ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.19, No.7, July 2008, pp.1753−1757
DOI: 10.3724/SP.J.1001.2008.01753

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

两个指定验证人签名方案的安全性分析*

曹正军[1+], 刘丽华[2]

[1](上海大学 数学系,上海 200444)

[2](上海海事大学 信息与计算科学系,上海 200135)

Security Analysis of Two Designated-Verifier Signature Schemes

CAO Zheng-Jun[1+], LIU Li-Hua[2]

[1](Department of Mathematics, Shanghai University, Shanghai 200444, China)

[2](Department of Information and Computation Sciences, Shanghai Maritime University, Shanghai 200135, China)

+ Corresponding author: E-mail: caozhj@shu.edu.cn

Cao ZJ, Liu LH. Security analysis of two designated-verifier signature schemes. *Journal of Software*, 2008, 19(7):1753−1757. http://www.jos.org.cn/1000-9825/19/1753.htm

Abstract: In 2005, Wang, *et al*. proposed a threshold proxy multi designated-verifiers signature scheme (Wang-Fu) by combining the properties of the threshold proxy signature and the multi designated-verifiers signature. In the same year, Chen, *et al*. also proposed a designated-verifier signature scheme. It is shown that the manager of the set of all verifiers can directly forge signatures, so that, each verifier should give zero knowledge proof for the partial data generated in verifying phase by using his secret key, and that CFT (Chen-Feng-Tan) scheme does not satisfy the non-transferability, i.e., the designated-verifier can prove to a third party that the signature is generated by the signer. The reason is that the scheme directly follows from the technique in Schnorr signature. The designated-verifier can easily transform the signature into a common signature with respect to the signer's public parameters.

Key words: designated-verifier signature; threshold proxy signature; non-transferability; nominative signature; Schnorr signature

摘 要: 2005 年,王晓明等人把多重指定验证人签名与门限代理签名结合起来,提出了一个门限代理多重指定验证人签名(Wang-Fu).同年,陈伟东等人也提出了一个指定验证人的数字签名方案(Chen-Feng-Tan).证明 Wang-Fu 方案中指定验证人集合的管理者可以直接伪造签名.为此,每个验证人对在验证阶段使用私钥产生的部分数据必须进行零知识证明.CFT 方案不满足非传递性,即指定验证人可以向第三方证明其拥有的签名是由签名人签署的.其原因在于,该方案直接利用了 Schnorr 签名技巧,指定验证人很容易把拥有的签名转化为关于原始签名人公钥参数的一个普通签名.

关键词: 指定验证人签名;门限代理签名;非传递性;提名人签名;Schnorr 签名

中图法分类号: TP309 **文献标识码**: A

* Supported by the National Natural Science Foundation of China under Grant No.90304012 (国家自然科学基金)
Received 2007-01-28; Accepted 2007-04-26

普通签名的一个共同特点是,任何一方都可以验证签名的合法性.但是在某些特定情况下,要求只有预先指定的一个或一组验证方可以验证签名的合法性.指定验证人签名的公钥特征在于,验证人在验证签名时必须使用自己的私钥,而且不能把该签名转化为关于签名人公钥参数的一个普通签名.关于这一特点,Steinfeld等人[1]在2003年亚密会上强调:Given the designated-signature,the designated-verifier can verify that the message was signed by the signer,but is unable to convince anyone else of this fact.指定验证人签名在生活中有许多具体应用,例如电子投标、电子产品知识产权的保护等.关于指定验证人签名的若干设计问题可以参考文献[2−5].

在代理签名方案中引入秘密分存就形成了门限代理签名方案[6,7],门限代理签名的目的是当原始签名人因公务或身体健康等原因不能行使签名权利时,将签名权委托给其他人替自己行使签名权.门限代理签名在许多领域都有重要的应用,如电子商务中CA(certificate authority)证书的签发、电子支票的分发等.

2005年,王晓明等人把多重指定验证人签名与门限代理签名结合起来,提出了一个门限代理多重指定验证人签名方案(Wang-Fu)[8].同年,陈伟东等人采用了文献[9]的设计思想,提出了一种指定验证方的签名方案[10],为方便起见,称其为CFT(Chen-Feng-Tan)方案.本文将证明Wang-Fu方案中指定验证人集合的管理者可以直接伪造签名.为此,每个验证人对在验证阶段使用私钥产生的部分数据必须进行零知识证明.CFT方案不满足非传递性,即指定验证人可以向第三方证明其拥有的签名是由签名人签署的.其原因在于,该方案直接利用了Schnorr签名技巧,指定验证人很容易把拥有的签名转化为关于签名人公钥参数的一个普通签名,因此,该方案是不安全的.

1 Wang-Fu 方案及安全性分析

1.1 Wang-Fu方案的描述

设u_0是一个原始签名人,$G_p=\{u_{p1},u_{p2},\ldots,u_{pn}\}$是由$n$代理签名人的集合,$G_v=\{u_{v1},u_{v2},\ldots,u_{vm}\}$为指定验证人组成的集合.在每个集合里都有一个管理人,集合G_p的管理人为GP,主要负责系统的初始化,验证部分代理签名,结合部分代理签名产生代理签名.集合G_v的管理人为GV,主要帮助指定验证人验证代理签名.假定$P=\{u_{p1},u_{p2},\ldots,u_{pn}\}$($t\le n$)代表$G_s$对信息$M$进行签名.

[初始化] 需完成以下几个步骤:

(1) GP选择两个大素数p和q,且$q|p-1$,选择一个阶为q的元素g(即$g^q=1 \bmod p$),一个安全的单向Hash函数h,然后公布p,q,g,h.

(2) 原始签名人u_0,代理签名人u_{p_i}和指定验证人u_{v_j}的密钥分别是$\rho_0,k_i,v_j \in Z_q^*$($i=1,2,\ldots,n,j=1,2,\ldots,m$),公钥为$Y_0=g^{\rho_0} \bmod p$, $y_i=g^{k_i} \bmod p$,$i=1,2,\ldots,n$, $y_{v_j}=g^{v_j} \bmod p$($j=1,2,\ldots,m$),公钥都经过CA验证过.

(3) ID_i,$i=1,2,\ldots,n$为代理签名人u_{p_i}的身份标识.

(4) 代理集合G_p的密钥是$k_G \in Z_q^*$,公钥为$Y_G=g^{k_G} \bmod p$,指定验证人集合G_v的公钥为$Y_v=\prod_{j=1}^{m} y_{v_j} \bmod p$.

[分存秘密的生成] GP首先选择一个随机多项式$f(x)=k_G+a_1x+a_2x^2+\ldots+a_{t-1}x^{t-1} \bmod p$,其中,$a_i \in Z_q^*$($i=1,2,\ldots,t-1$)为随机整数,然后计算:

$$z_i=f(ID_i) \bmod q, u_i=g^{z_i}, w_i=z_i y_i^{k_G} \bmod p, i=1,2,\ldots,n.$$

最后送w_i给u_{p_i},并公布u_i($i=1,2,\ldots,n$).

[代理密钥的生成] 原始签名人u_0委托他的签名权给代理签名人u_{p_i}($i=1,2,\ldots,n$),u_0和每个u_{p_i}需要完成以下步骤:

(1) u_0首先选择一个随机整数$\alpha \in Z_q^*$,计算$A=g^{\alpha} \bmod p$,$c=\alpha+\rho_0 h(m_w \| A) \bmod p$,其中,$m_w$是一个含有门限值、委托签名的有效期、原始签名人和代理签名人身份标志的委托证书.然后,再选择一个随机多项式$f'(x)=c+c_1x+\ldots+c_{t-1}x^{t-1} \bmod q$,其中,$c_i \in Z_q^*$($i=1,2,\ldots,t-1$)为随机整数,计算$b_i=f'(ID_i) \bmod q$, $D_i=b_i y_i^{\rho_0} \bmod p$,$i=1,2,\ldots,n$.最后,送$D_i$给$u_{p_i}$,并公布$m_w,A,C_j=g^{c_j} \bmod p, j=1,\ldots,t-1$.

(2) 收到D_i后,u_{p_i} 首先计算 $z_i = w_i Y_G^{-k_i}$, $b_i = D_i Y_0^{-k_i} \pmod p$,然后验证

$$u_i = g^{z_i},\ g^{b_i} = AY_0^{h(m_w\|A)} \prod_{j=1}^{t-1} C_j^{ID_i^j} \pmod p.$$

如果成立,则 u_{p_i} 计算$\gamma_i=b_i+z_i h(m_w\|A) \bmod q$作为他的代理密钥.

[代理签名的生成] 若代理签名G_p中的任意t个代理签名人代表原始签名人对信息M进行签名,则每个代理签名人 $u_{p_i} \in P$需要完成以下步骤:

(1) 每个 $u_{p_i} \in P$选择随机数$\beta_i, \delta_i \in Z_q^*$,计算 $d_{i_1} = g^{\beta_i}$, $d_{i_2} = g^{\delta_i}$, $d_{i_3} = Y_v^{\beta_i d_{i_2} d_{i_1}^{-1} + \delta_i} \pmod p$,送$(ID_i, d_{i_1}, d_{i_2}, d_{i_3})$给GP.

(2) 收到$(ID_i, d_{i_1}, d_{i_2}, d_{i_3})$($i$=1,2,…,$t$)后,GP计算 $R = \prod_{i=1}^{t} d_{i_3}^{d_{i_1}}$, $\tilde{S} = \prod_{i=1}^{t} d_{i_2}^{d_{i_1}} \pmod p$,送 $(R, \tilde{S})$ 给P中的每个代理签名人.

(3) 收到 $(R, \tilde{S})$ 后,$u_{p_i} \in P$计算 $e = h(R \| \tilde{S} \| M \| PSID)$,$s_i=\beta_i d_{i_2} +(L_i\gamma_i+k_i)e \bmod p$,送给GP.其中,

$$L_i = \prod_{j=1, j\neq i}^{t} -ID_j (ID_i - ID_j)^{-1} \bmod q.$$

PSID 是所有代理签名人的身份标志的连接.

(4) GP 计算 $e = h(R \| \tilde{S} \| M \| PSID)$,验证

$$g^{s_i} = d_{i_1}^{d_{i_2}} \left\{ \left[A(Y_0 u_i)^{h(m_w\|A)} \prod_{j=1}^{t-1} C_j^{ID_i^j} \right]^{L_i} y_i \right\}^e \bmod p.$$

若成立,则$(s_i, d_{i_1}, d_{i_2}, d_{i_3})$是有效的部分代理签名,GP计算 $S = \sum_{i=1}^{t} s_i \bmod p$,则信息$M$的代理签名是

$$(S, \tilde{S}, e, A, m_w, PSID).$$

[代理签名的验证] 为了验证信息 M 的代理签名,验证集合中所有指定验证人一起完成以下步骤:

(1) 每个 $u_{v_j} \in G_v$,计算 $R_j = \{\tilde{S} g^S [A(Y_0 Y_G)^{h(m_w\|A)} \prod_{i=1}^{t} y_i]^{-e}\}^{v_j} \bmod p$,送$R_j$给GV.

(2) 收到R_j(j=1,2,…,m),GV计算 $R' = \prod_{j=1}^{m} R_j \bmod p$,送$R'$给$G_v$中的每个验证人.

(3) 每个 $u_{v_j} \in G_v$验证 $e = h(R' \| \tilde{S} \| M \| PSID)$,若成立,则信息$M$的代理签名是有效的.

1.2 Wang-Fu方案的安全性分析

原方案在安全性论述时没有对原始签名人、代理签名集合的管理者 GP 以及验证人集合的管理者 GV 的行为能力加以说明.如果这几个参与方在协议中是不诚实的,事实上,我们也不能假定他们是诚实的,那么该方案是不安全的.据此,我们将给出两种攻击方法.

(1) 不诚实的u_0与GP的合谋攻击方法.给定消息M以及公开参数m_w,$PSID$,y_i,i=1,…,n, y_{v_j},j=1,…,m,他们随机选取 $\alpha, \beta, \gamma \in Z_q^*$,计算

$$\tilde{S} = g^{\alpha},\ R = \prod_{j=1}^{m} y_{v_j}^{\alpha+\beta},\ A = (\prod_{i=1}^{t} y_i)^{-1} g^{\gamma} \pmod p,$$

$$e = h(R \| \tilde{S} \| M \| PSID),\ S = \beta + e[\gamma + (\rho_0 + k_G) h(m_w \| A)] \bmod q,$$

所得到的签名为 $(S, \tilde{S}, e, A, m_w, PSID)$.

正确性.

$$\begin{aligned} R_j &= \{\tilde{S} g^S [A(Y_0 Y_G)^{h(m_w\|A)} \prod_{i=1}^{t} y_i]^{-e}\}^{v_j} \\ &= \{g^{\alpha} g^S [(\prod_{i=1}^{t} y_i)^{-1} g^{\gamma} (Y_0 Y_G)^{h(m_w\|A)} \prod_{i=1}^{t} y_i]^{-e}\}^{v_j} \\ &= \{g^{\alpha} g^S g^{-e[\gamma + (\rho_0 + k_G) h(m_w\|A)]}\}^{v_j} \\ &= \{g^{\alpha} g^{S - e[\gamma + (\rho_0 + k_G) h(m_w\|A)]}\}^{v_j} = (g^{\alpha+\beta})^{v_j} = y_{v_j}^{\alpha+\beta} \pmod p. \end{aligned}$$

所以, $R'=\prod_{j=1}^{m}R_j=\prod_{j=1}^{m}y_{v_j}^{\alpha+\beta}=R \pmod p$,即伪造的签名能够通过指定验证人的验证.

注 1:该方案未能有效阻止u_0与GP合谋攻击的原因在于,验证表达式中的 $A(Y_0Y_G)^{h(m_w\|A)}\prod_{i=1}^{t}y_i$ 含有孤悬因子(见文献[9]中的定义),因此,它们能够成功地消除 $\prod_{i=1}^{t}y_i$,即无须使用代理签名人的私钥k_i,i=1,…,t.因原方案中$A=g^{\alpha} \bmod p$,指定验证人可以要求签名人提供离散对数知识证明,即Pr[log$_g A$],这样便能阻止上述合谋攻击.

(2) 不诚实的GV的攻击方法.由代理签名验证阶段的描述中可知,每个指定验证人 $u_{v_j}\in G_v$不能直接验证 $(S,\tilde{S},e,A,m_w,PSID)$ 的有效性,需要使用自己的私钥产生部分数据R_j,然后通过管理者GV提供的合成数据R',最后再借助等式 $e=h(R'\|\tilde{S}\|M\|PSID)$ 加以验证.如果GV是不诚实的,则他可以伪造签名.具体方法如下:

给定消息M以及公开参数A,m_w,$PSID$,GV随机选取α,β,γ,令 $S=\gamma,\tilde{S}=\beta$ 计算 $e=h(\alpha\|\tilde{S}\|M\|PSID)$,输出签名 $(S,\tilde{S},e,A,m_w,PSID)$.

在验证阶段,等每个指定验证人提交部分数据R_j,j=1,…,m后,GV可以直接返回$R'=\alpha$.

注 2:去掉 GV 这一角色可以阻止上述攻击.此时,每个指定验证人在验证阶段计算:

$$R_j=\{\tilde{S}g^{S}[A(Y_0Y_G)^{h(m_w\|A)}\prod_{i=1}^{t}y_i]^{-e}\}^{v_j} \bmod p,$$

并广播 $\left\{R_j,\Pr\left[\log_g y_{v_j}=\log_{(\tilde{S}g^{S}[A(Y_0Y_G)^{h(m_w\|A)}\prod_{i=1}^{t}y_i]^{-e})}R_j\right]\right\}$,即需要利用零知识证明确保$R_j$具有上述结构.这样,每个验证人就可以合成$R'$,验证签名的有效性.

2 CFT 方案及安全性分析

2005 年,陈伟东等人提出了一个指定验证方的数字签名方案[10].该方案利用了Eu-Jin Goh等人签名方案[11]的基本设计思想.

2.1 CFT方案的描述

[**系统参数**] 设H:$\{0,1\}^*\to G_{p,g}=\{g^0,g,\ldots,g^{p-1}\}$, $H':G_{p,g}^8\to Z_q$ 为两个独立的安全Hash函数.验证方的公钥为 $y_v=g^{x_v} \bmod p$,私钥为$x_v\in_R Z_q$,g的阶为q,$q|p-1$.签名方私钥$x_v\in_R Z_q$,公钥$y=g^x \bmod p$.设待签名的消息为m.

[**签名**] 选取随机数 r,k,l,利用 Hash 函数 H 计算:

$$h=H(m,r),\ z=h^x,\ u=g^k,\ v=h^k,\ w=g^l,\ w'=g^{lx_v} \pmod p,$$

$$c=H'(g,h,y,z,u,v,w,w'),\ s=k+cx \bmod q.$$

输出签名$\sigma=(z,r,s,w,c)$.

[**验证**] 计算 $h=H(m,r)$,验证等式 $c=H'(g,h,y,z,g^sy^{-c},h^sz^{-c},w,w^{x_v})$.

2.2 CFT方案的安全性分析

在前面引言中我们已经指出,指定验证人签名的公钥特征在于:(1) 指定验证人在验证签名时必须使用自己的私钥;(2) 指定验证人不能把签名转化为关于签名人公钥参数的一个普通签名.

CFT 方案验证等式

$$c=H'(g,h,y,z,g^sy^{-c},h^sz^{-c},w,w^{x_v})$$

中确实使用了验证人的私钥x_v,这一点是符合要求(1)的.关于第 2 点,CFT方案是不满足的.CFT方案利用Schnorr签名的设计技巧,即把Hash值c反馈到输入项g^sy^{-c}中.由于g,y是签名人的公钥参数,如果攻击者不知道y关于g的离散对数,则攻击者便无法伪造签名.关于这一结论可以参看Pointcheval和Stern的论文[12].因此,

指定验证人只需计算 $w'=w^{x_v} \bmod p$,把(z,r,s,w,c,w')提交给第三方,通过等式$c=H'(g,h,y,z,g^sy^{-c},h^sz^{-c},w,w')$直接向第三方证明这是签名人产生的签名.

注 3:指定验证方是否有能力向第三方证明某个签名是由签名人签署的,这关系到两个不同的数字签名模型.如果指定验证方有能力向第三方证明某个签名是由签名人签署的,则这种数字签名模型称为nominative

signature[13](中文可译成提名人签名).根据上面的分析,我们认为CFT方案可以看作是一个提名人签名协议.

3 结束语

本文分析了两个指定验证人签名方案,即 Wang-Fu 方案与 CFT 方案.Wang-Fu 方案中原始签名人与管理者 GP 可以合谋伪造签名,验证方的管理者 GV 也可以直接伪造签名.CFT 方案则不满足非传递性要求.实质上,CFT 方案可以看成是一个提名人签名.

致谢 对审稿人提出的有益的修改建议,我们在此表示衷心的感谢.

References:

[1] Steinfeld R, Bull L, Wang HX, Pieprzyk J. Universal designated-verifier signatures. In: Sung C, ed. Proc. of the ASIACRYPT 2003. LNCS 2894, Berlin: Springer-Verlag, 2003. 523−542.

[2] Jakobsson M, Sako K, Impagliazzo R. Designated verifier proofs and their applications. In: Ueli M, ed. Proc. of the Eurocrypt'96. LNCS 1070, Berlin: Springer-Verlag, 1996. 143−154.

[3] Saeednia S, Kremer S, Markowitch O. An efficient strong designated verifier signature scheme. In: Jong L, Hoon D, eds. Proc. of the ICISC 2003. LNCS 2836, Berlin: Springer-Verlag, 2003. 40−54.

[4] Steinfeld R, Wang HX, Pieprzyk J. Efficient extension of standard Schnorr/RSA signatures into universal designated-verifier signatures. In: Bao F, Deng R, Zhou J, eds. Proc. of the PKC 2004. LNCS 2947, Berlin: Springer-Verlag, 2004. 86−100.

[5] Susilo W, Zhang F, Mu Y. Identity-Based strong designated verifier signatures schemes. In: Wang H, Pieprzyk J, Varadharajan V, eds. Proc. of the ACISP 2004. LNCS 3108, Berlin: Springer-Verlag, 2004. 313−324.

[6] Hsu CL, Wu TS, Wu TC. New nonrepudiable threshold proxy signature scheme with known signers. The Journal of Systems and Software, 2001,58(2):119−124.

[7] Hwang MS, Lu JL, Lin IC. A practical (*t*,*n*) threshold proxy signature scheme based on the RSA cryptosystem. IEEE Trans. on Knowledge and Data Engineering, 2003,15(6):1552−1560.

[8] Wang XM, Fu FW. A (*t*,*n*) threshold proxy signature scheme with specified verifiers, Journal of Software, 2005,16(11):1967−1974 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/16/1967.htm

[9] Cao ZJ, Liu ML. Suspending factor and redundant data in signature schemes. Chinese Journal of Computers, 2006,29(2):249−255 (in Chinese with English abstract).

[10] Chen WD, Feng DG, Tan ZW. Signature scheme for specified threshold verifiers and security proofs. Journal of Software, 2005,16(6):1190−1196 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/16/1190.htm

[11] Goh EJ, Jarecki S. A signature scheme as secure as the Diffie-Hellman problem. In: Eli B, ed. Proc. of the EUROCRYPT 2003. LNCS 2656, Berlin: Springer-Verlag, 2003. 401−415.

[12] Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures. Journal of Cryptology, 2000,13(3):361−396.

[13] Kim SJ, Park SJ, Won DH. Zero-Knowledge nominative signatures. In: Proc. of the PragoCrypt'96, Int'l Conf. on the Theory and Applications of Cryptology. Czech Technical University Publishing House, 1996. 380−392.

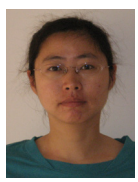
附中文参考文献:

[8] 王晓明,符方伟.指定验证人的(*t*,*n*)门限代理签名方案.软件学报,2005,16(11):1967−1974. http://www.jos.org.cn/1000-9825/16/1967.htm

[9] 曹正军,刘木兰.数字签名方案中的孤悬因子和冗余数据.计算机学报,2006,29(2):249−255.

[10] 陈伟东,冯登国,谭作文.指定验证方的门限验证签名方案及安全性证明.软件学报,2005,16(6):1190−1196. http://www.jos.org.cn/1000-9825/16/1190.htm

曹正军(1970－),男,江苏响水人,博士,讲师,主要研究领域为密码学,信息安全.



刘丽华(1978－),女,博士,讲师,主要研究领域为组合设计,编码,密码学.