群签名中成员删除问题的更新算子解决方案*

王尚平[1,2+], 王育民[2], 王晓峰[1], 秦 波[1], 何 成[1], 邹又姣[1]

[1](西安理工大学 理学院,陕西 西安 710048)

[2](西安电子科技大学 ISN 国家重点实验室,陕西 西安 710071)

A New Solution Scheme for the Member Deletion Problem in Group Signature by Use of Renew Operator

WANG Shang-Ping[1,2+], WANG Yu-Min[2], WANG Xiao-Feng[1], QIN Bo[1], HE Cheng[1], ZOU You-Jiao[1]

[1](Institute of Natural Science, Xi'an University of Technology, Xi'an 710048, China)

[2](National Key Laboratory on ISN, Xidian University, Xi'an 710071, China)

+ Corresponding author: Phn: 86-29-2312848, E-mail: spwang@mail.axut.edu.cn

http://www.xaut.edu.cn

Received 2002-10-09; Accepted 2003-04-30

Wang SP, Wang YM, Wang XF, Qin B, He C, Zou YJ. A new solution scheme for the member deletion problem in group signature by use of renew operator. *Journal of Software*, 2003,14(11):1911~1917.
http://www.jos.org.cn/1000-9825/14/1911.htm

Abstract: A new solution scheme for the member deletion problem in Camenisch-Stadler's group signature schemes is proposed by use of the group member's secret property key renew operator. In the new scheme whenever a member joins or leaves the group, its manager computes a new group public property key and a group member's secret property key renew operator and then publishes them. Each group member modifies the secret property key by using the renew operator without the need to re-issue membership certificates. Hence the new scheme is an acceptable solution for a large group where its membership changes frequently. The group public key, member's secret key, and signature are all of constant size. The new scheme is better than Bresson-Stern's member deletion scheme because in Bresson-Stern's scheme the signature is dependent on the witness and the number of the witness is linear with respect to the number of the deletion members. The idea of the key renew operator is first used in the member deletion problem in Camenisch-Stadler's group signature schemes by Kim-Lim-Lee, but the scheme in this paper is more concise. The security of the scheme relies on the RSA assumption. The scheme is resistant to forging attack and forging a valid signature is equivalent to solving the RSA problem.

Key words: group signature; signature of knowledge; renew operator; member deletion problem

摘 要: 提出了 Camenisch-Stadler 群数字签名方案中成员删除问题的一个新的解决方案.新方案使用了群组成员秘密特性钥更新算子方法.新方案中当一个成员加入或被群组删除后,群主管计算并公布群组新的特性公钥及群组成员秘密特性钥更新算子,群中的每个成员只需要利用公开的更新算子重新计算各自的秘密特性钥,系统不需要对

* Supported by the National Natural Science Foundation of China under Grant No.60273089 (国家自然科学基金)

第一作者简介: 王尚平(1963－),男,陕西扶风人,博士,教授,主要研究领域为密码理论,网络安全.

每个成员更新颁发成员证书.因此,新方案对大的群组是一个可接受的方案.群组的公开钥、成员的秘密钥及签名的长度都是固定不变的.新方案比 Bresson-Stern 的群组成员删除方案要好,因为 Bresson-Stern 的群组成员删除方案中对信息的签名含有证据,这些证据的个数随着被删除对象的个数呈线性增长.更新算子的思想受到了 Kim-Lim-Lee 的启发,但是该签名算法更为简明.所提出的方案的安全性是基于 RSA 问题的困难性假设,新方案是抗伪造攻击的,伪造成功等同于求解 RSA 问题.

关键词: 群数字签名;知识签名;更新算子;成员删除问题

中图法分类号: TP309 **文献标识码**: A

群签名的概念是由 D.Chaum 和 Van Heyst 首先提出的[1].群签名允许群中合法成员代表群组对信息匿名签名,该签名可以利用群组公开钥验证.在发生纠纷时,只有指定的群主管可以打开签名,确定签名成员的身份.最初提出的群签名方案[1~4]其签名长度或群组公钥长度与群组成员个数呈线性关系.群签名的一个重要进展是 Camenisch-Stadler 于 1997 年提出的群签名方案[5],该方案中群签名的长度及群组公钥的长度是固定的,与群组成员的个数无关,群组建立后,可以加入新成员,且新成员的加入不改变群组的公开钥.

但是在实际中,群组的成员是动态的.群组中不仅有新成员的加入,同时还有群组成员的删除问题.群组中成员可能因人事变动或工作岗位的调整而退出群组.或者因某个成员做了不体面的事,群主管必须将该成员驱逐出群组.这时,需要追踪该成员所签署的所有签名,同时保证其他成员签名的匿名性.群成员的删除问题及抗伪造攻击问题是影响群签名应用的主要障碍.

E.Bresson 和 J.Stern 于 2001 年首次提出了针对 Camenisch-Stadler 群签名方案中的群成员删除解决方案[8].该删除方案使用的思想为使用“证据”(witness)的技巧.合法成员在签名时,必须提供证据,证明签名者的身份不是所公布的被删除成员列表 L 中的成员.假如被删除的成员有 k 个,则必须提供 k 个证据.这样,该方案的效率较低,特别是当群组较大,被删除成员个数 k 较大时,实际上是不可行的.

本文提出了对 Camenisch-Stadler 群签名方案中成员删除问题的一个新的解决方案.我们的方案在 Camenisch-Stadler 中使用更新算子算法,当一个成员加入或被群组删除后,群组的特性公钥及每个成员的秘密钥通过一个公开的更新算子被重新计算而不需要对每个成员更新颁发身份证书.每个更新计算仅需一次乘法.因此,我们的方案对大的群组是一个可接受的方案.群组的公开钥、成员的秘密钥及签名的长度都是固定不变的.本文中更新算子的思想受到了文献[10]的启发,但与之不同的是,我们的签名算法更简明.本文所提出的方案是抗伪造攻击的,伪造成功等同于求解 RSA 问题.因此在 RSA 困难的假设下,所提出的方案是安全的.

1 Camenisch-Stadler 群签名方案

Camenisch-Stadler[5]群签名方案使用了知识签名(特别是 SKROOTLOG 签名及 SKLOGLOG 签名)的概念.知识签名可使证明方对验证方证明其拥有某些秘密值的知识,而不泄露有关秘密值的任何信息.关于群签名及知识签名的有关知识请参考文献[4,5],下面我们使用 Camenisch-Stadler 群签名方案中的记号.

1.1 系统建立

群主管(group manager)计算下列值:

- 一个 RSA 模 n 及两个公开的指数 $e_1,e_2>1$,且 e_2 与 $\varphi(n)$ 互素;
- 两个整数 $f_1,f_2>1$,使得其 e_1 次根及 e_2 次根在不知 n 的因式分解的情况下计算是困难的;
- 一个阶为 n 的循环群 $G=\langle g\rangle$,使 G 中计算离散对数问题是困难的;
- 一个元素 $h\in G$,使得 h 关于以 g 为基的离散对数计算困难;
- 任选一个整数 $w\in Z_n^*$,令 $y_R:=h^w$ 为群主管的公开钥.

群组的公开钥 $Y=(n,e_1,e_2,f_1,f_2,G,g,h,y_R)$,而 $\frac{1}{w}$ 及 n 的素因子为群主管的秘密钥.

1.2 成员注册

假设用户 Alice 欲成为群组中的成员.Alice 首先计算她的成员私钥,任选一个 $x\in Z_n^*$,令 $y:=x^{e_1} \bmod n$.Alice 保密 y 及 x 作为她的成员身份秘钥,然后,Alice 计算 $z:=g^y$,公开 z 并以 z 代表 Alice 的身份,z 是 Alice 成员身份的公开钥.

为了成为群组成员,Alice 必须向群主管注册这些值,并获得成员证书.Alice 不能将 y 直接送给群主管,否则群主管可能冒充 Alice,因此 Alice 传送 z, y 的盲化值 $\tilde{y}$ 以及 z 和 $\tilde{y}$ 按规定格式的知识证明.Alice 计算:

$\tilde{y}:=r^{e_2}(f_1y+f_2) \bmod n$,其中 $r\in_R Z_n^*$;

$U:=SKROOTLOG[\alpha:z=g^{\alpha^{e_1}}]('')$;

$V:=SKROOTLOG[\beta:g^{\tilde{y}}=(z^{f_1}g^{f_2})^{\beta^{e_2}}]('')$.

Alice 发送 $z,\tilde{y},U,V$ 给群主管,若群主管验证 U,V 都正确,群主管确信 $\tilde{y}$ 是 z 所含的成员密钥的正确盲化值,群主管计算

$$\tilde{v}:=\tilde{y}^{\frac{1}{e_2}} \bmod n,$$

并发送 $\tilde{v}$ 给 Alice,Alice 去掉盲化因子 r 得到成员证书

$$v:=\frac{\tilde{v}}{r}=(f_1y+f_2)^{\frac{1}{e_2}} \bmod n.$$

1.3 信息签名

为了代表群组对信息 M 签名,Alice 计算对信息的知识签名,证明她是群组的注册成员.同时,利用群主管的公开钥对其成员公钥进行加密,这样可以使群主管在必要的时候打开签名.具体的实现为:Alice 任选一个随机数 $r\in Z_n^*$,计算

$\tilde{z}:=h^r g^y$;

$d:=y_R{}^r$;

$V_1:=SKROOTREP[\alpha,\beta:\tilde{z}=h^{\alpha}g^{\beta^{e_1}}]\ (M)$;

$V_2:=SKROOTREP[\gamma,\delta:\tilde{z}^{f_1}g^{f_2}=h^{\gamma}g^{\delta^{e_2}}(M)$;

$V_3:=SKREP[\varepsilon,\varsigma:d=y_R{}^{\varepsilon}\wedge\tilde{z}=h^{\varepsilon}g^{\varsigma}](M)$,

则 Alice 对 M 的签名为 $(\tilde{z},d,V_1,V_2,V_3)$.

1.4 签名验证

Alice 对 m 签名 $(\tilde{z},d,V_1,V_2,V_3)$ 的正确性是通过对 (V_1,V_2,V_3) 同时成立的验证.事实上,通过对 (V_1,V_2,V_3) 的正确性验证可使验证者确信

$$\gamma=\alpha f_1 \bmod n,\ \delta^{e_2}=f_1\beta^{e_1}+f_2 \bmod n.$$

上述第 2 个等式表示 Alice 拥有成员证书 $v=\delta$ 且其成员秘密钥为 $x=\beta$,通过对 V_3 的验证,验证者确信 $\tilde{z}$ 与 d 的计算使用了同一个随机数 $r=\varepsilon$,即 $(d,\tilde{z})$ 是 Alice 利用群主管公开钥 (h,y_R) 对成员公开钥 z 的一个 ElGamal 加密.V_3 的正确性确保了当需要时,签名可被群主管打开.

1.5 打开签名

事实上,打开签名就是对签名中作为密文的解密.群主管计算

$$z:=\frac{\tilde{z}}{d^{\frac{1}{w}}}.$$

群主管得到签名者的公开钥 z.为了证明这一事实,群主管生成 $\tilde{z}$ 及 h 关于基 $\{z,d,y_R\}$ 表示的知识签名,即

$$SKREP[\rho:\tilde{z}=zd^{\rho}\wedge h=y_R{}^{\rho}]('')\ ,$$

其中 ρ 表示 $\frac{1}{w}$,即群主管的秘密钥.

2 一种新 Camenish-Stadler 的群签名方案中成员删除问题的解决方案

Bresson-Stern[8]使用'证据'技巧给出了 Camenisch-Stadler 签名方案中 $(d,\tilde{z})=(y_R^r, zh^r)$ 身份公钥 z 不同于一个公开的被删除的公开钥 z_1 的方案.此时,在签名中增加的证据,通过知识签名证明签名者的公钥不同于 z.

设 Γ 是 l 个被删除成员的列表,记其成员公开钥分别为 $z_1,z_2,...,z_l$.在签名者 Alice 对信息 m 的签名中,通过零知识证明她自己的公开钥 z 不在删除公开钥列表 Γ 中,这使得签名中证据的个数随被删除对象个数呈线性增长,这对较大的群组显然不合适,尽管 V_3 的长度并未增加.这一性质决定了 Bresson-Stern 方案在实际中不可行.

本节提出一个关于 Camenish-Stadler 群签名方案中成员删除问题的一个新的解决方案.文中更新算子的思想受到了文献[10]的启发,但是我们的签名算法与之不同,更简明.本节完全采用第 1 节的记号.

2.1 系统建立

群主管在系统建立阶段与 Camensch-Stadler 方案中基本保持一致(第 1.1 节).所不同的是增加了一个 RSA 模 n 的公开指数 e,且 e 与 $\varphi(n)$ 互素.这样,群组的公开钥 $Y=(n,e,e_1,e_2,f_1,f_2,G,g,h,y_R)$, $y_R:=h^w$ 为群主管公开钥,$\frac{1}{w}$ 及 n 的素因子为群主管的秘密钥.

2.2 成员注册及更新算子

设用户 Alice 欲成为群组成员,获得成员证书的过程与 Camenisch-stadler 方案中成员注册(第 1.2 节)完全一致.设 Alice 加入群组时,群组的合法成员列表 $C:=\{G_1,G_2,...,G_{m-1}\}$,即群组已有 $m-1$ 个成员.设 Alice 是群组的第 m 个成员 G_m.记成员 G_m(Alice)的成员秘钥为 (x_{G_m},y_{G_m}),其中 $y_{G_m}=x_{G_m}^{e_1} \bmod n$,成员 G_m(Alice)的成员公开钥为 $z_{G_m}:=g^{y_{G_m}}$,Alice 的成员证书为 $V_{G_m}:=(f_1y_{G_m}+f_2)^{\frac{1}{e_2}}$.

设 Alice 加入群组时,群组的公开特性秘钥: $U_G:=z_{G_1}z_{G_2}....z_{G_{m-1}}z'$,其中 z_{G_i} 是群组成员 G_i 的公开钥 $(1\le i\le m-1)$,且 $z'\in_R G$ 群主管计算下列值:

① 群组新的公开特性钥 $U_G:=z_{G_1}z_{G_2}....z_{G_{m-1}}z_{G_m}z''$,其中 $z''\in_R G$;

② 群组成员的秘密特性钥公开更新算子 $U:=\left(\frac{z_{G_m}z''}{z'}\right)^{\frac{1}{e}}$;

③ 新成员 G_m(Alice)的秘密特性钥 $U_{G_m}:=(z_{G_1}z_{G_2}...z_{G_{m-1}}z'')^{\frac{1}{e}}$.

群主管公开群组新的公开特性钥 U_G 及群组成员的秘密特性钥公开更新算子 U,秘密发送秘密特性钥 U_{G_m} 给 G_m(Alice).新成员 G_m(Alice)通过验证 $(U_{G_m})^e z_{G_m}=U_G$ 成立,确定群主管传送的秘密特性钥 U_{G_m} 正确.

接下来,群组中各个合法成员 G_i $(1\le i\le m-1)$ 除 G_m 外利用群组成员的秘密特性钥公开更新算子 U 及其秘密特性钥 $U_{G_i}:=(z_{G_1}...z_{G_{i-1}}z_{G_{i+1}}...z_{G_{m-1}}z')^{\frac{1}{e}}$ 计算其新的秘密特性钥 $U_{G_i}:=U_{G_i}U$,即

$$U_{G_i}:=(z_{G_1}...z_{G_{i-1}}z_{G_{i+1}}...z_{G_{m-1}}z')^{\frac{1}{e}}\left(\frac{z_{G_m}z''}{z'}\right)^{\frac{1}{e}}$$

$$=(z_{G_1}...z_{G_{i-1}}z_{G_{i+1}}...z_{G_{m-1}}z_{G_m}z'')^{\frac{1}{e}},$$

并通过验证式子 $(U_{G_i})^e y_{G_i}=U_G$ 成立来确定 U_{G_i} 的正确性.

至此,当群组中有一个新成员加入时,通过群主管计算一个新的群组公开特性钥 U_G 及更新算子 U,使每个成员的秘密特性钥得到更新.而群组的公开钥则保持不变,即群组的公开钥与群组的成员个数是无关的.

2.3 成员删除及更新算子

成员删除是成员加入的逆过程,下面假设群主管欲从群组中删除成员 G_j.利用更新算子,群主管要在群组中的公开特性钥 U_G 中删除其公开钥 z_{G_j},并改变随机数,发布新的群组公开特性钥 U_G 及群组成员的秘密特性钥更新算子 U,使群中其余成员利用更新算子更新其各自的成员秘密特性钥,使其在 G_j 删除后可继续生成有效的群签名.

设当前群组的特性公开钥为 $U_G := z_{G_1}...z_{G_m}z'$,其中 $z' \in_R G$,为了删除群组成员 G_j,群主管计算下列值:

① 群组新的公开特性钥 $U_G := U_G \dfrac{z''}{z_{G_j}z'}$,即 $U_G := z_{G_1}...z_{G_{j-1}}z_{G_j}...z_{G_m}z''$,其中 $z'' \in_R G$.

② 群组成员的秘密特性钥更新算子 $U := \left(\dfrac{z''}{z_{G_j}z'}\right)^{\frac{1}{e}}$.

③ 公开群组新的特性公钥及更新算子(U_G,U).

群组中每个合法成员 G_i 通过更新算子 U 更新其秘密特性秘钥 U_{G_i} 为 $U_{G_i} := U_{G_i}U$.

$$U_{G_i} := (z_{G_1}...z_{G_{i-1}}z_{G_{i+1}}...z_{G_m}z')^{\frac{1}{e}}\left(\frac{z''}{z_{G_j}z'}\right)^{\frac{1}{e}} = (z_{G_1}...z_{G_{i-1}}z_{G_{i+1}}...z_{G_{j-1}}z_{G_{j+1}}...z_{G_m}z'')^{\frac{1}{e}},\ i<j.$$

每个合法的成员 G_i 通过验证 $(U_{G_i})^e y_{G_i} = U_G$ 是否成立来判断更新后 U_{G_i} 的正确性.

2.4 签名过程

设群组合法成员有 $G_1,...,G_m$, 群组的特性公开钥 $U_G = z_{G_1}...z_{G_m}z''$, $(z'' \in G)$,群组成员 G_i $(1 \le i \le m)$ 代表群组对信息 M 签名. G_i 计算:

① $\tilde{z} := h^r z_{G_i}$,其中 $r \in_R Z_n^*$;

② $d := y_R{}^r$;

③ $A = U_{G_i}g^r$;

④ $B = h^r g^{re}$;

⑤ $V_1 := SKROOTREP[\alpha,\beta : \tilde{z} = h^\alpha g^{\beta^{e_1}}](M)$;

⑥ $V_2 := SKROOTREP[\gamma,\delta : \tilde{z} = h^\gamma g^{\delta^{e_2}}](M)$;

⑦ $V_3 := SKREP[\varepsilon,\varsigma : d = y_R{}^\varepsilon \wedge \tilde{z} = h^\varepsilon g^\varsigma \wedge B = h^\varepsilon g^{\varepsilon e}](M)$,

则成员 G_i 对信息 M 的签名为 $(\tilde{z},d,A,B,V_1,V_2,V_3)$.

注意到,上述 $\tilde{z},d,V_1,V_2$ 的计算过程与 Camenisch-Stadler 方案中的完全一致,这里增加了 A,B,其中 A 含有成员 G_i 的秘密特性钥 U_{G_i},B 则是为验证 A 的正确性而设立的(见第 2.5 节中验证过程),V_3 中则增加了对 B 正确性的证明过程.

2.5 签名的验证与打开

验证签名的正确性,只要在 Camenisch-Stadler 的验证过程(第 1.4 节)中补充验证

$$\frac{U_G}{A^e}B = \tilde{z}$$

成立即可.上式的正确性保证了签名者秘密特性钥 U_{G_i} 的合法性.签名的打开与 Camenisch-Stadler 方案中完全一致.

3 新方案的安全性分析

下面主要讨论新方案中伪造签名攻击的安全性,考虑伪造者在已知某一成员 G_i 公开钥 z_{G_i}, h,g,e,n 及群组

成员公开特性钥 U_M 的条件下,攻击者伪造 G_i 对信息 M 签名的可能性.结果表明,伪造成功相当于可求解 RSA 问题.

① RSA 问题:设 l_g 是安全参数,循环群 G 的阶长为 l_g,且其阶可分解为两个长为 $\frac{l_g-2}{2}$ 的素数的乘积,给定群 G 及 $(z,e)\in G\setminus\{\pm 1\}\times Z$,求出 $u\in G$ 使 $u^e=z$ 成立.

设 T 是输入为 1^{l_g},输出为 G 和 $z\in G\setminus\{\pm 1\}$ 的概率多项式时间算法,设 RSA 问题是一个困难问题,即有

② RSA 困难性假设:存在一个概率多项式时间算法 T,使得对任何概率多项式时间算法 ϕ,对所有多项式 $p(\cdot)$ 及对所有充分大的 l_g 有

$$P_r[z=u^e\mid (G,z,e):=T(1^{l_g}),u:=\phi(G,z,e)]<\frac{1}{p(l_g)}.$$

关于新方案中伪造攻击有:

定理 1. 在新方案中给定 z_{G_i}, h,g,e,G,U_G,存在一个概率多项式时间算法 ϕ,可求得(A,B)满足 $\frac{U_G}{A^e}B=\tilde{z}$ (其中 $B=h^r g^{re},\tilde{z}=h^r z$),当且仅当 ϕ 可以求解 RSA 问题.

证明:设存在概率多项式时间算法 ϕ,对给定的 z_{G_i},h,g,e,G,U_G,可求得(A,B)满足 $\frac{U_G}{A^e}B=\tilde{z}$,即 $\left(\frac{U_G}{z}\right)^{\frac{1}{e}}=\frac{A}{g^r}$,由 U_G 的随机性,任给 u^e,用 u^e 代替 $\frac{U_G}{z}$,得到 $u=\frac{A}{g^r}$,即可求解 RSA 问题.

反过来,若可解 RSA 问题,则可构造算法 ϕ 如下:

$$\forall r\in R,\ 令\ B:=h^r g^{re},\tilde{z}:=h^r z_{G_i}.$$

解 RSA 问题 $A^e=\frac{U_G}{\tilde{z}}\beta$,即求得 A 满足上式,故有(A,B)满足

$$\frac{U_G}{A^e}B=\tilde{z}.$$ □

由以上定理可知,伪造群签名相当于求解 RSA 问题,在 RSA 困难假设下,新方案是抗伪造攻击的.

4 小 结

本文所采用的更新算子方法,使得群组中当成员加入成员或删除时,群组的公开钥不变,而仅需更新群组的公开特征钥,利用群组成员的秘密特性钥更新算子,每个合法成员更新其特征秘密钥,而签名的长度与群组的成员个数及被删除的成员个数无关.新方案与 Bresson-Stern 的成员删除的证据法相比有很大的进步,因为 Bresson-Stern 的签名中证据个数随删除的成员个数呈线性增长,这在大的群组中是不现实的.而本文提出的更新算子法,群签名的长度与被删除成员个数无关,故可适用于大的群组系统.且新方案在RSA问题困难的假设下是抗伪造攻击的.

References:

[1] Chaum D, Van Heyst E. Group signtures. In: Advances in Cryptology-EUROCRYPT'91. LNCS 547, Berlin: Springer-Verlag, 1991. 257~265.

[2] Chen L, Pedersen TP. On the efficiency of group signatures providing information-theoretic anonymity. In: DeSantis A, ed. Advances in Cryptology-EUROCRYPT'94. LNCS 950, Berlin: Springer-Verlag, 1995. 171~181.

[3] Camenisch J. Efficient and generalized grorp signtures. In: Walter F, ed. Advances in Cryptology-EUROCRYPT'97. LNCS 1233, Berlin: Springer-Verlag, 1997. 465~479.

[4] Petersen H. How to convert any digital signature scheme into a group signature scheme. In: Lomas M, Vaudenay M, eds. Proceedings of the Security Protocols Workshop'97. LNCS 1361, Berlin: Springer-Verlag, 1997. 67~78.

[5] Camenisch J, Stadler M. Efficient group signatures schemes for large groups. In: Kaliski BS, ed. Advances in Cryptology-CRYPT'97. LNCS 1294, Berlin: Springer-Verlag, 1997. 410~423.

[6] Ateniese G, Tsudik G. Some open issues and new directions in group signatures. In: Franklin M, ed. Financial Cryptography Conference. LNCS 1648, 1999. 196~211.

[7] Lysyanskaya A, Ramzan Z. Group blind digital signatures: A scalable solution to electronic cash. In: Hitschfeld R, ed. Financial Cryptography Conference. LNCS 1465, Berlin: Springer-Verlag, 1998. 184~197.

[8] Camenisch J, Michels M. Separability and efficiency for generic group signature schemes. In: Wiener M, ed. Advances in Cryptology-EUROCRYPT'99. LNCS 1666, Berlin: Springer-Verlag, 1999. 411~430.

[9] Bresson E, Stern J. Efficient revocation in group signature. In: Kim K, ed. PKC 2001. LNCS 1992, Berlin: Springer-Verlag, 1999. 190~206.

[10] Kim HJ, Lim JI, Lee DH. Efficient and secure member deletion in group signature schemes. In: Dorgho won, ed. Information Security Cryptology 2000. LNCS 2015, Berlin: Springer-Verlag, 2000. 150~161.

敬 告 作 者

《软件学报》创刊以来,蒙国内外学术界厚爱,收到许多高质量的稿件,其中不少在发表后读者反映良好,认为本刊保持了较高的学术水平.但也有一些稿件因不符合本刊的要求而未能通过审稿.为了帮助广大作者尽快地把他们的优秀研究成果发表在我刊上,特此列举一些审稿过程中经常遇到的问题,请作者投稿时尽量予以避免,以利大作的发表.

1. 读书偶有所得,即匆忙成文,未曾注意该领域或该研究课题国内外近年来的发展情况,不引用和不比较最近文献中的同类结果,有的甚至完全不列参考文献.

2. 做了一个软件系统,详尽描述该系统的各个方面,如像工作报告,但采用的基本上是成熟技术,未与国内外同类系统比较,没有指出该系统在技术上哪几点比别人先进,为什么先进.一般来说,技术上没有创新的软件系统是没有发表价值的.

3. 提出一个新的算法,认为该算法优越,但既未从数学上证明比现有的其他算法好(例如降低复杂性),也没有用实验数据来进行对比,难以令人信服.

4. 提出一个大型软件系统的总体设想,但很粗糙,而且还没有(哪怕是部分的)实现,很难证明该设想是现实的、可行的、先进的.

5. 介绍一个现有的软件开发方法,或一个现有软件产品的结构(非作者本人开发,往往是引进的,或公司产品),甚至某一软件的使用方法.本刊不登载高级科普文章,不支持在论文中引进广告色彩.

6. 提出对软件开发或软件产业的某种观点,泛泛而论,技术含量少.本刊目前暂不开办软件论坛,只发表学术文章,但也欢迎材料丰富,反映现代软件理论或技术发展,并含有作者精辟见解的某一领域的综述文章.

7. 介绍作者做的把软件技术应用于某个领域的工作,但其中软件技术含量太少,甚至微不足道,大部分内容是其他专业领域的技术细节,这类文章宜改投其他专业刊物.

8. 其主要内容已经在其他正式学术刊物上或在正式出版物中发表过的文章,一稿多投的文章,经退稿后未作本质修改换名重投的文章.

本刊热情欢迎国内外科技界对《软件学报》踊跃投稿.为了和大家一起办好本刊,特提出以上各点敬告作者.并且欢迎广大作者和读者对本刊的各个方面,尤其是对论文的质量多多提出批评建议.