第 26 卷第 12 期 电子与信息学报 Vol.26No.12
2004 年 12 月 Journal of Electronics & Information Technology Dec. 2004

指名签名与指名代理签名 [1]

黄振杰 * ** 郝艳华 * 王育民 *

*(西安电子科技大学综合业务网国家重点实验室 西安 710071)
**(漳州师范学院计算机科学系 漳州 363000)

摘 要: 该文分别对一个指名签名方案 (KPW 方案) 和一个指名代理签名方案 (PL 方案) 进行分析，结果表明：在 KPW 方案中签名人不仅能验证而且也能向第三方证明签名的有效性，甚至能将签名转化为通常的自认证签名，因此不是指名签名方案；在 PL 方案中任何人都可验证签名的有效性，它只是一个自认证签名方案．该文进一步给出了 KPW 方案的一个改进方案，使之具有指名签名的全部性质，同时也给出了一个基于该方案的指名代理签名方案．

关键词: 应用密码学，数字签名，指名签名，指名代理签名
中图分类号: TN918 **文献标识码:** A **文章编号:** 1009-5896(2004)12-1996-06

Nominative Signature and Nominative Proxy Signature

Huang Zhen-jie* ** Hao Yan-hua* Wang Yu-min*

*(*State Key Lab of Integrated Service Networks, Xidian Univ., Xi'an* 710071, *China*)
**(*Dept of Computer Science, Zhangzhou Teachers College, Zhangzhou* 363000, *China*)

Abstract Analyses of a nominative signature scheme (KPW scheme) and a nominative proxy signature scheme (PL scheme) are given, respectively. The results show that the KPW scheme is not a nominative signature scheme since the nominator not only can verify and prove the validity of given signatures but also can convert given signatures into universally verifiable signatures, and that the PL scheme is only a self-authentication signature scheme since anyone can verify the validity of given signatures. Furthermore, an improvement of the KPW scheme, in which all properties of the nominative signature are held, and a nominative proxy signature scheme based on the proposed nominative signature scheme are proposed.

Key words Applied cryptography, Digital signature, Nominative signature, Nominative proxy signature

1 引言

数字签名是信息安全领域的关键技术之一，已在许多应用系统中得到广泛应用。对于一般数字签名，任何人用签名人的公钥都可验证其有效性，这个性质就是所谓的自认证性 (self-authentication), 它使得数字签名适用于诸如公布信息、颁发公钥证书等许多应用场合，同时也使得数字签名因容易被复制和传播而不适用于其他一些场合，比如 Bob 需要某权威人士 Alice 对其私人消息签名，如公证机关对个人财产的公证， Bob 需向第三方证明这些消息，但因为签名涉及的是私人消息， Bob 自然得防止其他人滥用签名去向别人示证，如 Bob 不想让其他人，包括公证机关，能向他人证明其财产的相关信息，在这种情况下一般的数字签名是不适用的。为了防止签名被滥用， Kim 等人提出指名签名体制 [1], 在这里只有签名接收人才能验证和向第

[1] 2003-06-24 收到， 2004-02-05 改回
国家自然科学基金重点项目 (19931010) 和国家 973 项目 (G1999035803) 资助课题

三方证明签名的有效性，即使是签名人也不能验证或证明签名的有效性，签名的使用完全由签名的接收人控制，它最适用于对签名接收人的私秘消息进行签名。

指名签名不仅能满足特定场合对签名的特殊要求，具有实际应用背景和意义，它还是不可否认签名 [2,3] 的对偶，与不可否认签名和指定证实人签名 [4] 一起使签名滥用的控制有了三种可能的可选方案，即只由签名人控制，签名人和接收人共同控制和只由接收人控制，三者一起构成理论上的完整性，在数字签名的理论方面也具有重要意义。

指名签名的进一步工作有 Kim, Park, Won 的零知识指名签名 [5] 和 Park, Lee 的指名代理签名 [6], 下文我们称前者为 KPW 方案，称后者为 PL 方案。本文对这两个方案进行了分析，我们遗憾地发现：在 KPW 方案中，签名人不仅能验证而且也能向第三方证明签名的有效性，甚至还能将签名转化为通常的自认证签名；而在 PL 方案中，任何人都可验证签名的有效性，它只是一个通常的自认证签名方案。本文还对 KPW 方案进行改进，使之具有指名签名的全部性质，同时给出一个基于我们的指名签名方案的指名代理签名方案，该方案达到了对代理签名和指名签名所要求的所有性质。

2 KPW 指名签名方案与分析

本节介绍并分析 Kim, Park, Won 于文献 [5] 提出的零知识指名签名方案。

2.1 KPW 指名签名方案

设 p, q 为两个大素数，其中 $q|(p-1)$, g 为 Z_p^* 的某 q 阶素子群的生成元。除特别声明外，本文的所有运算都在 Z_p^* 中进行。设签名人 s 的私钥为 x_s, 对应公钥 $y_s = g^{x_s}$, 签名接收人 v 的私钥为 x_v, 对应公钥 $y_v = g^{x_v}$, H 为防碰撞 Hash 函数， Kim 等人提出的指名签名方案如下：

(1) 签名　签名人 s 随机选取 r, $R \in_R [1, q-1]$, 计算

$$c = g^{R-r}, \quad C = y_v^R, \quad e = H(y_v||c||C||m), \quad S = r - x_s \cdot e(\mathrm{mod} q)$$

对消息 m 的签名为 $\sigma = (y_v, c, C, S)$ 。

(2) 验证　接收人 v 使用其私钥 x_v 可验证签名 (y_v, c, C, m), 先计算 $e = H(y_v||c||C||m)$, 然后验证

$$(g^S \cdot y_s^e \cdot c)^{x_v} = C$$

(3) 证明　签名接收人 v 通过向第三方证明 $(g^S \cdot y_s^e \cdot c)^{x_v} = C$ 且 $g^{x_v} = y_v$ 来证明签名的有效性，同时也证明签名是发给他的，这可通过文献 [3] 的交互式零知识证明协议完成。

2.2 KPW 方案分析

文献 [5] 指出指名签名方案应具有这样的性质：只有签名的接收人才能验证和向第三方证明签名的有效性，即使是签名人自己也不能验证或向第三方证明，遗憾的是他们的方案并不能做到这点. 通过分析我们发现，在他们的方案中，签名人不仅能验证而且也能向第三方证明签名的有效性，甚至还能将签名转化为通常的具有自认证性的签名。

(1) 签名人可验证签名　KPW 方案提供的签名验证方程是 $(g^S \cdot y_s^e \cdot c)^{x_v} = C$, 其他人 (包括签名人) 因为不知道接收人的私钥 x_v, 自然不能通过这个方程来验证签名，可是这个验证方程等价于 $g^S \cdot y_s^e \cdot c = g^R$, 而签名人知道 R, 所以他能通过后一个式子来验证签名。实际上在 KPW 方案中向第三方证明 $(g^S \cdot y_s^e \cdot c)^{x_v} = C$ 且 $g^{x_v} = y_v$, 就是要证明这个式子。

(2) 签名人可向第三方证明签名　分析 KPW 方案我们可以知道，该签名的实质是存在一个随机数 $R \in_R [1, q-1]$ 使得 $g^S \cdot y_s^e \cdot c = g^R$ 且 $C = y_v^R$, 因为签名接收人不知道这个 R, 所以他不能用它来向第三方证明， KPW 方案为签名接收人提供了一个等价的方法：证明存在一个 x_v 使得 $(g^S \cdot y_s^e \cdot c)^{x_v} = C$ 且 $g^{x_v} = y_v$, 可是签名人知道 R, 他可以直接用它来向第三方证明，证明协议如 KPW 方案的相应协议。

(3) 签名人可将签名转化成自认证签名　签名人除了可用上述的交互式零知识证明来证明签名的有效性外，还可以用非交互式知识证明来证明，比如离散对数相等知识签名 [7]，由于非交互式知识证明是自认证的，所以把它与签名捆绑在一起就可将 KPW 的签名转化为通常的具有自认证性的签名。在 KPW 方案中，签名人知道 R，他可以通过为签名附上一个证明 $\log_g(g^S \cdot y_s^e \cdot c) = \log_{y_v} C$ 的知识签名而签名转化为自认证签名。

总之，在 KPW 方案中，签名人能通过其他途径与签名接收人一样验证签名并向第三方证明，还可将签名转化为自认证签名，即 KPW 方案不是指名签名方案。

3 PL 指名代理签名方案与分析

本节介绍并分析 Park 和 Lee 于 2001 年提出的指名代理签名方案 [6]。

3.1 PL 指名代理签名方案

参数 p, q, g 和 Hash 函数 H 同上，原始签名人 s 的私钥为 x_s，对应公钥为 $y_s = g^{x_s}$，签名接收人 v 的私钥为 x_v，对应公钥为 $y_v = g^{-x_v}$，代理签名人 a 的私钥为 x_a，对应公钥为 $y_a = g^{x_a}$，Park 等人提出的代理指名签名方案如下：

(1) 产生代理　原始签名人 s 随机选取 $b_i \in_R [1, q-1]$，并计算

$$d_i = H(m||T_i), \qquad l = g^{b_i}, \qquad s_i = x_s \cdot d_i + b_i \cdot l (\mathrm{mod} q)$$

其中 m 为被签消息，T_i 为时戳。

(2) 代理传递　原始签名人 s 以安全方式传递 (s_i, l, m, T_i) 给代理签名人 a。

(3) 代理验证　代理签名人 a 验证

$$g^{s_i} = y_s^{H(m||T_i)} \cdot l^l$$

(4) 指名代理签名　代理签名人 a 随机选取 r, $R \in_R [1, q-1]$，并计算

$$K = g^{R - r \cdot x_a}, \quad D = y_v^R, \quad e = H(y_v||K||D||m), \quad S = x_a \cdot r - R \cdot s_i \cdot e (\mathrm{mod} q)$$

(5) 代理签名传递　代理人发送 (m, T_i, l, K, D, R, S) 给签名验收人 v。

(6) 指名代理签名验证　签名验收人 v 先计算

$$e = H(y_v||K||D||m), \qquad b = y_s^{H(m||T_i)} \cdot l^l$$

然后验证

$$D = (g^S \cdot b^{R \cdot e} \cdot K)^{x_v}$$

3.2 PL 方案分析

下面分析 PL 方案，我们将发现：在 PL 方案中，任何人都可验证签名的有效性，它只是一个通常的自认证签名方案。

(1) 不是指名的也不具有用户机密性　文献 [6] 中作者称他们的方案具有用户机密性，即除指定的签名接收人外，任何第三方不能从签名中得到签名人的身份，其实他们的方案并不具有用户机密性。该方案提供的验证方程是 $D = (g^S \cdot b^{R \cdot e} \cdot K)^{x_v}$，它的验证确需知道签名接收人的私钥 x_v，可是上述方程与方程 $g^R = g^S \cdot b^{R \cdot e} \cdot K$ 等价，而验证后一个方程所需的值除两个公钥外全在签名中了，因此任何人均可验证，这就是说，PL 方案给出的签名是自认证的，不是指名代理签名，因此不具有基于指名签名的用户机密性，任何人都可验证签名人的身份，因为签名中含有签名人的公钥。

(2) 无法认证代理，代理人可否认签名，原始签名人可单独完成签名　在 PL 方案所提供的签名算法和验证算法中，把代理签名人的私钥换成任意数不会影响签名和验证，也就是说代理签名人的私钥在方案中不起实质性作用，从签名无法知道谁是代理，因此代理人可否认签名，任何得到 (s_i, l, m, T_i) 的人都可产生有效签名，当然原始签名人可单独完成签名。在 PL 方案中，代理人实际起的只是运算器的作用，这不只是因为原始签名人可单独完成签名，还因为该方案中原始签名人参与了对每条消息的签名。

4 本文的方案

本节给出两个指名签名方案，一个是对 KPW 方案的改进，使之成为真正的指名签名方案，另一个是指名代理签名方案。

4.1 指名签名方案

由 2.2 节的分析可知， KPW 方案中签名人之所以能做与签名接收人一样的事，是因为那个控制签名验证的随机数 R 是签名人选的，下面我们给出 KPW 方案的一个改进，主要思想是将随机数 R 改由签名接收人选，加密发送给签名人，对其他所有人保密。

参数 p, q, g, Hash 函数 H, 签名人和接收人的公钥 / 私钥对均如 KPW 方案，我们的改进方案如下：

(1) 签名

(a) 接收人 v 随机选取 $R, r' \in_R [1, q-1]$, 计算

$$c' = g^R, \quad C = y_v^R, \quad A_1 = y_s^{r'}, \quad A_2 = g^{r'} \cdot c', \quad A_3 = g^{r'} \cdot C$$

发送 (A_1, A_2, A_3) 给签名人 s 。

(b) 签名人 s 解密出

$$c' = A_2 / A_1^{x_s^{-1}}, \qquad C = A_3 / A_1^{x_s^{-1}}$$

然后随机选取 $r \in_R [1, q-1]$, 并计算

$$c = c' \cdot g^{-r}, \qquad e = H(y_v || c || C || m), \qquad S = r - x_s \cdot e (\mathrm{mod} q)$$

对消息 m 的签名为 $\sigma = (c, S)$ 。

(2) 验证　接收人 v 使用其私钥 x_v 可验证签名 (c, S), 先计算 $e = H(y_v || c || C || m)$, 然后验证

$$(g^S \cdot y_s^e \cdot c)^{x_v} = C$$

(3) 证明　证明如 KPW 方案。

安全性分析　本改进方案与 KPW 方案一样都是由 Schnorr 签名方案改进而来的，改进的只是验证的方法，因此其安全性仍与 Schnorr 签名方案 [8] 相同。

本改进方案与 KPW 方案一样，要验证或向第三方证明签名的有效性必须知道随机数 R 或签名接收人的私钥 x_v, 在本方案中这二者都只有签名接收人才知道，所以只有他才能验证和向第三方证明签名的有效性。签名人虽然知道 $c' = g^R$, 可他不能验证 g^R 中的 R 是否与 $C = y_v^R$ 中的 R 相同，因为 $g^S \cdot y_s^e \cdot c = g^R$ 与 $(g^S \cdot y_s^e \cdot c)^{x_v} = C$ 等价的充要条件是上述的两个 R 相同，因此他只能验证他是否正确运行了签名算法，而不能验证所得的签名是否有效，当然就更不可能向第三方证明。

4.2 指名代理签名方案

基于上述的指名签名方案，我们可以构造下面的指名代理签名方案，该方案同时也基于文献 [9] 的代理签名方案。

(1) 建立　参数 p, q, g 和 Hash 函数 H 的选择如上。原始签名人 s 、代理签名人 a 和签名接收人 v 各自随机选取自己的私钥 $x_s, x_a, x_v \in_R [1, q-1]$, 计算并公布对应的公钥 y_s, y_a 和 y_v, 这里 $y_* = g^{x_*}$ 。

(2) 产生代理私钥

(a) 原始签名人 s 随机选取 $k_s \in_R [1, q-1]$, 计算

$$r_s = g^{k_s}, \qquad s_s = x_s \cdot H(w||r_s) + k_s (\mathrm{mod} q)$$

其中 w 为权限信息，包含代理签名人 a 和签名接收人 v 的身份以及其他授权信息。

(b) 原始签名人 s 秘密发送授权证书 (w, r_s, s_s) 给代理签名人 a 。

(c) 代理签名人 a 验证

$$g^{s_s} = y_s^{H(w||r_s)} \cdot r_s$$

(d) 如果上式成立，代理签名人 a 计算代理私钥：

$$x_p = s_s + x_a (\mathrm{mod} q)$$

(3) 签名　以 x_p 为私钥用 4.1 节的指名签名方案对消息 m 签名，得到签名 (c, S), m 须满足权限 w 的要求。发送代理签名 (c, S, r_s, w) 给签名接收人 v 。

(4) 验证

(a) 检查消息 m 是否满足 w 的要求， y_s, y_a 是否分别为 w 中指定的原始签名人和代理签名人的公钥。

(b) 计算

$$y_p = y_s^{H(w||r_s)} \cdot r_s \cdot y_a, \qquad e = H(y_v||c||C||m)$$

验证

$$(g^S \cdot y_s^e \cdot c)^{x_v} = C$$

(5) 证明　使用与 KPW 方案相同的证明协议，签名接收人 v 通过证明 $(g^S \cdot y_p^e \cdot c)^{x_v} = C$ 且 $g^{x_v} = y_v$ 向第三方证明签名的有效性，同时也证明签名是发给他的。

本方案具有如下性质：

(1) 强不可伪造性 (Strong unforgeability)　除指定的代理签名人外，任何其他人，包括原始签名人，都不可能生成有效的代理签名，这是因为只有指定的代理签名人才能产生有效的代理私钥，而要生成有效的代理签名需要有效的代理私钥。

(2) 可验证性 (Verifiability)　指定接收人可以由代理签名确认原始签名人授权代理人签署该消息，因为签名中嵌入了原始签名人的授权和他的私钥。

(3) 强可识别性 (Strong identifiability)　指定接收人可以从有效的代理签名中确定出相应代理签名人的身份，因为签名中嵌入了代理签名人的私钥。

(4) 强不可否认性 (Strong undeniability)　代理签名人一旦代表原始签名人生成一个有效的代理签名，则该代理签名人就不能否认其所作的代理，因为只有他才能签名，这与性质 1 相同。

(5) 防滥用性 (Prevention of misuse)　代理授权证书不会被用于其他用途，即代理证书只能由指定的代理人用于对符合授权要求的消息进行签名。因为代理授权证书载明了代理人的身份和授权信息，代理签名人不可能转给他人或签署不符合授权证书要求的消息，这使得代理人不能滥用授权证书。原始签名人也不能滥用授权证书，因为他不能生成有效签名。

(6) 指名性 (Nominative)　只有指定的接收人才能验证签名，也只有该接收人才能向第三方证明签名的有效性，即使是签名人自己也不能验证或向第三方证明签名的有效性。这一点由 4.1 节的安全分析可知。

(7) 用户机密性 (User confidentiality)　除指定的接收人外，任何第三方不能从签名中得到原始签名人或代理签名人的身份，因为只有指定的接收人才能验证签名。

5 结论

指名签名是适用于对隐私消息进行签名的一种特殊数字签名，适用于许多特定的场合，同时它又是不可否认签名的对偶，因此对其研究具有理论和实际意义。本文对两个指名签名方案进行了分析，并提出一个改进的指名签名方案和一个指名代理签名方案。目前关于指名签名的研究成果还不多，继续提出更多的指名签名方案是进一步工作的可能方向。

参 考 文 献

[1] Kim S J, Park S J, Won D H. Nominative signatures. Proc. of ICEIC'95, International Conference on Electronics, Information and Communications, Yanji, Jilin, China, August 7-12, 1995: II-68–II-71.

[2] Chaum D, Antwerpen H. Undeniable signature. Proc. of Crypto'89, LNCS 435, Berlin: Springer-Verlag, 1989: 212–216

[3] Chaum D. Zero-knowledge undeniable signature. Proc. of Eurocrypt'90, LNCS 473, Berlin: Springer-Verlag, 1990: 458–464.

[4] Chaum D. Designated confirmer signatures. Proc. of Eurocypt'94, LNCS 950, Berlin: Springer-Verlag, 1994: 86–91.

[5] Kim S J, Park S J, Won D H. Zero-knowledge nominative signatures. Proc. of PragoCrypt'96, International Conference on the Theory and Applications of Cryptology, Prague, Czech, September 30-October 3, 1996: 380–392.

[6] Park H U, Lee I Y. A digital nominative proxy signature scheme for mobile communication. Proc. of ICICS'01, LNCS 2229, Berlin: Springer-Verlag, 2001: 451–455.

[7] Camenisch J. Efficient and generalized group signatures. Proc. of Eurocrypt'97, LNCS1233, Berlin: Springer-Verlag, 1997: 465–479.

[8] Schnorr C P. Efficient signature generation for smart cards. *Journal of Cryptology*, 1991, 4(3): 161–174.

[9] Lee B C, Kim H S, Kim K J. Strong proxy signature and its applications, SCIS'01, the 2001 Symposium on Cryptography and Information Security. Oiso, Japan. January 2001: 603-608.

黄振杰：　男，1964 年生，副教授，博士生，主要研究方向为电子商务安全和网络安全.

郝艳华：　女，1976 年生，博士生，主要研究方向为椭圆曲线密码体制与电子商务安全.

王育民：　男，1936 年生，教授，博士生导师，IEEE 高级会员，长期从事信息论、信道编码、密码学及通信网安全等方面的研究.