一种支持悬赏的匿名电子举报方案的安全性分析及设计

王化群[1,2],于 红[1],吕显强[1],张福泰[3]
(1.大连水产学院信息工程学院,辽宁大连 116023;2.福建师范大学网络安全与密码技术重点实验室,福建福州 350007;
3.南京师范大学数学与计算机科学学院,江苏南京 210097)

摘 要: 对Miao-Wang-Miao-Xiong匿名电子举报方案进行了安全性分析,指出其存在的安全性缺陷,该方案不满足其要求的举报信息机密性,以及不满足对举报人提供有效的激励机制.设计了破坏这两种性质的攻击方法.为设计满足要求的支持悬赏的匿名电子举报方案,利用安全的基于双线性对的举报受理者公钥加密方案、安全的指定验证者的环签名方案提出了一种支持悬赏的匿名电子举报方案设计模式.经安全性分析,设计模式是安全的.

关键词: 匿名电子举报; 指定验证者环签名; 双线性对
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2009) 08-1826-04

Cryptanalysis and Design of an Anonymous E-Prosecution Scheme with Reward Support

WANG Hua-qun[1,2], YU Hong[1], LV Xian-qiang[1], ZHANG Fu-tai[3]
(1. *School of Information Engineering, Dalian Fisheries University, Dalian, Liaoning* 116023, *China*;
2. *Key Laboratory of Network Security and Cryptology, Fujian Nomal University, Fuzhou, Fujian* 350007, *China*;
3. *College of Mathematics and Computer Science, Nanjing Normal University, Nanjing, Jiangsu* 210097, *China*)

Abstract: Miao-Wang-Miao-Xiong's anonymous E-Prosecution scheme was analyzed. The security flaws were pointed out. The original scheme can't guarantee the security of prosecution contents and effective reward support. We design the attack methods to break the two properties. In order to design an anonymous E-Prosecution scheme with reward support, we make use of the secure public key encryption scheme from bilinear pairings, secure designated verifier ring signature scheme to propose the design model of anonymous E-Prosecution scheme. Through security analysis, our design model is secure.

Key words: anonymous E-Prosecution; designated verifier ring signature; bilinear pairings

1 引言

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.针对这类举报系统独特的应用需求,文献[1]利用环签名算法提出了一种支持悬赏的匿名电子举报方案.但是,经安全性分析,该方案并不满足这类举报系统独特的应用需求,即不满足举报信息机密性和对举报人提供有效的激励机制.同样的,基于一类特定的环签名,我们设计了一种满足这类举报系统独特的应用需求的电子举报方案.

从本质上看,环签名可理解为一种简化了的群签名,它没有通常情况下群签名的群创建和匿名性撤销过程,也没有群管理.签名人可以自己选择包括自己在内的一个群体,在签名时,把所有群体成员的信息(公钥)

收稿日期:2007-07-18;修回日期:2009-01-15
基金项目:国家自然科学基金(No.60673070);辽宁省教育厅科技研究资助项目(No.2008140,05L09,2008150);大连水产学院人才引进项目(No.SYYJ200612);大连水产学院科研计划(No.SY2007032);福建师范大学网络安全与密码技术重点实验室开放课题(No.09A005);大连市基金(No.2005J22JH038)

作为签名的一部分.任何人可以验证签名是指定群体中的一个成员所做的,但无法推断出到底是哪一个成员所做的.群体中的任何一个成员为签名者的概率都相等.因此,环签名可以实现对签名者的无条件匿名.环签名的这种无条件匿名性非常适合一个群体的成员以群体的名义对外泄漏秘密,而不至于事后被追查出究竟是谁.虽然环签名的思想最早出现在有关群签名的文献中[2~4],但是直到 2001 年,Rivest, Shamir 和 Tauman 才形式化提出了环签名的概念,并且利用组合函数和对称加密算法设计了一种高效的环签名方案[5].环签名提出以后引起了信息安全研究领域的广泛关注,各种环签名方案及其扩展环签名方案被提出[6,7].将环签名跟指定确认者签名相结合,设计了一些指定确认者环签名方案[8,9].利用安全的基于双线性对的举报受理者公钥加密方案、安全的指定验证者的环签名方案提出了一种支持悬赏的匿名电子举报方案设计模式.经安全性分析,我们的设计模式是安全的.

2　一些数学基础

设 G_1 为一生成元为 P 的加法循环群,G_2 为乘法循环群,其阶都为素数 p.群 G_1, G_2 中的离散对数问题都是困难的.

定义双线性对 $e: G_1 \times G_1 \to G_2$,$e$ 满足如下条件:

(1)双线性性: $e(aP, bQ) = e(P, Q)^{ab}$,其中 $P, Q \in G_1, a, b \in Z_p^*$.

(2)非退化性: 存在 $P, Q \in G_1$,满足 $e(P, Q) \neq 1$,其中 1 为循环乘法群 G_2 的幺元.

(3)可计算性: 任取 $P, Q \in G_1$,存在有效算法计算 $e(P, Q)$.

群 G 可取有限域上超奇异椭圆曲线或超椭圆曲线,双线性对可利用该曲线上的 Weil 配对或 Tate 配对改进后进行实现.

假设 G_1 为一加法群,在群 G_1 上定义以下密码学问题:离散对数问题(DLP):任取 $Q \in G_1$,求满足 $Q = nP$ 的 $n \in Z_p^*$.

计算 Diffie-Hellman 问题(CDHP):$\forall (P, aP, bP) \in G_1^3$,其中 $a, b \in Z_p^*$,求出 abP.

决策 Diffie-Hellman 问题(DDHP):$\forall (P, aP, bP, cP) \in G_1^4$,其中 $a, b, c \in Z_p^*$,判断 $ab \equiv c \bmod p$ 是否成立.

Gap Diffie-Hellman(GDH)问题:一类 CDHP 困难而 DDHP 容易的问题.

假设 DLP 问题和 CDHP 问题是困难的,即不存在多项式时间算法以不可忽略的概率求解 DLP 问题、CDHP 问题.群 G_1 的选取可满足 DLP 问题、CDHP 问题难解,而 DDHP 问题易解的条件,即,群 G_1 为 GDH 群.

3　Miao-Wang-Miao-Xiong 匿名电子举报方案及其安全性分析

3.1　Miao-Wang-Miao-Xiong 匿名电子举报方案

Miao-Wang-Miao-Xiong 匿名电子举报方案包含六个步骤: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 G_1 为一个由 P 生成的阶为素数 q 的循环加法群,而 G_2 是一个阶同为 q 的循环乘法群.假设 $e: G_1 \times G_1 \to G_2$ 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:$H_1: \{0,1\}^* \to G_1$, $H_2: \{0,1\}^* \to Z_q^*$,构造函数:$F(m, L, PK_R, R_i, P_{pub}) = H_2(e(R_i, P)e(H_2(L \| m)PK_R, P_{pub}))$(其中 R_i 为 G_1 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 $U = \{N_1, N_2, \cdots, N_n\}$,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 $b \in Z_q^*$,计算:

$$t = H_2(e(P_{pub}, PK_R)^b), c = E_t(m),$$
$$r = H_2(L \| c), S = bPK_R - rPK_R,$$

其中 E_t 表示对称加密算法.

(b)对于 $i \in \{1, \cdots, n\} \setminus \{k\}$,在 G_1 上随机选择一个元素 R_i,利用 $F(\cdot)$ 函数,计算:

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

(c)随机选择 $x \in_R Z_q^*$,计算:

$$R_k = (x + t)PK_k - \sum_{i \neq k} \{R_i + h_i tPK_i\}$$

(d)计算:

$$h_k = H_2(e(R_k, P)e(H_2(L \| m)PK_R, P_{pub}))$$
$$\sigma = (x + th_k + t)SK_k$$

(e)则最终生成的举报为:

$$rSign = \{L, R_1, \cdots, R_n, \sigma, c, S, r\}$$

(4)举报受理:举报受理者 N_R 在收到举报后,执行如下解密和验证操作:

(a)计算 $t = H_2(e(P_{pub}, S)e(P, SK_R)^r)$,并使 t 保密;

(b)以 t 为解密密钥,对密文 c 进行解密,得到 $m = D_t(c)$.

(c)计算:$h_i = F(m, L, PK_R, R_i, P_{pub}) = H_2(e(R_i, P)e(H_2(L \| m)PK_R, P_{pub})), \quad i \in \{1, \cdots, n\}$

验证:$e\left(P_{pub}, \sum_{i=1}^{n}\{R_i + h_i tPK_i\}\right) \stackrel{?}{=} e(P, \sigma)$

如果成立,则举报有效;否则,举报无效.

(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,真正的举报者必须使举报受理机构确信其收到的举报来自 M,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,计算

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

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

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.

3.2 Miao-Wang-Miao-Xiong 匿名电子举报方案的安全性分析和攻击方法

一个良好的举报系统应满足:(1)举报人身份是模糊的;(2)举报信息具有机密性,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)对举报人提供有效的激励机制.对于 Miao-Wang-Miao-Xiong 匿名电子举报方案,经过分析,我们发现不满足条件(2)、(3),下面具体给出攻击方法:

(1)举报受理不满足机密性.当攻击者截获到举报 $rSign = \{L, R_1, \cdots, R_n, \sigma, c, S, r\}$ 后,攻击者利用截获的举报和举报受理者的公钥、系统公钥计算:

$\hat{t} = H_2(e(P_{pub}, S)e(P_{pub}, PK_R)^r)$

又由于:$H_2(e(P_{pub}, S)e(P_{pub}, PK_R)^r) = H_2(e(P_{pub}, S)e(P, SK_R)^r) = t$

所以:$\hat{t} = t$

由于攻击者能够独立计算出 t,不满足原方案要求的使 t 保密的要求.

根据原方案的方法,利用 t 可解密得到举报内容的明文 $m = D_t(c)$,计算 $h_1, h_2, \cdots, h_n$,并验证:

$e\left(P_{pub}, \sum_{i=1}^{n}\{R_i + h_i tPK_i\}\right) \stackrel{?}{=} e(P, \sigma)$

如果上式成立,则为有效的举报;否则,举报无效.

从以上攻击方法可以看出,举报受理不满足机密性.

(2)不满足悬赏领取的自证明性,即不满足对举报人提供有效的激励机制.当攻击者接收到举报 $rSign = \{L, R_1, \cdots, R_n, \sigma, c, S, r\}$ 后,攻击者计算 $\hat{t} = H_2(e(P_{pub}, S)e(P_{pub}, PK_R)^r)$

又由于:$H_2(e(P_{pub}, S)e(P_{pub}, PK_R)^r) = H_2(e(P_{pub}, S + rPK_R))$

$= H_2(e(P_{pub}, bPK_R)) = H_2(e(P_{pub}, PK_R)^b) = t$

所以 $\hat{t} = t$

因而,利用 t',攻击者加密 $c' = E_{t'}(ID_a \| t')$,并将(ID_a, c')发送给举报受理机构 N_R,收到举报后,N_R 计算如下:

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

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

如果 $D_t(c') = (ID_a \| t)$,则说明 $t' = t$,而身份为 ID_a 的攻击者 N_a 就是举报者.由于 $\hat{t} = t$,所以上式成立,因而,任何人都能冒充举报者进行悬赏领取.原方案不满足悬赏领取的自证明性,即,不满足对举报人提供有效的激励机制.

4 支持悬赏的匿名电子举报方案的设计模式和安全性分析

我们利用安全的基于双线性对的举报受理者公钥加密方案(E_{pk_R}, D_{sk_R})[10]、安全的指定验证者的环签名方案($Sign(pk_1, \cdots, pk_n, sk_i, pk_R, m)$, $Verify(pk_1, \cdots, pk_n, sk_R, m)$)[8,9]设计一种支持悬赏的匿名电子举报方案,其中举报受理者 N_R 的公钥-私钥对为(E_{pk_R}, D_{sk_R}),假设成员 N_k 欲举报的消息为 m,步骤如下:

初始化、密钥生成分别按相应的举报受理者公钥加密方案、指定验证者的环签名方案的对应步骤进行;下面步骤中的参数含义跟 Miao-Wang-Miao-Xiong 匿名电子举报方案相同:

举报生成:

(1)N_k 随机选取 $b \in Z_q^*$,计算 $B = bP$, $c = E_{pk_R}(m \| B)$;

(2)N_k 对消息 m 进行指定验证者 N_R 的环签名 $S = Sign(pk_1, \cdots, pk_n, sk_k, pk_R, m)$;

(3)N_k 将(c, B, S)发送给举报受理者 N_R;

举报受理:

举报受理:

(1)N_R 计算 $m \| B = D_{sk_R}(c)$,利用 B 已知,将 m 从 $m \| B$ 中提取出来;

(2)N_R 对签名 S 进行验证:

$$Verify(pk_1, \cdots, pk_n, sk_R, m) \stackrel{?}{=} True$$

如果成立,则接受举报;否则,拒绝接受.

悬赏领奖:

真正的举报人利用 B 的离散对数 b 作为保密的知识,与举报受理者 N_R 进行零知识证明,使得受理者 N_R 确认真正的举报人.

安全性分析:

(1)举报人身份的匿名性由于本方案是基于指定验证者的环签名方案和公钥加密方案,因而满足举报人身份的无条件匿名性.

(2)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 B 的离散对数 b,从而证明其是真正的举报人.任何非真正签名者要想知道 b,必须解决椭圆曲线离散对数问题.在 ECC DLP 困难性假设下,攻击者不能冒充举报人.

(3)举报的不可传递性由于本方案是基于指定验证者的环签名方案和公钥加密方案,根据指定验证者的环签名方案的不可传递性,和公钥加密方案的公开性,举报受理机构能够仿真举报,满足举报的不可传递性.

(4)举报内容的机密性和第三方不可伪造性对任何第三方,要想获得明文,必须解密密文 c;在公钥加密方案(E_{pk_R}, D_{sk_R})安全的条件下,满足了举报内容的机密性.对于任何第三方,要想伪造举报的内容和签名,必须伪造指定验证者的环签名;在指定验证者的环签名方案安全的条件下,满足了第三方不可伪造性.

5　总结

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.通过对 Miao-Wang-Miao-Xiong 匿名电子举报方案[1]进行了安全性分析,指出了该方案不满足其要求的举报信息机密性,以及不满足对举报人提供有效的激励机制,并设计了相应的攻击方法.为设计满足要求的支持悬赏的匿名电子举报方案,我们利用安全的基于双线性对的举报受理者公钥加密方案、安全的指定验证者的环签名方案提出了一种支持悬赏的匿名电子举报方案设计模式.经安全性分析,我们的设计模式是安全的.

参考文献:

[1] 苗付友,王行甫,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
Miao Fuyou, Wang Xingfu, et al. An anonymous E-Prosecution scheme with reward support[J]. Acta Electronica Sinica, 2008, 36(2):320 - 324(in Chinese)

[2] Chaum D, Heyst E. Group signatures[A]. Eurocrypt'91[C]. LNCS547, Berlin: Springer-Verlag, 1991. 257 - 265.

[3] Cramer R, Damgard I, et al. Proofs of partial knowledge and simplified design of witness hiding protocols[A]. Crypt'94[C]. LNCS 839, Berlin: Springer-Verlag, 1994. 174 - 187.

[4] Camenisch J. Efficient and generalized group signatures[A]. Eurocrypt'97[C]. LNCS 1233, Berlin: Springer-Verlag, 1997. 465 - 479.

[5] Rivest R L, Shamir A, et al. How to leak a secret [A]. Asiacrypt'01[C]. LNCS 2248, Berlin: Springer-Verlag, 2001. 552 - 565.

[6] Liu Y W, Liu J K, et al. Revocable ring signature[J]. Journal of Computer Science and Technology. 2007, 22(6): 785 - 794.

[7] Au M H, Liu J K, et al. Certificate based(linkable) ring signature[A]. ISPEC 2007[C]. LNCS 4464, 2007. 79 - 92.

[8] Jin Li, Yanming Wang. Universal designated verifier ring signature(proof) without random oracles [A]. ENC2006 [C]. LNCS4097, 2006. 332 - 341.

[9] Ji-Seon Lee, Jik Hyun Chang. Strong designated verifier ring signature scheme[A]. 2007 Innovations and Advanced Techniques in Computer and Information Sciences and Engineering [C]. Springer Netherlands. 2007. 543 - 547.

[10] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[A]. Crypto'01[C]. LNCS 2139, Berlin: Springer-Verlag, 2001. 213 - 229.

作者简介:

王化群　男,1974 年生于山东济宁,博士,大连水产学院副教授、硕士生导师,主要研究方向为信息安全.
E-mail: whq@dlfu.edu.cn

于　红　女,1968 年生于辽宁瓦房店,博士,大连水产学院教授,主要研究方向为数据挖掘、数据库安全、计算机应用等.

吕显强　男,1957 年生于辽宁大连,大连水产学院副教授,信息工程学院副院长,主要研究方向为计算机应用技术等.

张福泰　男,1965 年生于陕西陇县,南京师范大学教授,博士生导师,主要研究方向为密码学及其应用.