一种支持悬赏的匿名电子举报方案

苗付友, 王行甫 苗 辉, 熊 焰
(中国科学技术大学计算机系, 安徽合肥 230027)

摘 要: 本文针对举报系统应该有效保护和激励举报人等应用需求, 基于环签名和环签密提出了一种支持悬赏的匿名电子举报方案. 该方案能够通过身份模糊性有效保护举报人, 通过举报内容的机密性、举报的不可传递性以及第三方不可伪造性确保举报信息的安全, 并通过举报人身份的自证明性为悬赏机制提供支持. 分析表明, 该方案能够有效满足此类电子举报系统的应用需求.

关键词: 举报系统; 身份模糊; 自证明性; 环签密
中图分类号: TP393.08 文献标识码: A 文章编号: 0372-2112 (2008) 02-0320-05

An Anonymous E-Prosecution Scheme with Reward Support

MIAO Fu-you, WANG Xing-fu, MIAO Hui, XIONG Yan
(*Department of Computer Science and Technology, University of Science and Technology of China, Hefei, Anhui 230027, China*)

Abstract: In view of that e-Prosecution system should effectively protect and encourage informants, this paper provides an anonymous e-prosecution scheme with reward support based on the technology of ring signature and ring signcryption. The scheme can effectively protect an informant for his/her identity is ambiguous; it can also guarantee the security of prosecution contents because all prosecutions are encrypted, non-transferable and can't be forged. Furthermore, the scheme could provide effective reward support by informant's ability of self-proof. Analysis shows that the scheme can effectively meet the requirement of such electronic prosecution system.

Key words: prosecution system; identity ambiguous; self-proof; ring signcryption

1 引言

举报机制在当今社会中发挥着极其重要的监督作用, 被广泛应用于各种领域. 目前, 网络应用已经渗透到了人们生活的方方面面, 对人们的工作和日常生活的影响也日益加深. 因此, 如何基于网络环境建立有效的电子举报系统, 在充分利用网络带来的便利的同时, 提高举报机制的工作效率、更好地保护和激励举报人, 从而建立良好的监督机制至关重要.

一个较为完善的电子举报系统应该能够保证举报人举报的内容以及举报人的身份不会轻易被泄露, 并且能够支持对举报人的悬赏功能, 从而为举报系统提供一个有效的激励机制. 具体而言, 一个良好的举报系统: (1) 应该能够允许举报人隐藏自己的身份, 或者说身份是模糊的, 以利于举报人的自我保护, 防止举报人因身份泄露而遭到恶意报复; (2) 应该能够保护举报信息不会被攻击者窃取, 而且不会被举报受理人故意泄露, 即举报信息应该具有机密性, 其明文在传输过程中不会被非法攻击者截获, 同时举报受理机构也无法以令人信服的方式将收到的举报信息泄露给任意第三方; (3) 还应该能够对举报人提供有效的激励机制, 比如悬赏. 当举报人举报有功而领取悬赏时, 应该能够向举报机构证明自己的身份.

由以上可以看出, 一个较为完善的举报方案应该具有举报人身份模糊性和自证明性、举报内容的机密性和不可传递性. 就目前而言, 尚不存在一种现有的协议或算法完全具备这些特性, 并能够有效满足这类举报系统的应用需求. 因此, 如何针对这类举报系统独特的应用需求, 基于现有的密码学算法构造合适的应用方案是本文研究的关键.

环签名[1~3]是一种签名者身份模糊(Signer-ambiguous)的数字签名, 接收者只知道收到的签名来自某个实体的集合, 但不能确切地知道签名者的身份. 因此, 能够很好地保护签名者身份隐私性.

收稿日期: 2007-03-12; 修回日期: 2007-08-08
基金项目: 安徽省自然科学基金(No. 070412045, No. 050420211); 国家自然科学基金(No. 60573044), 安徽省计算与通信软件重点实验室开放基金; 中国科技大学青年基金

鉴于此, 本文将基于环签名算法, 构造一种具有签名者身份模糊性、消息机密性、不可传递性和自证明性的安全协议, 实现一种支持悬赏的匿名举报方案.

2　背景知识

本举报方案所依据的背景知识主要涉及基于身份的密码系统、双线性对(bilinear pairings)、环签名、环签密.

2.1　基于身份的密码系统和双线性对

在基于身份的密码系统中, 节点的身份标识就代表其公开密钥, 知道了节点的身份标识也就获得了该节点的公开密钥. 在基于身份的密码系统中, 双线性对计算是一种主要的操作, 双线性对的基本概念如下:

假设 $G1$ 是一个由 P 生成的阶(order)为素数 q 的循环加法群, $G2$ 为一个循环乘法群, 其阶也为 q; 映射 $e: G1 \times G1 \rightarrow G2$ 是一个双线性映射, 如果它满足如下条件:

(1)双线性: $e(mX, nY) = e(X, Y)^{mn}$, $X, Y \in G1$ 并且 $m, n \in Z_q^*$.

(2)非退化: 存在 $X \in G1$ 和 $Y \in G1$ 使得 $e(X, Y) \neq 1$;

(3)可计算性: 对于所有的 $X, Y \in G1$, 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.

下面我们给出 $G1$ 上几个数学问题的描述:

定义**1**　离散对数问题(Discrete Logarithm Problem—DLP):

给定 $G1$ 上的两个元素 X 和 Y, 如果存在这样的整数 n, 使得 $Y = nX$, 求整数 n.

定义 **2**　计算性 Diffie-Hellman 问题(Computational Diffie-Hellman Problem—CDHP):

对于 $a, b \in Z_q^*$, $X \in G1$; 给定 (X, aX, bX), 计算 abX.

定义 **3**　判定性 Diffie-Hellman 问题(Decisional Diffie-Hellman Problem—DDHP):

对于 $a, b, c \in Z_q^*$; 给定 $X \in G1$, (cX, aX, bX), 判断 $c \equiv ab \bmod q$ 是否成立.

定义**4**　Gap Diffie-Hellman 问题(Gap Diffie-Hellman Problem—GDHP):

如果存在多项式时间的算法可以解决 $G1$ 上的 DDHP, 但不存在任何算法可以在多项式时间内以不可忽略的概率解决 $G1$ 上的 CDHP, 则 $G1$ 是一个 GDH 群.

在本文中, 我们总假定 DDHP 在 $G2$ 上是难解性问题, 而 CDHP 和 DLP 在 $G1$ 和 $G2$ 上都是难解性问题, 即不存在任何算法能够在多项式时间内以不可忽略的概率解决这些问题.

2.2　基于身份的环签名与环签密

环签名的概念是 2001 年由 Rivest, Shamir 和 Tauman 三人提出的[2], 它是一种签名者模糊(Signer-ambiguous)的数字签名. 在环签名生成过程中, 真正的签名者任意选取一组成员(包含它自身)作为可能的签名者, 用自己的私有密钥和其他成员的公开密钥对文件进行签名. 真正签名者选取的这组成员称作环(Ring), 生成的签名称作环签名(Ring Signature). 该方案假设 RSA 问题难解的基础上, 证明了在自适应选择消息情况下, 其签名方案的不可伪造性. 该方案使用了对称加密算法和组合函数的概念.

Herranz 和 Saez 在文献[3]中提出了 Herranz-Saez 通用环签名定义, 并给出了一种基于身份的环签名方案, 然后通过环签名分支引理[4]证明了该方案在随机预言模型(ROM—Random Oracle Model)下具有不可伪造性. Bresson[5]等人对 Rivest 等人的方案进行了修改, 并且证明在 Random Oracle 模型下, 新方案可以与原方案具有相同的安全性.

Zhang 和 Kim[6]提出了一种基于身份的环签名算法, 并简单分析了其安全性和效率; Chow 等人[7]提出的基于身份的环签名方案在签名构造中需要进行 $4n-1$ 次 $G1$ 上的加法运算, 而在验证过程中只需要两次双线性对运算. 相对于以前的环签名方案提高了签名的效率.

从文献调研来看, 对基于身份的环签密的研究极少, 典型的工作就是文献[8]. 环签密是一种融合信息保密功能的环签名, 相对于简单的先签名后加密方式具有更高的效率. 环签密包括 Setup, Extract, Signcrypt 和 Unsigncrypt 四个算法:

(1)Setup: 给定一个安全参数 k, 系统利用 Setup 生成系统公共参数.

(2)Extract: 每个成员, 如 N_i 通过该算法获取自己的密钥对 (PK_i, SK_i).

(3)Signcrypt: 签密者通过该算法代表某个环 L 生成消息 m 的环签密 $rSigen$.

(4)Unsigncrypt: 验证者通过该算法解密签密中的明文 m 并验证环签密 $rSigen$ 的真伪.

3　支持悬赏的匿名举报方案设计

本文提出的支持悬赏的匿名举报包含六个步骤: 初始化、密钥获取、举报生成、举报受理、悬赏领取以及举报伪造, 具体步骤如下:

(**1**)初始化: 假设 $G1$ 为一个由 P 生成的阶为素数 q 的循环加法群, 而 $G2$ 是一个阶同为 q 的循环乘法群. 假设 $e: G1 \times G1 \rightarrow G2$ 是一个双线性映射, 系统中的私有密钥生成器 PKG 随机选取一个值 $s \in Z_q^*$ 作为其主

密钥, 令 $P_{pub}=sP$; 选择两个普通的哈希函数: $H1:\{0,1\}^* \rightarrow G1^*$, $H_2:\{0,1\}^* \rightarrow Z_q^*$, 构造函数: $F(m, L, PK_R, R_i, P_{pub})=H_2(e(R_i, P_{pub})e(H_2(L\|m)PK_R, P_{pub}))$ (其中 R_i 为 $G1$ 上的随机数, PK_R 为举报受理者的公钥, m 为举报消息明文, L 为可能的举报者集合); 系统中可能的举报者的个数为 n, 将系统参数集 $PARAMS=\{P, q, e, n, H_1, H_2, F, P_{pub}\}$ 向系统内的所有成员公开.

(**2**) 密钥获取: 对于一个成员 N_i 而言, 如果其身份标识为 ID_i, 则其公开密钥为 $PK_i=H_1(ID_i)$, 私有密钥为 $SK_i=sPK_i$, 设举报受理机构的身份标识为 ID_R, 则其公钥为 $PK_R=H_1(ID_R)$, 私有密钥为 $SK_R=sPK_R$.

(**3**) 举报生成: 假设举报方案中包含 n 个可能的举报人, 真正的举报人 N_k 随机地选择其他 $n-1$ 个成员, 从而形成一个可能的举报人集合 $U=\{N_1, \cdots, N_i, \cdots, N_n\}$. 令 $L=\{ID_1, \cdots, ID_i, \cdots, ID_n\}$, 其中 ID_i 是 N_i 的身份. N_k 生成举报的过程如下:

(a) 在 Z_q^* 上随机秘密选取一个值 b, 即 $b \in_R Z_q^*$, 计算

$$t=H_2(e(P_{pub}, PK_R)^b) \quad (1)$$

$$c=E_t(m) \quad (2)$$

$$r=H_2(L\|c) \quad (3)$$

$$S=bPK_R-rPK_R \quad (4)$$

(b) 对于 $i\in\{1, \cdots, n\}\setminus\{k\}$, 在 $G1$ 上随机选择一个元素 R_i, 利用 $F(.)$ 函数, 计算

$$h_i=F(m, L, PK_R, R_i, P_{pub})=H_2(e(R_i, P)e(H_2(L\|m)PK_R, P_{pub})) \quad (5)$$

(c) 随机选择 $x\in_R Z_q^*$, 计算

$$R_k=(x+t)PK_k-\sum_{i\neq k}\{R_i+h_itPK_i\} \quad (6)$$

(d) 计算

$$h_k=H_2(e(R_k, P)e(H_2(L\|m)PK_R, P_{pub})) \quad (7)$$

$$\sigma=(x+th_k+t)SK_k \quad (8)$$

(e) 则最终生成的举报为: $rSig=\{L, R_1, \cdots, R_n, \sigma, c, S, r\}$

(**4**) 举报受理: 举报受理者 N_R 在收到举报后, 执行如下的解密和验证操作:

(a) 计算: $t=H_2(e(P_{pub}, S)e(P, SK_R)^r)$ (9)

并使 t 保密.

(b) 以 t 为解密密钥, 对密文 c 进行解密, 获取举报内容的明文 $m=D_t(c)$.

(c) 依据式(5)计算 $h_1, h_2, h_3, \cdots, h_n$. 如果

$$e\left(P_{pub}, \sum_{i=1}^{n}\{R_i+h_itPK_i\}\right)=e(P, \sigma) \quad (10)$$

则举报为有效; 否则举报无效, 忽略此举报.

(**5**) 悬赏领取: 举报受理机构根据举报, 成功处理完被举报事件后向举报人发放悬赏, 此时, 真正的举报者 N_k 必须使举报受理机构 N_R 确信其收到的举报来自 N_k, 他必须进行如下操作:

(a) 计算 $t'=H_2(e(P_{pub}, PK_R)^b)$, 其中 b 为 N_k 当初生成举报时随机选择的那个值.

(b) 执行加密操作: $c'=E_{t'}(ID_k\|t')$, 以 t' 为加密密钥, 对 $ID_k\|t'$ 进行加密;

(c) 将 (ID_k, c') 发送给举报受理机构 N_R.

(d) N_R 在收到 (ID_k, c') 后, 利用式(9)计算得到的 t 对 c' 进行解密:

$$D_t(c')=D_t(E_{t'}(ID_k\|t'))$$

如果 $D_t(c')=(ID_k\|t)$, 则说明 $t'=t$, 而 N_k 就是真正的举报者, 否则就不是.

(**6**) 举报伪造: 为了防范举报受理机构 N_R 将受理的举报非法外泄, 需要赋予其伪造举报的能力, 使其他人无法相信其所泄露举报的真实性. 事实上, N_R 在收到举报 $rSig=\{L, R_1, \cdots, R_n, \sigma, c, S, r\}$ 后, 可以很容易成功伪造另一个举报内容为 m' 的举报. 具体如下: N_R 计算

$$c'=E_t(m') \quad (11)$$

$$r'=H_2(L\|c') \quad (12)$$

$$R_i'=(H_2(L\|m)-H_2(L\|m'))PK_R+R_i \quad (13)$$

$$\sigma'=\sigma+n(H_2(L\|m)-H_2(L\|m'))SK_R$$

(其中 n 为 L 中实体的个数) (14)

则 N_R 可以伪造出一个有效的举报 $rSig'=\{L, R_1', \cdots, R_n', \sigma', c', S, r'\}$, 为了使第三方能够判断举报的正确性并恢复出举报内容, N_R 必须将 t 与举报一起发送给第三方.

4 方案分析

下面将对该方案的正确性、举报人身份模糊性、自证明性、举报的不可传递性、机密性和第三方不可伪造性进行分析, 从而说明该举报方案的合理性.

4.1 正确性

在举报 $rSigen=\{L, R_1, \cdots\cdots, R_n, \sigma, c, S, r\}$ 的受理中, N_R 为了恢复参数 t, 需要按式(9)进行计算这是因为:

$$\begin{aligned}&H_2(e(P_{pub}, S)e(P, SK_R)^r)\\&=H_2(e(P_{pub}, bPK_R-rPK_R)e(P_{pub}, rPK_R))\\&=H_2(e(P_{pub}, PK_R)^b)\\&=t\end{aligned}$$

另外在受理中, $e(P_{pub}, \sum_{i=1}^{n}\{R_i+h_itPK_i\})=e(P, \sigma)$ 成立时举报才有效, 是因为:

$$e(P_{pub}, \sum_{i=1}^{n}\{R_i+h_itPK_i\})=e(P, s((x+t)PK_k-$$

$$\sum_{i\neq k}\{R_i + h_i tRK_i\}) + st\, h_k PK_k + s\sum_{i\neq k}\{R_i + h_i tPK_i\})$$
$$= e(P, (x + t\,h_k + t)\,SK_k)$$
$$= e(P, \sigma)$$

4.2 举报人身份模糊性

首先, 举报人在初始化阶段按照式(1)构造参数 $t = H_2(e(P_{pub}, PK_R)^b)$, 除了随机选取的参数 $b \in RZ_q^*$ 外, 其他参数都是公开的, 任何人都可以非常容易地获取到. 也就是说 t 中不包含任何可以标识举报人身份的信息, 是举报人身份模糊的; 同样, 按照式(4)构造的参数 S 也具有举报人身份模糊性; 其次, 由举报生成的过程可以看出, 对于一个可能的举报人集合 L, 其中的任何一个成员都有能力生成一个有效的举报. 虽然在举报生成过程中, 举报人分别在式(6)和式(8)中用到了自己的公开密钥和私有密钥, 但是在计算过程中都通过随机数 x 将计算结果 R_k 和 σ 随机化了, 从而使得 R_k 和 σ 在 $G1$ 上的分布概率在多项式时间内具有不可区分性. 因此, 该方案具有举报人模糊性.

4.3 举报人身份的自证明性

举报人通过悬赏领取过程向举报受理机构证明它知道加密密钥 t, 从而证明其是真正的举报人. 这是因为在整个举报方案中, t 只在举报人与举报受理机构间共享, 而对其他任何第三方都是保密的.

4.4 举报的不可传递性

举报受理机构 NR 在接收到举报 $rSig = \{L, R_1, \cdots, R_n, \sigma, c, S, r\}$ 后, 可以对任意的消息 m' 采用伪造算法成功伪造一个有效的举报 $rSig' = \{L, R_1', \cdots, R_n', \sigma', c', S, r'\}$, 使 $rSig'$ 通过任意第三方的验证. 这是因为任意第三方在收到 $rSig'$ 和 t 后就可获取举报内容的明文信息 $m' = D_t(c')$, 然后计算出所有 h_i' :

$$h_i' = H_2(e(R_i', P_{pub})\, e(H_2(L \| m')\, PK_R, P_{pub}))$$
$$= H_2(e(R_i, P_{pub})\, e(H_2(L \| m)\, PK_R, P_{pub})) = h_i$$

证明: $H_2(e(R_i', P_{pub})\, e(H_2(L \| m')\, PK_R, P_{pub}))$
$$= H_2(e((H_2(L \| m) - H_2(L \| m'))\, PK_R + R_i, P_{pub}) \cdot e(H_2(L \| m')\, PK_R, P_{pub}))$$
$$= H_2(e(R_i, P_{pub})\, e(H_2(L \| m)\, PK_R, P_{pub}))$$
$$= h_i$$

然后根据式(10)验证举报 $rSig'$ 的正确性:

$$e(P_{pub}, \sum_{i=1}^{n}\{R_i' + th_i PK_i\})$$
$$= e(P, s\sum_{i=1}^{n}\{R_i + th_i PK_i\} + sn(H_2(L \| m) - H_2(L \| m'))\, PK_R)$$
$$= e(P_{pub}, \sum_{i=1}^{n}\{R_i + th_i PK_i\})\, e(P, n(H_2(L \| m) - H_2(L \| m'))\, SK_R)$$
$$= e(P, \sigma)\, e(P, n(H_2(L \| m) - H_2(L \| m'))\, SK_R)$$
$$= e(P, \sigma')$$

可见, 举报受理机构 N_R 可以任意伪造来自 L 的举报, 当 N_R 试图将收到的举报透露给第三方的时候, 他无法证明该举报不是自己伪造的, 从而使得 N_R 泄漏的消息不具可信性.

4.5 举报内容的机密性

对于任何第三方 M 而言, 如果它想获得举报内容的明文 m, 那么它必须设法恢复出加密密钥 t. 一方面, 如果 M 可以获得 b, 那么它就可以根据式(1)计算出参数 t. 但是, 举报人 N_k 是将 b 保密的. 而 b 在 Z_q^* 上是均匀分布的, 当 q 很大时, M 成功猜测出 b 的概率可以忽略. 因此, 要成功猜测出 b, 在计算上是不可行的. 另一方面, 如果 M 不能以不可忽略的概率获得 b, 那么它必须通过 NR 的私有密钥按照式(9)才能恢复出 t, 然而其他任何节点要获得 N_R 的私有密钥在计算上也是不可行的. 因此该举报方案能够确保举报内容的机密性.

4.6 第三方不可伪造性

本举报方案的第三方不可伪造性, 是指除举报人 N_k 指定的集合 L 中的成员和特定的举报受理机构 N_R 以外的其他任何第三方, 在不知道真正举报人私有密钥的情况下, 都不可能在多项式时间内以不可忽略的概率成功伪造出有效的举报. 本方案生成的举报实质上符合文[3]中的通用环签名定义, 因此, 其在随机预言模型 ROM 下的不可伪造性可以用环签名分支引理[4]加以证明. 由于篇幅所限, 具体的证明过程请参考文献[9].

5 结论

本文针对举报系统应该有效保护和激励举报人等应用需求, 基于环签名和环签密提出了一种支持悬赏的匿名电子举报方案. 该方案能够通过身份模糊性有效保护举报人, 通过举报内容的机密性、举报的不可传递性以及第三方不可伪造性确保举报信息的安全, 通过举报人身份自证明为悬赏机制提供有效支持. 分析表明, 该方案能够有效满足此类电子举报系统的应用需求. 目前, 该系统尚未考虑如何对举报人的举报行为进行有效约束, 避免恶意举报问题, 这也是本文未来工作的方向.

参考文献:

[1] Miao Fuyou, Xiong Yan, Yang Shoubao, Wang Xingful. Approvable encrypted ring signature from bilinear pairings[J]. Chinese Journal of Electronics, 2006, 15(2): 204– 208.

[2] Ronald L Rivest, Adi Shamir, Yael Tauman. How to leak a secret[A]. 7th International Conference on the Theory and Appli-

cation of Cryptology and Information Security[C]. Springer Verlag, 2001, LNCS2248. 552– 565.

[3] Javier Herranz, German Saez. New identity-based ring signature schemes[A]. Proceedings of Information and Communications Security, 6th International Conference[C]. Springer Verlag, 2004. ICICS 2004, LNCS 3269. 27– 39.

[4] Javier Herranz, German Saez. Forking lemmas for ring signature schemes[A]. INDOCRYPT 2003[C]. Springer Verlag, 2003. LNCS 2904. 266– 279.

[5] Emmanuel Bresson, Jacques Stern, Michael Szydlo. Threshold ring signatures and applications to Ad-hoc groups[A]. Advances in Cryptology-CRYPTO' 02[C]. Springer Verlag, 2002. LNCS 2442. 465– 480.

[6] Fangguo Zhang, Kwangjo Kim. ID-based blind signature and ring signature from pairings[A]. Advances in Cryptology-Asiacrypt 2002[C]. Springer Verlag, 2002. LNCS 2501. 533– 547.

[7] Sherman S M Chow, S M Yiu, Lucas C K Hui. Efficient Identity Based Ring Signature [DB/OL]. http://eprint.iacr.org/2004/327.pdf, 2004.

[8] Xinyi Huang, Willy Susilo, Yi Mu, Futai Zhang. Identity-based ring signcryption schemes: Cryptographic primitives for preserving privacy and authenticity in the ubiquitous world[A]. 19th International Conference on Advanced Information Networking and Applications (AINA' 05) Volume 2[C]. IEEE Computer Society, Washington, DC, USA, 2005. 649– 654.

[9] 苗付友. 移动自组网环境下的自证明环签名与环签密算法研究[D]. 中国科学技术大学研究生院博士学位论文, 安徽合肥, 2005. 11. 77– 79.

作者简介:

苗付友 男, 1973 年出生, 讲师、博士. 研究方向为移动计算与应用密码学.
E-mail: mfy@ustc.edu.cn

王行甫 男, 1964 年出生, 高级工程师、学士. 研究方向为计算机网络

苗 辉 男, 1982 年出生, 硕士研究生. 研究方向为计算机网络与信息安全

熊 焰 男, 1964 年出生, 教授/博导. 研究方向为计算机网络与分布式计算.