文章编号:1000－2367(2015)01－0158－07 DOI:10.16366/j.cnki.1000－2367.2015.01.030

无证书的 XML 多重签名

柳菊霞[1],苏靖枫[2]

(1.洛阳师范学院 信息技术学院,河南 洛阳 471022;
2.河南城建学院 计算机科学与工程学院,河南 平顶山 467036)

摘 要:针对 XML 电子公文流转系统中公文审批存在多重签名的需求,构建了两种新的 XML 多重签名研究模型.基于相应的研究模型,提出了一种无证书的 XML 有序多重签名方案和无证书的 XML 广播多重签名方案,以解决传统签名在此类应用中存在的签名效率低、可扩展性差等问题.同时分析了两种方案的正确性、在随机预言模型下的不可伪造性,而且无证书的 XML 有序多重签名方案,克服了已有方案相邻成员可以擅自交换签名顺序的缺点.最后,按照 XML 数字签名规范化要求,对多重签名的实现过程进行了设计,为 XML 多重签名在电子政务中的应用提供了可行的解决途径.

关键词:XML 签名;双线性对;多重签名;无证书签名;不可伪造性

中图分类号:TP309 **文献标志码**:A

随着 XML(Extensible Markup Language 可扩展的标记语言)技术的发展和应用,XML 正在成为互联网上数据交换的标准,目前已经广泛应用在电子商务、电子政务等领域[1,2].针对 XML 数据存储和传输的安全性需求,尤其是数据的完整性、可验证性和不可抵赖性的要求,W3C(World Wide Web Consortium)和 IETF(Internet Engineering Task Force)联合发布了 XML 数字签名规范[3].XML 数字签名不仅可以像传统数字签名一样对任意类型的数据签名,而且在处理 XML 文档签名的时候,表现出了许多传统数字签名不可比拟的技术优势,从而满足更深层次的签名需求.如基于网络平台的公文流转系统中,某些重要公文需要经过多方签署方可生效,将多重签名应用于 XML 电子公文的签名,具有很好的灵活性,可扩展性,能够提高业务处理的效率和安全性.

2003 年,AL-Riyami 等[4]首次提出了无证书公钥密码体制(CL-PKC).无证书的公钥签名方案不需要公钥证书,KGC 为用户生成部分私钥,用户基于部分私钥和用户自己生成的秘密参数生成用户的私钥.CL-PKC 解决了 PKI/CA 技术中证书管理问题和基于身份系统中的密钥托管问题.之后,几种新的无证书签名方案相继被提出[5－12],但研究发现,已有的无证书有序多重签名方案不能满足真正的按序签名,如相邻签名成员可以交换签名顺序.基于此,本文提出了一种新的无证书有序多重签名方案,在保证签名效率的前提下,可以抵抗相邻签名成员的换序攻击.然后就如何实现对 XML 文档进行多重签名,构建了新的无证书 XML 多重签名(XML Multi-Signature)模型,并提出具体的无证书的 XML 有序多重签名方案和无证书的 XML 广播多重签名方案.最后基于 XML 的签名规范,实现了无证书的 XML 多重签名.

1 XML 数字签名规范

由 IETF 和 W3C 共同组建的 XML Signature 工作组在 2001 年 8 月 20 日公布了 XML 数字签名的推荐版本.W3C 将 XML 数字签名解释为:定义一种与 XML 语法兼容的数字签名语法描述规范,描述数字签名本身和签名的生成与验证过程.其语法定义结构如下,结构中各标记的含义可参见文献[3].

收稿日期:2014-03-19;**修回日期**:2014-09-17.

基金项目:国家自然科学基金(61202317);河南省自然科学基金(112300410192).

作者简介:柳菊霞(1980－),女,河南洛阳人,洛阳师范学院讲师,研究方向为信息安全、密码学,E-mail:380600223@qq.com.

```
<Signature ID? >
    <SignedInfo>
      <CanonicalizationMethod/>
      <SignatureMethod/>
      (<Reference URI? >
        (<Transforms/>)?
        <DigestMethod/>
        <DigestValue/>
      </Reference>)+
    </SignedInfo>
    <SignatureValue/>
    (<KeyInfo/>)?
    (<Object ID? >)*
</Signature>
```

XML 数字签名充分利用了 XML 本身强大的表达能力和扩展能力，不仅可以像传统的数字签名技术一样对整个文档签名，还可以实现较细粒度的签名及多重签名. 在 XML 签名的<Reference>元素中，其 URI 属性不仅可指定本地或网络上的文本或二进制数据，还可指定 XML 文档内部的某个元素. 如果想对多份数据签名，可以采用多个<Reference>元素分别指向不同的签名对象[13]. 根据签名元素和被签名对象之间的关系，XML 数字签名又可分为封装式签名、嵌入式签名和分离式签名 3 种签名方式[3].

2　无证书的 XML 多重数字签名模型

在公文流转系统中通常会涉及到多人对同一份公文进行签名，即需要进行多重签名. 多重签名分为两种：有序多重签名和广播多重签名.

XML 有序多重签名是指：消息发送者对 XML 待签文档进行规范化并计算摘要值，然后确定签名的顺序，将摘要值发送给第一位签名成员. 其它每位签名成员收到签名文档后，首先验证上一位签名成员部分签名的有效性，若有效，继续签名并将生成的部分签名发送给下一位签名成员；若签名无效，拒绝对所收到的签名文档继续签名，并终止整个签名过程. 直到最后一位签名成员完成部分签名，并由验证者验证无误后，即完成了 XML 有序多重签名，上述过程如图 1 所示.

XML 广播多重签名是并行的，签名者之间没有顺序关系，消息发送者对 XML 待签文档进行规范化并计算摘要值，然后将摘要同时发送给所有签名成员，每个成员完成自己的部分签名，然后将部分签名发送给签名收集者，签名收集者将所有签名整理成消息的多重签名后，再发送给验证者验证签名的有效性，上述过程如图 2 所示.

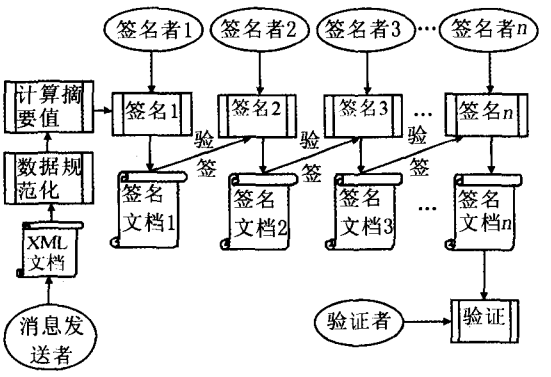

图1 XML有序多重签名模型

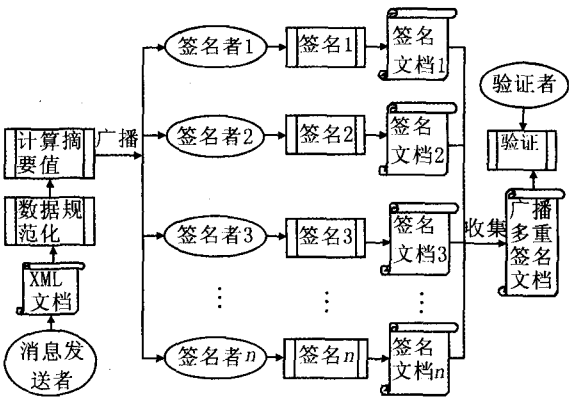

图2 XML广播多重签名模型

3　无证书的 XML 多重数字签名方案

3.1　系统初始化

基于第 2 节给出的模型，将无证书签名与 XML 多重签名相结合，分别提出无证书的 XML 有序多重签名方案和无证书的 XML 广播多重签名方案. 方案的参与者有：消息发送者 A、消息签名者 $U=(U_1,U_2,U_3,\cdots,U_n)$，签名收集者 U_C，签名验证者 V，M 为待签名的摘要值，方案中出现的其它符号说明详见文献[5]，这里不再赘述.

1) 参数生成. KGC 输入安全参数 k,输出系统参数 $Params=(k,e,P,q,G_1,G_2,P_{pub},H_1,H_2,H)$,其中 $P_{pub}=sP$,s 是系统主密钥,双线性对映射 $e:G_1\times G_1\to G_2$,选取 3 个安全的 Hash 函数 $H_1:\{0,1\}^*\to G_1$,$H_2:\{0,1\}^*\to\{0,1\}^*$ 和 $H:\{0,1\}^*\to Z_q^*$,KGC 将 s 秘密保存,公开 $Params$.

2) 公钥生成. 签名者 $U_i(1\leq i\leq n)$ 随机选择秘密值 $x_i\in Z_q^*$,并计算其公钥 $(X_i,Y_i)=(x_iP,x_isP)$.

3) 部分私钥生成. 给定用户身份 $ID_i\in\{0,1\}^*$ 及其公钥 Y_i,KGC 计算 $Q_i=H_1(ID_i,Y_i)$,将 $D_i=sQ_i$ 作为用户部分私钥.

4) 私钥生成. 签名者 $U_i(1\leq i\leq n)$ 计算私钥 $R_i=x_iD_i$.

3.2 无证书的 XML 有序多重签名方案(CLSMS)

3.2.1 生成多重签名 考虑到实际的公文流转系统中,公文的签署顺序通常是确定的,不妨设消息发送者 A 预先设计签名顺序为 $\Gamma=(ID_1,ID_2,\cdots,ID_n)$,公开 Γ,以便所有参与者都了解签名顺序.

1) 消息发送者 A 根据 XML 文档中的 URL 获得需要签名的 XML 文档,选择一种规范化算法对待签消息进行规范化.

2) 选择一种摘要算法对规范化的待签文档计算其摘要值 M.

3) A 将摘要值 M 发送给第一位签名者 U_1,U_1 随机选取 $k_1\in Z_q^*$,计算:$r_1=k_1P$,$h_1=H_2(\Gamma,ID_1)$ 和 $S_1=H(M)R_1h_1+r_1k_1h_1$ 将签名消息 $(M,(S_1,r_1))$ 发送给下一位签名者 U_2.

4) 签名者 $U_i(2\leq i\leq n)$ 收到 U_{i-1} 发送的签名 $(M,(S_{i-1},r_1,r_2,\cdots,r_{i-1}))$ 后,验证等式(1) 是否成立,

$$e(S_{i-1},P)=\prod_{j=1}^{i-1}e(Q_j,Y_j)^{H(M)h_j}\prod_{j=1}^{i-1}e(r_j,r_j)^{h_j},\tag{1}$$

若等式(1) 成立继续签名,随机选择 $k_i\in Z_q^*$,计算:$r_i=k_iP$,$h_i=H_2(\Gamma,ID_i)$ 和 $S_i=S_{i-1}+H(M)R_ih_i+r_ik_ih_i$.

将签名消息 $(M,(S_i,r_1,r_2,\cdots,r_i))$ 发送给下一位签名者 U_{i+1}. 最后一位签名者 U_n 的签名 $(M,(S_n,r_1,r_2,\cdots,r_n))$ 作为签名文档中元素 < SignatureValue > 的值,并将签名文档发送给验证者 B.

3.2.2 验证签名 当 V 收到 XML 签名文档时,通过解析 XML 签名文档得到签名 $(M,(S_n,r_1,r_2,\cdots,r_n))$,验证等式(2) 是否成立,

$$e(S_n,P)=\prod_{j=1}^{n}e(Q_j,Y_j)^{H(M)h_j}\prod_{j=1}^{n}e(r_j,r_j)^{h_j},\tag{2}$$

如果等式(2) 成立,V 认为所有签名者对消息的有序多重签名有效,否则签名无效.

3.3 无证书的 XML 广播多重签名方案(CLBMS)

3.3.1 生成多重签名 1) 消息发送者 A 根据 XML 文档中的 URL 获得需要签名的 XML 文档,选择一种规范化算法对待签消息进行规范化. 2) 选择一种摘要算法对规范化的待签文档计算其摘要值 M. 3) A 将摘要值 M 发送给所有签名者 U,每个签名者 $U_i(1\leq i\leq n)$ 收到消息后,随机选取 $k_i\in Z_q^*$,计算 $r_i=k_iP$ 和 $S_i=H(M)R_i+r_ik_i$,将签名消息 $(M,(S_i,r_i))$ 发送给签名收集者 U_C. 4) 签名收集者 U_C 收到所有签名者的签名消息 $(M,(S_i,r_i))(1\leq i\leq n)$ 后,计算 $\hat{S}=\sum_{i=1}^{n}S_i$,最终的广播多重签名 $(M,(\hat{S},r_1,r_2,\cdots,r_n))$ 作为签名文档中元素 < SignatureValue > 的值,将签名文档发送给验证者 V.

3.3.2 验证签名 V 收到 XML 签名文档后,通过解析 XML 签名文档得到签名 $(M,(\hat{S},r_1,r_2,\cdots r_n))$,验证等式(3) 是否成立,

$$e(\hat{S},P)=\Big(\prod_{j=1}^{n}e(Q_j,Y_j)\Big)^{H(M)}\prod_{j=1}^{n}e(r_j,r_j),\tag{3}$$

如果等式(3) 成立,V 认为所有签名者对消息的广播多重签名有效,否则签名无效.

4 方案分析

4.1 正确性分析

定理 1 CLSMS 方案是正确的.

证明　$e(S_n,P)=e(S_{n-1}+H(M)R_nh_n+r_nk_nh_n,P)=e(S_{n-2}+H(M)R_nh_n+r_nk_nh_n+H(M)R_{n-1}h_{n-1}+r_{n-1}k_{n-1}h_{n-1},P)=e\left(\sum_{j=1}^{n}(H(M)R_jh_j+r_jk_jh_j),P\right)=e\left(\sum_{j=1}^{n}(H(M)\cdot x_jsQ_jh_j+r_jk_jh_j),P\right)=e\left(\sum_{j=1}^{n}H(M)\cdot x_jsQ_jh_j,P\right)e\left(\sum_{j=1}^{n}r_jk_jh_j,P\right)=e\left(\sum_{j=1}^{n}H(M)Q_jh_j,Y_j\right)e\left(\sum_{j=1}^{n}r_jh_j,r_j\right)=\prod_{j=1}^{n}e(Q_j,Y_j)^{H(M)h_j}\prod_{j=1}^{n}e(r_j,r_j)^{h_j}$.

方案 CLBMS 的正确性同样可以通过直观运算来验证，这里不再赘述.

4.2　有序性分析

针对有序多重签名的有序性攻击，可以分为两种情况：非相邻成员的合谋换序签名攻击和相邻成员的合谋换序签名攻击，已有的有序多重签名方案都可以抵抗第一种攻击，多数方案却无法抵抗相邻成员的换序签名攻击，如文献[6]给出的方案 CL-DMS，新方案 CLSMS 通过在签名中加入 $h_i=H_2(\Gamma,ID_i)$，可满足定理 2.

定理 2　CLSMS 方案能够抵抗相邻成员擅自交换签名顺序攻击.

不妨设两个恶意的相邻签名成员为 (U_t,U_{t+1})（其中 $1\leq t<n$），攻击方法有交换签名顺序不换身份和交换签名顺序并换身份两种，其它签名者都进行正确签名.

证明　假设相邻成员交换签名顺序不换身份，U_{t+1} 随机选择 $k_t\in Z_q^*$，计算：$r_t=k_tP$，$h_{t'}=H_2(\Gamma,ID_{t+1})$ 和 $S_t=S_{t-1}+H(M)R_{t+1}h_{t'}+r_tk_th_{t'}$，将 $(M,(S_t,r_1,r_2,\cdots r_t))$ 作为 U_{t+1} 的签名. U_t 从 U_{t+1} 传递的签名文档中解析出 $(M,(S_t,r_1,r_2,\cdots,r_t))$ 后，随机选择 $k_{t+1}\in Z_q^*$，计算：$r_{t+1}=k_{t+1}P$，$h_{(t+1)'}=H_2(\Gamma,ID_t)$ 和 $S_{t+1}=S_t+H(M)R_th_{(t+1)'}+r_{t+1}k_{t+1}h_{(t+1)'}$，然后将签名 $(M,(S_{t+1},r_1,r_2,\cdots,r_{t+1}))$ 作为签名文档中元素 < SignatureValue > 的值，发送给下一位签名者 U_{t+2}. U_{t+2} 验证等式(4)：

$$e(S_{t+1},P)=\prod_{j=1}^{t+1}e(Q_j,Y_j)^{H(M)h_j}\prod_{j=1}^{t+1}e(r_j,r_j)^{h_j}. \tag{4}$$

只需从中抽取 U_t,U_{t+1} 的签名部分进行验证，等式左边经计算结果为：$(Q_t,Y_t)^{H(M)h_{(t+1)'}}(Q_{t+1},Y_{t+1})^{H(M)h_{t'}}(r_t,r_t)^{h_{t'}}(r_{t+1},r_{t+1})^{h_{(t+1)'}}$，等式右边经计算结果为 $(Q_t,Y_t)^{H(M)h_t}(Q_{t+1},Y_{t+1})^{H(M)h_{t+1}}(r_t,r_t)^{h_t}(r_{t+1},r_{t+1})^{h_{t+1}}$，由于 $h_{(t+1)'}=h_t$、$h_{t'}=h_{t+1}$，所以等式(4) 不成立.

假设恶意的相邻成员交换签名顺序并更换身份，U_{t+1} 计算 $h_{t'}=H_2(\Gamma,ID_t)$，U_t 计算 $h_{(t+1)'}=H_2(\Gamma,ID_{t+1})$，同样可以证明出等式(4) 无法通过验证. 因此，CLSMS 方案能够抵抗相邻成员擅自交换签名顺序攻击.

4.3　不可伪造性分析

假定 CDH 问题是困难的，下面证明新方案 CLSMS 在适应性选择消息下的 A_I 伪造攻击和 A_{II} 伪造攻击是安全的.

定理 3　在随机预言模型下，若存在攻击者 A_I 以一个不可忽略的概率伪造一个 XML 无证书多重签名，则可以得到解决 CDH 问题的一个实例.

证明　设 A_I 是第一类型攻击者，A_I 从签名成员集合 U 中随机选取 n 个人作为多重签名者，其中每个用户的公钥为 P_i. B 是 CDH 问题的挑战者，B 给定 (P,aP,bP)，B 的目标是利用 A_I 解决 CDH 问题，即计算 abP.

B 保持表 $L=(ID_i,x_i,(X_i,Y_i),l_i,l'_i,h_i,h'_i,D_i,R_i)$，初始为空，用来存储身份 ID_i 所对应的秘密值、公钥、随机数 l_i 和 l'_i、H_1 询问的结果 h_i、H_2 询问的结果 h'_i、部分私钥以及私钥. A_I 执行以下询问，询问结果保存在表 L 中.

系统参数建立：B 设 $P_{pub}=bP$，并随机选择 $l\in Z_q^*$，计算挑战用户 ID^* 的公钥 $P^*=lP_{pub}=lbP$，将系统参数 $Params=(k,e,P,q,G_1,G_2,P_{pub},H_1,H_2,H)$ 及挑战公钥 P^* 发送给 A_I.

H_1 询问：当 B 收到 A_I 对 (ID_i,Y_i) 的 Hash 值询问时，若 $ID_i\neq ID^*$，则 B 首先在表 L 中查找，若 $ID_i\in L$，则返回 h_i 给 A_I，若 $ID_i\notin L$，则随机选择 $l_i\in Z_q^*$，计算 $h_i=l_iP$，并返回 h_i；若 $ID_i=ID^*$，则令 $h_i=aP$，并将 h_i 的值添加到表 L 中，返回 h_i 作为 (ID_i,Y_i) 的 Hash 值询问结果.

H_2 询问：当 A_I 对 (Γ,ID_i) 的 Hash 值询问时，若列表 L 中存在询问项，B 将 h'_i 返回给 A_I，否则，B 随机选择 $l'_i\in Z_q^*$，计算 $h'_i=l'_iP$，返回 h'_i 给 A_I，并将 (h'_i,l'_i) 的值添加到表 L 中.

公钥询问:当 A_I 询问用户 ID_i 的公钥时,则 B 首先在表 L 中查找,若 $ID_i \in L$,则返回对应的 P_i 给 A_I,否则随机选择 $x_i \in Z_q^*$,计算 $P_i = x_i bP$,返回 P_i 作为 A_I 对 ID_i 的公钥询问回答,并将(x_i, P_i) 的值存储到表 L 中.

公钥替换询问:当 A_I 自己产生一个 P'_i 来替换用户 ID_i 的公钥时,则 B 首先在表 L 中查找,若 $ID_i \in L$,则用$(ID_i, \perp, P'_i)$ 替换已有记录,否则,B 在表 L 中增加记录$(ID_i, \perp, P'_i)$.

秘密值询问:当 A_I 询问用户 ID_i 的秘密值时,B 首先在表 L 中查找,若 $ID_i \in L$,且 $x_i \neq \perp$,则返回对应的 x_i 给 A_I,若 $x_i = \perp$,则返回对应的 $\perp$,这种情况是由于公钥被替换的结果.若 $ID_i \notin L$,则 B 向自身对 ID_i 做公钥询问,并返回 x_i.

部分私钥询问:当 A_I 对 ID_i 的部分私钥询问时,若 $ID_i \neq ID^*$,则 B 首先在表 L 中查找,若 $ID_i \in L$,则返回对应的 D_i 给 A_I,若 $ID_i \notin L$,则随机选择 $l_i \in Z_q^*$,计算 $D_i = l_i bP$,并返回 D_i;若 $ID_i = ID^*$,则 B 终止对 A_I 的询问回答.

通过以上各种询问模拟,B 可以很容易得到 A_I 对于消息 M^* 的一个伪造多重签名,记作(M^*, S_n^*, U^*),其中 $ID^* \in U^*$,不失一般性,设 $ID^* = ID_1^*$. B 通过验证方程得到:$e(S_n^*, P) = e(Q_1^*, Y_1^*)^{H(M^*)h_1^*} e(r_1, r_1)^{h_1^*} \prod_{i=2}^{n} e(Q_i^*, Y_i^*)^{H(M^*)h_i^*} \prod_{i=2}^{n} e(r_i, r_i)^{h_i^*} = e(aP, lbP)^{H(M^*)h'_1} e(r_1, r_1)^{l'_1 P} \prod_{i=2}^{n} e(l_i P, x_i bP)^{H(M^*)h'_i} \prod_{i=2}^{n} e(r_i, r_i)^{l'_i P} = e\left(H(M^*)h'_1 labP + \sum_{i=2}^{n} H(M^*)h'_i l_i x_i bP + \sum_{i=1}^{n} r_i^2 l'_i, P\right)$.

解得 $abP = H(M^*)^{-1} h'^{-1}_1 l^{-1} \left(S_n^* - \sum_{i=2}^{n} H(M^*)h'_i l_i x_i bP - \sum_{i=1}^{n} r_i^2 l'_i\right)$. 由此 B 成功地解决了 CDH 问题实例,出现矛盾.

定理 4 在随机预言模型下,若存在攻击者 A_{II} 以一个不可忽略的概率伪造一个 XML 无证书多重签名,则可以得到解决 CDH 问题的一个实例.

证明 设 A_{II} 是第二型攻击者,A_{II} 拥有系统主密钥,但不能替换任何用户的公钥. B 随机选择 $s \in Z_q^*$,并计算挑战用户 ID^* 的公钥 $P^* = sbP$,然后将主密钥 s、系统参数 $Params = (k, e, P, q, G_1, G_2, P_{pub}, H_1, H_2, H)$ 及挑战公钥 P^* 发送给 A_{II},其中 $P_{pub} = sP$.

H_1 询问、H_2 询问:B 用定理 3 的方法来对 A_{II} 的询问做出回答.

公钥询问:当 A_{II} 询问用户 ID_i 的公钥时,则 B 首先在表 L 中查找,若 $ID_i \in L$,则返回对应的 P_i 给 A_{II},否则随机选择 $x_i \in Z_q^*$,计算 $P_i = x_i sP = x_i P_{pub}$,返回 P_i 作为 A_{II} 对 ID_i 的公钥询问回答,并将(x_i, P_i) 的值存储到表 L 中.

秘密值询问:当 A_{II} 询问用户 ID_i 的秘密值时,若 $ID_i \neq ID^*$,则 B 首先在表 L 中查找,若 $ID_i \in L$,则返回对应的 x_i,若 $ID_i \notin L$,则 B 向自身对 ID_i 做公钥询问,并返回 x_i;若 $ID_i = ID^*$,则 B 终止对 A_{II} 的询问回答.

通过上面各种询问模拟,A_I 输出关于消息 M^* 的一个伪造多重签名(M^*, S_n^*, U^*). B 通过验证方程可以得到:

$$e(S_n{}^*, P) = e(Q_1^*, Y_1^*)^{H(M^*)h_1^*} e(r_1, r_1)^{h_1^*} \prod_{i=2}^{n} e(Q_i^*, Y_i^*)^{H(M^*)h_i^*} \prod_{i=2}^{n} e(r_i, r_i)^{h_i^*} =$$

$$e(aP, sbP)^{H(M^*)h'_1} e(r_1, r_1)^{l'_1 P} \prod_{i=2}^{n} e(l_i P, x_i sP)^{H(M^*)h'_i} \prod_{i=2}^{n} e(r_i, r_i)^{l'_i P} =$$

$$e\left(H(M^*)h'_1 sabP + \sum_{i=2}^{n} H(M^*)h'_i l_i x_i sP + \sum_{i=1}^{n} r_i^2 l'_i, P\right).$$

解得 $abP = H(M^*)^{-1} h'^{-1}_1 s^{-1} \left(S_n^* - \sum_{i=2}^{n} H(M^*)h'_i l_i x_i sP - \sum_{i=1}^{n} r_i^2 l'_i\right)$. 由此 B 成功地解决了 CDH 问题实例. 这与 CDH 问题的困难性相矛盾,因此,方案 CLSMS 对适应性选择消息下的两类攻击是安全的,本文所提出的方案 CLBMS 的存在不可伪造性证明类似.

5 方案实现

CLSMS 方案和 CLBMS 方案实现过程类似，这里以 CLSMS 方案为例，对签名的生成和验证过程进行描述. 方案的实现基于 JAVA 技术，JAVA 平台为安全和加密服务提供了 JCA(Java Cryptography Architecture). 在 JDK1.2 中，JCA 不但包括用于数字签名和报文摘要的 API，而且引入了划分细致、可配置性强、功能灵活、可扩展的访问控制机制. 现有的 JCA 中没有提供实现无证书多重签名体制的密码服务，因此在 JAVA 平台上实现 CLBMS 需要实现和集成提供 CLBMS 密码服务的“提供者”，然后使用 CLBMS 生成并验证 XML 签名.

5.1 实现和集成提供 CLSMS 密码服务的“提供者”

首先，基于 JCA 中定义的密码服务各方面的引擎类，实现 CLSMS 密码服务，定义密钥提取类 CLSMSKeyPairGenerator、签名类 CLSMSSignature 和验证类 CLSMSVerification；然后，根据服务提供者接口规范创建 CLSMS 方案的服务提供者“CLSMSProvider”；最后，将 CLSMSProvider 集成到现有的 JCA 中.

5.2 使用签名算法 CLSMS 生成 XML 签名

1) 创建 XML 签名工厂，在 XMLSignatureFactory 实例化时引用“CLSMSProvider”.

2) 创建对象 Reference 和 SignedInfo，引用摘要算法 SHA-1 和签名类 CLSMSSignature 中的签名算法 CLSMS，这两个对象分别对应于元素＜Reference＞和＜SignedInfo＞.

3) 使用 CLSMSProvider 中的 CLSMSKeyPairGenerator 生成公私密钥对，创建 KeyInfo 对象包含生成的公钥，该对象对应于元素＜KeyInfo＞.

4) 根据 JAXP DocumentBuilderFactoyr 创建的文档，生成 XMLSignature 对象，对应于元素＜Signature＞，TransformerFactory 输出签名结果.

5.3 使用签名算法 CLSMS 验证 XML 签名

1) 使用 DocumentBuilderFactory 解析包含签名的 XML 文档，使用 DocumentBuilde 加载签名后的 XML 文档.

2) 向 DOM 方法 Document. getElementsByTagNameNS 传入 XML 签名命名空间的 URI 和＜Signature＞元素的标记来实现指定签名元素.

3) 实例化 XMLSignatureFactory，引用 CLSMS 算法，提取＜Signature＞元素.

4) 调用 XMLSignature 对象上的 validate 方法，进行签名验证.

重复以上的步骤，即可完成多重签名，实现无证书的 XML 多重签名.

6 结　论

本文方案 CLSMS 是对文献[6]的改进，文献[6]只能保证非相邻成员不能交换签名顺序，而相邻成员合谋是可以成功实施换序攻击的. 分析表明，新方案能够实现真正意义上的有序多重签名，计算量上，新方案仅在签名阶段增加了一个 Hash 计算，对方案的整体效率影响不大. 本文提出的无证书 XML 多重签名方案，充分利用了 XML 文档的树形结构特点及无证书签名的灵活性，降低了公文流转系统签名的计算量和通信开销，克服了传统签名在公文流转应用中存在的证书管理问题或密钥托管问题. 随着 Internet 技术的发展与应用，XML 电子公文在电子政务中的应用会越来越广泛，研究安全可行的 XML 多重签名具有重要的意义.

参 考 文 献

[1] 张　腾，沈备军，杨　涛. 基于 DEB 和 XML 签名的电子证据管理[J]. 计算机工程，2012，34(12)：136-138.

[2] 冯　江，宋余庆，陈健美，等. 基于 DSA 的无证书电子病历签名方案[J]. 计算机应用研究，2011，28(5)：1910-1913.

[3] W3C XML Signature Working Group. XML Signature Syntxa and Processing[EB/OL]. [2002-02-12]. http://www.w3c.org./TR/xmldsigcore.

[4] AL-RIYAMI S S, PATERSON K G. Certificateless Public Key Cryptography[C]. Proceedings of Asiacrypt'03, Berlin, 2003.

[5] 梁红梅，黄　慧，吴晨煌，等. 无证书多重签名[J]. 集美大学学报，2008，13(2)：127-131.

[6] 韩亚宁,王彩芬.无证书广义指定多个验证者有序多重签名[J].计算机应用,2009,29(6):1643-1645.
[7] 侯红霞.一个新的无证书多重无链接签名方案[J].计算机应用研究,2011,28(6):2199-2200.
[8] 罗文俊,李长英.一种不含双线性对的无证书有序多重签名方案[J].计算机应用研究,2012,29(4):1427-1429.
[9] SK HAFIZUL ISLAM, BISWAS G P. Hafizul ICertificateless Strong Designated Verifier Multisignature Scheme using Bilinear Pairings [C]. Proceeding of the International Conference on Advances in Computing, Communications and Informatics, New York, 2012.
[10] SK HAFIZUL ISLAM, BISWAS G P. Certificateless short sequential and broadcast multisignature schemes using elliptic curve bilinear pairings[J]. Journal of King Saud University-Computer and Information Sciences, 2013, 25(1): 51-61.
[11] YONGJUN GENG, JUNFENG ZHANG. A New Multi-signature Scheme based on Bilinear Pairs[C]. E-Business and E-Government, Hongkong, 2011.
[12] 张 骏,陈力群.一种改进的 Elgamal 有序多重签名方案[J].计算机应用与软件,2009,26(3):258-259.
[13] 张 勇,冯玉才.XML 数字签名技术及其在 Java 中的具体实现[J].计算机应用,2003,23(9):93-95.

Certificateless XML Multi-Signature

LIU Juxia[1], SU Jingfeng[2]

(1. Academy of Information Technology, Luoyang Normal University, Luoyang 471022, China;
2. Institute of Computer Science and Engineering, Henan University of Urban Construction, Pingdingshan 467036, China)

Abstract: According to the demand for multi-signature in the electronic document flow system, two kinds of new XML multi-signature research models are built up. Based on the corresponding research model, this paper proposed a new XML sequential multi-signature scheme and a new XML broadcasting multi-signature scheme, which solve the problems of low efficiency and poor scalability using the traditional signature technology. This paper also analyzed that two kinds of scheme were correct and non-forgeable in the random oracle mode, and the signing sequence of the proposed XML sequential multi-signature scheme was fixed and unable to be changed freely by the signers. Finally, this paper designed the realization process of the proposed XML multi-signature schemes according to the XML signature syntax, which provides a feasible solution for the application of XML multi-signature in E-government system.

Keywords: XML digital signature; bilinear pairings; multi-signature; certificateless signature; unforgeability property