

## 对一种代理签名方案的密码学分析和改进

夏琦,许春香,高建彬

(电子科技大学 计算机科学与工程学院,成都 610054)

(xiaqi\_ueste@163.com)

**摘要:**对 Fu-Kou-Xiao 具有代理匿名性的代理签名方案<sup>[5]</sup>进行分析,指出该方案不具备强不可伪造性。给出了一种伪造攻击,利用这种攻击,一个恶意的原始签名人 can 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验证有效的代理签名。分析了方案不安全的原因,在此基础上提出了一个改进的代理密钥生成算法来修正 Fu-Kou-Xiao 的方案。

**关键词:**密码学分析;数字签名;代理签名

**中图分类号:** TP309.7 **文献标志码:** A

## Cryptanalysis and improvement of a proxy signature scheme

XIA Qi, XU Chun-xiang, GAO Jian-bin

(School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu Sichuan 610054, China)

**Abstract:** The security of the Fu-Kou-Xiao's proxy signature scheme with proxy signer's privacy anonymity was analyzed, and it was shown that the scheme did not possess the property of strong unforgeability. A forgery attack was given. Using this attack, a dishonest original signer can forge a proxy signing key and produce valid proxy signatures. The reason why the attack can work was analyzed and an improved scheme was proposed to remove the attack.

**Key words:** cryptanalysis; digital signature; proxy signature

### 0 引言

在代理签名<sup>[1]</sup>中,原始签名人 can 将其签名权利授权给代理签名人,代理签名人就可代表原始签名人签名。文献[2]引入了强代理签名的概念,强代理签名需要满足以下性质:可区分性、可验证性、强不可伪造性、强可识别性、强不可否认性和防止签名权利的滥用。在很多实际应用如电子投票或电子举报中,需要保护代理签名人的隐私,即代理签名人不想让其他人知道他是代理人这个事实。文献[3]提出了一个具有代理签名人保护功能的强代理签名方案,在该方案中,代理签名人可以代表原始签名人签名,但是除原始签名人之外的第三方无法追踪到代理签名人的身份。然而,文献[4]指出,该方案<sup>[3]</sup>不满足强不可伪造性。文献[5]提出一个新的具有代理匿名性的代理签名方案(后文简称 Fu 方案),并给出了安全性分析,声称所提方案满足代理签名的所有安全性。随后,文献[6]把代理签名和环签名相结合,提出了代理环签名的概念,用于解决代理签名中的代理隐私保护问题。最近,文献[7]规范了匿名代理签名的安全模型<sup>[7]</sup>,并提出了一个更加高效的匿名代理签名方案。本文对 Fu 方案提出的具有代理匿名性的代理签名方案进行分析,发现该方案不满足强不可伪造性,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 can 成功伪造代理签名密钥,从而可以冒充诚实的代理签名人生成有效的代理签名,威胁到代理签名人的权益。最后,分析了该方案不安全的原因并给出了一个改进的方案用于抵抗恶意原始签名人的伪造攻击。

### 1 Fu 方案介绍

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,  $h: \{0,1\}^* \rightarrow Z_q^*$  表示一个安全的 Hash 函数。原始签名人  $A$  的私钥为  $x_A \in Z_q^*$ , 相应的公钥为  $y_A = g^{x_A} \bmod p$ 。代理签名人  $B$  的私钥为  $x_B \in Z_q^*$ , 相应的公钥为  $y_B = g^{x_B} \bmod p$ , 方案包括以下算法。

**系统设置:**这个阶段的主要任务是原始签名人  $A$  对代理签名人  $B$  的身份进行盲化,令代理人的真实身份为  $ID_B$ ,  $A$  通过以下步骤将其盲化后得到一个代理身份  $ID_p$ 。随机选择  $k_B \in Z_q^*$ , 计算并秘密发送  $ID_p = h(k_B, ID_B)$  给  $B$ 。最后,为了方便以后的匿名撤销,  $A$  记录三元组  $(ID_B, ID_p, k_B)$  在自己的列表  $L$  中。

**授权生成:**原始签名人  $A$  用随机数  $k_B$  计算  $r = g^{k_B} \bmod p$ ,  $s_A = x_A h(w_B, r) + rk_B \bmod q$ , (原文中  $s_A = x_A h(w_B, r) + k_B \bmod q$  可能是作者笔误,从后文看,应该是  $s_A = x_A h(w_B, r) + rk_B \bmod q$ ),  $A$  发送  $(r, s_A, w_B)$  给  $B$ 。当收到  $(r, s_A, w_B)$  后,  $B$  通过检测  $g^{s_A} = y_A^{h(w_B, r)} r^r \bmod p$  是否成立来验证授权的有效性。

**代理签名生成:**  $B$  通过以下步骤生成一个有效的匿名代理签名。

- 1) 生成一对新的公钥、私钥对  $(x_{BP}, y_{BP})$ , 其中  $y_{BP} = g^{x_{BP}} \bmod p$ 。
- 2) 在代理身份  $ID_p$  下公布公钥  $y_{BP}$ 。
- 3) 计算  $x_p = (s_A + x_{BP}) \bmod q$  和  $T = ID_p ID_B y_A^{x_{BP}}$ 。
- 4) 用一个安全的离散对数类型的数字签名方案对消息  $m$  签名,得到签名  $s = \text{Sign}(m, x_p)$ 。

收稿日期:2008-08-18;修回日期:2008-09-28。

基金项目:国家自然科学基金资助项目(60573043);现代通信国家重点实验室基金资助项目(9140C1107010604)。

作者简介:夏琦(1979-),女,湖北武汉人,博士研究生,主要研究方向:密码学、信息安全;许春香(1965-),女,湖南长沙人,教授,博士生导师,主要研究方向:密码学与信息安全。高建彬(1976-),男,河北邢台人,博士研究生,主要研究方向:信息安全。

最终, 消息  $m$  的代理签名为  $(m, s, r, w_B, T, y_{BP})$ 。

代理签名验证: 验证人收到消息  $m$  的代理签名  $(m, s, r, w_B, T, y_{BP})$  后, 首先检验  $y_P = y_A^{h(w_B, r)} r^r y_{BP} \bmod p$  是否成立, 若检验通过, 按照离散对数类型的数字签名方案的签名验证算法 V 检验  $V(m, s, y_P) = \text{true}$  是否成立。如果验证式成立, 接受该代理签名; 否则, 拒绝。

匿名性打开: 当需要打开代理签名人的匿名性时, 原始签名人首先检验代理签名是否有效, 若有效, 计算  $a = \frac{T}{y_{BP}^{x_A}} \bmod p$ ,  $b = \frac{T}{ID_P y_{BP}^{x_A}} \bmod p$ , 然后在列表  $L$  中查找满足  $ID_B ID_P = a$ ,  $ID_B = b$  的三元组  $(ID_B, ID_P, k_B)$ , 此中的  $ID_B$  即为代理签名人的身份。

## 2 对 Fu 代理签名方案的分析和改进

### 2.1 对 Fu 方案的分析

强不可伪造性是代理签名最重要的一条性质, 为了防止原始签名人和代理签名人之间起争执, 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, Fu 方案并不具备强不可伪造性, 下面给出原始签名人的一种伪造攻击。

伪造攻击: 假设  $A^*$  是一个恶意的原始签名人, 他可以通过以下步骤伪造一个有效的代理签名密钥  $x_p^*$ 。

- 1) 为代理签名人  $B$  制作一个代理授权委托书  $w_B^*$ 。
- 2) 随机选择  $k_B^* \in \mathbf{Z}_q^*$ , 计算  $ID_P^* = h(k_B^*, ID_B)$ , 并添加三元组  $(ID_B, ID_P^*, k_B^*)$  到列表  $L$  中。
- 3) 随机选择  $r^*, t^* \in \mathbf{Z}_q$ , 计算  $y_{BP}^* = g^{t^*} (r^*)^{-r^*} \bmod p$ 。
- 4) 计算代理密钥  $x_p^* = t^* + x_A h(w_B^*, r^*) \bmod q$ 。
- 5) 计算  $T^* = ID_P^* ID_B (y_{BP}^*)^{x_A}$ 。

则  $x_p^*$  是一个有效的代理签名密钥, 此后, 原始签名人  $A^*$  可以使用私钥  $x_p^*$  和一个安全的离散对数类型的数字签名方案对任意消息  $m^*$  签名, 得到签名  $s^* = \text{Sign}(m^*, x_p^*)$ 。最终, 原始签名人  $A^*$  代表代理签名人  $B$  伪造的消息  $m^*$  的匿名代理签名为  $(m^*, s^*, r^*, w_B^*, T^*, y_{BP}^*)$ 。

伪造的有效性: 伪造的代理密钥和代理签名可以通过签名验证。根据原方案的验证步骤,

- 1) 计算  $y_P^* = y_A^{h(w_B^*, r^*)} (r^*)^{r^*} y_{BP}^* \bmod p$ 。下面我们说明  $y_P^* = g^{x_p^*} \bmod p$  成立:

$$\begin{aligned} y_P^* &= y_A^{h(w_B^*, r^*)} (r^*)^{r^*} y_{BP}^* = \\ &= y_A^{h(w_B^*, r^*)} (r^*)^{r^*} g^{t^*} (r^*)^{-r^*} = \\ &= g^{t^* + x_A h(w_B^*, r^*)} = g^{x_p^*} \bmod p \end{aligned}$$

因此, 原始签名人  $A^*$  伪造的代理签名密钥可以通过验证。

- 2) 由于  $x_p^*$  是一个有效的代理签名密钥, 因此,  $A^*$  使用  $x_p^*$  和一个安全的离散对数类型的签名方案对消息  $m^*$  签名后, 得到的签名一定可以通过相应的签名验证算法的检验, 即  $V(m^*, s^*, y_P^*) = \text{true}$  成立。

匿名性打开: 在匿名性打开过程中, 根据原方案的打开步骤, 原始签名人  $A^*$  计算  $a^* = \frac{T^*}{(y_{BP}^*)^{x_A}} \bmod p$  和  $b^* = \frac{T^*}{ID_P^* (y_{BP}^*)^{x_A}} \bmod p$ , 然后在列表  $L$  查找满足  $ID_B ID_P^* = a^*$ ,

$ID_B = b^*$  的三元组  $(ID_B, ID_P^*, k_B^*)$ , 其中的  $ID_B$  即为代理签名人的身份。下面说明  $A^*$  伪造的代理签名  $(m^*, s^*, r^*, w_B^*, T^*, y_{BP}^*)$  可以通过匿名性打开算法, 追踪到代理签名人  $B$  的身份  $ID_B$ , 因为:

$$\begin{aligned} a^* &= \frac{T^*}{(y_{BP}^*)^{x_A}} = \frac{ID_P^* ID_B (y_{BP}^*)^{x_A}}{(y_{BP}^*)^{x_A}} = ID_P^* ID_B \\ b^* &= \frac{T^*}{ID_P^* (y_{BP}^*)^{x_A}} = \frac{ID_P^* ID_B (y_{BP}^*)^{x_A}}{ID_P^* (y_{BP}^*)^{x_A}} = ID_B \end{aligned}$$

### 2.2 对 Fu 方案的改进

由上面的分析可以看出, Fu 代理签名方案<sup>[5]</sup>容易遭受原始签名人的伪造攻击, 主要原因在于原始签名人可以进行公钥冒充, 把代理签名人的公钥设置为  $y_{BP}^* = g^{t^*} (r^*)^{-r^*} \bmod p$ 。所以, 要想抵抗这种伪造攻击, 必须使得以上的公钥冒充不能奏效。我们提出一个改进方案用来消除 Fu 方案的伪造攻击。在此主要描述改进的部分, 其他部分与 Fu 方案相同。引入两个安全的密码学 Hash 函数  $h_1, h_2: \{0, 1\}^* \rightarrow \mathbf{Z}_q^*$ 。

系统设置:  $A$  将  $ID_B$  盲化后得到代理身份  $ID_P$ , 随机选择  $k_B \in \mathbf{Z}_q^*$ , 计算并秘密发送  $ID_P = h_1(k_B, ID_B)$  给  $B$ ;  $A$  记录三元组  $(ID_B, ID_P, k_B)$  在自己的列表  $L$  中;  $B$  生成一对新的公钥、私钥对  $(x_{BP}, y_{BP})$ , 其中  $y_{BP} = g^{x_{BP}} \bmod p$ , 并在代理身份  $ID_P$  下公布公钥  $y_{BP}$ 。

授权生成:  $A$  用随机数  $k_B$  计算  $r = g^{k_B} \bmod p$ ,  $s_A = x_A h_1(r, w_B) + k_B h_2(r, w_B, y_{BP}) \bmod q$ , 发送  $(r, s_A, w_B)$  给  $B$ 。收到  $(r, s_A, w_B)$  后,  $B$  通过检测  $g^{s_A} = y_A^{h_1(r, w_B)} r^{h_2(r, w_B, y_{BP})} \bmod p$  是否成立来验证授权的有效性。

代理签名生成:  $B$  通过以下步骤生成一个有效的匿名代理签名。

- 1) 计算  $x_p = (s_A + x_{BP}) \bmod q$  和  $T = ID_P ID_B y_{BP}^{x_p}$ 。
- 2) 用一个安全的离散对数类型的数字签名方案对消息  $m$  签名, 得到签名  $s = \text{Sign}(m, x_p)$ 。

最终, 消息  $m$  的代理签名为  $(m, s, r, w_B, T, y_{BP})$ 。

代理签名验证: 验证人收到消息  $m$  的代理签名  $(m, s, r, w_B, T, y_{BP})$  后, 首先检验  $y_P = y_A^{h_1(r, w_B)} r^{h_2(r, w_B, y_{BP})} y_{BP} \bmod p$  是否成立, 若检验通过, 按照离散对数类型的数字签名方案的签名验证算法 V 检验  $V(m, s, y_P) = \text{true}$  是否成立。如果验证式成立, 接受该代理签名; 否则, 拒绝。

匿名性打开: 与 FCX 方案相同。

改进的方案可以抵抗原始签名人的伪造攻击, 在改进的方案中, 代理签名密钥的生成方程为  $x_p = (x_A h_1(r, w_B) + k_B h_2(r, w_B, y_{BP}) + x_{BP}) \bmod q$ , 相应的代理验证公钥为  $y_P = y_A^{h_1(r, w_B)} r^{h_2(r, w_B, y_{BP})} y_{BP} \bmod p$ , 此时,  $r$  以  $r^{h_2(r, w_B, y_{BP})}$  的形式出现, 而不再以  $r^r$  的形式出现, 原始签名人若想通过设置特定的  $y_{BP}$  消除掉  $r$ , 或者通过设置特定的  $r$  消除掉  $y_{BP}$  都是困难的, 故这样的代理授权形式可以抵抗原始签名人的伪造攻击。

## 3 结语

分析了 Fu 等具有代理匿名性代理签名方案, 指出他们的方案不具备强不可伪造性, 一个不诚实的原始签名人可以成功伪造代理签名密钥, 从而可以冒充诚实的代理签名人生成验证有效的代理签名。分析了该方案不安全的原因, 并给出了一种改进的方案来抵抗原始签名人的这种伪造攻击。

(下转第 385 页)

单分类器所用特征向量或分类算法间均具有相关性。考虑到单分类器性能也对整个融合系统产生很大影响,为了使 D-S 证据理论融合系统达到优良的性能,就需要设计多个特征及分类算法均完全不相关且具有较高识别率的分类器,这在目前语音情感识别领域具有很大难度。多数投票法和专家系统融合对单分类器的相关性要求相对较低,因此其融合效果好于 D-S 证据理论。与之相比,改进的排序式选举法则具有明显的优势,它充分利用了情感的连续性和相似性特点,不要求单分类器间相互独立,只要分类器之间具有信息互补就可以得到较好的效果。

利用文献[7]方法对本文两种语音库进行实验,所得识别结果如表 8 所示。由于本文采用了更符合情感模型规律的融合算法,其融合效果明显优于一般的基于乘法或加法规则的融合算法。

表 8 文献[7]方法对本文语音库的识别率/%

识别系统	普通话语音库		德语语音库	
	说话人准相关	说话人无关	说话人准相关	说话人无关
HMM	67.38	44.83	79.20	53.42
PNN	79.17	43.92	81.03	47.64
乘法规则	74.73	39.45	81.57	49.66
加法规则	83.42	46.33	85.65	56.72

## 5 结语

多分类器融合是提高语音情感识别率的一条有效途径。相对于 D-S 证据理论等融合算法来说,本文提出的基于属性值加权的排序式选举法是一种更为有效的多情感分类器融合算法,可显著提高系统识别率;然而,尽管融合系统的使用降低了对单分类器性能的要求,但实验结果表明:当系统中单分类器性能很差时,融合系统将难以得到非常理想的效果,因此高效单分类器设计(尤其是说话人无关情况)依旧是语音情感识别领域的重要课题。

本文算法也可用于其他情感分类器的融合,如支持向量机(SVM)、K 最近邻法、模糊识别方法等。

### 参考文献:

- [1] KWON O W, CHAN K, HAO J, *et al.* Emotion recognition by speech signals[C]// 8th European Conference on Speech Communication and Technology. Geneva, Switzerland: [s. n.], 2003: 125 - 128.
- [2] ESAU N, KLEINJOHANN L, KLEINJOHANN B. Fuzzy emotion recognition in natural speech dialogue[C]// Proceedings of IEEE International Symposium on Robot and Human Interactive Communication. New York: IEEE, 2005: 317 - 322.
- [3] TAO JIANHUA, KANG YONGGUO. Features importance analysis for emotional speech classification[C]// Proceedings of lecture notes in computer science. Berlin: Springer, 2005: 449 - 457.
- [4] FU LIQIN, MAO XIA, CHEN LIJIANG. Speaker independent emotion recognition based SVM/HMMs fusion system[C]// IEEE Proceeding of ICALIP. New York: IEEE, 2008: 61 - 65.
- [5] MAO XIA, ZHANG BING, LUO YI. Speech emotion recognition based on a hybrid of HMM/ANN[C]// The 7th WSEAS International Conference. Stevens Point, Wisconsin: World Scientific and Engineering Academy and Society (WSEAS), 2007: 181 - 184.
- [6] LEE C M, SHRIKANTH N S. Toward detecting emotions in spoken dialogs[J]. IEEE Transactions on Speech and Audio, 2005, 13(2): 293 - 303.
- [7] 蒋丹宁, 蔡莲红. 基于语音声学特征的情感信息识别[J]. 清华大学学报: 自然科学版, 2006, 46(1): 86 - 69.
- [8] SCHULLER B, REITER S, MULLER R. Speaker independent speech emotion recognition by ensemble classification[C]// IEEE International Conference on Multimedia and Expo. New York: IEEE, 2005: 864 - 867.
- [9] RABINER L R. A tutorial on hidden Markov models and selected applications in speech recognition[EB/OL]. [2008 - 06 - 18]. <http://www.cs.ubc.ca/~murphyk/Bayes/rabiner.pdf>.
- [10] NICHOLSON J, TAKAHASHI K, NAKATSU R. Emotion recognition in speech using neural networks[J]. Neural Computing and Applications, 2000, 9(4): 290 - 296.
- [11] KIM K H, BANG S W, KIM S R. Emotion recognition system using short-term monitoring of physiological signals[J]. Medical & Biological Engineering & Computing, 2004, 42(9): 419 - 427.
- [12] COWIE R, COWIE E D, TSAPATSOU LIS N, *et al.* Emotion recognition in human-computer interaction[J]. IEEE Signal Processing Magazine, 2001, 18(1): 32 - 80.
- [13] 赵力, 蒋春晖, 邹采荣, 等. 语音信号中的情感特征分析和识别的研究[J]. 电子学报, 2004, 32(4): 606 - 609.
- [14] NEW T L, FOO S W, De SILVA L C. Speech emotion recognition using hidden Markov models[J]. Speech Communication, 2003, 41: 603 - 623.
- [15] MURRAY L R, ARNOTT J L. Towards the simulation of emotion in synthetic speech: a review of the literature on human vocal emotion[J]. Journal of the Acoustical Society of America, 1993, 93(2): 1097 - 1108.
- [16] COWIE R, COWIE E D, TSAPATSOU LIS N. Emotion recognition in human computer interaction[J]. IEE Signal Processing magazine, 2001, 18(1): 32 - 80.
- [17] 岳超源. 决策理论与方法[M]. 北京: 科学出版社, 2006.

(上接第 354 页)

### 参考文献:

- [1] MAMBO M, USUDA K, OKAMOTO E. Proxy signature: delegation of the power to sign messages[J]. IEICE Transactions on Fundamentals, 1996, E79-A(9): 1338 - 1353.
- [2] LEE B, KIM H, KIM K. Strong proxy signature and its applications[EB/OL]. [2008 - 06 - 10]. [http://caislab.icu.ac.kr/Paper/paper\\_files/2001/sultan/scis2001\\_sultan.ps](http://caislab.icu.ac.kr/Paper/paper_files/2001/sultan/scis2001_sultan.ps).
- [3] SHUM K, WEI V K. A strong proxy signature scheme with proxy signer privacy protection[C]// Proceedings of the 11th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise. Washington, DC: IEEE Computer Society, 2002: 55 - 56.
- [4] LEE N Y, LEE M F. The security of a strong proxy signature scheme with proxy signer privacy protection[J]. Applied Mathematics and Computation, 2005, 161(3): 807 - 812.
- [5] FU XIAOTONG, KOU WEIDONG, XIAO GUOZHEN. A proxy signature scheme with proxy signer's privacy anonymity[C]// Proceedings of the IEEE International Conference on E-Commerce Technology for Dynamic E-Business. Washington, DC: IEEE Computer Society, 2004: 257 - 260.
- [6] ZHANG FANGGUO, SAFAVI-NAINI R, LIN C. Some new proxy signature schemes from bilinear pairings[C]// Progress on Cryptography. Berlin: Springer Netherlands, 2004: 59 - 66.
- [7] YU YONG, XU CHUNXIANG, HUANG XINYI, *et al.* An efficient anonymous proxy signature scheme with provable security[J]. Computer Standards and Interfaces, 2008, 31(2): 348 - 353.