文章编号:1007-5321(2011)02-0008-04

基于聚合签名的多方合同签署协议

孙艳宾[1], 谷利泽[1], 郑世慧[1], 杨义先[1], 孙 燕[2]
(1. 北京邮电大学 网络与交换技术国家重点实验室, 北京 100876;
2. 石家庄陆军指挥学院 军事运筹中心, 石家庄 050084)

摘要: 利用无限制的聚合签名方案和公钥密码系统广播协议,提出了一个新的安全多方合同签署协议. 合同签署协议利用广播协议实现签署者之间消息的分发,利用无限制的聚合签名方案实现签署者之间合同的签署,执行过程分为2个阶段:签署者进行消息-凭证聚合签名的交换;广播发送合同签名. 如果执行过程中发生争议,签署者要求仲裁者介入,在保证其公平性的基础上结束协议. 该协议满足不可伪造性、不透明性、可提取性和公平性,且随着签署者人数的增加,消息交互次数呈线性增长,效率较高.

关 键 词: 聚合签名; 合同签署协议; 公平性; 中国剩余定理
中图分类号: TP309 **文献标志码**: A

An Aggregate Signature Based Multi-Party Contract Signing Protocol

SUN Yan-bin[1], GU Li-ze[1], ZHENG Shi-hui[1], YANG Yi-xian[1], SUN Yan[2]
(1. State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. Operation Research Center, Shijiazhuang Army Command Academy, Shijiazhuang 050084, China)

Abstract: Utilizing the unrestricted aggregate signature scheme and the public-key cryptosystem based broadcast protocol, a new multi-party contract signing protocol (MCSP) is proposed. The MCSP employes the public-key cryptosystem based broadcast protocol to distribute the messages of the signers, and employes the unrestricted aggregate signature scheme to sign the contract between the signers. The implementation of MCSP is divided into two phases: the signers exchange the aggregate signatures on the message and voucher in the first phase; then, they exchange their signatures on the contract. If a dispute occurs in the process of implementing, any signer can ask the adjudicator to settle the dispute to ensure fairness. Analysis shows that the proposed multi-party contract signing protocol satisfies the requirements of unforgeability, opacity, extractability and fairness. The proposed MCSP is with more efficience, and the interactions of messages grow linearly with the increase of the parties.

Key words: aggregate signature; contract signing protocol; fairness; Chinese remainder theorem

Baum-Waidner 等[1]提出适合于异步网络的多方合同签署协议后,异步网络多方合同签署协议[2-4]逐渐受到广泛关注. 然而,异步网络中的多方合同签署协议的消息延迟没有上限,需要的轮数较多,效率比较低. 基于 Shao[5]提出的公平交易协议的思想,利用 Bellare 等[6]提出的无限制聚合签名和 Chiou 等[7]提出的基于公钥密码系统的广播协议(PCBP, public-key cryptosystem based broadcast protocol),提出了一个新的多方合同签署协议. 协议中不规定签署者发送消息的次序,同时设置了凭证的

收稿日期: 2010-07-02
基金项目: 国家自然科学基金项目(60970135,90718001, 60821001); 国家重点基础研究发展计划项目(2007CB311203); 国家重大科技专项项目(2009ZX03004-003-03)
作者简介: 孙艳宾(1980—), 男, 博士生, E-mail: ybsun@foxmail.com; 杨义先(1961—), 男, 教授, 博士生导师.

有效期，运行环境为同步网络或半同步网络. 协议无需提前确定不诚实签署者数，允许最大不诚实签署者数为 $n-1$. 该协议的交互轮数和消息发送次数较少，效率较高.

1　预备知识

1.1　双线性对及困难假设

设 G_1、G_2 分别具有相同素数阶 q 的加法和乘法循环群，P 为 G_1 的生成元，$H:(0,1)^* \rightarrow G_1$ 为抗碰撞密码学单向哈希函数. 假设离散对数问题在 G_1 和 G_2 上是难解的，称具有下列性质的映射 $e:G_1 \times G_1 \rightarrow G_2$ 为双线性对.

1）双线性性. 对任意的 $P、Q \in G_1$ 和 $a、b \in Z_q$ 有 $e(aP,bQ)=e(P,Q)^{ab}$.

2）非退化性. 存在元素 $P、Q \in G_1$ 使得 $e(P,Q) \neq 1$.

3）可计算性. 存在有效算法可计算 $e(P,Q)$，对任意 $P、Q \in G_1$.

定义 1　CDH 问题. 设 P 为 G_1 的生成元，给定 $aP、bP \in G_1(\forall a,b \in Z_q^*)$，计算 abP.

定义 2　CoCDH 问题. 给定 $P、aP \in G_1(\forall a \in Z_q^*)$ 和 $Q \in G_1$，计算 $aQ \in G_1$.

若不存在某个算法在时长 t' 内以 ε' 的概率解决 CoCDH 问题，则 CoCDH 问题是 (t',ε') 困难的.

1.2　PCBP 算法

主体 U 要把某个消息 M 发送给 n 个接收者，每个接收者 P_i 被分配 1 个大整数 N_i，且任意 N_i 与 N_j $(\forall i \neq j)$ 互素. U 首先用每个接收者 P_i 的公钥加密 M 得 $E_{\mathrm{PK}_i}(M)$. 由于 N_i 与 $N_j(\forall i \neq j)$ 两两互素，由中国剩余定理可知，n 个同余方程组成的方程组 $X=E_{\mathrm{PK}_i}(M) \bmod N_i (i=1,2,\cdots,n)$ 必有唯一解 $E_P(M)$. U 广播 $E_P(M)$ 给全体接收者，每个接收者 P_i 计算 $E_P(M) \bmod N_i \equiv E_{\mathrm{PK}_i}(M)$，利用对应私钥解密 $E_{\mathrm{PK}_i}(M)$ 获得消息 M.

1.3　BNN 无限制聚合签名

1）密钥生成. 对于聚合签名的某个签署者随机选择私钥 $x \in Z_q^*$，然后计算公钥 $Y=xP$.

2）一般签名. 对于聚合签名的某个签署者给定私钥 x 和消息 $m \in \{0,1\}^*$，计算 $\sigma \leftarrow xH(Y \| m) \in G_1$，则一般签名为 $\sigma \in G_1$.

3）一般签名验证. 给定签署者的公钥 Y，签名消息 m，消息签名为 σ，如果等式 $e(\sigma,P)=e(H(Y \| m),Y)$ 成立，验证通过.

4）聚合签名. 给定 n 个签名者 $\{Y_i\}_{i=1}^n$，分别对 n 个消息 $\{m_i\}_{i=1}^n$ 的签名 $\{\sigma_i\}_{i=1}^n$ 计算 $\sigma_{\mathrm{agg}} \leftarrow \sum_{i=1}^{n} \sigma_i$，则聚合签名为 $\sigma_{\mathrm{agg}} \in G_1$（$n$ 个签名消息可相同）.

5）聚合签名验证. 给定一个聚合签名 $\sigma_{\mathrm{agg}} \in G_1$ 和 n 个消息 $(m_i)_{i=1}^n$ 以及 n 个签名者的公钥 $(Y_i)_{i=1}^n$，如果等式 $e(\sigma_{\mathrm{agg}},P)=\prod_{i=1}^{n} e(H(Y_i \| m_i),Y_i)$ 成立，验证通过.

2　多方合同签署协议

假设 n 个签署者为 $\{P_i\}_{i=1}^n$，对于任意签署者 P_i 拥有两对密钥对 (x_i,Y_i) 和 $(\mathrm{SK}_i,\mathrm{PK}_i)$，分别用于签名验证和加密解密，且公布公钥 Y_i 和 PK_i. 以下不加说明，仲裁者（adjudication）即为离线仲裁者. 与文献[5]中的协议相同，假设 n 个签署者已商榷并同意 m 和 m' $(H(m) \neq H(m'))$ 为具有相同意义的合同. l 表示一次性协议标签（签署者身份、仲裁者身份等相关信息的哈希值）. 同时假设签署者与仲裁者之间的信道为安全信道，签署者之间为不安全信道.

2.1　正常子协议

1）密钥生成. 签署者 P_i 随机选择 $x_i \in Z_q^*$ 作为自己的私钥，并计算 $Y_i=x_iP$ 为公钥. 选择与公钥密码系统 $E_{\mathrm{PK}}(\cdot)$ 相对应的密钥对 $(\mathrm{SK}_i,\mathrm{PK}_i)$，仲裁者的签名验证密钥对为 $(x_{\mathrm{adj}},Y_{\mathrm{adj}})$.

2）凭证签名生成. 仲裁者生成签署者 P_i 的凭证 $V_i \in \{0,1\}^*$. 对于 $V_i \neq V_j(\forall i \neq j)$，仲裁者对每个凭证 V_i 计算其签名为

$$\sigma_{V_i}=x_{\mathrm{adj}}H(V_i \| l \| T_1 \| T_2), i=1,2,\cdots,n$$

其中，$T_1<T_2$ 为 2 个时间戳，T_1 表示凭证签名的有效期，T_1 与 T_2 之间签署者可要求仲裁者执行子协议，在时间 T_2 之后协议将自动终止. 然后选择 n 个随机数 $\{r_i\}_{i=1}^n \in Z_q$，并计算 $S_i=r_iP$，$\Sigma_i=\sigma_{V_i}+r_iY_{\mathrm{adj}}$. 最后仲裁者通过安全信道发送 (S_1,Σ_1,T_1,T_2,l) 给 $P_1,\cdots$，发送 (S_n,Σ_n,T_1,T_2,l) 给 P_n.

3）主协议. 签署者 P_i 收到 (S_i,Σ_i) 后，首先利用其私钥 x_i，通过计算 $\sigma_{V_i}=\Sigma_i-x_iS_i$ 获取凭证签名 σ_{V_i}，并通过检查等式

$$e(\sigma_{V_i},P)=e(H(V_i \| l \| T_1 \| T_2),Y_{\mathrm{adj}})$$

是否成立来验证凭证签名的正确性. 对于合同 $m \in \{0,1\}^*$，P_i 计算消息签名 $\sigma_i=x_iH(Y_i \| m)$ 和消息

-凭证签名 $W_i=\sigma_i+\sigma_{V_i}$. 然后 P_i 利用 PCBP 算法计算 $E_{\overline{P}_i}(W_i\|V_i)$. 最后 P_i 广播发送 $E_{\overline{P}_i}(W_i\|V_i)$ 给其他 $n-1$ 个签署者 $\overline{P}_i$($\overline{P}_i$ 表示除 P_i 之外其他 $n-1$ 个签署者组成的集合). 记作

$$\mathrm{M1}:P_i\Rightarrow\overline{P}_i:E_{\overline{P}_i}(W_i\|V_i)$$

如果 P_i 在 T_1 之前未收到来自其他 $n-1$ 个签署者的全部消息,则 P_i 不发送合同签名,且在时间 T_2 之后安全退出协议. 如果 P_i 在 T_1 之前收到所有来自 $\overline{P}_i$ 的广播消息后,利用 PCBP 算法解密得到其他 $n-1$ 签署者的消息 $\{(W_j,V_j)\}_{j=1,j\neq i}^{n}$, 并检查 $n-1$ 个等式 $\{e(W_j,P)=e(H(Y_j\|m),Y_j)e(H(V_j\|l\|T_1\|T_2),Y_{\mathrm{Adj}})\}_{j=1,j\neq i}^{n}$ 是否全部成立. 只要有 1 个不成立,P_i 不发送合同签名,且在时间 T_2 之后安全退出协议. 否则签署者 P_i 计算合同 $m'\in\{0,1\}^*$ 的签名 $\sigma'_i=x_iH(Y_i\|m')$, 并利用 PCBP 算法计算 $E_{\overline{P}_i}(\sigma'_i)$. 最后,签署者 P_i 广播发送 $E_{\overline{P}_i}(\sigma'_i)$ 给其他 $n-1$ 个签署者 $\overline{P}_i$,记作

$$\mathrm{M2}:P_i\Rightarrow\overline{P}_i:E_{\overline{P}_i}(\sigma'_i)$$

如果 P_i 在 T_1 之前未收到来自其他 $n-1$ 个签署者的全部合同签名消息,则 P_i 运行争端解决子协议. 如果签署者 P_i 收到来自其他全部 $n-1$ 个签署者的广播消息 $\{E_{\overline{P}_j}(\sigma'_j)\}_{j=1,j\neq i}^{n}$,则签署者 P_i 利用 PCBP 算法恢复出其他 $n-1$ 个签署者的签名 $\{\sigma'_j\}_{j=1,j\neq i}^{n}$,并检查等式 $e(\sigma'_j,P)=e(H(Y_j\|m'),Y_{\mathrm{Adj}})(j=1,2,\cdots,n,j\neq i)$ 是否全部成立. 只要有 1 个不成立,P_i 运行争端解决子协议;否则 P_i 计算聚合签名 $\sigma=\sum_{i=1}^{n}\sigma'_i$,聚合签名 σ 即为 n 个签署者的最终合同签名. 任何人都可以通过等式

$$e(\sigma,P)=\prod_{i=1}^{n}e(H(Y_i\|m'),Y_i)$$

验证合同签名的有效性.

2.2 争端解决子协议

如果某个签署者 P_i 在 T_1 之前声称未收到全部其他 $n-1$ 个签署者的合同签名,或者有未通过验证的合同签名,则签署者 P_i 发送消息 l 与 $\{(W_i,m,V_i)\}_{i=1}^{n}$ 给仲裁者,要求执行争端解决子协议,记作

$$P_i\rightarrow\mathrm{adjudicator}:\{l,\{(W_i,m,V_i)\}_{i=1}^{n}\}$$

当仲裁者收到签署者 P_i 的消息 l 和 $(W_i,M,V_i)_{i=1}^{n}$ 后,首先检查 $\{V_i\}_{i=1}^{n}$ 是否是签署者 $\{P_i\}_{i=1}^{n}$ 当前的凭证,且是否在有效期内. 如果不在有效期内,仲裁者拒绝 P_i 的争端解决请求;否则,仲裁者验证 n 个等式

$$\{e(W_i,P)=e(H(Y_i\|m),Y_i)e(H(V_i\|l\|T_1\|T_2),Y_{\mathrm{Adj}})\}_{i=1}^{n}$$

是否全部成立. 如果不全部成立,仲裁者拒绝 P_i 的争端解决请求;如果全部成立,仲裁者计算

$$\{\sigma_i=W_i-x_{\mathrm{adj}}H(V_i\|l\|T_1\|T_2)\}_{i=1}^{n}$$

恢复 n 个签署者 $\{P_i\}_{i=1}^{n}$ 的消息签名. 仲裁者在有效期 T_1 之后 T_2 之前发送 $\{\sigma_j\}_{j=1,j\neq i}^{n}$ 给 $P_i,i=1,2,\cdots,n$,记作

$$\mathrm{adjudicator}\rightarrow P_i:\{\sigma_j\}_{j=1,j\neq i}^{n}$$

3 安全性分析

聚合签名的组成部分包括签署者的消息签名和仲裁者的凭证签名,均利用 Boneh 等[8]提出的短签名方案生成,因此,这些签名能抵抗适应性选择消息攻击下存在性伪造. 除此之外,合同签署协议满足以下 4 个安全性条件.

1) 不可伪造性. 某个签署者 P_i 在没有得到仲裁者凭证签名的情况下,伪造消息-凭证聚合签名 W_i 和合同签名 σ 是困难的;仲裁者独自伪造消息-凭证聚合签名 W_i 和合同签名 σ 是困难的.

引理 1[8] 如果 CoCDH 问题是 (t',ε') 困难的,则对于任意 t、q_S、q_H、ε,BLS 签名方案是 (t,q_S,q_H,ε) 困难的,且满足 $\varepsilon\geqslant e(q_S+1)\varepsilon'$ 和 $t\leqslant t'-t_{\exp}(q_H+2q_S)$. 其中,$e$ 为自然对数,(t,ε) 与 (t',ε') 意义相同;q_H 表示至多进行 q_H 哈希值询问;q_S 表示至多进行 q_S 签名询问.

证明过程参见文献[8].

定理 1 如果 BLS 签名方案是 $(t',q'_S,q'_H,\varepsilon')$ 安全的,则对于任意 t、q_S、$n_{\max}$、q_H、ε,合同签署方案是 $(t,q_S,n_{\max},q_H,\varepsilon)$ 安全的,且满足 $\varepsilon\geqslant\varepsilon'$,$q_S\leqslant q'_S-n_{\max}$,$q_H\leqslant q'_H$ 和 $t\leqslant t'-t_{\exp}(q_H+n_{\max}+1)$. 其中 $n_{\max}$ 为公钥-消息对数,其他符号意义同引理 1.

证明过程参见文献[8].

2) 不透明性. 签署者 P_i 从消息-凭证聚合签名 $W_j(j\neq i)$ 中提取消息 M 的一般签名 σ_j 是困难的.

定理 2[5] 假设存在敌手 $\mathscr{A}$ 至多进行 q_{as} 次自适应消息-凭证聚合签署询问,至多进行 q_{ae} 次自适应消息-凭证聚合签名提取查询,且至多运行时长为 t 的情况下能以大于 ε 的概率从消息-凭证聚合签名中提取消息签名. 则存在算法 $\mathscr{B}$ 在运行时长

为 t'的情况下以大于 ε'的概率解决 CDH 问题，其中

$$\varepsilon \leqslant (e(q_{as}+1))\varepsilon', \quad t \approx t' - (q_{ae}+4q_{as}+1)c_{G_1}$$

证明过程参见文献[5].

由定理 2 可知，给定签署者 P_i 消息-凭证聚合签名 $W_j(j\neq i)$，如果 CDH 问题是难解的，则 P_i 在没有仲裁者的帮助下将无法从签署者 P_j 消息-凭证聚合签名 $W_j(j\neq i)$ 中得到 P_j 的消息签名. 因此多方合同签署协议中的消息-凭证聚合签名是不透明的.

3) 可提取性. 签署者生成消息-凭证聚合签名而仲裁者从中无法提取消息签名是困难的，也就是说，仲裁者从签署者生成的消息-凭证聚合签名中提取消息签名是容易的.

定理 3　多方合同签署协议中签署者的消息-凭证聚合签名满足可提取性.

证明　任意签署者 P_i 的消息-凭证聚合签名为 W_i，验证等式 $e(W_i,P)=e(H(Y_i\|m),Y_i)e(H(V_i\|l\|T_1\|T_2),Y_{\text{adj}})$，有 $e(H(Y_i\|m),Y_i)=e(W_i,P)/e(H(V_i\|l\|T_1\|T_2),x_{\text{adj}}P)$，则仲裁者可以利用自己的私钥 x_{adj} 计算出签署者 P_i 的消息签名 $\sigma_i=W_i-x_{\text{adj}}H(V_i\|l\|T_1\|T_2)$. 因此，多方合同签署协议中签署者的消息-凭证聚合签名满足可提取性.

4) 公平性. 协议在任何情况下结束时，任意签署者都可得到其他 $n-1$ 个签署者的消息签名，或无人得到.

定理 4　多方合同签署协议满足公平性.

证明　不失一般性，假设签署者 P_i 为发起者，可分 2 种情况讨论合同签署协议的公平性：1) 签署者 P_i 已广播发送消息-凭证聚合签名；2) 签署者 P_i 已广播发送消息签名.

情况 1　发起者 P_i 已广播发送合同-凭证聚合签名，由协议的具体过程可知，不管是否有签署者退出，只要 P_i 在 T_1 之前未收到其他全部 $n-1$ 签署者的消息-凭证聚合签名，P_i 不会发送其合同签名. 在此情况下，P_i 只需等到时间 T_2 过后即可安全退出协议. 最坏情况下，其他 $n-1$ 个签署者合谋欺骗 P_i，$n-1$ 个签署者得到的只是 P_i 的消息-凭证聚合签名. 由定理 2 可知，即使 $n-1$ 个签署者合谋也无法从 P_i 的消息-凭证聚合签名中提取合同签名. 如果这 $n-1$ 个签署者想得到 P_i 的合同签名，一是发送各自消息-凭证聚合签名给 P_i，P_i 得到来自其他 $n-1$ 个签署者的消息-凭证聚合签名后发送合同签名，这样其他 $n-1$ 个签署者就得到了 P_i 的合同签名. 而 P_i 在有效期 T_1 内未收到全部其他 $n-1$ 个签署者的合同签名，P_i 可以要求仲裁者执行争端解决子协议来获得其他 $n-1$ 个签署者的合同签名. 二是 $n-1$ 个签署者中某个签署者 $P_j(j\neq i)$ 通过运行争端解决子协议来获取 P_i 的合同签名. 由争端解决子协议可知，仲裁者在发送 P_i 的合同签名给其他 $n-1$ 个签署者的同时也会发送其他 $n-1$ 个签署者的合同签名给 P_i.

情况 2　发起者 P_i 已广播发送其合同签名，此情况可以认定 P_i 收到了来自其他 $n-1$ 个签署者的有效消息-凭证聚合签名. 如果 P_i 在有效期 T_1 之前收到全部其他 $n-1$ 个签署者的消息签名，则合同签署协议成功结束；否则，P_i 在有效期 T_1 之前要求仲裁者执行争端解决子协议来获得其他 $n-1$ 个签署者的合同签名. 此情况下，同样能保证发起者 P_i 的公平性.

由上面 2 种情况分析可知，协议结束后，任意签署者都能得到其他 $n-1$ 个签署者的合同签名，或无有人得到. 因此，多方合同签署协议满足公平性.

4　效率分析

多方合同签署协议中通信主要包括：1) 仲裁者分发凭证签名和有效期等信息给签署者，共为 n 条消息；2) 签署者相互发送合同-凭证聚合签名，为 n 条消息；3) 签署者相互发送最终合同签名，为 n 条消息. 因此，本文所提的多方合同签署协议在签署者诚实的情况下，共需发送 $3n$ 条消息. 如果有争议发生，签名者要求仲裁者介入，增加 $n+1$ 次消息通信，总通信次数为 $4n+1$；最坏情况下，n 个签署者皆发送消息要求仲裁者介入，则总通信次数不超过 $5n$，且随着签署者人数的增加，通信次数呈线性增长. 表 1 所示为新协议与适合异步网络的多方合同签署协议的消息交换次数与交互轮数的对比结果(正常协议阶段).

表 1　消息交换次数与交互轮数对比

协议	消息/次	交互/轮
GM 协议[2]	$O(n^3)$	$O(n^2)$
MR 协议[3]	$n(n-1)(\lceil n/2\rceil+1)$	$\lceil n/2\rceil+1$
MRD 协议[4]	n^2+1	n
本文协议	$2n$	2

(下转第 21 页)