注意到 $(1+m_0-l)\geqslant 1$, 从而上述不等式对任意 k 成立只需要

$$T_0>\frac{d_1(d_1+3)}{2}.$$

综上, 定理得证.

注释14 从上述证明中可以看出, T_0 越大, 式 (19) 和 (20) 所表示的方程组中未知量所在的解空间越大. 但过大的 T_0 会影响估计, 使得估计更新变慢. 同时, 定理 1 也指出, 为保证正确加密解密, 对于给定 N, T_0 也不能任意大.

4.3 收敛误差分析

观察系统 (1) 和实际计算的最小二乘估计式 (17), 我们可以知道 $\bar{\theta}_k$ 的收敛性与回归向量 $\bar{\varphi}_k$、系统噪声 ω_k 和由整数化引入的量化误差等因素有关. 同时, 若想达到好的收敛效果, 算法运行过程中的加密解密也必须保证正确.

为了分析的方便, 我们暂且假定算法中的加密解密总能正确完成, 在此前提下考虑整数化引入的量化误差影响. 又考虑到系统 (1) 中回归项的存在, 我们引入 Lyapunov 函数和鞅差理论为工具的方法来分析 [21, 22, 24]. 注意到式 (17) 亦可改写为用恢复的回归向量 $\hat{\varphi}_k$ 和输出 $\hat{y}_k$ 来表示:

$$\bar{\theta}_k = \sum_{i=0}^{\tau_k T_0 - 1} (\hat{P}_0^{-1} + \hat{\varphi}_i \hat{\varphi}_i^{\mathrm{T}})^{-1} \left(\sum_{i=0}^{\tau_k T_0 - 1} \hat{\varphi}_i \hat{y}_{i+1} \right),$$

其中 $\hat{P}_0^{-1} = \frac{1}{\tau^2} \bar{P}_0^{-1}$. 进而, 我们将式 (17) 等价地写为如下递推形式 [25, page 84]:

$$\bar{\theta}_{k+1} = \bar{\theta}_k + \hat{a}_k \hat{P}_k \hat{\varphi}_k (\hat{y}_{k+1} - \hat{\varphi}_k^{\mathrm{T}} \bar{\theta}_k), \tag{21}$$

$$\hat{P}_{k+1} = \left(\hat{P}_0^{-1} + \sum_{i=0}^{k} \hat{\varphi}_i \hat{\varphi}_i^{\mathrm{T}} \right)^{-1} = \hat{P}_k - \hat{a}_k \hat{P}_k \hat{\varphi}_k \hat{\varphi}_k^{\mathrm{T}} \hat{P}_k, \tag{22}$$

$$\hat{a}_k = (1 + \hat{\varphi}_k^{\mathrm{T}} \hat{P}_k \hat{\varphi}_k)^{-1}, \tag{23}$$

其中, $\bar{\theta}_0 = \mathbf{0}_{d_1}$.

我们引入如下与系统相关的假设:

假设1 噪声序列 $\{\omega_k, \mathscr{F}_k\}$ 是一鞅差序列 (其中 $\{\mathscr{F}_k\}$ 是一非降子 -σ 代数序列), 并且存在常数 $\beta \geqslant 2$ 使

$$\sup_k \mathrm{E}(|\omega_{k+1}|^{\beta} | \mathscr{F}_k) < \infty, \quad \text{a.s.}$$

假设2 控制输入序列 $\{\varphi_k, \mathscr{F}_k\}$ 是适应序列, 即 $\varphi_k \in \mathscr{F}_k, \forall k \geqslant 0$;

同时, 类似 Chen 等 [25] 中定理 3.2.1 的证明部分, 我们不加证明地给出如下需要用到的引理:

引理1 对递推算法 (21)∼(23), 对任意 $k \geqslant 0$ 有

$$\sum_{i=0}^{k} \hat{a}_i \hat{\varphi}_i^{\mathrm{T}} \hat{P}_i \hat{\varphi}_i \leqslant \ln |\hat{P}_{k+1}^{-1}| - \ln |\hat{P}_0^{-1}|.$$

基于以上假设, 我们首先给出最小二乘估计式 (17) 如下的重要中间结果.

引理2 对系统 (1), 在假设 1 和 2 下, 相应的最小二乘估计式 (17) 具有如下渐近性质:

$$\begin{aligned} &\tilde{\theta}_{k+1} \hat{P}_{k+1}^{-1} \tilde{\theta}_{k+1} + \left(1 - \frac{1}{\gamma} + o(1)\right) \sum_{i=0}^{k} \hat{a}_i (\hat{\varphi}_i^{\mathrm{T}} \tilde{\theta}_i)^2 \\ &\quad = O(\ln r_k (\ln(e + \ln r_k))^{\kappa 1_{\{\beta=2\}}}) + (2+\gamma) s_k, \quad \text{a.s.}, \end{aligned}$$

其中, $\tilde{\theta}_k = \theta - \bar{\theta}_k, s_k = \sum_{i=0}^{k}(\theta^{\mathrm{T}}(\varphi_i - \hat{\varphi}_i) + \hat{y}_{i+1} - y_{i+1})^2, r_k = e + \sum_{i=0}^{k} \|\hat{\varphi}_i\|^2$, γ, κ 均为任意大于 1 的常数.

证明 令 $\eta_k = \hat{y}_k - y_k$, 将式 (2) 代入式 (21) 有

$$\bar{\theta}_{k+1} = \bar{\theta}_k + \hat{a}_k \hat{P}_k \hat{\varphi}_k (\theta^{\mathrm{T}} \varphi_k + \omega_{k+1} + \eta_{k+1} - \bar{\theta}_k^{\mathrm{T}} \hat{\varphi}_k),$$

从而

$$\begin{aligned}
\tilde{\theta}_{k+1} &= \theta - \bar{\theta}_{k+1} \\
&= \tilde{\theta}_k - \hat{a}_k \hat{P}_k \hat{\varphi}_k (\theta^{\mathrm{T}} \varphi_k + \omega_{k+1} + \eta_{k+1} - \bar{\theta}_k^{\mathrm{T}} \hat{\varphi}_k) \\
&= \tilde{\theta}_k - \hat{a}_k \hat{P}_k \hat{\varphi}_k (\theta^{\mathrm{T}} \varphi_k - \theta^{\mathrm{T}} \hat{\varphi}_k + \theta^{\mathrm{T}} \hat{\varphi}_k - \bar{\theta}_k^{\mathrm{T}} \hat{\varphi}_k + \omega_{k+1} + \eta_{k+1}) \\
&= \tilde{\theta}_k - \hat{a}_k \hat{P}_k \hat{\varphi}_k [\hat{\varphi}_k^{\mathrm{T}} \tilde{\theta}_k + \theta^{\mathrm{T}} (\varphi_k - \hat{\varphi}_k) + \omega_{k+1} + \eta_{k+1}] \\
&= \tilde{\theta}_k - \hat{a}_k \hat{P}_k \hat{\varphi}_k (\hat{\varphi}_k^{\mathrm{T}} \tilde{\theta}_k + \xi_k + \omega_{k+1}),
\end{aligned} \tag{24}$$

其中, $\xi_k = \theta^{\mathrm{T}}(\varphi_k - \hat{\varphi}_k) + \eta_{k+1}$.

接着, 我们定义如下形式的 Lyapunov 函数:

$$V_k = \tilde{\theta}_k^{\mathrm{T}} \hat{P}_k^{-1} \tilde{\theta}_k.$$

将式 (24) 代入上式可推知

$$\begin{aligned}
V_{k+1} &= \tilde{\theta}_{k+1}^{\mathrm{T}} \hat{P}_{k+1}^{-1} \tilde{\theta}_{k+1} \\
&= [\tilde{\theta}_k - \hat{a}_k \hat{P}_k \hat{\varphi}_k (\hat{\varphi}_k^{\mathrm{T}} \tilde{\theta}_k + \xi_k + \omega_{k+1})]^{\mathrm{T}} \cdot \hat{P}_{k+1}^{-1} \\
&\quad \cdot [\tilde{\theta}_k - \hat{a}_k \hat{P}_k \hat{\varphi}_k (\hat{\varphi}_k^{\mathrm{T}} \tilde{\theta}_k + \xi_k + \omega_{k+1})] \\
&= \tilde{\theta}_k^{\mathrm{T}} \hat{P}_{k+1}^{-1} \tilde{\theta}_k - 2\hat{a}_k \tilde{\theta}_k^{\mathrm{T}} \hat{P}_{k+1}^{-1} \hat{P}_k \hat{\varphi}_k (\hat{\varphi}_k^{\mathrm{T}} \tilde{\theta}_k + \xi_k + \omega_{k+1}) \\
&\quad + \hat{a}_k^2 \hat{\varphi}_k^{\mathrm{T}} \hat{P}_k \hat{P}_{k+1}^{-1} \hat{P}_k \hat{\varphi}_k (\hat{\varphi}_k^{\mathrm{T}} \tilde{\theta}_k + \xi_k + \omega_{k+1})^2.
\end{aligned} \tag{25}$$

对式 (25) 中的第 1 项, 由式 (22) 可知

$$\tilde{\theta}_k^{\mathrm{T}} \hat{P}_{k+1}^{-1} \tilde{\theta}_k = \tilde{\theta}_k^{\mathrm{T}} (\hat{P}_k^{-1} + \hat{\varphi}_k \hat{\varphi}_k^{\mathrm{T}}) \tilde{\theta}_k = \tilde{\theta}_k^{\mathrm{T}} \hat{P}_k^{-1} \tilde{\theta}_k + (\hat{\varphi}_k^{\mathrm{T}} \tilde{\theta}_k)^2, \tag{26}$$

又由式 (23) 可知

$$\begin{aligned}
\hat{a}_k \hat{P}_{k+1}^{-1} \hat{P}_k \hat{\varphi}_k &= \hat{a}_k (I + \hat{\varphi}_k \hat{\varphi}_k^{\mathrm{T}} \hat{P}_k) \hat{\varphi}_k \\
&= \hat{a}_k \hat{\varphi}_k (1 + \hat{\varphi}_k^{\mathrm{T}} \hat{P}_k \hat{\varphi}_k) \\
&= \hat{\varphi}_k,
\end{aligned}$$

并且

$$\hat{a}_k \hat{\varphi}_k^{\mathrm{T}} \hat{P}_k \hat{\varphi}_k = 1 - \hat{a}_k.$$

从而对式 (25) 中第 2 和 3 项分别有

$$\hat{a}_k \tilde{\theta}_k^{\mathrm{T}} \hat{P}_{k+1}^{-1} \hat{P}_k \hat{\varphi}_k (\hat{\varphi}_k^{\mathrm{T}} \tilde{\theta}_k + \xi_k + \omega_{k+1})$$

$$
\begin{aligned}
&= \tilde{\theta}_k^{\mathrm{T}}(\hat{a}_k\hat{P}_{k+1}^{-1}\hat{P}_k\hat{\varphi}_k)(\hat{\varphi}_k^{\mathrm{T}}\tilde{\theta}_k+\xi_k+\omega_{k+1})\\
&= \hat{\varphi}_k^{\mathrm{T}}\tilde{\theta}_k(\hat{\varphi}_k^{\mathrm{T}}\tilde{\theta}_k+\xi_k+\omega_{k+1})\\
&= (\hat{\varphi}_k^{\mathrm{T}}\tilde{\theta}_k)^2+\hat{\varphi}_k^{\mathrm{T}}\tilde{\theta}_k\xi_k+\hat{\varphi}_k^{\mathrm{T}}\tilde{\theta}_k\omega_{k+1}, \qquad (27)
\end{aligned}
$$

和

$$
\begin{aligned}
&\hat{a}_k^2\hat{\varphi}_k^{\mathrm{T}}\hat{P}_k\hat{P}_{k+1}^{-1}\hat{P}_k\hat{\varphi}_k(\hat{\varphi}_k^{\mathrm{T}}\tilde{\theta}_k+\xi_k+\omega_{k+1})^2\\
&\quad= \hat{a}_k\hat{\varphi}_k^{\mathrm{T}}\hat{P}_k(\hat{a}_k\hat{P}_{k+1}^{-1}\hat{P}_k\hat{\varphi}_k)(\hat{\varphi}_k^{\mathrm{T}}\tilde{\theta}_k+\xi_k+\omega_{k+1})^2\\
&\quad= \hat{a}_k\hat{\varphi}_k^{\mathrm{T}}\hat{P}_k\hat{\varphi}_k(\hat{\varphi}_k^{\mathrm{T}}\tilde{\theta}_k+\xi_k+\omega_{k+1})^2\\
&\quad= (1-\hat{a}_k)(\hat{\varphi}_k^{\mathrm{T}}\tilde{\theta}_k+\xi_k+\omega_{k+1})^2. \qquad (28)
\end{aligned}
$$

利用前面三项分析结果, 将式 (26)∼(28) 代入式 (25) 得

$$
\begin{aligned}
V_{k+1} &= \tilde{\theta}_k^{\mathrm{T}}\hat{P}_k^{-1}\tilde{\theta}_k+(\hat{\varphi}_k^{\mathrm{T}}\tilde{\theta}_k)^2-2[(\hat{\varphi}_k^{\mathrm{T}}\tilde{\theta}_k)^2+\hat{\varphi}_k^{\mathrm{T}}\tilde{\theta}_k\xi_k+\hat{\varphi}_k^{\mathrm{T}}\tilde{\theta}_k\omega_{k+1}]\\
&\quad+(1-\hat{a}_k)(\hat{\varphi}_k^{\mathrm{T}}\tilde{\theta}_k+\xi_k+\omega_{k+1})^2\\
&= \tilde{\theta}_k^{\mathrm{T}}\hat{P}_k^{-1}\tilde{\theta}_k+[1-2+(1-\hat{a}_k)](\hat{\varphi}_k^{\mathrm{T}}\tilde{\theta}_k)^2+[-2+2(1-\hat{a}_k)]\hat{\varphi}_k^{\mathrm{T}}\tilde{\theta}_k\xi_k\\
&\quad+[-2+2(1-\hat{a}_k)]\hat{\varphi}_k^{\mathrm{T}}\tilde{\theta}_k\omega_{k+1}+(1-\hat{a}_k)\xi_k^2+2(1-\hat{a}_k)\xi_k\omega_{k+1}+(1-\hat{a}_k)\omega_{k+1}^2\\
&= V_k-\hat{a}_k(\hat{\varphi}_k^{\mathrm{T}}\tilde{\theta}_k)^2-2\hat{a}_k\hat{\varphi}_k^{\mathrm{T}}\tilde{\theta}_k\xi_k-2\hat{a}_k\hat{\varphi}_k^{\mathrm{T}}\tilde{\theta}_k\omega_{k+1}\\
&\quad+(1-\hat{a}_k)\xi_k^2+2(1-\hat{a}_k)\xi_k\omega_{k+1}+(1-\hat{a}_k)\omega_{k+1}^2.
\end{aligned}
$$

进而, 将上式从时刻 0 累加到时刻 $k+1$ 得

$$
\begin{aligned}
&V_{k+1}+\sum_{i=0}^{k}\hat{a}_i(\hat{\varphi}_i^{\mathrm{T}}\tilde{\theta}_i)^2\\
&\quad= V_0-2\sum_{i=0}^{k}\hat{a}_i\hat{\varphi}_i^{\mathrm{T}}\tilde{\theta}_i\xi_i-2\sum_{i=0}^{k}\hat{a}_i\hat{\varphi}_i^{\mathrm{T}}\tilde{\theta}_i\omega_{i+1}+\sum_{i=0}^{k}(1-\hat{a}_i)\xi_i^2\\
&\quad\quad+\sum_{i=0}^{k}(1-\hat{a}_i)\omega_{i+1}^2+2\sum_{i=0}^{k}(1-\hat{a}_i)\xi_i\omega_{i+1}. \qquad (29)
\end{aligned}
$$

现在, 我们逐一分析式 (29) 中右边各项的渐近敛散情况.

(1) 注意到对任意实数 a,b, 任给实数 $\gamma>1$, 有 $2ab\leqslant\gamma a^2+\frac{1}{\gamma}b^2$. 因此,

$$
\begin{aligned}
-2\sum_{i=0}^{k}\hat{a}_i\hat{\varphi}_i^{\mathrm{T}}\tilde{\theta}_i\xi_i &\leqslant \sum_{i=0}^{k}2|\hat{a}_i\hat{\varphi}_i^{\mathrm{T}}\tilde{\theta}_i\xi_i|\\
&\leqslant \sum_{i=0}^{k}\left[\gamma\xi_i^2+\frac{1}{\gamma}(\hat{a}_i\hat{\varphi}_i^{\mathrm{T}}\tilde{\theta}_i)^2\right]\\
&\leqslant \sum_{i=0}^{k}\left[\gamma\xi_i^2+\frac{1}{\gamma}\hat{a}_i(\hat{\varphi}_i^{\mathrm{T}}\tilde{\theta}_i)^2\right]\\
&= \gamma s_k+\frac{1}{\gamma}\sum_{i=0}^{k}\hat{a}_i(\hat{\varphi}_i^{\mathrm{T}}\tilde{\theta}_i)^2. \qquad (30)
\end{aligned}
$$

(2) 注意到 $\hat{a}_k\hat{\varphi}_k^{\mathrm{T}}\tilde{\theta}_k \in \mathscr{F}_k$ 及假设 1 成立, 则由 Chen 等 [25] 中的定理 1.2.14 知, 对加权鞅差列 $\{\hat{a}_k\hat{\varphi}_k^{\mathrm{T}}\tilde{\theta}_k\omega_{k+1}\}$ 存在 $\delta_1 > 0$ 和 $\delta_2 \in (0, \frac{1}{2})$ 使得

$$\begin{aligned}-2\sum_{i=0}^{k}\hat{a}_i\hat{\varphi}_i^{\mathrm{T}}\tilde{\theta}_i\omega_{i+1} &= O\left(\left[\sum_{i=0}^{k}(\hat{a}_i\hat{\varphi}_i^{\mathrm{T}}\tilde{\theta}_i)^2\right]^{\frac{1}{2}}\left(\ln\left(e+\sum_{i=0}^{k}(\hat{a}_i\tilde{\theta}_i^{\mathrm{T}}\hat{\varphi}_i)^2\right)\right)^{\frac{1}{2}+\delta_1}\right)\\ &= O\left(\left[\sum_{i=0}^{k}(\hat{a}_i\hat{\varphi}_i^{\mathrm{T}}\tilde{\theta}_i)^2\right]^{\frac{1}{2}}\left(O(1)+o\left(\left[\sum_{i=0}^{k}(\hat{a}_i\hat{\varphi}_i^{\mathrm{T}}\tilde{\theta}_i)^2\right]^{\delta_2}\right)\right)\right)\\ &= O(1)+o\left(\sum_{i=0}^{k}\hat{a}_i(\hat{\varphi}_i^{\mathrm{T}}\tilde{\theta}_i)^2\right)\quad \text{a.s.},\end{aligned} \tag{31}$$

其中, 第 2 个等式成立是由于 $\lim_{x\to\infty}\frac{(\ln(e+x))^{\frac{1}{2}+\delta_1}}{x^{\delta_2}} \to 0$.

(3) 由式 (23) 可知对任意整数 k, $0 \leqslant \hat{a}_k \leqslant 1$. 从而,

$$\sum_{i=0}^{k}(1-\hat{a}_i)\xi_i^2 \leqslant \sum_{i=0}^{k}\xi_i^2 = s_k. \tag{32}$$

(4) 注意到对任意 $k \geqslant 0$, $\hat{P}_{k+1}^{-1} = P_0' + \sum_{i=0}^{k}\hat{\varphi}_k\hat{\varphi}_k^{\mathrm{T}}$ 是正定的, 从而

$$|\hat{P}_{k+1}^{-1}| \leqslant (\lambda_{\max}(\hat{P}_{k+1}^{-1}))^{d_1} < (\mathrm{tr}\hat{P}_{k+1})^{d_1} = \left(\sum_{i=0}^{k}\|\hat{\varphi}_k\|^2\right)^{d_1}.$$

再由 r_k 的定义可知

$$\ln|\hat{P}_{k+1}^{-1}| = O(\ln r_k). \tag{33}$$

在假设 1 下, 由 C_r- 不等式和 Lyapunov 不等式 [25, page 6] 可知, 对任意实数 $\alpha \in [2, \min\{\beta, 4\}]$ 有

$$\begin{aligned}&\sup_k \mathrm{E}[|\omega_{k+1}^2 - \mathrm{E}(\omega_{k+1}^2|\mathcal{F}_k)|^{\frac{\alpha}{2}}|\mathcal{F}_k]\\ &\quad\leqslant \sup_k 2^{\frac{\alpha}{2}-1}(\mathrm{E}[|\omega_{k+1}^2|^{\frac{\alpha}{2}}|\mathscr{F}_k] + \mathrm{E}[|\mathrm{E}(\omega_{k+1}^2|\mathscr{F}_k)|^{\frac{\alpha}{2}}|\mathscr{F}_k])\\ &\quad\leqslant \sup_k 2^{2-1}(\mathrm{E}[|\omega_{k+1}^2|^{\frac{\alpha}{2}}|\mathscr{F}_k] + |\mathrm{E}(\omega_{k+1}^2|\mathscr{F}_k)|^{\frac{\alpha}{2}})\\ &\quad\leqslant 2\sup_k(\mathrm{E}[|\omega_{k+1}|^{\alpha}|\mathscr{F}_k] + (\mathrm{E}[|\omega_{k+1}|^{\alpha}|\mathscr{F}_k])^{\frac{1}{\alpha}\cdot\alpha})\\ &\quad= 4\sup_k \mathrm{E}[|\omega_{k+1}|^{\alpha}|\mathscr{F}_k] < \infty,\quad \text{a.s.}\end{aligned}$$

再注意到 $1-\hat{a}_k = \hat{a}_k\hat{\varphi}_k^{\mathrm{T}}\hat{P}_k\hat{\varphi}_k \in \mathscr{F}_k$, $\{\omega_{k+1}^2 - \mathrm{E}(\omega_{k+1}^2|\mathscr{F}_k)\}$ 是关于 $\{\mathscr{F}_k\}$ 的鞅差序列, 并利用 Chen 等 [25] 中的定理 1.2.14 及引理 1 可知, 对任意 $\delta_3 > 0$ 有

$$\begin{aligned}&\sum_{i=0}^{k}(1-\hat{a}_i)(\omega_{i+1}^2 - \mathrm{E}(\omega_{i+1}^2|\mathscr{F}_i))\\ &\quad= O\left(\left[\sum_{i=0}^{k}(1-\hat{a}_i)^{\frac{\alpha}{2}}\right]^{\frac{2}{\alpha}}\left[\ln\left(e+\sum_{i=0}^{k}(1-\hat{a}_i)^{\frac{\alpha}{2}}\right)\right]^{\frac{2}{\alpha}+\delta_3}\right)\end{aligned}$$

$$
\begin{aligned}
&= O\left(\left[\sum_{i=0}^{k}(1-\hat{a}_i)\right]^{\frac{2}{\alpha}}\left[\ln\left(e+\sum_{i=0}^{k}(1-\hat{a}_i)\right)\right]^{\frac{2}{\alpha}+\delta_3}\right)\\
&= O((\ln|\hat{P}_{k+1}^{-1}|-\ln|\hat{P}_0^{-1}|)^{\frac{2}{\alpha}}(\ln(e+\ln|\hat{P}_{k+1}^{-1}|-\ln|\hat{P}_0^{-1}|))^{\frac{2}{\alpha}+\delta_3})\\
&= O(1)+O((\ln r_k)^{\frac{2}{\alpha}}(\ln(e+\ln r_k))^{\frac{2}{\alpha}+\delta_3}) \quad \text{a.s.}
\end{aligned}
$$

考察上式中的最后一项. 根据 Chen 等 [25] 中定理 1.2.14, 如果假设 1 只对 $\beta=2$ 成立, 则 $\alpha=2$, 即 $\frac{2}{\alpha}=1$. 记 $\kappa=\frac{2}{\alpha}+\delta_3$, 则由 δ_3 取法知 κ 为大于 1 的任意常数. 此时有

$$
O((\ln r_k)^{\frac{2}{\alpha}}(\ln(e+\ln r_k))^{\frac{2}{\alpha}+\delta_3})=O((\ln r_k)(\ln(e+\ln r_k))^{\kappa}).
$$

如果假设 1 对某一 $\beta>2$ 成立, 则由 α 取法, 可取 $\alpha>2$. 此时, 对任意 $\delta_4\in(0,1-\frac{2}{\alpha})$ 有

$$
O((\ln r_k)^{\frac{2}{\alpha}}(\ln(e+\ln r_k))^{\frac{2}{\alpha}+\delta_3})=O((\ln r_k)^{\frac{2}{\alpha}}(O(1)+o((\ln r_k)^{\delta_4})))=O(1)+O(\ln r_k).
$$

综合 β 取值的两种情况, 我们总有

$$
\sum_{i=0}^{k}(1-\hat{a}_i)(\omega_{i+1}^2-\mathrm{E}(\omega_{i+1}^2|\mathscr{F}_i))=O(1)+O(\ln r_k(\ln(e+\ln r_k))^{\kappa 1_{\{\beta=2\}}}) \quad \text{a.s.}
$$

从而, 再由假设 1, 引理 1, 式 (33) 和上式有

$$
\begin{aligned}
\sum_{i=0}^{k}(1-\hat{a}_i)\omega_{i+1}^2 &= \sum_{i=0}^{k}(1-\hat{a}_i)(\omega_{i+1}^2-\mathrm{E}(\omega_{i+1}^2|\mathscr{F}_i))+\sum_{i=0}^{k}(1-\hat{a}_i)\mathrm{E}(\omega_{i+1}^2|\mathscr{F}_i)\\
&\leqslant \sum_{i=0}^{k}(1-\hat{a}_i)(\omega_{i+1}^2-\mathrm{E}(\omega_{i+1}^2|\mathscr{F}_i))+\sigma\sum_{i=0}^{k}(1-\hat{a}_i)\\
&= O(1)+O(\ln r_k(\ln(e+\ln r_k))^{\kappa 1_{\{\beta=2\}}})+O(\ln r_k)\\
&= O(1)+O(\ln r_k(\ln(e+\ln r_k))^{\kappa 1_{\{\beta=2\}}}) \quad \text{a.s.}, \qquad (34)
\end{aligned}
$$

其中, $\sigma=\sup_k \mathrm{E}(\omega_{k+1}^2|\mathscr{F}_k)$.

(5) 利用 (1) 中所用不等式及式 (34), 有

$$
\begin{aligned}
2\sum_{i=0}^{k}(1-\hat{a}_i)\xi_i\omega_{i+1} &\leqslant \sum_{i=0}^{k}(1-\hat{a}_i)(\xi_i^2+\omega_{i+1}^2)\\
&\leqslant s_k+\sum_{i=0}^{k}(1-\hat{a}_i)\omega_{i+1}^2\\
&= s_k+O(1)+O(\ln r_k(\ln(e+\ln r_k))^{\kappa 1_{\{\beta=2\}}}) \quad \text{a.s.} \qquad (35)
\end{aligned}
$$

将式 (30)~(32), (34), (35) 代入式 (29) 计算可得

$$
\begin{aligned}
&V_{k+1}+\left(1-\frac{1}{\gamma}+o(1)\right)\sum_{i=0}^{k}\hat{a}_i(\hat{\varphi}_i^{\mathrm{T}}\tilde{\theta}_i)^2\\
&\quad = O(1)+(2+\gamma)s_k+O(\ln r_k(\ln(e+\ln r_k))^{\kappa 1_{\{\beta=2\}}}) \quad \text{a.s.}
\end{aligned}
$$

注意到由 r_k 的定义有 $\ln r_k\geqslant 1$, 结合上式可证引理结论.

下面, 我们借助引理 2 给出系统 (1) 和安全多方最小二乘算法的步骤 1∼5 的收敛性结果. 考虑到门限 Paillier 加密体制明文空间的有界性, 为保证算法运行过程中加密对象始终落在明文空间, 我们再引入如下假设:

假设3 系统 (1) 是渐近稳定的, 即系统的特征方程 $\zeta(z) := 1-a_1z-a_2z^2-\cdots-a_pz^p \neq 0, \forall |z| \leqslant 1$.

假设4 系统 (1) 的初值和输入是有界的, 即存在 c_2 使得 $|y_0| \leqslant c_2, |u_{i,k}| \leqslant c_2, \forall i = 1,2,\ldots,m_0$, $k \geqslant 0$.

假设5 系统噪声 $\{\omega_k\}$ 是鞅差列, 且存在 c_3 使得 $|\omega_k| \leqslant c_3$.

注释15 对于系统 (1) 的特征方程 $\zeta(z)$, 可以定义如下的系统矩阵:

$$A = \begin{bmatrix} a_1 & a_2 & a_3 & \cdots & a_{n_0-1} & a_{n_0} \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix}. \tag{36}$$

由假设 3 易知存在 $c_4 > 0$ 和 $\lambda \in (0,1)$ 使得

$$\|A^k\| \leqslant c_4\lambda^k, \quad k = 1,2,\ldots. \tag{37}$$

定理3 对系统 (1) 和安全多方最小二乘算法的步骤 1∼5, 在假设 2∼5 下, 若所用门限 Paillier 密码体制的模数 N 满足

$$N \geqslant 2T_0\lceil \tau c_5 \rceil^2 + 1, \tag{38}$$

且系统满足持续激励条件

$$\eta = \liminf_{k>0} \lambda_{\min}\left(\frac{1}{k}\hat{P}_k^{-1}\right) > 0 \quad \text{a.s.}, \tag{39}$$

则

$$\|\tilde{\theta}_k\|^2 \leqslant O\left(\frac{\ln k}{k}\right) + \frac{6(1+\|\theta\|^2)}{\eta\tau^2}, \quad \text{a.s.}, \tag{40}$$

其中,

$$\begin{aligned} c_5 =& \sqrt{1+\sum_{i=1}^{m_0}\sum_{j=1}^{n_i} b_{i,j}^2}\sqrt{\left(\sum_{i=1}^{m_0} n_i\right)c_2^2 + c_3^2} \\ &+ \frac{c_4\lambda}{1-\lambda}\max\left\{c_2\sqrt{n_0}, \sqrt{1+\sum_{i}^{m_0}\sum_{j=1}^{n_i} b_{i,j}^2}\sqrt{\left(\sum_{i=1}^{m_0} n_i\right)c_2^2 + c_3^2}\right\}, \end{aligned}$$

c_4 和 λ 则均由式 (37) 给出.

证明 我们首先证明在条件式 (38) 下, 算法运行过程中可以正确加密解密, 即 $\bar{S}_{\tau_k}$ 和 $\bar{R}_{\tau_k}$ 中的元素未超出 $\mathscr{M}^{(N)}$ 的范围. 记

$$
\begin{aligned}
&X_k = [y_k, y_{k-1}, \dots, y_{k-n_0+1}]^{\mathrm{T}},\\
&U'_k = [u_{1,k}, \dots, u_{1,k-n_1+1}, u_{2,k}, \dots, u_{2,k-n_2+1}, \dots, u_{m_0,k}, \dots, u_{m_0,k-n_{m_0}+1}, \omega_{k+1}]^{\mathrm{T}},\\
&B = \begin{bmatrix}
b_{1,1} & \cdots & b_{1,n_1} & b_{2,1} & b_{2,n_2} & \cdots & b_{m_0,1} & b_{m_0,n_{m_0}} & 1\\
0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0\\
\vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots\\
0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0
\end{bmatrix},
\end{aligned}
$$

则由系统 (1) 知

$$X_{k+1} = AX_k + BU'_k,$$

其中, A 由式 (36) 给出. 由此知

$$X_{k+1} = A^{k+1}X_0 + \sum_{j=0}^{k} A^j BU'_{k-j}.$$

进而根据式 (37), 对任意 $k \geqslant 0$ 有

$$
\begin{aligned}
\|X_{k+1}\| &\leqslant \|A^{k+1}X_0\| + \left\|\sum_{j=0}^{k} A^j BU'_{k-j}\right\|\\
&\leqslant \|A^{k+1}\|\|X_0\| + \sum_{j=0}^{k}\|A^j\|\|B\|\|U'_{k-j}\|\\
&\leqslant \|B\|\left(\sup_k \|U'_k\|\right) + c_4\lambda^{k+1}\|X_0\| + c_4\|B\|\left(\sup_k \|U'_k\|\right)\sum_{j=1}^{k}\lambda^j.
\end{aligned}
$$

由假设 4 和 5 有 $\|X_0\| \leqslant c_2\sqrt{n_0}$ 和 $\sup_k \|U'_k\| \leqslant \sqrt{(\sum_{i=1}^{m_0} n_i)c_2^2 + c_3^2}$. 又因

$$\|B\| \leqslant \|B\|_F = \sqrt{1 + \sum_{i=1}^{m_0}\sum_{j=1}^{n_i} b_{i,j}^2},$$

所以, 我们有

$$
\begin{aligned}
\|X_{k+1}\| &\leqslant \sqrt{1 + \sum_{i=1}^{m_0}\sum_{j=1}^{n_i} b_{i,j}^2}\sqrt{\left(\sum_{i=1}^{m_0} n_i\right)c_2^2 + c_3^2} + c_4c_2\sqrt{n_0}\lambda^{k+1}\\
&\quad + c_4\sqrt{1 + \sum_{i=1}^{m_0}\sum_{j=1}^{n_i} b_{i,j}^2}\sqrt{\left(\sum_{i=1}^{m_0} n_i\right)c_2^2 + c_3^2}\sum_{j=1}^{k}\lambda^j\\
&\leqslant \sqrt{1 + \sum_{i=1}^{m_0}\sum_{j=1}^{n_i} b_{i,j}^2}\sqrt{\left(\sum_{i=1}^{m_0} n_i\right)c_2^2 + c_3^2}
\end{aligned}
$$

$$
\begin{aligned}
&+c_4\max\left\{c_2\sqrt{n_0},\sqrt{1+\sum_{i}^{m_0}\sum_{j=1}^{n_i}b_{i,j}^2}\sqrt{\left(\sum_{i=1}^{m_0}n_i\right)c_2^2+c_3^2}\right\}\sum_{j=1}^{\infty}\lambda^j\\
=&\sqrt{1+\sum_{i=1}^{m_0}\sum_{j=1}^{n_i}b_{i,j}^2}\sqrt{\left(\sum_{i=1}^{m_0}n_i\right)c_2^2+c_3^2}\\
&+\frac{c_4\lambda}{1-\lambda}\max\left\{c_2\sqrt{n_0},\sqrt{1+\sum_{i}^{m_0}\sum_{j=1}^{n_i}b_{i,j}^2}\sqrt{\left(\sum_{i=1}^{m_0}n_i\right)c_2^2+c_3^2}\right\}\\
=&\,c_5.
\end{aligned}
$$

因此, 对任意 $k\geqslant 1$, 我们有

$$\|y_k\|\leqslant\|X_k\|\leqslant c_5. \tag{41}$$

又 $\sum_{i=0}^{m_0}n_i\geqslant 1$, 否则系统无参数辨识必要, 故而 $c_5>c_2$. 于是, 根据定理 1, 在式 (18) 中取 $c_1=c_5$, 则取模数 N 满足

$$N>2T_0\lceil\tau c_5\rceil^2+1$$

时, 算法运行过程中可以正确加密和解密.

现在, 证明式 (40). 由假设 5, $|\omega_k|<c_3$, 可知对任意 $\beta>2$, 有 $\sup_k\mathrm{E}[|\omega_{k+1}|^\beta|\mathscr{F}_k]<\infty$ a.s.. 由假设 4 及式 (41) 可知, $\ln r_k=O(k)$. 又由式 (39) 可知, 存在足够大的 k_1 使得对任意 $k\geqslant k_1$ 有

$$\lambda_{\min}(\hat{P}_k^{-1})\geqslant\frac{\eta}{2}k.$$

从而, 根据引理 2, 对足够大的 k 有

$$
\begin{aligned}
\|\tilde{\theta}_k\|^2&\leqslant\frac{\tilde{\theta}_k^{\mathrm{T}}\hat{P}_k^{-1}\tilde{\theta}_k}{\lambda_{\min}(\hat{P}_k^{-1})}\\
&\leqslant\frac{1}{\lambda_{\min}(\hat{P}_k^{-1})}\left[\tilde{\theta}_k\hat{P}_k^{-1}\tilde{\theta}_k+\left(1-\frac{1}{\gamma}+o(1)\right)\sum_{i=0}^{k-1}\hat{a}_i(\hat{\varphi}_i^{\mathrm{T}}\tilde{\theta}_i)^2\right]\\
&=\frac{1}{\lambda_{\min}(\hat{P}_k^{-1})}[(2+\gamma)s_{k-1}+O(\ln r_{k-1}(\ln(e+\ln r_{k-1}))^{\kappa 1_{\{\beta=2\}}})]\\
&\leqslant(4+2\gamma)\frac{s_{k-1}}{\eta k}+O\left(\frac{\ln k}{k}\right)\quad\text{a.s.}
\end{aligned}
$$

又由 Cauchy 不等式有 $s_{k-1}=\sum_{i=0}^{k-1}(\theta^{\mathrm{T}}(\varphi_i-\hat{\varphi}_i)+\hat{y}_{i+1}-y_{i+1})^2\leqslant\frac{k(1+\|\theta\|^2)}{\tau^2}$, 代入上式即得

$$\|\tilde{\theta}_k\|^2\leqslant O\left(\frac{\ln k}{k}\right)+\frac{(4+2\gamma)(1+\|\theta\|^2)}{\eta\tau^2}\quad\text{a.s.}$$

再注意到引理 2 中 γ 为大于 1 的任意实数, 在上式中令 $\gamma\to 1$ 即得式 (40), 从而定理得证.

注释16 式 (40) 说明算法估计误差主要由两部分构成. 第 1 部分为最小二乘算法原有的误差, 即为右边第 1 项, 这个与 Chen 等 [25] 中相关结果一致; 第 2 部分为由于整数化引入的误差, 即为右边第 2 项. 可以看出, 只要取整数化导致的量化误差 $\delta=\frac{1}{\tau}$ 任意小, 算法估计的最终误差也将任意小.

注释17 可以看出, 满足零均值均匀分布的独立噪声是符合假设 5 要求的.

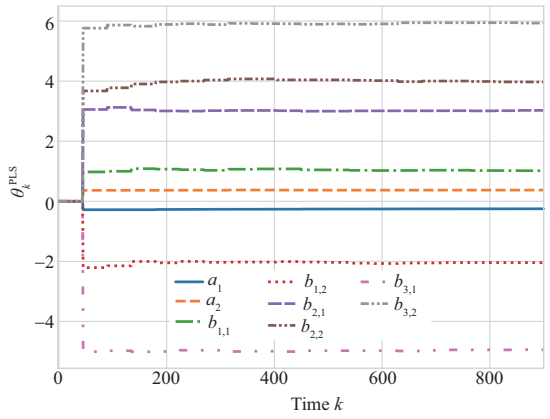

图 1 (网络版彩图) **PLS 估计轨线**

Figure 1 (Color online) Estimation trajectories of PLS

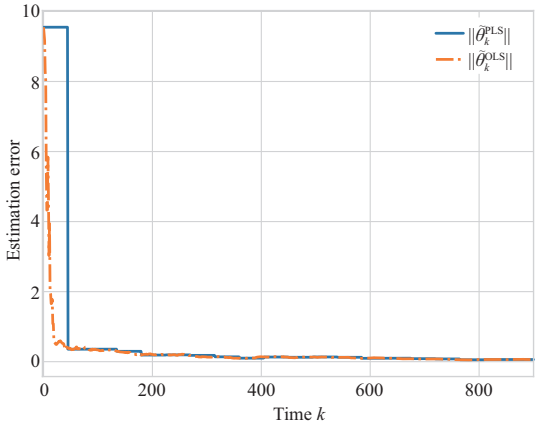

图 2 (网络版彩图) **PLS 与 OLS 估计误差比较**

Figure 2 (Color online) Comparison of estimation errors between PLS and OLS

5 仿真与验证

我们考虑如下系统的参数辨识:

$$\begin{aligned} y_{k+1} = &-\frac{1}{4}y_k + \frac{3}{8}y_{k-1} + u_{1,k} - 2u_{1,k-1} + 3u_{2,k} + 4u_{2,k-1} \\ &- 5u_{3,k} + 6u_{3,k-1} + \omega_{k+1}, \\ y_k = 0,\ k \leqslant 0;\ u_{i,k} = 0,\ i = 1,2,3,\ k < 0, \end{aligned}$$

其中系统的输入满足 $u_{i,k} \sim U(-10,10), i = 1,2,3,\ k \geqslant 0$; 系统的噪声满足 $\omega_k \sim U(-10,10),\ k \geqslant 0$. 此时, $\theta = [-\frac{1}{4}, \frac{3}{8}, 1, -2, 3, 4, -5, 6]^{\mathrm{T}}, d_1 = 8,\ A = \left[\begin{smallmatrix} -\frac{1}{4} & \frac{3}{8} \\ 1 & 0 \end{smallmatrix}\right]$.

在算法运行过程中, 我们取量化误差参数 $\tau = 1000$, 即整数化误差 $\delta = 0.001$, 相应的门限 Paillier 密码体制中密钥生成阶段的素数 p, q 的长度为 1024 比特, 时间分段长度 $T_0 = 45$, 初始估计 $\bar{\theta}_0 = [0,0,0,0,0,0,0,0]^{\mathrm{T}}$, 常数正定矩阵 $\bar{P}_0 = I$. 由定理 1 可以验证此时算法能够正确加密解密. 基于门限 Paillier 密码体制的安全多方最小二乘算法 (Paillier-based least squares, PLS) 的估计轨线如图 1 所示, 其与传统最小二乘算法 (ordinary least squares, OLS) 相比, 两个算法的估计误差如图 2 所示.

在整数化误差 $\delta = 0.001$ 时, 从图 1 可以看出, 算法估计的参数基本收敛于真实参数. 进一步, 结合图 2 可以看出, 基于门限 Paillier 密码体制的多方安全最小二乘算法与传统最小二乘算法的估计误差在开始时有些许不同, 但随着迭代次数的增加, 很快趋于一致. 这说明在量化误差足够小的情况下, 基于门限 Paillier 加密体制的安全多方最小二乘方法有能力满足实际应用中的估计精度要求.

6 结论

本文针对多方参与的随机线性系统, 考虑了参与者彼此不信任情形下系统参数的隐私安全协作辨识问题, 提出了基于门限 Paillier 密码体制的安全多方最小二乘辨识算法. 具体来说, 本文设计了正负整数的合理编码, 使得门限 Paillier 密码体制能够适用于负整数并保持其同态特性; 利用门限 Paillier 密码体制和将数据在时间上切分的思想, 设计了相应的安全多方辨识算法. 针对该算法, 本文给出了

正确加密解密所需要的明文空间大小条件, 用于指导密钥长度的选择; 给出了沿时间轴切分的长度条件, 用于保证算法的隐私安全性; 在几乎处处意义下给出了算法估计误差与加密带来的量化误差之间的定量关系, 表明了可通过选取合适的量化误差使得估计误差任意小.

参考文献

1 Chen T M. Stuxnet, the real start of cyber warfare? IEEE Network, 2010, 24: 2–3
2 Fidler D P. Was Stuxnet an act of war? Decoding a cyberattack. IEEE Secur Privacy Mag, 2011, 9: 56–59
3 Zhou K, Doyle J C, Glover K. Robust and Optimal Control. Upper Saddle River: Prentice Hall, 1996
4 Chen H, Guo L. Identification and Stochastic Adaptive Control. Stochastics & Stochastic Reports, 1991. 123–128
5 Guan X H, Shen C, Liu T. Data security is the foundation of cyberspace security. China Netw Inform, 2022, 1: 233–236 [管晓宏, 沈超, 刘烃. 数据安全是网络空间安全的基础. 中国网信, 2022, 1: 233–236]
6 Zhang J F, Tan J W, Wang J M. Privacy security in control systems. Sci China Inf Sci, 2021, 64: 176201
7 Ny J L, Pappas G J. Differentially Private Filtering. IEEE Trans Automat Contr, 2012, 59: 341–354
8 Wang J M, Tan J W, Zhang J F. Differentially private distributed parameter estimation. J Syst Sci Complex, 2023, 36: 187–204
9 Zhu M, Lu Y. On confidentiality preserving monitoring of linear dynamic networks against inference attacks. In: Proceedings of American Control Conference, 2015. 359–364
10 Katz J, Lindell Y. Introduction to Modern Cryptography. 3rd ed. Boca Raton: CRC Press, 2020
11 Paillier P. Public-key cryptosystems based on composite degree residuosity classes. In: Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques, 1999. 223–238
12 Fouque P, Pointcheval D. Threshold cryptosystems secure against chosen-ciphertext attacks. In: Proceedings of International Conference on the Theory and Application of Cryptology and Information Security, 2001. 351–368
13 Damgård I B, Jurik M J. Efficient protocols based on probabilistic encryption using composite degree residue classes. BRICS Report Series, 2000. doi: 10.7146/brics.v7i5.20133
14 Zhang Z F. Secret sharing and multi-party computation. Dissertation for Ph.D. Degree. Beijing: Chinese Academy of Sciences, 2007
15 Huo W, Yu Y, Yang K, et al. Privacy-preserving cryptographic algorithms and protocols: a survey on designs and applications. Sci Sin Inform, 2023, 53: 1688–1733 [霍炜, 郁昱, 杨糠, 等. 隐私保护计算密码技术研究进展与应用. 中国科学: 信息科学, 2023, 53: 1688–1733]
16 Xu C, Zhao Y L, Zhang J F. Information security protocol based system identification with binary-valued observations. J Syst Sci Complex, 2018, 31: 946–963
17 Tan J W, Zhang J F. Privacy-preserving secure least square algorithm. In: Proceedings of Chinese Control Conference (CCC), 2018. 243–248
18 Ruan M, Gao H, Wang Y Q. Secure and privacy-preserving consensus. IEEE Trans Automat Contr, 2019, 64: 4035–4049
19 Hadjicostis C N, Domínguez-García A D. Privacy-preserving distributed averaging via homomorphically encrypted ratio consensus. IEEE Trans Automat Contr, 2020, 65: 3887–3894
20 Lu Y, Zhu M H. Privacy preserving distributed optimization using homomorphic encryption. Automatica, 2018, 96: 314–325
21 Moore J B. On strong consistency of least squares identification algorithms. Automatica, 1978, 14: 505–509
22 Lai T L, Wei C Z. Least squares estimates in stochastic regression models with applications to identification and control of dynamic systems. Annals Statistics, 1982, 10: 154–166
23 Chen H F, Guo L. Convergence rate of least-squares identification and adaptive control for stochastic systems. Int J Control, 1986, 44: 1459–1476
24 Guo L, Chen H F. The åström-Wittenmark self-tuning regulator revisited and ELS-based adaptive trackers. IEEE Trans Automat Contr, 1991, 36: 802–812
25 Chen H F, Zhao W. Recursive Identification and Parameter Estimation. Boca Raton: CRC Press, 2014
26 Bryant R E, O'Hallaron D R. Computer Systems: A Programmer's Perspective. 3rd ed. Boston: Pearson, 2016

Cooperative secure parameter identification of multi-participant ARX systems — a threshold Paillier cryptosystem-based least-squares identification algorithm

Jianwei TAN[1,2], Jimin WANG[3*] & Jifeng ZHANG[1,2]

1. *Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing* 100190*, China*;
2. *School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing* 100049*, China*;
3. *School of Automation and Electrical Engineering, University of Science and Technology Beijing, Beijing* 100083*, China*

* Corresponding author. E-mail: jimwang@ustb.edu.cn

Abstract In this paper, the cooperative secure parameter identification problem of stochastic linear systems with multiple participants is studied, and a threshold Paillier cryptosystem-based secure multiparty least-squares identification algorithm is proposed. Specifically, by encoding positive and negative integers properly, the encryption object and homomorphic properties of the (threshold) Paillier cryptosystem are extended from nonnegative integers to integers. Using the threshold Paillier cryptosystem and the method for data segmentation along the time axis, the corresponding secure multiparty parameter identification algorithm is designed. The condition of plaintext space size required for correct encryption and decryption, the condition of the time slicing length to ensure privacy security, and the quantitative relationship between estimation error and encryption quantization error under certain conditions are given. We prove that as long as an appropriate length for time slicing is chosen, the specific private information of any given participant still cannot be obtained, even if all other participants colluded. Finally, the efficiency of the algorithm is verified using a numerical example.

Keywords multi-participant ARX system, privacy security, system identification, threshold Paillier cryptosystem, least squares method