一种基于环签名的区块链电子投诉举报方案

张子松　张博文　童新海
（北京电子科技学院　北京 100070）

摘　要　针对当前投诉举报平台中出现的问题，如投诉举报数据集中存储容易被篡改伪造、举报人不能完全匿名、存在恶意举报的问题等，提出一种基于环签名的区块链电子投诉举报方案。方案通过智能合约自动执行机制取代了传统的可信第三方收集、处理投诉举报信息，并在方案中加入环签名算法，有效确保举报人的匿名性，而基于区块链的分布式存储也解决了集中存储可能引起的投诉举报内容被恶意删除、篡改等问题。经过证明分析，该方案安全可行。

关键词　区块链　环签名　投诉举报　匿名性　防恶意举报

中图分类号　TP3　　**文献标志码**　A　　DOI:10.3969/j.issn.1000-386x.2024.07.047

A BLOCKCHAIN ELECTRONIC COMPLAINT REPORTING SCHEME BASED ON RING SIGNATURE

Zhang Zisong　Zhang Bowen　Tong Xinhai
(*Beijing Electronic Science and Technology Institute*, *Beijing 100070*, *China*)

Abstract　This paper proposes a blockchain electronic complaint reporting scheme based on ring signature, aiming at the problems in the current complaint reporting platform, such as the problems that the centralized storage of complaint reporting data is easy to be tampered and forged, the informant cannot be completely anonymous, and there are malicious reports. The scheme replaced the traditional trusted third party to collect and deal with the complaint information through the smart contract automatic execution mechanism, and added the ring signature algorithm in the scheme to effectively ensure the anonymity of the whistleblower, while the distributed storage based on the blockchain also solved the problem that the complaint content might be maliciously deleted and tampered by the centralized storage. It is proved that the scheme is safe and feasible.

Keywords　Blockchain　Ring signature　Complaints report　Anonymity　Prevent malicious report

0　引　言

在现代社会中，社会治理地位日益重要，投诉举报作为群众监督的主要方式，在社会治理中也发挥着不可或缺的作用。随着社会信息化程度不断增长，人类活动也逐渐走向电子化、信息化，因此，一种能够极大方便投诉举报者的电子投诉举报方式应运而生。

基于投诉举报的特殊功能需求，一个良好的投诉举报方案应满足以下几点要求：（1）投诉举报信息的机密性。（2）投诉举报信息防止被恶意篡改、删除。（3）举报人的匿名性。（4）自证明性。（5）防止恶意举报。

目前国外的投诉举报平台多在电子举报形式上进行创新，无论是应用程序开发水平和功能优化方面都有很先进的水平，以美国的市民服务管理系统为例[20]，将原来的 C/S 架构优化为 B/S 架构，让市民更加方便地进行举报，同时通过高效、完善的后台数据库管理制度，为政府决策提供了更有效的信息服务[19]。

在国内研究领域，在投诉举报防篡改、删除方面，目前主要采用人工监管、制度约束的方式[1]，通过制定

收稿日期：2020－06－29。**张子松**，硕士生，信息安全，区块链。**张博文**，硕士生。**童新海**，研究员级高工。

规章制度防止内部人员将投诉举报信息篡改删除。但实践表明,传统监管方法不能有效适应当今环境的复杂性,不但增加人工成本还降低了举报作为群众监督的效果。

针对举报平台中涉及的几项安全性问题,早在2008 年,一种基于环签名的线上匿名举报方案被苗付友等[2]提出,该方案利用环签名无条件匿名性的特点,对举报人进行匿名性保护,同时提出悬赏机制,将悬赏功能运行在电子举报系统上,在中心化存储结构上实现了对举报信息的防伪造、防传递,并且具有了身份模糊性,是在举报领域对环签名技术的一次有效利用,紧接着在 2009 年,王化群等[3]研究出了一种通过安全指定验证者来保证匿名性的新线上匿名举报方案,通过指定的验证者也进一步保证了举报内容的安全性,2013 年 Wu 等[4]在详细分析了王化群等提出的举报方案后,提出了一种基于强指定验证者的线上匿名举报方案,此方案极大程度地弥补了之前方案的安全缺陷,解决了原来的安全问题。2015 年张瑞丽等[5]利用矩阵多项式幂乘运算的性质,将其应用到信息安全中的密钥交换中,增加了密钥破解的难度,在一定程度上提高了安全性。

上述解决方案均是基于中心化架构和依托环签名技术来实现投诉举报信息防篡改、删除,举报人匿名等特性,但仅仅依靠环签名技术只能在举报信息的传递过程中实现举报人的匿名性,除此之外,在中心化架构下目前仍存在以下两类问题:

(1) 若举报者实名举报,则举报受理方内部可获取到举报人的身份信息,此时举报信息及举报人存在安全风险。

(2) 若举报者匿名举报,其一是在领取悬赏时仍会暴露真实身份,存在安全隐患;其二是无法实时跟踪举报案件处理情况;其三是无法防止恶意举报。

因此,中心化架构的存储若内部监管不到位仍会发生投诉举报信息被恶意篡改、删除的情况,同时并不能有效约束举报者的恶意举报行为。此前提出的方案在安全性及功能方面仍有一定的局限性,无法切实保证投诉举报者的合理诉求。针对以上问题,本文提出了一种基于环签名的区块链投诉举报方案。

区块链去中心化、不可篡改的特性更适合投诉举报信息的存储[6-8],分布式存储能够极大程度地解决投诉举报信息被投诉举报受理机构内部人员恶意篡改删除的问题。区块链账户身份信息的非对称加密对举报者的身份信息进行了一定程度的模糊处理,再结合环签名技术无条件匿名性的特点基本保证了举报者能够隐藏自己的身份。同时,基于这些分布式存储的区块中可信的不可篡改的数据,在链上可灵活地对这些数据进行智能合约开发,利用保证金思想约束举报者的行为,将保证金放置于区块链中,一旦发现恶意举报,将强制扣除。本方案有效地同时解决了上述存在的两个问题,在实现举报者完全匿名的同时,能够在区块链上实时接收举报案件的反馈,并且在一定程度上约束了恶意举报情况的发生,因此,本方案既保留了实名举报的优点,又实现了举报人的隐私性。结合区块链技术、环签名技术,以及智能合约技术,实现可靠、高效、智能的投诉举报平台,从根本上解决现行投诉举报系统中的一系列问题。

1 预备知识

本投诉举报平台设计方案的核心技术包括双线性对、群 G_1 上的困难性问题、环签名技术,以及智能合约技术。

1.1 双线性对

设 G_1 是一个阶为素数 k 的循环加法群,该群由 P 生成,G_2 也是一个阶为 k 的循环乘法群;若双线性映射 $e:G_1\times G_1\rightarrow G_2$ 满足如下条件:

(1) 双线性。$e(mX,nY)=e(X,Y)^{nm}$,$X,Y\in G_1$ 并且 $m,n\in Z_q^*$。

(2) 非退化。存在 $X\in G_1$ 和 $Y\in G_1$ 使得 $e(X,Y)\neq 1$。

(3) 可计算性。对于所有的 $X,Y\in G_1$,存在有效的算法可以计算出 $e(X,Y)$,即可以在多项式时间内完成对 $e(X,Y)$ 的计算。

1.2 困难性问题

下面我们给出 G_1 上几个困难性问题。

定义 1 DLP(离散对数问题)[9]。给定 G_1 上任意两点 X 和 Y,若存在整数 n,使 $Y=nX$,求整数 n。

定义 2 CDHP(计算性 Diffie-Hellman 问题)。对于 $a,b\in Z_q^*$,$X\in G_1$,给定(X,aX,bX),计算 abX。

定义 3 DDHP(判定性 Diffle-Hellman 问题)。对于 $a,b,c\in Z_q^*$,给定 $X\in G_1$,(cX,aX,bX),判断 $c\equiv ab \bmod q$ 是否成立。

定义 4 GDHP(Gap Diffie-Hellman 问题)。若存在一个群 G_1,可利用多项式算法解决 G_1 上的 DDHP,

但无法在多项式时间内解决 G_1 上的 CDHP,则称此群 G_1 是一个 GDH 群。

本文中,总假定 DLP 问题和 CDHP 问题是困难性问题,即在多项式时间内均无法解决 DLP 问题、CDHP 问题。

1.3　智能合约

智能合约是由被誉为“智能合约之父“的尼克·萨博在 20 世纪 90 年代首次提出[10],其致力于将已有的合约法律法规以及相关的商业实践转移到互联网上来,使得陌生人通过互联网就可以实现以前只能在线下进行的商业活动,并能够实现真正的、完全的电子商务。

智能合约又称链上代码,即在区块链上预设的执行代码,区块链将智能合约的代码和状态作为一种交易保存到区块中,已被部署实施的智能合约若能满足预设的执行条件,无须可信第三方参与,则自动触发智能合约预设指令[11]。

本方案使用智能合约处理投诉举报平台的业务逻辑,并利用保证金思想有效约束举报者的行为,防止恶意举报,智能合约自动化执行预设指令的机制保证了方案的高效、权威、智能、透明。

1.4　环签名

2001 年由 Rivest,Shamir 和 Tauman 三位密码学家首次提出基于大整数分解困难性的 RSA 签名方案[12]即环签名(Ring Signature)方案。环签名由群签名[13]演化而来,不需要环成员之间的合作,签名者利用自己的私钥和集合中其他成员的公钥就能独立地进行签名,集合中的其他成员可能不知道自己被包含在了其中。如图 1 所示,若某一成员需要对消息进行签名,则需按相应规则形成环。同时当环中任一成员需要对消息进行签名时,都需要利用个人的私钥和其他成员的公钥。最后第三方可采用环签名算法对签名后的消息进行验证,但只能知道该签名来自这个环,却不知道具体是由哪个环成员发起的签名。

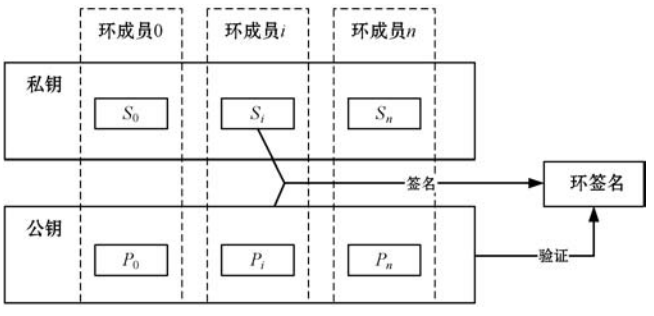

图 1　环签名实现机制

区块链利用非对称加密技术在提供分布式节点和地址交易上一定程度上保证了匿名性,但公共账本也带来了通过记录分析推断关联性的风险。因此本方案通过嵌入环签名算法进一步保证举报人的匿名性。

2　电子投诉举报方案

2.1　安全模型

(1) 投诉举报信息的机密性。在实名举报的情况下,能够保证第三方不能有效收到举报处理方泄露的投诉举报信息。

(2) 投诉举报内容防篡改。投诉举报信息能够防止被恶意篡改、恶意删除,包括对投诉举报受理方的制约,解决中心化存储平台的弊端。

(3) 举报人的匿名性。为防止被举报方的打击报复,在实名举报情况下应保护举报人的个人信息。在匿名举报情况下举报人应具有完全匿名性。

(4) 自证明性。在具有高度匿名性的同时,系统还应具有自证明性,即证明自己是真实举报人。

(5) 防止恶意举报。在确保举报人高度匿名性的同时,能够约束举报行为,防止恶意举报的发生。

至此,本方案能够在实现举报人匿名性,保护举报人个人信息的同时能够有效防止不法分子恶意举报,在矛盾中找到一个平衡点,实现了方案的突破。

2.2　电子投诉举报方案设计

在日前的基于身份的加解密方案中,使用最为广泛的就是 Boneh 等提出的基于双线性对[14]的公钥加密算法[15],因此本文是在这种公钥加密方案的基础上,结合区块链公共账本的特点对张瑞丽等设计的基于身份的环签名方案[5]进行了改进,使其虽搭载在公共透明的区块链上但仍能保证投诉举报数据的机密性。

本方案通过区块链及智能合约取代传统可信第三方投诉举报受理机构进行举报信息的收集及存储,通过区块链中的共识机制推选记账人,将举报信息写入区块中,其他用户节点可对其进行验证。同时利用区块链的分布式存储特点防止举报受理机构对投诉举报信息的恶意篡改删除。

通过将环签名技术嵌入到区块链投诉举报系统中,通过环签名代替举报人自己的签名,以此举报人可以达到无条件匿名,并且通过环签名技术能够保证举

报信息的不可传递性及举报人的自证明性。同时通过区块链中的保证金思想可在一定程度上约束举报人的举报行为,防止恶意举报。

本电子投诉举报方案共分为 9 个过程:部署合约、填写举报信息、缴纳保证金、系统初始化、生成密钥、产生投诉举报信息、投诉举报受理并验证、返还保证金、举报者领取悬赏,由投诉举报受理机构、智能合约和投诉举报者三部分完成。图 2 展示了整个投诉举报方案的流程。

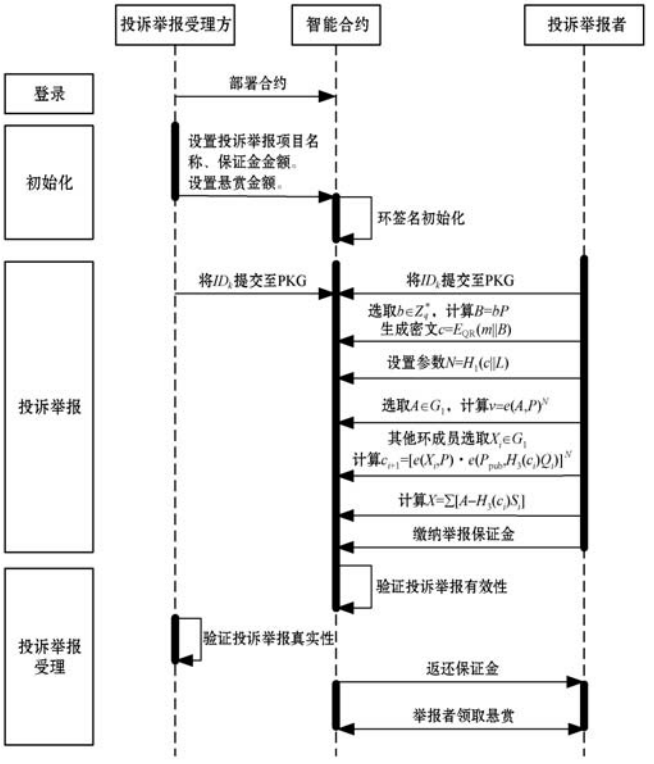

图 2 电子投诉举报方案流程

具体实施过程如下:

(1) 部署合约。投诉举报受理方需设置投诉举报项目名称,是否实名举报,实名举报、投诉所需身份信息,缴纳保证金金额,悬赏金额(非必填项)。

(2) 填写举报信息。若为投诉或实名举报:填写身份信息及投诉举报信息,上传支撑材料,经区块链做哈希处理后密文传输至投诉举报受理方。

(3) 缴纳保证金。举报信息生成后,投诉举报者需使用代币缴纳规定数量的保证金。

(4) 系统初始化。P 是群 G_1 的一个生成元;双线性映射 $e:G_1\times G_1\rightarrow G_2$,$H_1:\{0,1\}^*\rightarrow Z_q^*$,$H_2:\{0,1\}^*\rightarrow G_1$,$H_3:G_2\rightarrow Z_q^*$,$H_1$、$H_2$、$H_3$ 均为单项哈希函数。私钥生成器 PKG 随机选择 $s\in Z_q^*$,令 $P_{pub}=sP$。同时 PKG 将 $\{G_1,G_2,e,q,P,P_{pub},H_1,H_2\}$ 公开,s 作为主密钥只有 PKG 知道。

(5) 生成密钥。将一段时间内缴纳保证金的成员形成环,每个环成员将其身份信息 ID_k 提交至 PKG,PKG 将 $Q_k=H_2(ID_k)$ 作为公钥公开,同时将 $S_k=sQ_k$ 作为私钥保留,举报受理方的公私钥同理。

(6) 产生投诉举报信息。若平台中有 r 个可能的投诉举报者,则其公钥集合为 L:

$$L=\{ID_1,ID_2,\cdots,ID_r\}$$

其中,ID_i 是它们的身份信息,m 是待投诉举报信息。投诉举报者通过以下 6 个步骤进行投诉举报:

步骤 1 投诉举报者选取 $b\in Z_q^*$,计算 $B=bP$,使用公钥加密算法对 m 进行加密,生成密文:

$$c=E_{QR}(m\|B) \tag{1}$$

步骤 2 设置参数 N,计算:

$$N=H_1(c\|L) \tag{2}$$

步骤 3 随机选择 $A\in G_1$,计算初始值 v:

$$v=e(A,P)^N \tag{3}$$

步骤 4 为其他环成员随机选择 $X_i\in G_1$,计算:

$$c_{i+1}=[e(X_i,P)\cdot e(P_{pub},H_3(c_i)Q_i)]^N \tag{4}$$

步骤 5 形成环:投诉举报者解如下的方程,当 $i=k$ 时:

$$c_{k+1}=[e(X_k,P)\cdot e(P_{pub},H_3(c_k)Q_k)]^N=v \tag{5}$$

解得:

$$X_k=A-H_3(c_k)S_k \tag{6}$$

计算:

$$X=\sum X_i \tag{7}$$

步骤 6 为确保投诉举报信息的机密性,此处只输出举报信息 $(L;X;c;c_1,c_2,\cdots,c_r)B$,使得只有投诉举报受理机构才能查看并验证此投诉举报信息。

(7) 投诉举报受理并验证。投诉举报受理方接收到举报信息后,进行如下步骤:

步骤 1 解密运算:$m\|B=D_{S_Q}$,利用 b 已知,计算 $B=bP$,再从 $m\|B$ 中提取出 m。

步骤 2 计算 $N=H_1(m\|L)$。

步骤 3 验证 $\prod_i c_i=[e(X,P)\cdot e(P_{pub},\prod_i H_3(c_i)Q_i)]^N$ 是否正确,如果成立,则举报信息投递成功。

(8) 返还保证金。举报信息经举报受理方验证后,如举报信息真实有效,则向原地址返还保证金。

(9) 举报者领取悬赏。在举报者的举报过程中 b 一直在举报者手中,在领取悬赏时,可通过向受理方出示 b,通过 b 来验证正确性,因此举报者只需出示 b,通过验证后则可领取奖励。

电子投诉举报系统框架如图 3 所示。

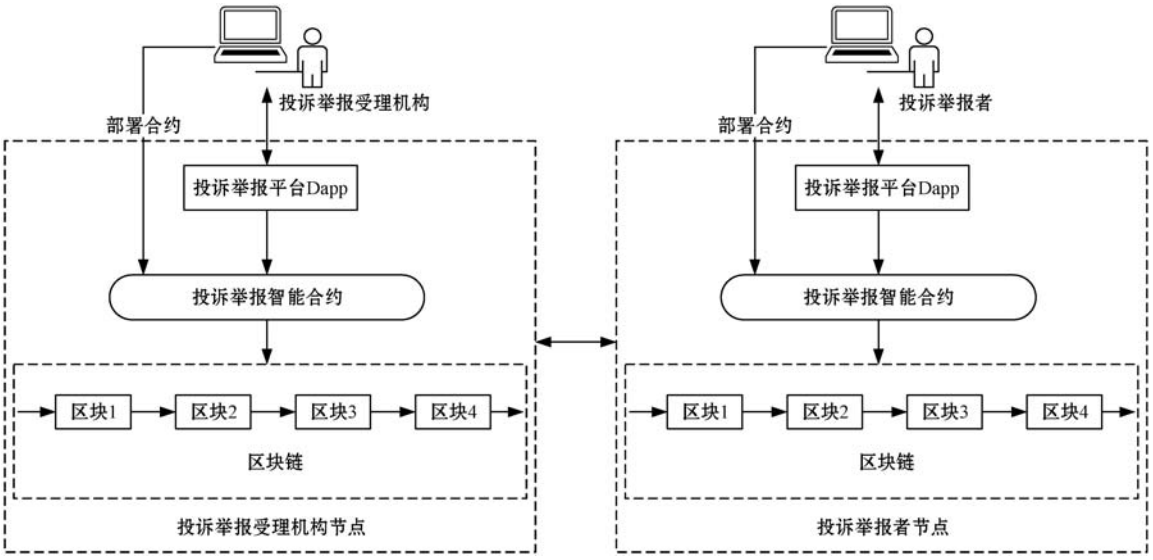

图 3　电子投诉举报系统框架

3　方案分析

本方案的投诉举报系统基于环签名的高强度匿名性及区块链可保证的强安全性,因此结合区块链与环签名技术可保证投诉举报过程的公开可验证、数据防篡改、强匿名性等特点。本投诉举报方案的安全性分析如下:

3.1　投诉举报内容机密性

此投诉举报方案将环签名技术写入智能合约中,增加了访问控制[16]机制,只有环签名中授权的节点可以使用私钥获取投诉举报信息。环签名技术中的公钥加密算法是基于椭圆曲线点群上的 CDHP 的困难性问题,在文献[15]中已证明了其在基于 Random Oracle 模型的选择密文攻击下是安全的。

同时,智能合约是运行在区块链上的根据本方案特定的业务逻辑编写的公开可验证的代码,智能合约代码可方便主链上的用户判断一个合约的正确性,其他节点用户可不定期检查核对合约代码的正确性。本方案主要利用共识算法来将智能合约的运行结果输入至区块链账本中,其他节点可对其进行验证,不会发生合约内容规定以外的其他行为,因此可以保证环签名技术及投诉举报功能的正确性、有效性。

3.2　举报人匿名性

本方案的匿名性有双层保证,第一层为环签名技术实现。首先通过环签名技术保证了举报者的身份信息,通过签名信息,攻击者不能确定举报人是哪个环成员。其次若没有环签名技术,则在举报人领取悬赏后拿到数字交易所进行货币交易时,该节点很有可能会暴露其真实身份,但通过环签名技术的无条件匿名特性则进一步模糊了举报者的身份。

环签名完全匿名正确性如式(8)所示。

$$\begin{aligned} c_1 &= [e(P_{\text{pub}}, H_3(c_0)Q_0) \cdot e(X_0, P)]^N \\ c_2 &= [e(P_{\text{pub}}, H_3(c_1)Q_1) \cdot e(X_1, P)]^N \\ c_3 &= [e(P_{\text{pub}}, H_3(c_2)Q_2) \cdot e(X_2, P)]^N \\ &\vdots \\ c_{i+1} &= [e(P_{\text{pub}}, H_3(c_i)Q_i) \cdot e(X_i, P)]^N \end{aligned} \tag{8}$$

则:

$$\begin{aligned} &\prod_{i=0}^{r} c_{i+1} = \prod_{i=0}^{r} [e(P_{\text{pub}}, H_3(c_i)Q_i) \cdot e(X_i, P)]^N = \\ &[\prod_{i=0}^{r} e(P_{\text{pub}}, H_3(c_i)Q_i) \cdot \prod_{i=0}^{r} e(X_i, P)]^N = \\ &[e(P_{\text{pub}}, \sum_{i=0}^{r} H_3(c_i)Q_i) \cdot e(\sum_{i=0}^{r} X_i, P)]^N, \prod_i c_i = \\ &[e(P_{\text{pub}}, \sum_i H_3(c_i)Q_i) \cdot e(X, P)]^N \end{aligned} \tag{9}$$

在环签名的验证过程和生产过程中,序列$\{c_i\}$是一致的,所以有 $c_{r+1} = c_0$。

第二层为区块链本身所具有的匿名性,链上各节点通过非对称算法保证节点账户身份信息的加密存储,若无私钥授权,则攻击者无法访问账户信息,因此链上的信息传递也可匿名进行,即使攻击者获取到举报人(即某个节点)的数据,也无法确定该节点的身份。且若投诉举报受理机构对举报行为发出悬赏,则可利用区块链系统中的代币进行奖励,使用节点钱包账户代替个人真实账户信息,保证了在整个举报过程中,从投递举报信息到领取奖励均未泄露举报者的真实身份,且任何货币传递均以代币形式进行,从而更加有效地防止了打击报复行为的发生。

3.3 投诉举报信息的不可传递性

当第三方机构 ID_m 在收到举报信息 $(L;X;c;B;c_1,c_2,\cdots,c_r)$ 后,可利用公钥加密的公开性对任意的消息 m' 采用仿真投诉举报伪造一个有效的投诉举报信息 $(L';X';c';c'_1,c'_2,\cdots,c'_r)$,使其可以通过验证。

伪造过程如下。

(1) 攻击者利用公钥加密算法输出公私钥,使得:

$$S_i = sH_2(ID_i) = sQ_i$$

(2) 随机选取 $c' \in Z_q^*$。

(3) 令 $r = |L|, i = 0,1,\cdots,r-2$,对真实举报者的举报过程进行仿真,产生环(即执行举报生成中的(4))。

(4) 令:

$$c' = [e(X_{k-1},P) \cdot e(P_{\text{pub}},H_3(c_{k-1})Q_{k-1})]^N$$

(5) 输出举报信息:

$$(L';X';c';c'_1,c'_2,\cdots,c'_r)$$

可见,投诉举报受理机构可以任意伪造来自 L 的投诉举报,但正是因为其可以任意伪造有效举报信息,当其将真正的举报信息传递给第三方时,并不能证明此信息不是伪造的,从而使此信息不具有可信性,因此本方案的投诉举报信息具有不可传递性。

3.4 投诉举报行为有效性

本投诉举报方案采用区块链技术来传递及存储投诉举报信息,区块链结合分布式存储和去中心化实现了数据的强可靠性,区块链上的任一节点都有一份完整的主链信息,除非攻击者能够掌握一半以上的非诚实节点,否则只是链上某单个节点数据的篡改都将是无效的,在此系统中,投诉举报受理机构也只是链上的一个节点,因此去中心化存储将能够最大程度上防止受理机构内部及外部人员的篡改。

此外,区块链区块中的 Merkle 哈希树[17]式存储能够快速进行数据完整性验证,若想快速检验某一举报信息是否存在于某一区块中,可利用 Merkle 树根和哈希列表,有效确保区块数据的完整性。

3.5 投诉举报信息的不可伪造性

本方案对于举报受理机构而言是可以伪造的,目的是保证举报信息具有不可传递性,但对于除举报受理机构以外的其他第三方,本方案具有不可伪造性。

本方案所使用的环签名为通用的基于身份的环签名方案,符合 Herranz-Saez 通用环签名定义[18],因此可利用定理 1 证明其在 ROM 模型下的不可伪造性。

证明如下:

(1) 攻击者从私钥生成算法中得到 q_E 个私钥:利用已知参数和 $ID_i(ID_i \notin L, i = 1,2,\cdots,q_E)$,求得对应的私钥为:

$$S_i = sH_2(ID_i) = sQ_i$$

(2) 随机选择 $c_0 \in Z_q$。

(3) 令 $r = |L|, i = 0,1,\cdots,r-2$,计算:

$$c_{i+1} = [e(X_i,P) \cdot e(P_{\text{pub}},H_3(c_i)Q_i)]^N$$

形成环序列。

(4) 同时指定:

$$c_0 = [e(X_{k-1},P) \cdot e(P_{\text{pub}},H_3(c_{k-1})Q_{k-1})]^N$$

(5) 最后输出举报信息:

$$(L;X;c;c'_1,c'_2,\cdots,c'_r)$$

在步骤(1)中,若攻击者可以通过计算 $S_i = sH_2(ID_i)$ 拿到 S_m,则伪造是成功的,但事实上 H_2 是随机预言机,私钥生成算法中产生的随机数是随机而且分布均匀,因此私钥生成算法并不能得到有效私钥;同时在步骤(4)中,因为 H_3 为随机预言机,X_i 也是在 G_1 中随机选择,因此式(4)正确的概率只有 $\frac{1}{q}$,可以忽略。因此本方案中的举报信息具有不可伪造性。

3.6 举报人自证明性

本方案的投诉举报过程中 B 的离散对数 b 在真正的举报者及投诉举报受理机构之间共享,其他节点并不能根据举报信息获取 b,因此举报者只需出示 b 即可领取奖励。

3.7 对举报行为的约束性

本方案利用区块链中的保证金思想对举报行为进行约束,即举报者若确有举报信息要进行举报而非恶意举报,则需使用区块链系统中的代币缴纳一定数量的保证金,在举报受理机构认定举报信息属实后返还保证金;若举报信息不属实则扣除保证金,以此对举报者的举报行为进行有效约束,最大程度避免恶意举报行为的发生。

4 结 语

近年来投诉举报系统使用非常广泛,在社会治理中的作用也日益重要,举报渠道也越来越多样化,但是却无法保证其安全需求,更多的是依靠人为监管、内部保密等措施来保证,但近年来人们对其研究较少,且因投诉举报行为较为敏感,不少掌握了投诉举报信息的人们因为担心系统的安全性而放弃了行使自己的权利,因此研究一套具有高度安全性的投诉举报系统就显得尤为重要,因此本文通过应用环签名技术及区块链技术设计了一种高效、安全、有效的投诉举报系统。

在实现投诉举报信息机密性、不可传递性的同时,还有效地保护了举报者的身份信息,并且利用区块链中的保证金思想在一定程度上约束了举报行为,节省了社会资源。因此,本方案已满足了文初提到的一个良好的投诉举报系统所应具备的几个功能,并通过对其进行六个方面的分析后证明,此方案正确、安全而且可行。

参 考 文 献

[1] 马红军. 受理投诉举报的重要遵循—《社会组织登记管理机关受理投诉举报办法(试行)》解读[J]. 中国社会组织,2016(16):34 – 35.

[2] 苗付友,王行甫,苗辉,等. 一种支持悬赏的匿名电子举报方案[J]. 电子学报,2008,36(2):320 – 324.

[3] 王化群,于红,吕显强,等. 一种支持悬赏的匿名电子举报方案的安全性分析及设计[J]. 电子学报,2009,37(8):1826 – 1829.

[4] Wu L, Hu D. Strong designated verifier ID-based threshold ring signature scheme[J]. International Journal of Applied Mathematics and Statistics,2013,41(11):222 – 229.

[5] 张瑞丽,李顺东. 一种新的基于身份的匿名电子举报方案[J]. 计算机应用与软件,2015,32(2):288 – 290,294.

[6] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [EB/OL]. [2020 – 06 – 29]. https://bitcoin. org/bitcoin. pdf.

[7] Kiyomoto S, Rahman M S, Basu A. On blockchain-based anonymized dataset distribution platform[C]//15th International Conference on Software Engineering Research, Management and Applications,2017:85 – 92.

[8] Sasson E B, Chiesa A, Garman C, et al. Zerocash: Decentralized anonymous payments from bitcoin[C]//IEEE Symposium on Security and Privacy,2014:459 – 474.

[9] 高建平. 基于 CDH 的模糊身份多方加密方案[J]. 网络安全技术与应用,2020(1):45 – 47.

[10] Tapscott D, Tapscott A. Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world[M]. New York: Portfolio,2016:72,83,101,127.

[11] Lind J, Naor O, Eyal I, et al. Teechain: Reducing storage costs on the blockchain with offline payment channels[C]//11th ACM International Systems and Storage Conference, 2018:125.

[12] Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM,1983,26(1):96 – 99.

[13] Chaum D, Heyst E V. Group signatures[C]//Workshop on the Theory and Application of Cryptographic Techniques, 1991:257 – 265.

[14] Enge A. Bilinear pairings on elliptic curves[EB]. arXiv: 1301.5520v1,2013.

[15] Boneh D, Franklin M. Identity-based encryption from Weil pairing[C]//Annual International Cryptology Conference, 2001:213 – 229.

[16] Crampton J. Specifying and enforcing constraints in role-based access control[C]//8th ACM Symposium on Access Control Models and Technologies,2003:43 – 50.

[17] Merkle R C. A certified digital signature[C]//Conference on the Theory and Application of Cryptology,2001,218 – 238.

[18] Herranz J, Sáez G. New identity-based ring signature schemes [C]//6th International Conference on Information and Communications Security,2004:27 – 39.

[19] Castro P, Melnik S, Adya A. ADO. NET entity framework: Raising the level of abstraction in data programming[C]//ACM SIGMOD International Conference on Management of Data,2007:1070 – 1072.

[20] Blakeley J A, Campbell D, Muralidhar S, et al. The ADO. NET entity framework: Making the conceptual level real[J]. ACM SIGMOD Record,2006,35(4):32 – 39.

(上接第 322 页)

[19] Arunkumar B, Kousalya G. Blockchain-based decentralized and secure lightweight E-health system for electronic health records[C]//5th Intelligent Systems, Technologies and Applications,2020:273 – 289.

[20] 牛淑芬,陈俐霞,李文婷,等. 基于区块链的电子病历数据共享方案[J]. 自动化学报,2022,48(8):2028 – 2039.

[21] 左黎明,周庆,陈兰兰. 一种可证安全高效无证书短签名方案[J]. 计算机工程,2019,45(6):193 – 198.

[22] Zhang A Q, Lin X D. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain [J]. Journal of Medical Systems,2018,42(8):140 – 158.

[23] 袁勇,倪晓春,曾帅,等. 区块链共识算法的发展现状与展望[J]. 自动化学报,2018,44(11):2011 – 2022.

[24] Zhang J, Xue N, Huang X. A secure system for pervasive social network-based healthcare[J]. IEEE Access,2016,4: 9239 – 9250.

[25] 韩笑,曾琦,曹永明. 一种有效的带关键字搜索的代理重加密方案[J]. 计算机与现代化,2019,283(3):117 – 121.

[26] 郭丽峰,李婷. 改进的带关键字搜索的代理重加密方案[J]. 山西大学学报(自然科学版),2016,39(3):434 – 441.

[27] 张青,何为,戴阔斌,等. 一种可证明安全的代理聚合签名方案[J]. 武汉大学学报(理学版),2018,64(5):415 – 422.