基于秘密共享的匿名举报者回复方案

何琨，黄雅静，杜瑞颖，石闽，李思勤，陈晶
（武汉大学国家网络安全学院，湖北 武汉 430040）

摘　要：针对现有抗流量分析的匿名通信系统可以向攻击者隐藏通信双方的身份，但是通信双方之间无法彼此匿名，不适用于需保护举报者身份的匿名举报和回复场景这一问题，提出了一种高效的匿名举报者回复方案。通过分布式点函数和秘密共享技术将消息内容存储至两个互不勾结服务器的邮箱数据库中，向攻击者隐藏数据接收者身份。通过秘密共享和加密技术隐藏举报者邮箱地址，受理机构在不知道举报者身份信息的情况下可完成回复。安全性分析表明，所提方案能够同时保证数据接收者匿名性和举报者匿名性。实验结果表明，相比于Express方案，所提方案回复时受理机构计算复杂度从O（log$N$）降到O（1），减少60%计算开销，服务器减少50%计算开销。

关键词：秘密共享；分布式点函数；匿名举报；身份隐私
中图分类号：TP309
文献标志码：A
DOI：10.11959/j.issn.1000−436x.2024272

Anonymous whistleblowers reply scheme based on secret sharing

HE Kun, HUANG Yajing, DU Ruiying, SHI Min, LI Siqin, CHEN Jing
School of Cyber Science and Engineering, Wuhan University, Wuhan 430040, China

Abstract: Existing anonymous communication systems that resisted traffic analysis could hide the identities of the communicating parties from the attacker. However, the identities of the communicating parties couldn’t be hidden from each other, and thus these systems did not apply to the scenario of anonymous whistleblowing and replying, where it was necessary to protect the identity of the whistleblower. To address this issue, an efficient anonymous whistleblower response scheme was proposed. With the technology of distributed point functions and secret sharing, the message was stored in two separate mailbox databases of non-colluding servers, so that the identity of the data receiver was hidden from the attacker. With the technology of secret sharing and encryption, the email address of the whistleblower was hidden, so that the receiving organization could reply without learning the whistleblower’s identity. The security analysis showed that the proposed scheme enabled the anonymity of both data receivers and whistleblowers at the same time. The experimental results show that compared to the Express scheme, the proposed scheme reduces the computational complexity during a reply to $O(1)$ from $O(\log N)$, resulting in a 60% reduction in computational overhead for the receiving organization and a 50% reduction for the server.

Keywords: secret sharing, distributed point function, anonymous whistleblowing, identity privacy

收稿日期：2024−07−29；**修回日期：**2024−12−19
通信作者：杜瑞颖，duraying@126.com
基金项目：国家重点研发计划基金资助项目（No.2022YFB3103300）；国家自然科学基金资助项目（No.62172303）；湖北省重点研发计划基金资助项目（No.2022BAA039）；山东省重点研发计划基金资助项目（No.2022CXPT055）
Foundation Items: The National Key Research and Development Program of China (No.2022YFB3103300), The National Natural Science Foundation of China (No.62172303), The Key Research and Development Program of Hubei Province (No.2022BAA039), The Key Research and Development Program of Shandong Province (No.2022CXPT055)

0 引言

随着信息时代的来临，全球用户能够通过网络进行跨地域的即时通信，但同时这也引发了日益严峻的信息安全问题。通常，网络通信中的数据内容机密性保障通过传输层安全性（TLS, transport layer security）协议、端到端加密等方式实现，但任何具有窃听能力的个体都可以获得通信中产生的元数据，从而了解相关隐私信息。通信元数据是一类具备描述、解释等功能的附加数据，包括通信双方的身份、交流时间等信息。美国国家安全局前法律总顾问斯图尔特·贝克尔曾强调，无需了解具体的数据内容，仅凭足够的元数据就足以揭示一个人生活的各个方面。在匿名举报这类敏感身份的通信场景中，当举报者向受理机构发送信息时，即使加密了通信内容，相关元数据的泄露仍会威胁举报者的身份安全[1-2]，被举报者可以通过匹配受理机构公布处理结果的时间和通信人员记录，确定举报者的身份以实施报复。因此，保护通信中元数据的隐私安全至关重要。

匿名通信技术作为保护通信元数据的防御手段，能够隐藏通信双方的关系，确保攻击者无法关联数据发送者和数据接收者[3]。现有匿名通信模型主要包括洋葱路由、匿名广播和匿名邮箱3种。

以Tor[4]为代表的洋葱路由网络通过一系列中继服务器代理用户的流量来隐藏用户身份，因其配置简单且性能优良，每天约有800万用户访问，已经成为目前使用最广泛的匿名通信系统之一[5]。然而，这类网络并不能有效抵御流量关联分析[6-8]和网页指纹识别[9-11]等被动流量分析攻击，研究表明Tor的去匿名成功率可以达到90%以上。

匿名广播模型可以抵御流量分析，允许数据发送者将消息以匿名的方式发布到公告板上，用户能够自由访问并读取自己感兴趣的信息。Corrigan-gibbs等[12]通过分布式点函数（DPF, distributed point functions）将消息随机发布到由2个不合谋服务器共同维护的公告板上，并基于安全多方计算（MPC, multiparty computation）技术，利用一台审计服务器检测恶意用户发送的错误格式消息。Kwon等[13]基于并行Mix网络提出了一种水平可扩展的方案，支持大量短消息的匿名发送。该方案通过一组包含至少一个可信服务器的随机服务器集合模拟一个现实服务器以构建可信网络环境，并利用ElGamal算法在可信网络中传输消息和进行密钥洗牌以隐藏数据发送者和消息之间的关联，该方案采用非交互式零知识（NIZK, non-interactive zero knowledge）证明防止恶意服务器篡改用户消息，但计算开销和消息大小成正比。Kwon[14]提出了一种理论混合分析方法避免模拟诚实的服务器，但无法抵御恶意实体的攻击。Langowski等[15]消除了Kwon等[13]使用NIZK证明带来的消息大小限制，并基于签名和主动秘密共享提出了针对恶意用户和服务器的责备与恢复协议。该方案利用回旋镖加密将路由令牌匿名分发到随机网络的各层，路由令牌保证了路径选择的随机均匀性，而基于洋葱路由的回旋镖加密保证了消息的匿名交付。

匿名邮箱模型可以抵御流量分析，允许用户将消息发送至一个预先注册的邮箱，邮箱拥有者可以访问并读取对应的邮件内容。Gelernter等[16]基于Mix网与服务器进行通信，在实现邮件收发功能的同时隐藏数据发送者的身份。该方案采用request-pool技术确保移动设备用户断开连接后，入口节点能代替用户发送虚拟消息以保持用户的匿名性，同时利用时间戳技术防止恶意服务器的重放攻击。Cheng等[17]提出了一种私人群组通信方案，通过访问序列的不可区分性保护用户的隐私。该方案提供一个私有日志的抽象模型，只允许单一的数据发送者写入消息，而掌握日志秘密的多个用户可以读取消息，在实际部署中，私有日志由多个服务器共同维护和管理，并利用布谷鸟哈希技术提升效率。Eskandarian等[18]利用秘密共享的非交互互证明（SNIP, secret-shared non-interactive proof）[19-20]消除Corrigan-Gibbs等[12]提出的审计协议中对第三方审计服务器的需求，将审计时数据发送者的通信开销和计算开销从根号级别降低到常数级别。Vadapalli等[21]在多验证者MPC-in-the-head的基础上提出了一个新的SNIP，通过验证DPF格式的正确性完成审计。这一方法首次将服务器审计时的计算开销从线性级别降低到对数级别，适用于公告板模型和邮箱模型。

综上所述，现有抗流量分析的匿名通信方案能向攻击者有效隐藏数据发送者和数据接收者的身份，其中匿名广播模型适用于群组通信场景，匿名邮箱模型适用于点对点通信场景，但在发送消息时需要知道数据接收者的邮箱地址，存在通信双方之

间无法保持身份匿名性的问题，不能直接应用于匿名举报及回复系统中，因为在此类系统中举报者通常期望保持身份匿名性，避免向相关受理机构透露个人信息。针对上述问题，本文基于邮箱模型设计了基于秘密共享的匿名举报者回复方案，在保证举报者匿名性的同时降低了受理机构回复时的计算开销。本文的主要贡献如下。

1) 针对匿名举报者的回复问题，提出了一种安全回复方案，利用秘密共享和加密技术隐藏举报者的邮箱地址，确保相关受理机构对举报者进行回复时仍能保持举报者身份的匿名性。

2) 对所提方案的安全性进行理论分析和性能评估。实验结果表明，本文方案具有数据接收者匿名性、举报者匿名性和实际可行性。

1　预备知识

本节对本文方案中用到的基础密码学知识进行介绍，包括 Diffie-Hellman 密钥交换、加性秘密共享和分布式点函数。

1.1　Diffie-Hellman 密钥交换

Diffie-Hellman 密钥交换[22]（DHKE, Diffie-Hellman key exchange）允许通信双方在没有交换任何秘密信息的情况下，协商一个共享密钥。双方共享一个大素数 q 以及该素数的本原根 g，各自生成一个随机数 $a,b \in Z_q^*$，并将 g^a 和 g^b 发送给对方，双方可计算共享密钥为 $g^{ab}=(g^a)^b=(g^b)^a$。协议的安全性基于有限域上计算离散对数问题的困难性。

1.2　加性秘密共享

秘密共享[23]将秘密数据分割成多个与原始秘密无关的份额，并将这些份额分散存储于不同的实体中，抵御多方合谋的风险。加性秘密共享（ASS, additive secret sharing）是秘密共享的一种具体实现方式，包括秘密分发阶段和秘密重构阶段。在秘密分发阶段，生成 n 个随机数 $\{d_1,d_2,\cdots,d_n\}$ 作为秘密数据 d 的份额。在秘密重构阶段，将所有份额相加恢复原始数据 $d=d_1+d_2+\cdots+d_n$。

1.3　分布式点函数

点函数 $P_{x,y}:\{0,1\}^{|x|}\to\{0,1\}^{|y|}$，对 $x,y\in\{0,1\}^*$ 满足

$$P_{x,y}(i)=\begin{cases} y, i=x \\ 0^{|y|}, i\neq x \end{cases} \tag{1}$$

定义 1　分布式点函数[24-25]。方案包括以下 2 个多项式时间算法。

1) $\mathrm{DpfGen}(x,y)$：密钥生成算法。该算法输入点函数的参数 x,y，输出一对共享函数密钥 k_A,k_B。单个共享函数密钥不会透露 $P_{x,y}$ 的任何信息。

2) $\mathrm{Eval}(k,i)$：求值算法。该算法输入共享函数密钥 k 和要计算的点 i，输出共享函数在该点的值。点函数 $P_{x,y}$ 生成的共享函数密钥对在求值时满足

$$\mathrm{Eval}(k_A,i)+\mathrm{Eval}(k_B,i)=\begin{cases} y, i=x \\ 0^{|y|}, i\neq x \end{cases} \tag{2}$$

2　系统模型

本节对本文方案的系统模型进行介绍，包括系统架构、威胁模型、安全目标和形式化定义。

2.1　系统架构

本文方案系统架构如图 1 所示，主要包括服务器和用户两类实体。

1) 服务器。系统包含 2 个服务器，负责将接收到的邮件消息写入本地维护的邮箱数据库。此外，2 个服务器共同维护一个公告板，用来记录举报者

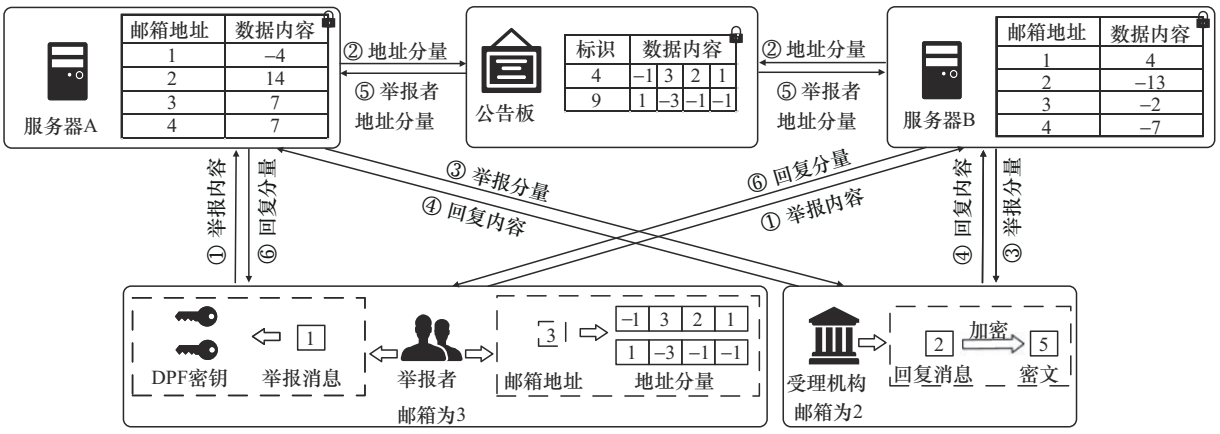


图1　本文方案系统架构

发送的邮箱地址分量信息。

2) 用户。系统包含多个用户，根据通信时消息的流通方向分为数据发送者和数据接收者两类，根据发送的消息内容分为举报者和受理机构两类。用户可以通过服务器读取和写入邮箱数据库中的内容，但只能从公告板中读取内容。

当举报者和受理机构进行一轮相互通信时，各个实体之间的交互流程如下。举报者将自己的举报消息与邮箱地址分别进行DPF和秘密共享操作后作为举报内容发送给2个服务器，并在举报内容中说明邮箱地址分量对应的随机索引标识；每个服务器对接收到的举报内容进行处理后，将对应消息写入邮箱数据库和公告板中；受理机构读取自己邮箱中的举报消息，并将回复消息和举报消息中的索引作为回复内容发给对应的服务器；服务器将该受理机构邮箱中的内容置为0，并根据索引从公告板中读取举报者地址分量，将回复消息写入邮箱数据库；举报者读取回复消息后，服务器将该举报者邮箱中的内容置为0。当同一对举报者和受理机构按照此交互流程进行多次通信时，因公告板中已存在该举报者地址分量，故其只需向服务器发送举报消息即可。

2.2 威胁模型

假设系统中的实体间通过TLS等安全信道进行通信。当一对举报者和受理机构通过2个服务器进行通信时，将面临以下威胁。

1) 半诚实受理机构。与举报者通信的受理机构遵循协议规定，但试图了解举报者的邮箱地址。

2) 恶意攻击者。当双方进行通信时，恶意攻击者可以观察到双方交互时的密文信息，并控制一个服务器和非通信双方的任意数量合法用户来试图了解用户的通信内容和邮箱地址，其中服务器遵循协议规定处理用户的通信请求。

2.3 安全目标

1) 数据接收者匿名性。当双方进行通信时，非参与方不知道目标邮箱地址，即举报时无法关联对应的受理机构，回复时无法关联对应的举报者。

2) 举报者匿名性。受理机构可以回复举报者消息，但无法了解举报者的邮箱地址，即真实身份。

3) 数据机密性。当双方进行通信时，非参与方不知道数据发送者向数据接收者发送的消息内容。

2.4 形式化定义

定义2 基于秘密共享的匿名举报者回复方案。该方案包括以下9个多项式时间算法。

1) Setup(λ,n)：系统初始化算法。该算法由2个服务器共同执行。输入安全参数λ和用户的数量n，输出DHKE公共参数q和g、服务器A的密钥协商参数a和g^a、服务器B的密钥协商参数b和g^b、服务器一次性发布到公告板上的最少消息数量阈值t以及每个用户的索引$\mathrm{id}\in[1,n]$。

2) Regist(λ,id)：邮箱注册算法。该算法由用户和服务器共同执行。输入安全参数λ和用户的索引id，输出邮箱地址$\mathrm{addr}_{\mathrm{id}}$和加密密钥$\mathrm{key}^{\mathrm{A}}_{\mathrm{addr}_{\mathrm{id}}}$和$\mathrm{key}^{\mathrm{B}}_{\mathrm{addr}_{\mathrm{id}}}$。

3) ProvidWrite(addr_p,addr_j,mess_j,g^a,g^b)：举报邮件生成算法。该算法由举报者执行。输入举报者的邮箱地址addr_p、受理机构的邮箱地址addr_j、举报消息mess_j和2个服务器的密钥协商参数g^a和g^b，输出举报者的密钥协商参数x和g^x、举报邮件cont_j的共享函数密钥$k^{\mathrm{A}}_{\mathrm{cont}_j}$和$k^{\mathrm{B}}_{\mathrm{cont}_j}$、地址密文向量$\mathbf{caw}^{\mathrm{A}}_{\mathrm{addr}_p}$和$\mathbf{caw}^{\mathrm{B}}_{\mathrm{addr}_p}$以及随机索引$r_p^{\mathrm{A}}$和$r_p^{\mathrm{B}}$。

4) SerEvalJour($k^s_{\mathrm{cont}_j}$,n)：举报消息恢复算法。该算法由服务器执行。输入共享函数密钥$k^s_{\mathrm{cont}_j}$和用户的数量n，输出邮件向量$\mathbf{mw}_s$。

5) SerWrite($\mathbf{cdw}_s$,$\mathbf{mw}_s$,t,key^s_1,$\cdots$,key^s_n)：数据库更新算法。该算法由服务器执行。输入数据库密文向量$\mathbf{cdw}_s$、邮件向量$\mathbf{mw}_s$、消息数量t和每个用户的加密密钥，输出更新$\mathbf{cdw_s}$。

6) ReadMail($\mathrm{addr}_{\mathrm{id}}$,$\mathrm{key}^{\mathrm{A}}_{\mathrm{addr}_{\mathrm{id}}}$,$\mathrm{key}^{\mathrm{B}}_{\mathrm{addr}_{\mathrm{id}}}$)：读邮件算法。该算法由用户执行。输入用户的邮箱地址$\mathrm{addr}_{\mathrm{id}}$、加密密钥$\mathrm{key}^{\mathrm{A}}_{\mathrm{addr}_{\mathrm{id}}}$和$\mathrm{key}^{\mathrm{B}}_{\mathrm{addr}_{\mathrm{id}}}$，输出举报邮件$\mathrm{cont}_j$。

7) JourWrite(mess_p,cont_j)：回复邮件生成算法。该算法由受理机构执行。输入回复消息mess_p和举报邮件cont_j，输出回复邮件cont_p。

8) SerEvalProvid(cont_p,$r_p^{s/\{\mathrm{A,B}\}}$,g^x,k)：回复消息恢复算法。该算法由服务器执行。输入回复邮件cont_p、举报消息中提供的随机索引$r_p^{s/\{\mathrm{A,B}\}}$和密钥协商参数g^x、$k\in\{a,b\}$，输出邮件向量$\mathbf{mw}_s$。

9) ContDec(cont_p,key^j_p)：回复消息解密算法。

该算法由举报者执行。输入回复邮件 cont_p 和加密密钥 key_p^j，输出回复消息 mess_p。

3　方案设计

本节首先具体介绍了本文方案，之后给出了多个匿名举报者同时发起举报时的处理方案，最后对 Express[18] 方案进行了介绍。

3.1　本文方案

本节介绍了本文提出的基于秘密共享的匿名举报者回复方案。当举报者和受理机构两类用户实体进行一轮完整的通信交互时，该方案共分为系统初始化、邮箱注册、匿名举报、举报邮件读取、举报邮件回复和回复邮件读取 6 个算法。

3.1.1　系统初始化

使用系统初始化算法生成公共参数。首先 2 个服务器共同选择用于 DHKE 的参数 q 和 g，分别生成随机数 $a,b \in Z_q^*$，并公开 $\{q,g,g^a,g^b\}$，接着两服务器协商在公告板上发布信息时的消息数量阈值 t，最后为每个用户分配一个索引 $\mathrm{id} \in [1,n]$ 作为标识，n 为系统中用户的数量。

3.1.2　邮箱注册

使用邮箱注册算法进行用户注册。用户注册邮箱时，将自己的索引 id 分别发送给 2 个服务器，两服务器共同协商一个邮箱地址 $\mathrm{addr}_{\mathrm{id}}$，并将其发送给该用户，用户收到邮箱地址后生成用于加密 2 个服务器邮箱数据库对应内容的密钥 $\{\mathrm{key}_{\mathrm{addr}_{\mathrm{id}}}^{\mathrm{A}},\mathrm{key}_{\mathrm{addr}_{\mathrm{id}}}^{\mathrm{B}}\}$，并发送给 2 个服务器。每个服务器 $s \in \{\mathrm{A,B}\}$ 将邮箱数据库中该用户邮箱地址对应的内容 $\mathrm{dw}_s^{\mathrm{addr}_{\mathrm{id}}}$ 初始化为 0，根据收到的密钥使用对称加密算法进行加密得到密文 $\mathrm{cdw}_s^{\mathrm{addr}_{\mathrm{id}}}$，并存储在数据库中。

3.1.3　匿名举报

首先使用举报邮件生成算法对举报消息和举报者邮箱地址进行处理得到举报内容，接着使用举报消息恢复算法对举报内容进行处理计算，最后使用数据库更新算法将计算结果分别写入对应的邮箱数据库和公告板中。具体步骤如下。

1) 举报邮件生成算法

当索引 id 为 p 的举报者向索引 id 为 j 的受理机构发送举报消息 mess_j 时，如果希望得到受理机构的回复，则根据自己的邮箱地址生成邮箱地址向量 $\mathbf{aw}_{\mathrm{addr}_p} = [0,\cdots,0,1,0,\cdots,0]$，该向量共含有 n 个元素，第 addr_p 个元素的值为 1，其余为 0。为了隐藏自己的真实邮箱地址，举报者使用 ASS 对邮箱地址向量中的每一个元素进行随机化处理，为服务器 $s \in \{\mathrm{A,B}\}$ 生成随机向量 $\mathbf{aw}_{\mathrm{addr}_p}^s = [\mathrm{aw}_1^s,\cdots,\mathrm{aw}_n^s]$，随机向量中每个元素的值与之前无关，且满足

$$\mathrm{aw}_i^{\mathrm{A}} + \mathrm{aw}_i^{\mathrm{B}} = \begin{cases} 1, i = \mathrm{addr}_p \\ 0, i \neq \mathrm{addr}_p \end{cases} \tag{3}$$

举报者生成随机数 $x \in Z_q^*$，计算和 2 个服务器的共享密钥 g^{ax} 和 g^{bx}，根据 g^{bx} 使用对称加密算法对向量 $\mathbf{aw}_{\mathrm{addr}_p}^{\mathrm{B}}$ 中的元素进行加密得到地址密文向量 $\mathbf{caw}_{\mathrm{addr}_p}^{\mathrm{A}}$，根据 g^{ax} 使用对称加密算法对向量 $\mathbf{aw}_{\mathrm{addr}_p}^{\mathrm{A}}$ 中的元素进行加密得到地址密文向量 $\mathbf{caw}_{\mathrm{addr}_p}^{\mathrm{B}}$，之后生成 2 个随机数 r_p^{A} 和 r_p^{B} 分别作为向量 $\mathbf{aw}_{\mathrm{addr}_p}^{\mathrm{B}}$ 和 $\mathbf{aw}_{\mathrm{addr}_p}^{\mathrm{A}}$ 对应密文向量的索引，方便后续在公告板上进行查找。此外，举报者还生成随机数 r_p^j 和对称密钥 key_p^j 分别用来识别该受理机构和加密回复消息，此时发送给受理机构的举报邮件为 $\mathrm{cont}_j = \{r_p^{\mathrm{A}} \| r_p^{\mathrm{B}} \| g^x \| r_p^j \| \mathrm{key}_p^j \| \mathrm{mess}_j\}$。举报者根据 addr_j 和 cont_j 生成一对分布式点函数共享函数密钥 $k_{\mathrm{cont}_j}^{\mathrm{A}}$ 和 $k_{\mathrm{cont}_j}^{\mathrm{B}}$，将 $\{\mathbf{caw}_{\mathrm{addr}_p}^{\mathrm{A}}, r_p^{\mathrm{A}}, k_{\mathrm{cont}_j}^{\mathrm{A}}\}$ 发送给服务器 A，$\{\mathbf{caw}_{\mathrm{addr}_p}^{\mathrm{B}}, r_p^{\mathrm{B}}, k_{\mathrm{cont}_j}^{\mathrm{B}}\}$ 发送给服务器 B。

2) 举报消息恢复算法

服务器 $s \in \{\mathrm{A,B}\}$ 使用分布式点函数求值算法计算 $k_{\mathrm{cont}_j}^s$ 在每一个点上的值，得到邮件向量，表示为

$$\begin{aligned} \mathbf{mw}_s &= [\mathrm{mw}_s^1,\cdots,\mathrm{mw}_s^n] = \\ &[\mathrm{Eval}(k_{\mathrm{cont}_j}^s,1),\cdots,\mathrm{Eval}(k_{\mathrm{cont}_j}^s,n)] \end{aligned} \tag{4}$$

根据定义 1 可知，两向量相加满足式(5)，即结果向量中第 addr_j 个元素为举报邮件，其余为 0。

$$\mathbf{mw}_{\mathrm{A}} + \mathbf{mw}_{\mathrm{B}} = [0,\cdots,0,\mathrm{cont}_j,0,\cdots,0] \tag{5}$$

3) 数据库更新算法

服务器 $s \in \{\mathrm{A,B}\}$ 使用对称解密算法对邮箱数据库中存储的内容即密文向量 $\mathbf{cdw}_s = [\mathrm{cdw}_s^1,\cdots,\mathrm{cdw}_s^n]$ 进行解密，得到数据库向量，表示为

$$\begin{aligned} \mathbf{dw}_s &= [\mathrm{dw}_s^1,\cdots,\mathrm{dw}_s^n] = \\ &[D_{\mathrm{key}_1^s}(\mathrm{cdw}_s^1),\cdots,D_{\mathrm{key}_n^s}(\mathrm{cdw}_s^n)] \end{aligned} \tag{6}$$

若该处理机构邮箱中没有其他邮件，则数据库向量中第 addr_j 个元素满足

$$\mathrm{dw}_{\mathrm{A}}^{\mathrm{addr}_j} + \mathrm{dw}_{\mathrm{B}}^{\mathrm{addr}_j} = 0 \tag{7}$$

服务器将 $\mathbf{dw}_s$ 与 $\mathbf{mw}_s$ 两向量相加更新 $\mathbf{dw}_s$，根

据式(5)可知，更新后的两个$\mathbf{dw}_s$向量相加，结果向量中第addr_j个元素变为邮件内容，其他保持不变。服务器根据每位用户的对称密钥使用对称加密算法对$\mathbf{dw}_s$中的元素进行加密，以更新邮箱数据库，如式(8)所示。

$$\mathbf{cdw}_s = [E_{\mathrm{key}_1^s}(\mathrm{dw}_s^1 + \mathrm{mw}_s^1),\cdots,E_{\mathrm{key}_n^s}(\mathrm{dw}_s^n + \mathrm{mw}_s^n)] \tag{8}$$

其中，E_k表示对称加密算法，D_k表示对应的对称解密算法。

此外，当服务器收到的地址密文向量数量不少于t时，选择随机的时间将所有$\{r_{\mathrm{id}}^s,\mathbf{caw}_{\mathrm{addr_{id}}}^s\}$以随机顺序发布到公告板上。举报者可根据索引在公告板上查找对应的密文向量以检查其正确性。

3.1.4 举报邮件读取

使用读邮件算法读取邮件。受理机构向2个服务器发送邮箱地址addr_j，得到邮箱数据库中该地址的对应值$\mathrm{cdw}_{\mathrm{A}}^{\mathrm{addr}_j}$和$\mathrm{cdw}_{\mathrm{B}}^{\mathrm{addr}_j}$，根据式(5)和式(7)，受理机构使用对称解密算法解密$\mathrm{cdw}_{\mathrm{A}}^{\mathrm{addr}_j}$和$\mathrm{cdw}_{\mathrm{B}}^{\mathrm{addr}_j}$后相加可恢复邮件内容，获取举报消息$\mathrm{mess}_j$，如式(9)所示。

$$\begin{aligned}&D_{\mathrm{key}_{\mathrm{addr}_j}^{\mathrm{A}}}(\mathrm{cdw}_{\mathrm{A}}^{\mathrm{addr}_j}) + D_{\mathrm{key}_{\mathrm{addr}_j}^{\mathrm{B}}}(\mathrm{cdw}_{\mathrm{B}}^{\mathrm{addr}_j}) =\\ &\mathrm{dw}_{\mathrm{A}}^{\mathrm{addr}_j} + \mathrm{mw}_{\mathrm{A}}^{\mathrm{cont}_j} + \mathrm{dw}_{\mathrm{B}}^{\mathrm{addr}_j} + \mathrm{mw}_{\mathrm{B}}^{\mathrm{cont}_j} =\\ &\mathrm{mw}_{\mathrm{A}}^{\mathrm{cont}_j} + \mathrm{mw}_{\mathrm{B}}^{\mathrm{cont}_j} = \mathrm{cont}_j\end{aligned} \tag{9}$$

邮箱拥有者读取邮件后，服务器初始化对应邮箱数据库中的内容，通过该用户的密钥对0进行加密，并用密文替换该数据库中对应的数据。

3.1.5 举报邮件回复

首先使用回复邮件生成算法处理回复消息得到回复内容，接着使用回复消息恢复算法对回复内容进行处理计算，最后使用3.1.3节的数据库更新算法更新邮箱数据库。具体步骤如下。

1) 回复邮件生成算法

受理机构根据举报邮件cont_j中的对称密钥key_p^j使用对称加密算法加密回复消息mess_p，此时回复邮件$\mathrm{cont}_p = \{r_p^j \| E_{\mathrm{key}_p^j}(\mathrm{mess}_p)\}$。受理机构将$\{\mathrm{cont}_p, r_p^{\mathrm{B}}, g^x\}$发送给服务器A，$\{\mathrm{cont}_p, r_p^{\mathrm{A}}, g^x\}$发送给服务器B。

2) 回复消息恢复算法

服务器$s \in \{\mathrm{A,B}\}$首先根据索引查找公告板中对应的消息，得到回复地址密文向量。接着计算共享密钥g^{kx}，当s为服务器A时，k为a，当s为服务器B时，k为b，并根据共享密钥g^{kx}使用对称解密算法对回复地址密文向量中的元素进行解密得到随机向量$\mathbf{aw}_{\mathrm{addr}_p}^s$。最后根据式(10)将回复邮件$\mathrm{cont}_p$和向量$\mathbf{aw}_{\mathrm{addr}_p}^s$中的元素相乘得到邮件向量。根据式(3)，2个服务器的邮件向量相加得到的结果向量中第addr_p个元素为回复邮件cont_p，其余为0。

$$\begin{aligned}\mathbf{mw}_s &= \mathrm{cont}_p \mathbf{aw}_{\mathrm{addr}_p}^s =\\ &[\mathrm{cont}_p \mathrm{aw}_1^s,\cdots,\mathrm{cont}_p \mathrm{aw}_n^s]\end{aligned} \tag{10}$$

3) 数据库更新算法

每个服务器$s \in \{\mathrm{A,B}\}$使用SerWrite($\mathbf{cdw}_s$, $\mathbf{mw}_s, t, \mathrm{key}_1^s,\cdots,\mathrm{key}_n^s$)算法更新邮箱数据库。

3.1.6 回复邮件读取

首先使用3.1.4节的读邮件算法读取回复邮件，接着使用回复消息解密算法处理回复邮件恢复回复消息。具体步骤如下。

1) 读邮件算法

举报者使用ReadMail($\mathrm{addr}_p, \mathrm{key}_{\mathrm{addr}_p}^{\mathrm{A}}, \mathrm{key}_{\mathrm{addr}_p}^{\mathrm{B}}$)算法得到受理机构的回复邮件$\mathrm{cont}_p$。

2) 回复消息解密算法

举报者首先根据cont_p中的随机标识r_p^j找到key_p^j，接着使用对称解密算法解密密文得到回复消息mess_p。

3.2 多举报者匿名举报

当多个举报者同时发起举报时，存在以下两种情况，即分别向不同受理机构和相同受理机构进行举报。假设邮箱地址集合为$\{\mathrm{wb}_1,\cdots,\mathrm{wb}_k\}$，对应的举报消息集合为$\{\mathrm{mess}_1,\cdots,\mathrm{mess}_k\}$，当$k(k \leqslant n)$个举报者同时发起举报时，下面分别介绍针对两种情况的处理方案。

1) 不同受理机构举报

假设邮箱地址为$\mathrm{wb}_i(i \in [1,\cdots,k])$的举报者向邮箱地址为$\mathrm{rp}_i(i \in [1,\cdots,k])$的受理机构发送邮件，此时每个受理机构$\mathrm{rp}_i$有且仅有一个举报者。

对于受理机构rp_i来说，当系统中所有用户未发邮件时，根据3.1.2节可知，rp_i对应的2个邮箱内容满足$\mathrm{dw}_{\mathrm{A}}^{\mathrm{rp}_i} + \mathrm{dw}_{\mathrm{B}}^{\mathrm{rp}_i} = 0$。当所有举报者同时进行举报时，若举报者的邮箱地址不是wb_i，则其不会将举报消息写入邮箱地址rp_i中，根据3.1.3节可知，举报者更新邮箱数据库后$\mathrm{dw}_{\mathrm{A}}^{\mathrm{rp}_i} + \mathrm{dw}_{\mathrm{B}}^{\mathrm{rp}_i} = 0$仍然成立。若举报者的邮箱地址是$\mathrm{wb}_i$，则其会将举

报消息写入邮箱地址 rp_i 中，根据 3.1.3 节可知，举报者更新邮箱数据库后满足 $\mathrm{dw}_{\mathrm{A}}^{\mathrm{rp}_i} + \mathrm{dw}_{\mathrm{B}}^{\mathrm{rp}_i} = \mathrm{mess}_i$。每个举报者可独立按照 3.1 节中的交互流程进行举报。

当多个举报者同时向不同的受理机构进行举报时，可以并行开展，彼此之间不会产生任何干扰。

2) 相同受理机构举报

假设邮箱地址为 $\mathrm{wb}_i\,(i \in [1,\cdots,k])$ 的举报者同时向邮箱地址为 rp 的受理机构发送邮件。

对于受理机构 rp 来说，当系统中所有用户未发邮件时，根据 3.1.2 节可知，rp 对应的 2 个邮箱内容满足 $\mathrm{dw}_{\mathrm{A}}^{\mathrm{rp}} + \mathrm{dw}_{\mathrm{B}}^{\mathrm{rp}} = 0$。当 k 个举报者同时进行举报时，因为每一个举报者都将举报消息写入邮箱地址 rp 中，故所有举报者完成举报后，根据 3.1.3 节可知，该受理机构将从邮箱内容中获取信息 $\mathrm{dw}_{\mathrm{A}}^{\mathrm{rp}} + \mathrm{dw}_{\mathrm{B}}^{\mathrm{rp}} = \mathrm{mess}_1 + \cdots + \mathrm{mess}_k$，无法获得每一个信息的内容。为了解决此问题，在受理机构会及时查看邮箱内容的前提下，可以令每一个举报者在发送举报消息时都生成一个随机时间并将其放进举报消息中，若在此时间内举报者未收到回复，则会重新发送举报消息。

当多个举报者同时向相同的受理机构进行举报时，彼此之间会产生干扰，但可通过随机化举报时间解决该问题。

3.3　Express 方案

该方案主要分为邮箱注册、邮件写入和邮件读取 3 个阶段，其中邮箱注册阶段流程和本文方案相同。当用户向邮箱地址 rp 写入消息 mess 时，邮件写入和读取的流程如下。

1) 邮件写入

用户根据邮箱地址 rp 和消息 mess 生成一对分布式点函数共享函数密钥 $k_{\mathrm{mess}}^{\mathrm{A}}$ 和 $k_{\mathrm{mess}}^{\mathrm{B}}$，$k_{\mathrm{mess}}^{\mathrm{A}}$ 发送给服务器 A，将 $k_{\mathrm{mess}}^{\mathrm{B}}$ 发送给服务器 B。服务器调用 3.1.3 节中的举报消息恢复算法和数据库更新算法将消息写入自己的服务器数据库中。

2) 邮件读取

用户调用 3.1.4 节中的读邮件算法读取自己邮箱中的内容。

4　安全证明

本节对本文方案的安全性进行分析与证明。假设方案中使用的密码原语是安全的，即遵循 DPF、DHKE、ASS 和对称加密算法的基础操作为安全的。使用以下定义和定理证明协议是安全的。

4.1　数据接收者匿名性

定义 3　对于任何半诚实的概率多项式时间（PPT, probabilistic polynomial time）敌手 $\mathcal{A}_1$ 控制一个服务器和任意数量用户，同时和另一个不合谋服务器 S 处理剩余诚实用户的通信请求，如果存在模拟器 Sim_1 满足

$$\left|\Pr\left(\mathrm{Real}_{\mathcal{A}_1,L_1}(1^\lambda,M_{\mathcal{A}_1},M_S)=f(1^\lambda,\mathrm{addr})\right)-\right.$$
$$\left.\Pr\left(\mathrm{Ideal}_{\mathrm{Sim}_1,L_1}(1^\lambda)=f(1^\lambda,\mathrm{addr})\right)\right|\leqslant \mathrm{negl}(\lambda) \quad (11)$$

使敌手 $\mathcal{A}_1$ 无法区分现实视图和模拟器视图，则方案满足数据接收者匿名性。其中，addr 表示数据接收者的邮箱地址，$f(1^\lambda,\mathrm{addr})$ 表示获得的邮箱地址的相关信息，$M_{\mathcal{A}_1}$ 表示敌手控制服务器收到的信息，M_S 表示敌手 $\mathcal{A}_1$ 获得有关服务器 S 的信息，$\mathrm{negl}(\lambda)$ 表示可忽略函数，L_1 表示泄露的信息，包括消息的大小 len_1、邮箱地址的大小 len_2、用户的数量 n 和每个用户的邮箱地址 $\mathrm{addr}_{\mathrm{id}}$，其中 $\mathrm{id} \in [1,n]$。

定理 1　如果基于秘密共享的匿名举报者回复协议中的所有子协议是完美的模拟，即不可区分，则该协议是不可区分的[26]。

证明　当进行一轮完整的协议通信时，若子协议是不可区分的，则敌手在每个子协议执行完后无法区分现实世界视图和模拟世界视图中数据接收者的邮箱地址和举报者的邮箱地址，当按照协议依次执行完所有子协议后，敌手仍无法区分现实世界视图和模拟世界视图中数据接收者的邮箱地址和举报者的邮箱地址，因此整个协议对敌手来说是不可区分的，从而满足数据接收者匿名性和举报者匿名性。证毕。

引理 1　系统初始化协议和邮箱注册协议对敌手 $\mathcal{A}_1$ 是不可区分的。

证明　系统初始化协议和邮箱注册协议为初始化阶段，此时用户还未发送邮件，即使存在敌手 $\mathcal{A}_1$ 的威胁，两协议仍是安全的。证毕。

引理 2　匿名举报协议对敌手 $\mathcal{A}_1$ 是不可区分的。

证明　本文将构造模拟器 Sim_1，在理想世界中执行，其中 Sim_1 的构造过程如下。

模拟器 Sim_1 生成长度为 len_1 的随机数 η，调用分布式点函数密钥生成算法 $\mathrm{DpfGen}(0,\eta)$ 生成密钥 $k_{\mathcal{A}_1}$ 和 k_S，将 $(1^\lambda,k_{\mathcal{A}_1})$ 作为模拟视图发送给敌手 $\mathcal{A}_1$。

根据DPF算法的安全性，Sim_1生成的$k_{\mathcal{A}_1}$和$\mathrm{Real}_{\mathcal{A}_1,L_1}$中的$M_{\mathcal{A}_1}$不可区分，因此没有泄露任何地址信息。综合以上分析，模拟器Sim_1生成一种在计算上与现实世界无法区分的视图，因此匿名举报协议在理想和现实中是无法区分的理想执行[26]。证毕。

引理3 举报邮件读取协议对敌手$\mathcal{A}_1$是不可区分的。

证明 本文将构造模拟器Sim_1，在理想世界中执行，其中Sim_1的构造过程如下。

模拟器Sim_1根据引理2中模拟器的构造生成密钥$k_{\mathcal{A}_1}$和k_S，并生成对称密钥key，对长度为len_1的消息0进行加密得到对应的密文c为$E_{\mathrm{key}}(0^{\mathrm{len}_1})$，将$(1^\lambda,k_{\mathcal{A}_1},c)$作为模拟视图发送给$\mathcal{A}_1$。$\mathcal{A}_1$通过计算$\mathrm{Eval}(k_{\mathcal{A}_1},\mathrm{addr}_{\mathrm{id}})+D_{\mathrm{key}}(c)$是否为0来判断读取邮箱是否是目标邮箱，在$\mathcal{A}_1$不知道对称密钥key的情况下，根据对称加密算法的安全性，Sim_1生成的密文c和$\mathrm{Real}_{\mathcal{A}_1,L_1}$中的$M_S$不可区分，故无法获得计算结果的任何信息。综合以上分析，模拟器Sim_1生成一种在计算上与现实世界无法区分的视图，因此举报邮件读取协议在理想和现实中是无法区分的理想执行。证毕。

引理4 举报邮件回复协议对敌手$\mathcal{A}_1$是不可区分的。

证明 本文将构造模拟器Sim_1，在理想世界中执行，其中Sim_1的构造过程如下。

模拟器Sim_1生成n个长度为len_2的随机数作为向量$\mathbf{aw}_{\mathrm{addr}_p}^{\mathcal{A}_1}=[\eta_1,\cdots,\eta_n]$中的元素和全0向量$\mathbf{aw}_{\mathrm{addr}_p}^{S}=[0^{\mathrm{len}_2},\cdots,0^{\mathrm{len}_2}]$，根据DHKE算法生成对称密钥key，对向量$\mathbf{aw}_{\mathrm{addr}_p}^{S}$中的元素进行对称加密得到$\mathbf{caw}_{\mathrm{addr}_p}^{S}$，将$(1^\lambda,\mathbf{aw}_{\mathrm{addr}_p}^{\mathcal{A}_1},\mathbf{caw}_{\mathrm{addr}_p}^{S})$作为模拟视图发送给$\mathcal{A}_1$。$\mathcal{A}_1$计算两明文向量和中非零元素所在位置为目标邮箱，根据秘密共享的安全性，Sim_1生成的$\mathbf{aw}_{\mathrm{addr}_p}^{\mathcal{A}_1}$和$\mathrm{Real}_{\mathcal{A}_1,L_1}$中的$M_{\mathcal{A}_1}$不可区分，根据DHKE算法的安全性，$\mathcal{A}_1$无法获得对称密钥key，此时根据对称加密算法的安全性，Sim_1生成的$\mathbf{caw}_{\mathrm{addr}_p}^{S}$和$\mathrm{Real}_{\mathcal{A}_1,L_1}$中的$M_S$不可区分，故无法获得邮箱地址的任何信息。综合以上分析，模拟器Sim_1生成一种在计算上与现实世界无法区分的视图，因此举报邮件回复协议在理想和现实中是无法区分的理想执行。证毕。

引理5 回复邮件读取协议对敌手$\mathcal{A}_1$是不可区分的。

证明 本文将构造模拟器Sim_1，在理想世界中执行，其中Sim_1的构造过程如下。

模拟器Sim_1根据引理4中的模拟器构造$\mathbf{aw}_{\mathrm{addr}_p}^{\mathcal{A}_1}$，生成对称密钥$\mathrm{key}_1$和$\mathrm{key}_2$，根据对称加密算法对长度为$\mathrm{len}_1$的消息0进行加密，得到密文$c_1$为$E_{\mathrm{key}_1}(0^{\mathrm{len}_1})$、密文$c_2$为$E_{\mathrm{key}_2}(0^{\mathrm{len}_1})$，将$(1^\lambda,\{\mathbf{aw}_{\mathrm{addr}_p}^{\mathcal{A}_1},c_1\},c_2)$作为模拟视图发送给$\mathcal{A}_1$。$\mathcal{A}_1$通过计算消息$\mathbf{aw}_{\mathrm{addr}_p}^{\mathcal{A}_1}[\mathrm{addr}_{\mathrm{id}}]c_1+D_{\mathrm{key}_2}(c_2)$是否为0来判断读取邮箱是否是目标邮箱，在$\mathcal{A}_1$不知道对称密钥$\mathrm{key}_2$的情况下，根据对称加密算法的安全性，$\mathrm{Sim}_1$生成的密文$c_2$和$\mathrm{Real}_{\mathcal{A}_1,L_1}$中的$M_S$不可区分，故无法获得计算结果的任何信息。综合以上分析，模拟器Sim_1生成一种在计算上与现实世界无法区分的视图，因此回复邮件读取协议在理想和现实中是无法区分的理想执行。证毕。

定理2 即使存在敌手$\mathcal{A}_1$的威胁，本文方案仍满足数据接收者匿名性。

证明 由引理1~引理5可知，本文方案各子协议在敌手$\mathcal{A}_1$的威胁下仍然可保证安全，再由定理1得该方案在理想和现实的计算过程中是无法区分的。因此，本文方案满足数据接收者匿名性。证毕。

4.2 举报者匿名性

定义4 对于任何半诚实的PPT敌手$\mathcal{A}_2$，控制通信过程中的受理机构，如果存在模拟器Sim_2满足

$$\left|\Pr\left(\mathrm{Real}_{\mathcal{A}_2,L_2}(1^\lambda,\mathbf{caw}_{\mathrm{addr}}^{\mathrm{A}},\mathbf{caw}_{\mathrm{addr}}^{\mathrm{B}})=f(1^\lambda,\mathrm{addr})\right)-\Pr\left(\mathrm{Ideal}_{\mathrm{Sim}_2,L_2}(1^\lambda)=f(1^\lambda,\mathrm{addr})\right)\right|\leqslant\mathrm{negl}(\lambda)\tag{12}$$

使敌手$\mathcal{A}_2$无法区分现实视图和模拟器视图，则本文方案满足举报者匿名性。其中，addr表示举报者的邮箱地址，$f(1^\lambda,\mathrm{addr})$表示获得的邮箱地址的相关信息，$\mathbf{caw}_{\mathrm{addr}}^{\mathrm{A}}$和$\mathbf{caw}_{\mathrm{addr}}^{\mathrm{B}}$表示通过举报邮件读取协议获得的地址对应的密文向量，L_2表示泄露的信息，包括向量的长度n和地址的大小len。

引理6 匿名举报协议和回复邮件读取协议对敌手$\mathcal{A}_2$是不可区分的。

证明 受理机构不参与匿名举报协议和回复邮件读取协议，即使存在敌手$\mathcal{A}_2$的威胁，两协议仍

是安全的。证毕。

引理7　举报邮件回复协议对敌手$\mathcal{A}_2$是不可区分的。

证明　本文将构造模拟器Sim_2，在理想世界中执行，其中Sim_2的构造过程如下。

模拟器Sim_2根据DHKE算法生成密钥key_A和key_B，元素数量为n的全0邮箱地址向量$[0^{\mathrm{len}},\cdots,0^{\mathrm{len}}]$，使用密钥分别对向量中的元素进行加密，得到$\mathbf{caw}_0^{\mathrm{A}}$和$\mathbf{caw}_0^{\mathrm{B}}$，将$(1^\lambda,\mathbf{caw}_0^{\mathrm{A}},\mathbf{caw}_0^{\mathrm{B}})$作为模拟视图发送给$\mathcal{A}_2$。$\mathcal{A}_2$计算两明文向量和中非零元素所在位置为举报者地址，由于密文向量中的每一个元素都被加密，根据DHKE算法的安全性，$\mathcal{A}_2$无法获得密钥key_A和key_B，而在$\mathcal{A}_2$不知道密钥的情况下，根据对称加密算法的安全性，Sim_2生成的$\mathbf{caw}_0^{\mathrm{A}}$、$\mathbf{caw}_0^{\mathrm{B}}$和$\mathrm{Real}_{\mathcal{A}_2,L_2}$中的$\mathbf{caw}_{\mathrm{addr}}^{\mathrm{A}}$、$\mathbf{caw}_{\mathrm{addr}}^{\mathrm{B}}$不可区分。综合以上分析，模拟器$\mathrm{Sim}_2$生成一种在计算上与现实世界无法区分的视图，因此举报邮件回复协议在理想和现实中是无法区分的理想执行。证毕。

定理3　即使存在敌手$\mathcal{A}_2$的威胁，本文方案仍满足举报者匿名性。

证明　由引理1、引理6和引理7可知，本文方案各子协议在敌手$\mathcal{A}_2$的威胁下仍然可保证安全，再由定理1得该方案在理想和现实的计算过程中是无法区分的。因此，本文方案满足举报者匿名性。证毕。

4.3　数据机密性

定义5　对于任何半诚实的PPT敌手$\mathcal{A}_1$，控制一个服务器和任意数量的用户，同时处理剩余诚实用户的通信请求，如果存在模拟器Sim_3满足

$$\begin{aligned}&|\Pr(\mathrm{Real}_{\mathcal{A}_1,L_1}(1^\lambda,M_{\mathcal{A}_1},M_S)=f(1^\lambda,m))-\\&\Pr(\mathrm{Ideal}_{\mathrm{Sim}_3,L_1}(1^\lambda)=f(1^\lambda,m))|\leqslant\mathrm{negl}(\lambda)\end{aligned}\quad(13)$$

使敌手$\mathcal{A}_1$无法区分现实视图和模拟器视图，则本文方案满足数据接收者匿名性。其中，m表示数据发送者向数据接收者发送的消息。

定理4　即使存在敌手$\mathcal{A}_1$的威胁，本文方案仍满足数据机密性。

证明　敌手$\mathcal{A}_1$通过判断邮箱内容是否发生变化来确定数据接收者地址，由定理2可知，本文方案满足数据接收者匿名性，故敌手$\mathcal{A}_1$无法判断邮箱内容是否发生变化，即该方案在理想和现实的计算过程中是无法区分的，满足数据机密性。证毕。

5　性能分析

5.1　实验环境

为了对本文方案的实际性能进行评估，本节实现了匿名举报者回复方案，并与Express方案[18]进行对比。实验的硬件环境和软件环境如下：CPU为128 Intel(R) Xeon(R) Platinum 8336C CPU @ 2.30 GHz，操作系统为Ubuntu 20.04.6，对称加密算法为AES 128，编程语言为C和Go，其中DPF、AES、ASS等密码学操作和数据存储由C语言编写，基于libdpf库和OpenSSL 1.1.1f，数据传输由Go语言编写。

本节主要对本文方案中用户和服务器在初始化、写入和读取邮件阶段的计算开销进行了测试，实验设置消息大小分别为1 KB、10 KB、20 KB和30 KB，邮箱数量分别为2^{10}、2^{12}、2^{14}、2^{16}和2^{18}个，并对消息大小为1 KB时用户发送邮件的通信开销进行了测试。本节中的所有实验数据为10次实验结果的平均值。

5.2　用户计算开销

举报者发送邮件时的计算开销包括用户生成DPF密钥和地址密文向量两部分。用户生成DPF密钥的计算开销如图2所示，随着邮箱数量和消息大小的逐步增加。因用户生成DPF密钥的计算开销与消息大小相关，且举报者发送给受理机构的消息中含有对称密钥，故密钥的增大也会导致共享数据量的增加，从而增加用户生成DPF密钥的计算开销。

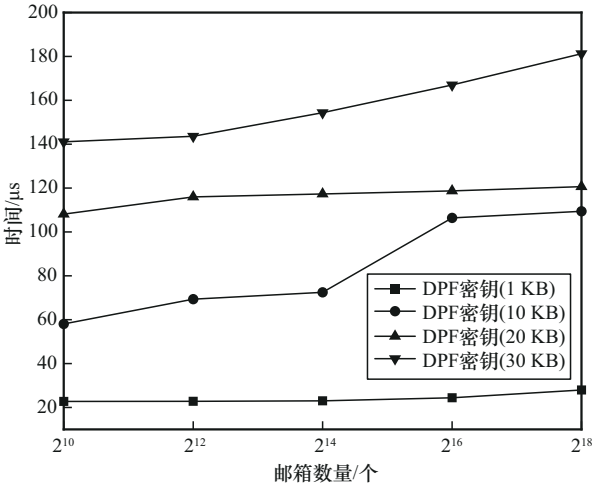


图2　用户生成DPF密钥的计算开销

举报者生成地址密文向量的计算开销如图3所示。由图3可知，举报者生成地址密文向量的计算开销不受消息大小的影响，仅与邮箱数量成正比。对比图2和图3可知，举报者的主要计算开销来自生成地址密文向量所需的秘密共享和对称加密操作，与只需要生成DPF密钥的Express方案相比计算开销较大，但此操作为一次性的，举报者只需生成一次，后续可一直使用该向量。

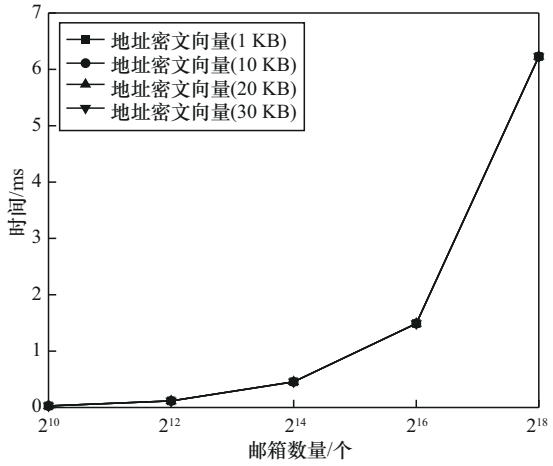


图3　举报者生成地址密文向量的计算开销

用户回复邮件的计算开销如图4所示。受理机构的计算开销主要集中在消息的加密操作上，与邮箱数量无关，与消息大小成正比。从图4中可以看出，在邮箱数量和消息大小保持一致的条件下，受理机构发送邮件的计算开销显著低于Express方案，约减少60%。

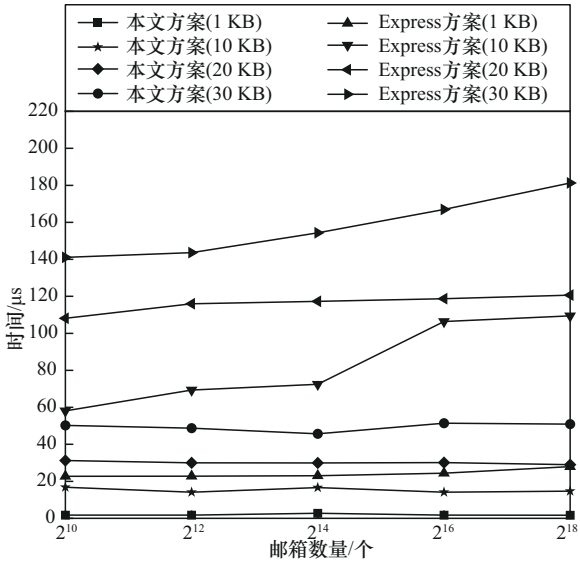


图4　用户回复邮件的计算开销

用户读取邮件的计算开销如图5所示。由图5可知，邮箱数量对用户读取邮件的计算开销没有影响，但随着邮件消息大小的增加，用户读取邮件的计算开销逐步增加。对比受理机构和举报者，可以看出举报者在读取邮件时增加了有限的计算开销，这主要是由于举报者需要进行额外的对称解密操作。

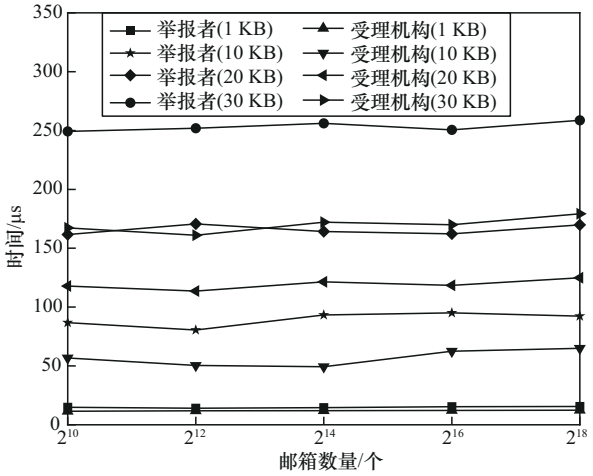


图5　用户读取邮件的计算开销

5.3　服务器计算开销

注册邮箱的总计算开销如图6所示，服务器为所有用户注册邮箱时的总计算开销与邮箱数量成正比，并随邮件消息大小的增加而升高。

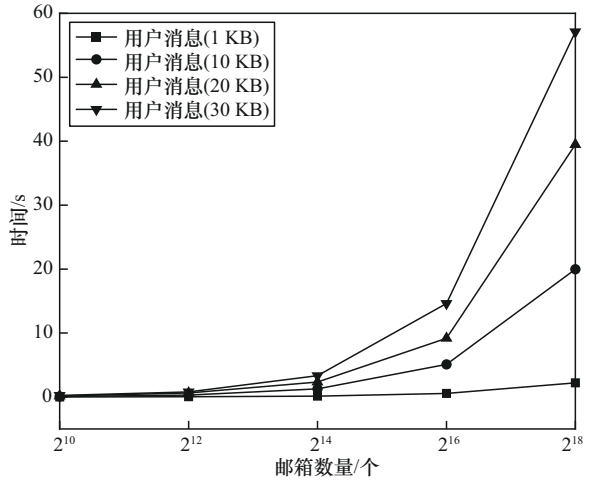


图6　注册邮箱的总计算开销

服务器写入邮件的计算开销如图7所示。从图7中可以看出，随着邮箱数量和消息大小的增加，服务器写入邮件的计算开销逐步增加。服务器写入举报者邮件时的计算开销和Express方案大体

相同，写入受理机构邮件时的计算开销小于举报者和Express方案的计算开销，约降低50%。

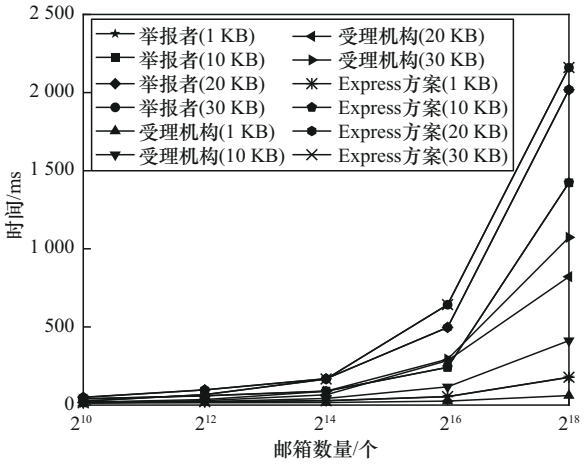


图7　服务器写入邮件的计算开销

5.4　通信开销

用户写入邮件时与单个服务器的通信开销如图8所示。当用户发送1 KB消息时，举报者的通信开销主要来自传输地址密文向量，和邮箱数量成正比，受理机构只传输密文消息，通信开销和邮箱数量无关，Express方案通信开销和邮箱数量的对数成正比。

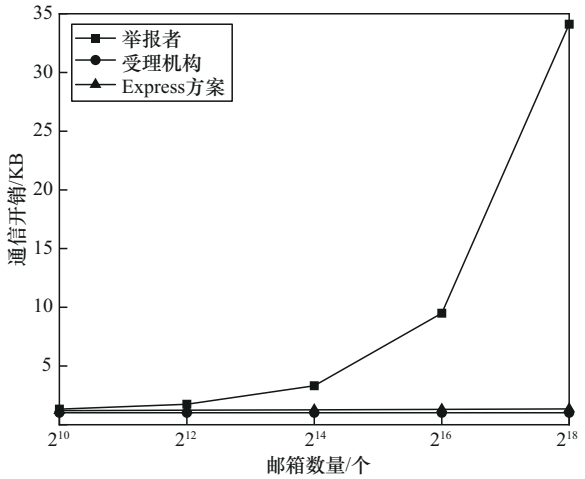


图8　用户写入邮件时与单个服务器的通信开销

6　结束语

本文提出了一个基于秘密共享的匿名举报者回复方案，旨在匿名举报场景下，解决目前匿名通信系统中公告板模型和邮箱模型无法回复匿名举报者的问题。通过秘密共享技术隐藏举报者的地址，并在举报邮件回复阶段降低了受理机构和服务器的计算开销。本文方案的安全性得到了充分验证，能够切实有效保护举报者的合法权益，为新闻自由、反腐败斗争等关键领域提供了技术支撑。此外，本文方案强大的隐私保护能力同样适用于隐私性需求更强的匿名群组通信、电子拍卖等应用场景，展现了强大的应用潜力和价值。下一步工作将研究如何统一举报者和受理机构的行为，同时致力于降低公告板的存储开销，提升本文方案的整体性能。

参考文献：

[1] POSETTI J. Protecting journalism sources in the digital age[M]. Paris: Unesco Publishing, 2017.

[2] CRETE-NISHIHATA M, OLIVER J, PARSONS C, et al. The information security cultures of journalism[J]. Digital Journalism, 2020, 8(8): 1068-1091.

[3] 马传旺, 张宇, 方滨兴, 等. 匿名网络综述[J]. 软件学报, 2023, 34(1): 404-420.
MA C W, ZHANG Y, FANG B X, et al. Survey on anonymous networks[J]. Journal of Software, 2023, 34(1): 404-420.

[4] DINGLEDINE R, MATHEWSON N, SYVERSON P. Tor: the second-generation onion router[C//Proceedings of the 13th USENIX Security Symposium. Berkeley: USENIX Association, 2004: 21.

[5] MANI A, WILSON-BROWN T, JANSEN R, et al. Understanding tor usage with privacy-preserving measurement[C]//Proceedings of the Internet Measurement Conference 2018. New York: ACM Press, 2018: 175-187.

[6] NASR M, BAHRAMALI A, HOUMANSADR A. DeepCorr: strong flow correlation attacks on tor using deep learning[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2018: 1962-1976.

[7] GRESCHBACH B, PULLS T, ROBERTS L M, et al. The effect of DNS on tor's anonymity[C]//Proceedings 2017 Network and Distributed System Security Symposium. Reston: Internet Society, 2017.

[8] OH S E, YANG T J, MATHEWS N, et al. DeepCoFFEA: improved flow correlation attacks on Tor via metric learning and amplification[C]//Proceedings of the 2022 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2022: 1915-1932.

[9] CHERUBIN G, JANSEN R, TRONCOSO C. Online website fingerprinting: evaluating website fingerprinting attacks on Tor in the real world[C]//Proceedings of the 31st USENIX Conference on Security Symposium. Berkeley: USENIX Association, 2022: 753-770.

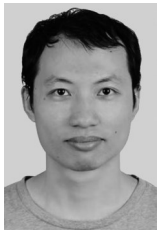
[10] RAHMAN M S, SIRINAM P, MATHEWS N, et al. Tik-tok: the utility of packet timing in website fingerprinting attacks[J]. Proceedings on Privacy Enhancing Technologies, 2020(3): 5-24.

[11] OH S E, MATHEWS N, RAHMAN M S, et al. GANDaLF: GAN for data-limited fingerprinting[J]. Proceedings on Privacy Enhancing Technologies, 2021, 2021(2): 305-322.

[12] CORRIGAN-GIBBS H, BONEH D, MAZIÈRES D. Riposte: an anonymous messaging system handling millions of users[C]//Proceedings of the 2015 IEEE Symposium on Security and Privacy. Piscat-

away: IEEE Press, 2015: 321-338.
[13] KWON A, CORRIGAN-GIBBS H, DEVADAS S, et al. Atom: horizontally scaling strong anonymity[C]//Proceedings of the 26th Symposium on Operating Systems Principles. New York: ACM Press, 2017: 406-422.
[14] KWON Y H. Towards anonymous and metadata private communication at Internet scale[D]. Commonwealth of Massachusetts: Massachusetts Institute of Technology, 2019.
[15] LANGOWSKI S, SERVAN-SCHREIBER S, DEVADAS S. Trellis: robust and scalable metadata-private anonymous broadcast[C]//Proceedings 2023 Network and Distributed System Security Symposium. Reston: Internet Society, 2023.
[16] GELERNTER N, HERZBERG A, LEIBOWITZ H. Two cents for strong anonymity: the anonymous post-office protocol[C]//International Conference on Cryptology and Network Security. Berlin: Springer, 2018: 390-412.
[17] CHENG R, SCOTT W, MASSEROVA E, et al. Talek: private group messaging with hidden access patterns[C]//Proceedings of the 36th Annual Computer Security Applications Conference. New York: ACM Press, 2020: 84-99.
[18] ESKANDARIAN S, CORRIGAN-GIBBS H, ZAHARIA M, et al. Express: lowering the cost of metadata-hiding communication with cryptographic privacy[C]//Proceedings of the 30th USENIX Conference on Security Symposium. Berkeley: USENIX Association, 2021: 1775-1792.
[19] CORRIGAN-GIBBS H, BONEH D. Prio: private, robust, and scalable computation of aggregate statistics[C]//Proceedings of the 14th USENIX Conference on Networked Systems Design and Implementation. Massachusetts: USENIX Association, 2017: 259-282.
[20] BONEH D, BOYLE E, CORRIGAN-GIBBS H, et al. Zero-knowledge proofs on secret-shared data via fully linear PCPs[C]//Annual International Cryptology Conference. Berlin: Springer, 2019: 67-97.
[21] VADAPALLI A, STORRIER K, HENRY R. Sabre: sender-anonymous messaging with fast audits[C]//Proceedings of the 2022 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2022: 1953-1970.
[22] DIFFIE W, HELLMAN M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.
[23] SHAMIR A. How to share a secret (1979)[J]. Communication of the ACM, 1979, 22(11): 612-613.
[24] GILBOA N, ISHAI Y. Distributed point functions and their applications[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2014: 640-658.
[25] BOYLE E, GILBOA N, ISHAI Y. Function secret sharing: improvements and extensions[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2016: 1292-1303.
[26] 余晟兴, 陈钟. 基于同态加密的高效安全联邦学习聚合框架[J]. 通信学报, 2023, 44(1): 14-28.
YU S X, CHEN Z. Efficient secure federated learning aggregation framework based on homomorphic encryption[J]. Journal on Communications, 2023, 44(1): 14-28.

[作者简介]



何琨（1986– ），男，湖北武汉人，博士，武汉大学副教授，主要研究方向为应用密码学、网络安全、云计算安全、人工智能安全、区块链安全等。

黄雅静（2001– ），女，河南新乡人，武汉大学硕士生，主要研究方向为匿名通信、零知识证明等。

杜瑞颖（1964– ），女，河南新乡人，博士，武汉大学教授，主要研究方向为网络安全、隐私保护等。

石闽（1993– ），男，安徽安庆人，武汉大学博士生，主要研究方向为网络安全、密码协议等。

李思勤（1999– ），女，湖北孝感人，武汉大学博士生，主要研究方向为应用密码学、匿名通信、隐私保护等。

陈晶（1981– ），男，湖北武汉人，博士，武汉大学教授，主要研究方向为网络安全、应用密码学、分布式系统安全等。