一种新的可证明安全的代理环签名方案

罗大文,何明星,李 虓
LUO Da-wen,HE Ming-xing,LI Xiao

西华大学 数学与计算机学院,成都 610039
School of Mathematics and Computer Engineering,Xihua University,Chengdu 610039,China

LUO Da-wen,HE Ming-xing,LI Xiao.New provably secure proxy ring signature scheme.Computer Engineering and Applications,2009,45(7):100-102.

Abstract: An efficient proxy ring signature scheme is proposed,the proxy ring signature scheme overcomes the common weakness that the operation field is unreasonable in the step of proxy key generation in the existed proxy ring schemes.The computational cost of bilinear pairings is reduced from $O(n)$ to $O(1)$,the computational efficiency is improved.The unforgeability is proved depending on the CDHP.The proxy ring signature scheme also satisfy the other security requirements of a proxy ring signature scheme: unconditional ambiguity,verifiability,distinguishability.

Key words: ring signature;proxy signature;proxy ring signature;provably security;Computation Diffie-Hellman Problem(CDHP)

摘 要:提出了一个有效的代理环签名方案,此方案克服了以往基于身份的方案在代理钥生成时运算域不合理的弱点。同时使方案的有效性提高:双线对的计算开销从 $O(n)$降到了 $O(1)$。在计算性 Diffie-Hellman 问题(CDHP)困难假设下,证明了它的不可伪造性。提出的方案也满足代理环签名方案的其他安全性要求:无条件匿名性、可验证性、可区分性。

关键词:环签名;代理签名;代理环签名;可证明安全;计算性 Diffie-Hellman 问题
DOI:10.3778/j.issn.1002-8331.2009.07.031 **文章编号**:1002-8331(2009)07-0100-03 **文献标识码**:A **中图分类号**:TN918.4

1 引言

2001 年,Rivest 等人在文献[1]中提出了环签名概念,环签名是一种简化的类群签名[2],环签名与群签名不同,没有群管理员,签名用户没有组织结构程序,不用协调一致。任何用户都可以用自己的私钥和其他环中成员公钥签名而不需要其他成员同意,环签名保护签名者的匿名性,它使得验证者可以确信签名来自一个环,但不知道谁是真正的签名者。环签名是一种很好的以匿名方式透露可靠消息的技术。代理签名是 1996 年由 M Mambo 等人在文献[3]中提出,利用代理签名原始签名人可以将他(她)的签名权委托给代理签名者,对任何消息代理人都可以进行签名,任何人只要知道原始签名人的公钥就可以对代理签名进行验证。在有些时候,代理签名者要代表原始签名者签名, 同时又想保护自己的匿名性。为了解决这种问题,2003 年张等人在文献[4]中提出了代理环签名的概念,它把代理签名和环签名结合起来,满足代理签名和环签名的特性。在这之后,文献[5-9]提出了几个代理环签名方案。文献[5-8]中的方案有两个共同的缺陷:(1)在代理钥生成的时候运算域不够合理;(2)需要太多的双线性对运算。文献[9]中的方案虽然没有这两种缺陷,但是它在生成代理环签名时没有使用代理密钥,在签名验证时没有使用环成员的公钥。给出了一个有效的代理环签名方案,它克服了以往基于身份的方案的缺陷,此方案在代理钥生成的时候运算域是合理地,双线对的计算开销从 $O(n)$降到了 $O(1)$,有效性提高了。与此同时提出的方案也满足代理环签名方案的安全性要求:可区分性、可验证性、不可伪造性、无条件匿名性。

2 双线性对与几个计算困难性问题及代理环签名的安全性要求

2.1 双线性对的性质

设 G_1 是由 P 生成的加法群,阶为素数 q,G_2 是阶为 q 的乘法群,双线性对是一个映射 $e:G_1\times G_1\to G_2$ 它满足如下性质:

(1)双线性性:设 $P,Q,R\in G_1$,则有:

$e(P,Q+R)=e(P,Q)e(P,R)$,$e(P+Q,R)=e(P,R)\ e(Q,R)$

$e(aP,bQ)=e(abP,Q)=e(P,abQ)=e(P,Q)^{ab}$

其中 $a,b\in Z_q$。

(2)非退化性:$\exists P,Q\in R_1$,使 $e(P,Q)\neq 1$。

(3)可计算性:存在有效的算法计算 $e(P,Q)$,其中 $P,Q\in G_1$。

2.2 几个计算困难性问题

(1)离散对数问题(DLP):已知 $P,Q\in G_1$ 寻找 $n\in z_q^*$,使 $Q=nP$。

(2)决定性 Diffie-Hellman 问题(DDHP):设 $P\in G_1,a,b,$

基金项目:国家自然科学基金(the National Natural Science Foundation of China under Grant No.60773035);西华大学人才培养项目(No.R0722612)。
作者简介:罗大文(1972-),男,讲师,主要研究领域:信息安全;何明星(1964-),男,工学博士,教授,主要研究领域:信息安全;李虓(1972-),男,副教授,主要研究领域:信息安全。
收稿日期:2008-09-10 **修回日期**:2008-11-19

$c \in z_q^*$,已知 P、aP、bP、cP 确定 $c=ab \bmod q$ 是否成立。

(3)计算性 Diffie-Hellman 问题(CDHP):设 $P \in G_1$,$a,b \in z_q^*$,已知 P、aP、bP,计算 abP。

(4)双线性对 Diffie-Hellman 问题(BDHP):设 $P \in G_1$,$a,b \in z_q^*$,已知 P、aP、bP、cP,计算 $e(P,P)^{abc}$。

假设:本文中假定 CDHP、DLP、BDHP 是计算困难的,也就是说没有多项式时间以不可忽略的概率去计算出它们。

2.3 代理环签名的安全性要求

代理环签名一般具有以下安全特性:

(1)无条件匿名性(Unconditional ambiguity):攻击者(包括原始签名者)不知道谁是真正的代理签名者。

(2)不可伪造性(Unforgeability):一个授权的代理签名者可以产生一个合法的代理环签名,但是原始签名者和第三方不能产生一个合法的代理环签名。

(3)可验证性(Verifiability):从代理环签名中,任何人都可以验证签名的正确性。

(4)可区分性(Distinguishability):代理环签名区别于代理签名者一般的环签名。

3 几个代理环签名方案的缺陷

3.1 C-L 方案和 L-L 方案的缺陷

在文献[6]和文献[8]中分别给出了一个基于身份的代理环签名方案,简称为 C-L 方案和 L-L 方案,这两个方案在生成代理钥的时候,原始签名者首先计算 $S_W=S_0H_1(W)$,发现这个等式的运算域是不合理的,因为 $S_W=S_0H_1(W)$ 中 $S_0 \in G_1$,$H_1(W) \in G_1$,在 G_1 中没有定义 $S_0H_1(W)$。

3.2 Y-Y 方案的缺陷

在文献[9]中给出了一个代理环签名方案,简称为 Y-Y 方案,在这个方案中,发现有两个错误。

(1)在代理环签名生成的第(3)步中:

$$V=(h_s+r_s)S_s-s_s\sum_{i=1}^{n}(R_i+h_iH_2(\omega))$$

这个等式中表面上含有代理密钥 S_s,但通过运算后发现:

$$V=(h_s+r_s)S_s-s_s\sum_{i=1}^{n}(R_i+h_iH_2(\omega))=$$

$$(h_s+r_s)S_s-s_s(R_s+h_sH_2(\omega))-s_s\sum_{i\neq s}(R_i+h_iH_2(\omega))=$$

$$(h_s+r_s)S_s-s_s(r_sH_2(\omega)-\sum_{i\neq s}(R_i+h_iH_2(\omega))+h_sH_2(\omega))-$$

$$s_s\sum_{i\neq s}(R_i+h_iH_2(\omega))=(h_s+r_s)S_s-(r_s+h_s)s_sH_2(\omega)=$$

$$(h_s+r_s)(s_0H_2(\omega)+s_sH_2(\omega))-(r_s+h_s)s_sH_2(\omega)=(r_s+h_s)s_0H_2(\omega)$$

它根本不含代理密钥 S_s,也就是说任何人都可以伪造这个签名。

(2)在签名验证等式 $e(P,V)=e(P_0,\sum_{i=1}^{n}(R_i+h_iH_2(\omega)))$ 中,没有用到环成员的公钥。

4 有效的代理环签名方案

(1)系统参数设置

设 G_1 是由 P 生成的阶为素数 q 的加法群,G_2 是阶为 q 的乘法群,$e:G_1\times G_1\to G_2$ 是双线性对。H_1、H_2 是两个安全的哈希函数,其中 $H_1:\{0,1\}^*\to z_q^*$,$H_2:\{0,1\}^*\to G_1$。原始签名者 Alice 的公钥是 $P_0=s_0P$,私钥是 $s_0 \in z_q^*$,$L=\{PS_i\}$,$i=1,2,\cdots,n$,L 表示代理签名人的集合,一个环成员 PS_i 的公钥是 P_i,私钥是 s_i。

(2)代理密钥的生成

①原始签名者 Alice 生成一个授权信息 ω,ω 包含了原始签名者把签名权委托给代理签名者的有关信息:比如授权期限、授权范围等。

②原始签名者计算 $s_0H_2(\omega)$并把它传给代理签名者。

③代理签名者验证 $e(s_0H_2(\omega),P)=e(H_2(\omega),P_0)$是否成立,若不成立则拒绝委托代理;如果成立,则代理签名者各自计算代理签名密钥 $S_{p_i}=s_0H_2(\omega)+s_iH_2(\omega)=i=1,2,\cdots,n$。

(3)签名生成

对于消息 m,真实的代理签名者(不妨设为第 k 个人)选择 $r_i \in_R z_q^*$,计算 $U_i=r_iP_i$,$h_i=H_1(m \parallel L \parallel U_i)(i\neq k)$;再选择 $r_k \in_R z_q^*$ 计算 $U_k=r_kP_k+r_kP_0-\sum_{i\neq k}(r_i+h_i)P_i$,$H_k=H_1(m \parallel L \parallel U_k)$,$V=r_kS_{pk}+h_ks_kH_2(\omega)$。

签名为:$\sigma=(m,U_1,U_2,\cdots,U_n,V)$。

(4)签名验证

①验证者计算 $h_i=H_1(m \parallel L \parallel U_i)$,$i=1,2,\cdots,n$。

②验证 $e(H_2(\omega),\sum_{i=1}^{n}(U_i+h_iP_i))=e(P,V)$,如果等式成立,则认为签名是正确的。否则认为签名无效。

5 安全性分析

以下从代理环签名需要满足的安全性需求的几个方面,证明了其安全性,在定理 2 的证明中用到了环签名分叉引理,有关环签名分叉引理,详见参考文献[10]。

定理 1 提出的代理环签名方案满足无条件匿名性。

证明 在一个合法的签名 $\sigma=(m,U_1,U_2,\cdots,U_n,V)$中,$U_i=r_iP_i$,$i\neq k$,$U_k=r_kP_k+r_kP_0-\sum_{i\neq k}(r_i+h_i)P_i$,$V=r_kS_{pk}+h_ks_kH_2(\omega)$。因为 r_i 是随机选择的,所以无论谁是真正的签名者$(U_1,U_2,\cdots,U_n,V)$在 G_1 上都是均匀分布的;同时由于 $V=r_kS_{pk}+h_ks_kH_2(\omega)$中含有随机选择的 r_k,故也不会泄露真实签名者的身份。综上所述,环成员之外的任何人(包括原始签名者)猜出真实代理签名者的概率不会超过$\frac{1}{n}$。

定理 2 提出的代理环签名方案在 CDHP 困难性假设下满足不可伪造性。

证明 令 $H_2(\omega)=aP$,$P_j=bP$,假设敌手 A 能成功伪造代理签名人 U_k 的一个有效的代理环签名:$(L,m,U_1,U_2,\cdots,U_n,V,h_1,h_2,\cdots,h_n,V)$,则由环签名分叉引理[10]可知,存在 1 个算法 A',能以不可忽略的概率输出 2 个有效的代理环签名:$(L,m,U_1,U_2,\cdots,U_n,V,h_1,h_2,\cdots,h_n,V)$和$(L,m,U_1,U_2,\cdots,U_n,V,h_1',h_2',\cdots,h_n',V')$其中 $h_i=h_i'$,$i\in\{1,2,\cdots,n\}\backslash\{j\}$,而 $h_j\neq h_j'$。由于 2 个签名均有效,故都满足签名验证方程,于是有:

$$e(H_2(\omega),\sum_{i=1}^{n}(U_i+h_iP_i))=e(P,V)$$

$$e(H_2(\omega),\sum_{i=1}^{n}(U_i+h_i'P_i))=e(P,V')$$

由以上两个等式得:$e(H_2(\omega),(h_j-h_j')P_j)=e(P,V-V')$,即:$e(aP,$

$(h_j-h_j')bP)=e(P,V-V')$,则有$(h_j-h_j')abP=V-V'$。所以 $abP=(h_j-h_j')^{-1}(V-V')$,即解决了 CDHP 的一个实例。

定理 3 原始签名者的密钥和代理签名者的代理密钥是安全的。

证明 (1)原始签名者的密钥是安全的,代理签名者和攻击者由 $s_0H_2(\omega)$不能得出 s_0,它面临的是 G_1 上的一个离散对数难题;

(2)代理签名者的代理密钥是安全的,因为代理密钥 $S_{p_i}=s_0H_2(\omega)+s_iH_2(\omega)$它是两个签名之和,要解出 S_{pi} 就要知道 s_0 和 s_i,由 $s_0H_2(\omega)$和 $s_iH_2(\omega)$去求 s_0 和 s_i,这也是 G_1 上的一个离散对数难题。

定理 4 提出的代理环签名方案也满足可验证性和可区分性。

证明 (1)可验证性

如果 $\sigma=(m,U_1,U_2,\cdots,U_n,V)$是代理签名者对消息 m 的数字签名,则有:

$$e(H_2(\omega),\sum_{i=1}^{n}(U_i+h_iP_i))=e(H_2(\omega),U_k+h_kP_k+\sum_{i\neq k}(U_i+h_iP_i))=$$

$$e(H_2(\omega),r_kP_k+r_kP_0-\sum_{i\neq k}(r_i+h_i)P_i+h_kP_k+\sum_{i\neq k}(U_i+h_iP_i))=$$

$$e(H_2(\omega),(r_k+h_k)P_k+r_kP_0)=e(H_2(\omega),((r_k+h_k)s_k+r_ks_0)P)=$$

$$e(P,(r_ks_0+r_ks_k+h_ks_k)H_2(\omega))=e(P,r_k(s_0+s_k)H_2(\omega)+h_ks_kH_2(\omega))=$$

$$e(P,r_kS_{pk}+h_ks_kH_2(\omega))=e(P,V)$$

(2)可区分性

代理环签名区别于一般的数字签名,因为代理钥 S_{p_i} 与私钥 s_i 不同。

6 有效性分析

(1)提出的方案在代理钥生成的时候运算域是合理地,因为 $s_0H_2(\omega)$中 $s_0\in z_q^*$,$H_2(\omega)\in G_1$,在 G_1 中可以计算 $s_0H_2(\omega)$。

(2)为了比较计算开销,用 G_{1A} 表示 G_1 中的加法运算,G_{1M} 表示 G_1 中的标量乘法,G_{2M} 表示 G_2 中的乘法运算,*PAIR* 表示双线性对运算。与文献[4,7]比较如表 1。

从表 1 中可以看出,提出的方案的 G_{1A} 和 G_{1M} 的计算复杂性与文献[4,7]相同,都是 O(n),但是文献[4,7]中双线性对 *PAIR* 运算的计算复杂性都是 O(n),而提出的方案中双线性对 *PAIR* 运算的计算复杂性从 O(n)降到了 O(1)。

表 1 本文算法与文献[4,7]的比较

方案	G_{1A}	G_{1M}	G_{2M}	*PAIR*
Zhang[4]	$2n$	$2n$	$n-1$	$4n-1$
Amit[7]	$5n-1$	$3n-1$	2	$n+2$
本文方案	$4n$	$4n$	0	2

7 结论

给出了一个有效的代理环签名方案,它克服了以往基于身份的方案的缺陷,此方案在代理密钥生成的时候运算域是合理的,双线对的计算开销从 O(n)降到了 O(1),有效性得到提高。在 CDHP 问题困难性假设下,证明了它的不可伪造性。同时提出的方案也满足代理环签名方案的其他安全性要求:可区分性、可验证性、无条件匿名性。在既需要代理签名又要保护代理签名者的匿名性时,该方案有一定的实用价值。

参考文献:

[1] Rivest R,Shamir A,Tauman M.How to leak a secret[C]//LNCS 2248:Advances in Cryptology_Asiacrypt 2001,2001:552-565.

[2] 王继林,张键红.基于环签名思想的一种类群签名[J].电子学报,2004,32(3):408-410.

[3] Mambo M,Usuda K,Okamoto E.Proxy signature:delegation of the power to sign messages[C]//IEICE Tran Fundamentals,1996,E79-A(9):1338-1353.

[4] Zhang F,Naini R S,Lin C Y.New proxy signature,proxy blind signature and proxy ring signature scheme from bilinear pairings[EB/OL].(2003).http://eprint.iacr.org/2003/104/.

[5] Awasthi A K,Lal S.A new proxy ring signature scheme[C]//Proceeding of RMS,2004:29-33.

[6] Cheng Wen-qing,Lang Wei-min,Yang Zong-kai,et al.An identity-based proxy ring signature scheme from bilinear pairings[C]//2004 IEEE,2004:424-429.

[7] Awasthi A K,Lal S.ID-based ring signature and proxy ring signature schemes from bilinear pairings[EB/OL].(2004).http://eprint.iacr.org.

[8] 吕小红,郎为民,夏婧.一种改进的代理环签名方案[J].微计算机信息,2006,22(9/3):79-81.

[9] 禹勇,杨波,李发根,等.一个有效的代理环签名方案[J].北京邮电大学学报,2007,30(3):23-26.

[10] Herranz J,Saez G.Forking lemmas for ring signature scheme[C]//LNCS 2904:Proceeding of Indocrypt'03,2003,266-279.

(上接 67 页)

参考文献:

[1] Zadeh L A.Fuzzy sets[J].Inform and Control,1965,8:338-356.

[2] Gau W L,Buehrer D J.Vague set[J].IEEE Trans on Systems,Man and Cybernetics,1993,23(2):610-614.

[3] Atanassow K.Intuitionistic fuzzy sets[J].Fuzzy Sets and Systems,1986,20(1):87-96.

[4] Atanassow K.Intuitionistic fuzzy sets theory and applications[M].New York:Springer-Verlag Company,1999.

[5] 马志锋,邢汉承,郑晓妹.决策表中规则获取的不确定性研究[J].控制与决策,2000,15(6):703-707.

[6] 李凡,饶勇.基于 Vague 集的加权多目标模糊决策方法[J].计算机科学,2001,28(7):60-65.

[7] 马志锋,邢汉承,郑晓妹.区间值 Vague 决策系统及其规则提取方法[J].电子学报,2001,29(5):585-589.

[8] Chen S M,Tan J M.Handing multi-criteria fuzzy decision-making problems based on vague set theory[J].Fuzzy Sets and Systems,1994,67(2):163-172.

[9] 李凡,卢安,蔡立晶.基于 Vague 集的多目标模糊决策方法[J].华中科技大学学报,2001,29(7):1-3.

[10] Hong D H,Choi C H.Multi-criteria fuzzy decision making problems based on vague set theory[J].Fuzzy Sets and Systems,2000,114:103-113.

[11] 周珍,吴祈宗.基于区间值 Vague 集的多准则模糊决策方法[J].北京理工大学学报,2005,25(11):1019-1023.

[12] 刘华文.多目标模糊决策的 Vague 集方法[J].系统工程理论与实践,2004,5(5):103-109.