对两个提名代理签名方案的密码学分析

禹　勇[①]　　许春香[①]　　周　敏[②]　　李发根[①③]
[①](电子科技大学计算机科学与工程学院　成都　610054)
[②](华南农业大学信息学院　广州　510642)
[③](西安电子科技大学计算机网络与信息安全教育部重点实验室　西安　710071)

摘　要：该文分析了 Seo 等(2003)和黄振杰等学者(2004)提出的两个提名代理签名方案，指出这两个方案都不具备强不可伪造性。分别给出了一种伪造攻击，利用这种攻击，一个不诚实的原始签名人通过设置特定的参数，可以成功伪造代理签名密钥，从而可以假冒诚实的代理签名人生成有效的提名代理签名，威胁到代理签名人的合法权益。

关键词：数字签名；代理签名；提名签名
中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1009-5896(2009)05-1218-03

Cryptanalysis of Two Nominative Proxy Signature Schemes

Yu Yong[①]　　Xu Chun-xiang[①]　　Zhou Min[②]　　Li Fa-gen[①③]
[①](*School of Computer Science and Engineering*, *University of Electronic Science and Technology of China*, *Chengdu* 610054, *China*)
[②](*College of Information*, *South China Agricultural University*, *Guangzhou* 510642, *China*)
[③](*Key Lab of Computer Networks and Information Security of Ministry of Education*, *Xidian University*, *Xi'an* 710071, *China*)

Abstract: Analyses of two nominative proxy signature schemes proposed by Seo *et al.*(2003) and Huang *et al.* (2004) are given in this paper. The results show that neither the scheme has the property of strong unforgeability. A forgery attack on the two schemes is given, respectively. Using the forgery attack, a dishonest original signer can forge a proxy signing key on behalf of the designated proxy signer by assigning some parameters and produce valid nominative proxy signatures, which does harm to the benefits of the proxy signers.

Key words: Digital signature; Proxy signature; Nominative signature

1　引言

一般地，普通的数字签名具有可公开验证性，即任何人都可以使用签名人的公钥验证签名的有效性，这使得数字签名适用于诸如信息公布、公钥证书颁发等场合。然而，当签名涉及到一些商业敏感信息或者对于签名接收人而言比较敏感的信息时，签名的可公开验证性就不适用了，签名的接收人希望签名仅能由自己验证。例如，签名人是一位医生，他为一个艾滋病患者签署体检报告，患者希望该签名只有自己能够验证，并且在必要的时候(如在艾滋病患者申请治疗时)，能向第三方证明自己是艾滋病患者。为此，Kim, Park和Won提出了提名签名[1,2]来解决这类问题。在提名签名方案中，只有签名接收人才能验证和向第三方证实签名的有效性，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。同时，Kim等提出了一个具体的方案。然而，在ACISP 2004会议上，Huang等[3]指出Kim等的方案并不具备提名的性质，签名人不仅能验证而且也能向第三方证明签名的有效性，并且，他们提出了一个新的提名签名方案。随后，在ACISP 2005会议上，Susilo等[4]指出Huang等的方案也不满足提名签名的要求，并讨论了构建安全的提名签名所需要的一些条件。最近，Wang和Bao[5]也指出Huang等的方案不满足证实/否认的不可传递性。2007年，Liu等[6]规范了提名签名的形式化定义和安全模型，开始研究提名签名的可证安全性。同年，他们又给出了一种利用环签名构造提名签名的方法[7]。

提名代理签名的概念[8]由Park和Lee于2001年提出，这种代理签名有如下性质：原始签名人可以把他的签名权利委托给代理签名人；只有指定的代理签名人可以提名验证人，并生成有效的提名代理签名，这个性质称为强不可伪造性；只有验证人即被提名人可以验证提名代理签名；必要的时候，只有被提名人可以向第三方证实签名的有效性。然而，Seo等[9]指出Park和Lee提出的方案达不到提名代理签名的安全要求，并且Park等的方案是代理不受保护的代理签名方案，

2008-02-01 收到，2008-06-25 改回
国家自然科学基金(60673075)，现代通信国家重点实验室基金(9140C1107010604)，西安电子科技大学计算机网络与信息安全教育部重点实验室开放基金(2008CNIS-02)，广东省/广州市信息安全技术(密码学)实验室开放基金和电子科技大学青年科技基金资助课题

无法提供不可否认性。同时，Seo等提出了一个代理受保护的提名代理签名方案[9]，并声称他们的方案克服了Park等方案的缺点，满足提名代理签名的所有安全要求。2004年，黄振杰等[10]学者也提出了一个新的提名代理签名方案，并给出了该方案的安全性分析。不幸的是，我们发现，Seo等和黄振杰等的提名代理签名方案并不具备强不可伪造性，一个不诚实的原始签名人可以伪造有效的代理签名密钥，从而可以冒充诚实的代理签名人生成有效的提名代理签名。

2　Seo 等的提名代理签名方案与分析

本节首先介绍 Seo 等的提名代理签名方案，然后给出原始签名人对该方案的一种伪造攻击，说明方案并不具备强不可伪造性。

2.1 Seo 等的方案

方案用到的参数如下：令 p 和 q 是两个大素数，其中 $q \mid p-1$，g 为 Z_p^* 的 q 阶乘法子群的生成元，$h:\{0,1\}^* \to Z_q^*$ 表示一个安全的 Hash 函数。$x_A \in Z_q$ 表示原始签名人的私钥，相应的公钥为 $y_A = g^{x_A} \bmod p$；$x_G \in Z_q$ 表示移动代理的私钥，相应的公钥为 $y_G = g^{x_G} \bmod p$；$x_B \in Z_q$ 表示验证人的私钥，相应的公钥为 $y_B = g^{x_B} \bmod p$。m 表示一个待签名消息，m_w 表示代理委托书，其中包括原始签名人和移动代理的身份、授权的有效期限等。Seo 等的方案包括以下算法：

代理密钥生成　原始签名人 A 随机选择 $k \in Z_q$，计算 $K = g^k \bmod p$，$e = H(m_w \,||\, K \,||\, T)$ 和 $\sigma = x_A \cdot e + k \cdot K \bmod q$，其中 T 表示时间戳。然后，A 发送 (σ, m_w, T, K) 给代理移动 G。G 通过下式来检验代理的有效性：$g^{\sigma} = y_A^{H(m_w||K||T)} \cdot K^K \bmod p$。如果验证通过，$G$ 计算代理签名密钥：$\sigma_p = \sigma + x_G \cdot K \bmod q$。

提名代理签名生成　移动代理 G 随机选择 $r, R \in Z_q$，计算 $\alpha = g^{R-r} \bmod p$，$D = y_B^R \bmod p$，$E = H(y_B \,||\, \alpha \,||\, D \,||\, m \,||\, m_w)$，$S_p = r - \sigma_p \cdot E \bmod q$，则消息 m 的提名代理签名为 $(y_B, D, \alpha, S_p, K, T, m_w)$。

提名代理签名验证　验证人计算 $E = H(y_B \,||\, \alpha \,||\, D \,||\, m \,||\, m_w)$ 和 $b = y_A^{H(m_w||K||T)} \cdot (y_G \cdot K)^K \bmod p$，然后检验 $(g^{S_p} \cdot b^E \cdot \alpha)^{x_B} = D \bmod p$ 是否成立。如果验证通过，签名有效；否则，拒绝签名。

2.2 Seo 等方案的分析

强不可伪造性是代理签名方案最重要的一条性质，要求只有合法的代理签名人才能生成有效的代理签名，包括原始签名人在内的其他人都不能生成有效的代理签名。遗憾的是，Seo 等的提名代理签名方案并不具备强不可伪造性。在原方案的设计中，代理签名密钥的生成为 $\sigma_p = \sigma + x_G \cdot K \bmod q$，由于其中含有移动代理的私钥 x_G，Seo 等认为除了移动代理之外，任何人都无法伪造这样一个代理签名密钥。这种说法是片面的，因为代理密钥中还有原始签名人选择的信息，某个不诚实的原始签名人可以通过设置一些特定的随机数，生成一个有效的代理签名密钥，从而可以伪造任意消息的提名代理签名。

伪造代理签名密钥　假设 A^* 是一个不诚实的原始签名人，他可以伪造一个有效的代理签名密钥 σ_p^*。A^* 随机选择 $t^* \in Z_q$，计算 $K^* = g^{t^*} \cdot y_G^{-1} \bmod p$，$e^* = H(m_w \,||\, K^* \,||\, T)$，则 $\sigma_p^* = x_A e^* + K^* t^* \bmod q$ 是一个有效的代理签名密钥，相应的验证公钥为 $y_p^* = g^{\sigma_p^*} \bmod p$，代理签名密钥正确性的推导如下：

$$y_p^* = g^{\sigma_p^*} = g^{x_A e^* + K^* t^*} = y_A^{e^*} \cdot g^{K^* t^*} = y_A^{e^*} \cdot (K^* \cdot Y_G)^{K^*}$$
$$= y_A^{e^*} \cdot K^{*K^*} \cdot y_G{}^{K^*} (\bmod p)$$

伪造提名代理签名　原始签名人 A^* 在成功伪造有效的代理签名密钥对 (σ_p^*, y_p^*) 后，在移动代理毫不知情的情况下，他可以伪造任意消息 m 的提名代理签名。A^* 随机选择 $r^*, R^* \in Z_q$，计算 $\alpha^* = g^{R^* - r^*} \bmod p$，$D^* = y_B^{R^*} \bmod p$，$E^* = H(y_B \,||\, \alpha^* \,||\, D^* \,||\, m \,||\, m_w)$，$S_p^* = r^* - \sigma_p^* \cdot E^* \bmod q$，则消息 m 的提名代理签名为 $(y_B, D^*, \alpha^*, S_p^*, K^*, T, m_w)$。伪造的签名可以通过签名验证：验证人计算 $E^* = H(y_B \,||\, \alpha^* \,||\, D^* \,||\, m \,||\, m_w)$ 和 $b^* = y_{A^*}^{H(m_w||K^*||T)} \cdot (y_G \cdot K^*)^{K^*} \bmod p$，此时

$$(g^{S_p^*} \cdot b^{*E^*} \cdot \alpha^*)^{x_B} = (g^{r^* - \sigma_p^* E^*} (y_{A^*}^{H(m_w||K^*||T)} (y_G K^*)^{K^*})^{E^*} g^{R^* - r^*})^{x_B}$$
$$= (g^{R^*} (g^{\sigma_p^*} y_{A^*}^{H(m_w||K^*||T)} (y_G K^*)^{K^*})^{E^*})^{x_B} = y_B^{R^*}$$

3　黄振杰等的提名代理签名方案与分析

本节介绍并分析黄等的提名代理签名方案[10]。

3.1 黄振杰等的方案

黄振杰等学者对 Kim 等的提名签名方案进行了分析，指出该方案并不具备提名的性质，然后给出了一个改进的方案，使之具备提名的性质，最后，基于改进的提名签名，他们提出了一个提名代理签名方案，并称该方案具有强不可伪造性。本节给出原始签名人对该方案的一种伪造攻击，说明方案并不具备强不可伪造性。

参数生成　参数 p, q, g, h 的选择如同 2.1 节 Seo 等的方案。原始签名人 S、代理签名人 A 和签名接收人 V 的私钥分别是 $x_s, x_a, x_v \in Z_q^*$，相应的公钥为 $y^* = g^{x^*} \bmod p$。

代理密钥生成　原始签名人 S 随机选择 $k_s \in Z_q^*$，计算 $r_s = g^{k_s} \bmod p$，$s_s = x_s \cdot h(w, r_s) + k_s \bmod q$，其中 w 为委托书，S 秘密发送授权证书 (w, r_s, s_s) 给代理人 A。A 检验 $g^{s_s} = y_s^{H(w,r_s)} \cdot r_s \bmod p$ 是否成立，如果验证式成立，代理签名人 A 计算其代理签名密钥 $x_p = s_s + x_a \bmod q$。

提名代理签名生成　以 x_p 为私钥，利用黄振杰等改进的提名签名方案对消息 m 签名，得到签名 (c, S)，这是一个交互式的签名生成协议，A 发送提名代理签名 (c, S, r_s, w) 给签名接收人 V。

提名代理签名验证　签名接收人 V 检查消息 m 是否满足委托书 w 的要求，然后计算 $y_p = y_s^{h(m,r_s)} \cdot r_s \cdot y_a \bmod p$，

$e=h(y_v,c,C,m)$，检验 $(g^S\cdot y_s^e\cdot c)^{x_v}=C$ 是否成立，其中 C 是在签名生成交互过程中，签名人和验证人都可以得到的信息。

3.2 黄振杰等方案的分析

同 Kim 等的方案一样，黄振杰等提出的提名代理签名方案也不具备强不可伪造性。代理签名人 A 用 $x_p=s_s+x_a \bmod q$ 生成他的代理签名密钥，相应的验证公钥为 $y_p=y_s^{h(m,r_s)}\cdot r_s\cdot y_a \bmod p$，虽然在 x_p 中包含代理人的私钥 x_a，但是其中还包含原始签名人选择的信息，某个不诚实的原始签名人可以通过设置一些特定的随机数，生成一个有效的代理签名密钥，从而可以伪造任意消息的提名代理签名。

伪造代理签名密钥 假设 S^* 是一个不诚实的原始签名人，他可以伪造一个有效的代理签名密钥 x_p^*。S^* 随机选择 $t^*\in Z_q^*$，计算 $r_s^*=g^{t^*}\cdot y_a^{-1} \bmod p$，则 $x_p^*=t^*+x_s h(w^*,r_s^*) \cdot \bmod q$ 是关于授权 w^* 的一个有效的代理签名密钥，相应的验证公钥为 $y_p^*=g^{x_p^*} \bmod p$，代理签名密钥正确性的推导如下：$y_p^*=g^{x_p^*}=g^{t^*+x_s h(w^*,r_s^*)}=g^{t^*}\cdot y_s^{h(w^*,r_s^*)}=y_s^{h(w^*,r_s^*)}\cdot r_s^*\cdot y_a (\bmod p)$。

伪造提名代理签名 原始签名人 S^* 在成功伪造有效的代理签名密钥对 (x_p^*,y_p^*) 后，在代理签名人毫不知情的情况下，他可以伪造任意消息 m 的提名代理签名，签名过程与黄振杰等的提名代理签名生成过程相同。

4 结束语

提名代理签名是一种适用于隐私消息保护的特殊的代理签名方案，目前关于这种签名的研究成果还不多。本文对 Seo 等和黄振杰等学者提出的两个提名代理签名方案进行了分析，指出这两个方案都不具备强不可伪造性，并给出了相应的攻击方法。提出可证安全的、计算高效的提名签名和提名代理签名是进一步的工作。

参 考 文 献

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

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

[3] Huang Z and Wang Y. Convertible nominative signatures. Proc. of Information Security and Privacy, ACISP 2004, Berlin: Springer-Verlag, 2004, LNCS 3108: 348–357.

[4] Susilo W and Mu Y. On the security of nominative signatures. Proc. of Information Security and Privacy, ACISP 2005, Berlin: Springer-Verlag, 2005, LNCS 3574: 329–335.

[5] Wang G and Bao F. Security remarks on a convertible nominative signature scheme. Proc. of IFIP International Federation for Information Processing, New Approaches for Security, Privacy and Trust in Complex Environments, Boston: Springer, 2007, Vol. 232: 265–275.

[6] Liu D Y, Wong D S, and Huang X, *et al.*. Formal definition and construction of nominative signature. Proc. of ICICS 2007, Berlin: Springer-Verlag, 2007, LNCS 4861: 57–68.

[7] Liu D Y, Chang S, and Wong D S, *et al.*. Nominative signature from ring signature. Proc. of IWSEC 2007, Berlin: Springer-Verlag, 2007, LNCS 4752: 396–411.

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

[9] Seo S H and Lee S H. New nominative proxy signature scheme for mobile communication. Proc. of SPI'2003, Security and Protection of Information, Brno, CZ, 2003: 149–154.

[10] 黄振杰, 郝艳华, 王育民. 指明签名与指明代理签名[J]. 电子与信息学报, 2004, 26(12): 1996–2001.
Huang Z, Hao Y, and Wang Y. Nominative signature and nominative proxy signature[J]. *Journal of Electronics & Information Technology*, 2004, 26(12): 1996–2001.

禹 勇： 男，1980 年生，博士，研究方向为信息安全.

许春香： 女，1965 年生，博士，教授，博士生导师，研究方向为信息安全.

周 敏： 女，1975 年生，博士生，讲师，研究方向为信息安全.

李发根： 男，1979 年生，博士，讲师，研究方向为密码学.