doi:10.11959/j.issn.1000-436x.2015189

基于博弈论的门限签名体制分析与构造

王洁[1,2]，蔡永泉[1]，田有亮[3]
（1. 北京工业大学 计算机学院，北京 100124；2. 山西师范大学 数学与计算机学院，山西 临汾 041004；3. 贵州大学 理学院，贵州 贵阳 550025）

摘 要：为了使门限签名体制更具有普适性，引入了“理性参与人”的概念，将所有参与者视为理性的个体，任何阶段以最大化自身利益为目标。基于博弈论对密钥生成和签名合成阶段各参与者的策略和效用进行了分析，证明了在传统门限签名方案中理性参与者没有动机参与签名，导致无法完成对消息的签名，并提出了理性密钥分发和理性签名合成的解决机制。经分析该方法能更好地满足实际需求。
关键词：博弈论；门限签名；双线性对；BDH 假设；纳什均衡
中图分类号：TP309 **文献标识码**：A

Analysis and construction for threshold signature scheme based on game theory

WANG Jie[1,2], CAI Yong-quan[1], TIAN You-liang[3]
（1. College of Computer Science, Beijing University of Technology, Beijing 100124, China;
2. College of Mathematics & Computer Science, Shanxi Normal University, Linfen 041004, China;
3. College of Science, Guizhou University, Guiyang 550025, China)

Abstract: The concept of “rational player” is introduced to make threshold signature system more general. In this new primitive, all players are regarded as rational individuals in the sense that they always try to maximize their profits as the goal at any phases. Each player’s strategy and utility in key generation and signature synthesis phases are analyzed based on game theory. It is proved that rational players have no motivation to participate in signature in traditional threshold signature scheme, which might cause it impossible to complete threshold signature. Finally, the mechanism of rational key distribution and rational signature synthesis is proposed. Analysis shows the new method is more applicable than the previous schemes in the real-world applications.
Key words: game theory; threshold signature; bilinear pairings; BDH assumption; Nash equilibrium

1 引言

门限签名(threshold signature)是数字签名中的群体签名形式，是现代密码学中一个重要工具。一个 (t,n) 门限签名协议允许签名集合中任意 t 个参与者合作生成某个消息的有效签名；而少于 t 个参与者就无法完成该消息的合法签名。任何一个验证者可以利用签名集合的公钥验证签名的正确性。门限签名中的每个参与者都保留一份签名密钥，可以生成一个子签名，当收集到足够的子签名后，就可以按指定的方式联合生成这个消息的门限签名。门限签名体制可以分散责任，避免滥用职权，有效解决单个成员权力过于集中的问题，大大提高了系统的安全性与健壮性。

1991 年 Desmedt 和 Frankel 首次提出了门限签名方案[1]，由于该方案可以在不暴露秘密密钥的情况下对消息进行签名，引起了密码学研究专家的广泛关注，并取得了一系列研究成果[2~7]。签名是现实生活中经常遇到的一种行为，在某一文件上签名表明作者对该文件的内容负责，或者同意文件的内

收稿日期：2014-10-27；修回日期：2015-01-20
基金项目：国家自然科学基金资助项目(61170221,61363068)；北京市自然科学基金资助项目(1102003)
Foundation Items: The National Natural Science Foundation of China(61170221,61363068); The Natural Science Foundation of Beijing(1102003)

容，并愿意承担相应的责任和义务。近年来随着研究的深入，针对不同的应用场景，各种功能各异的门限数字签名方案被相继提出，主要有前向安全门限数字签名方案[8]、无可信中心门限签名方案[9]、基于身份的在线/离线门限签名方案[10]等。然而现有的门限签名方案仅将参与者分为“诚实的”或者“恶意的”2 种类型：诚实者始终遵守协议，不做任何背离协议的行为；而恶意者则通过欺骗或者其他手段，伪造消息的合法签名而达到某种欺骗目的，即签名者希望最好方式就是在享有签名权利的同时不需要承担相应的责任，体现在门限签名中就意味着参与者希望通过提供一份非法的签名份额而得到整个合法门限签名，一旦出现需要承担相关责任的情况，该参与者将提供其非法的签名份额来证明自己并未真正对该消息进行有效签名。虽然门限签名中可利用各种验证方法检测到参与者的这种欺骗行为，但一般都是在参与者欺骗行为发生之后才能检测到，而此时欺骗者已经得到合成的签名结果。

2004 年 Halpern 和 Teague[11]将博弈论引入了秘密共享和安全多方计算，设计了理性秘密共享和安全多方计算方案，方案中假设每位参与者的行为都是自私的，总是尽最大可能让自己的收益最大化，通过设计随机多轮协议和随机策略来保证理性参与者没有动机偏离协议，有效防止了参与者欺骗，但是该方案仅对 $n \geq 3$ 的情况有效；Gordon 和 Katz 对 Halpern-Teague 协议进行了改进，通过引入测试轮实现了 $n \geq 2$ 的理性秘密共享[12]；Abraham 等考虑了理性参与者合谋欺骗的问题[13]；Maleka 等学者基于重复博弈研究了理性秘密共享问题[14]，用参与者的长远利益来激励理性参与者诚实地执行协议；田有亮等[15]提出“理性第三方”的概念，对一般的秘密共享体制进行了博弈论分析研究，并设计了秘密分发协议和重构协议，使博弈达到更优的纳什均衡；张恩等[16]基于双线性对构造了一个可验证的理性秘密共享方案，能有效检验参与者的欺骗行为。王伊蕾等人[17]讨论了理性两方安全计算的序贯结构，研究了带有序贯均衡的公平性实现问题。可见理性密码学的研究成果，在一定程度上可以弥补传统密码协议的缺陷和不足。

门限签名是秘密共享思想在数字签名中的应用，在签名阶段和签名合成阶段均涉及多个参与者，并且参与者之间是相互不信任的，各参与者进行签名以及签名验证阶段的验证签名的合法性，归根到底，可以视为参与者在行使其签名的“权利”和承担相应的签名“责任”。然而在现实生活中交互的参与者在行使权利的时候可能会受到某些利益的驱动，他们往往会为了追求更高的收益而作出对自己有利的选择，但现有的门限签名方案未对该研究方向进行深入剖析。针对传统门限签名方案中存在的问题，本文将博弈论中“理性参与人”的概念引入到门限签名的研究中，假定所有参与签名者都是理性的，他们希望自己获得最终的签名，同时希望获得签名的人越少越好。从各参与者所享有的“权利”和需承担的“责任”2 方面入手，重点对理性参与者的行为偏好及效用函数进行了分析，并设计相应的密钥分发机制来防止理性密钥分发者的欺骗行为。同时针对签名合成阶段，理性参与者没有动机发送子签名（或发送非法的子签名）的不合作行为问题，设计理性签名合成机制，保证当签名博弈达到纳什均衡时，参与者能够同时获得对消息的签名。

2　基础知识

2.1　双线性对

定义 1　双线性对。[18]设 $(G_1,+)$ 和 $(G_2,\cdot)$ 为 2 个阶数均为素数 p 的循环群，其中前者为加法群，后者为乘法群；令 P 为 G_1 的生成元，称变换 $e: G_1 \times G_1 \to G_2$ 为双线性对，如果满足下面的性质。

1) 双线性。对任意 P_1, P_2 和 $Q \in G_1$ 有 $e(P_1+P_2, Q)=e(P_1,Q)e(P_2,Q)$ 及 $e(Q_2,P_1+P)= e(Q,P_1)e(Q,P_2)$ 成立。

2) 非退化性。存在 $P \in G_1$ 即 $e(P,P) \neq 1$，也就是说 $e(P,P)$ 是 G_2 的生成元。

3) 可计算性。对任意 $P_1, P_2 \in G_1$，存在有效的算法计算 $e(P_1,P_2)$。

定义 2　(BDHP)[18]双线性 Diffie-Hellman 问题 (BDHP) 描述如下：在 (G_1,G_2,e) 中，给定 (P,aP, bP,cP)，对任意的 $a,b,c \in_R Z_q^*$，计算 $e(P,P)^{abc} \in G_2$。

BDH 假设可描述为：在求解 BDH 问题上，没有概率多项式时间算法有不可忽略的优势。

2.2　签名算法及安全性

定义 3　签名。设 $M=\{M_k\}$ 为消息空间，数字签名由 3 个多项式 $(Gen, Sign, Vrfy)$ 算法组成。

1) 密钥生成算法 Gen：输入安全参数 k, 输出一对匹配的公钥和私钥 (pk, sk)。

2) 签名算法 $Sign$：输入一个私钥 sk 以及一个消息 $m \in M_k$，输出签名 σ。

3) 验证算法 $Vrfy$：输入签名 σ、消息 $m\in M_k$ 和公钥 pk，验证签名是否有效。

定义 4 签名的安全性。签名方案在自适应选择消息攻击下的不可伪造性，如果对任意概率多项式时间敌手，其签名伪造的概率为 $\varepsilon(k)$($\varepsilon(k)$ 安全参数 k 的函数）是可忽略的，即

$$\varepsilon_A(k)=\Pr[(pk,sk)\leftarrow Gen(1^k),(m,\sigma)\leftarrow A^{Sign_{sk}}(pk):Vrfy_{pk}(m,\sigma)=1]$$

是可忽略的，则称 $(Gen,Sign,Vrfy)$ 签名方案在自适应选择消息攻击下是不可伪造的。

定义 5 门限秘密分享。给定秘密值 S，t 为门限值，按照一种合理的方式将秘密分割成 n 份,每一份分发给不同的参与者$(P_1,\cdots,P_n)$，任意 $t-1$ 个或者更少的参与者集合互相合作不能揭示 S 的信息，而存在有效算法使任意 t 个参与者合作时就可输出 S，此算法称为 (t,n) 门限秘密分享。

定义 6 门限签名。令 $(Gen,Sign,Vrfy)$ 是一个签名方案,k 是系统参数。相应的 (t,n) 门限签名方案 $(TGen,TSign,Vrfy)$ 由 3 个算法组成。

1) 门限密钥生成算法 $TGen$：输入系统参数 k，n 个成员交互运行，算法返回公钥 pk 以及每个成员的私有输出 x_i，使$(x_1,\cdots,x_n)$构成了 sk 的 (t,n) 门限秘密分享，这里 sk 是与 pk 相匹配的私钥。算法 $TGen$ 中产生的(pk,sk) 与算法 Gen 的输出同分布。

2) 门限签名算法 $TSign$：输入消息 M 和系统参数 k，每个成员拥有私有输入 x_i，算法输出消息 M 的签名。

3) 验证算法 $Vrfy$：输入签名 σ、消息 $m\in M_k$ 和公钥 pk，验证签名是否有效。

定义 7 门限签名方案的安全性。如果以下条件成立，称门限签名方案 $(TGen,TSign,Vrfy)$ 是安全的。

1) 不可伪造性：给定系统参数 k，敌手最多可以攻破 t 个成员，可以拥有算法 $TGen$ 和算法 $TSign$ 交互运行中的视图，可以进行 l 次适应性选择消息的门限签名查询，而最终敌手能产生一个新消息 m 的门限签名的伪造概率是可忽略的。

2) 健壮性：敌手最多可以攻破 t 个成员，算法 $TGen$ 和 $TSign$ 仍然能够成功地运行。

2.3 博弈论相关概念

博弈论是一门以数学为基础，主要研究存在利益冲突的决策主体间在相互对抗和竞争中相互依存的一系列策略和行动集合。

定义 8 博弈。博弈表达的基本式由参与者集合 P、策略空间 S 和效用函数 u 这 3 个要素组成。

$$G=\{P,S,u\} \tag{1}$$

其中，$P=\{P_1,\cdots,P_n\}$, $S=(S_1,\cdots,S_n)$,$u=(u_1,\cdots,u_n)$效用函数为 $u_i:S\rightarrow R$，表示参与者 P_i 在不同策略组合下所得到的收益。

定义 9 纳什均衡。在博弈 $G=\{P,S,u\}$ 中，如果由各个博弈方的各一个策略组成的某个策略组合 $s^*=\{s_1^*,\cdots,s_n^*\}\in S$ 中，任一博弈方 P_i 的策略 s_i^* 都是对其余博弈方策略的组合的最佳对策, 即对于所有的 $s_j\in S$,博弈保持

$$u_i(s_i^*)\geqslant u_i(s_j,s_{-i}^*) \tag{2}$$

则称 $s^*=\{s_1^*,\cdots,s_n^*\}$ 为 G 的一个纳什均衡。

根据定义不难判断，达到纳什均衡状态则意味着在其余参与者都不改变策略的情况下，任何参与者都不愿意打破这一稳定状态，因为参与者单独改变策略不会增加它的效用函数。

3 门限签名方案的博弈论分析

从上面的定义可知，门限签名方案一般分为密钥生成、签名和验证 3 个阶段。本节在传统门限签名方案中引入理性参与者，分析理性参与者行为对实现签名方案的影响以及解决方法，重点分析密钥生成和签名阶段参与者的策略及效用，并进一步构造理性门限签名机制。

3.1 密钥生成的博弈论分析

在传统 (t,n) 门限签名方案中，一般由一个可信中心利用秘密共享方案分发子密钥。然后签名者利用子密钥“行使他们的权利”，对需要签名的消息进行签名，然而在现实中找到一个可信中心是非常困难的，因此在密钥生成阶段, 假设用理性分发者 P_0 取代传统的可信中心，即由 P_0 将签名密钥分发给 n 位理性的参与者，用 $P_i(i=1,\cdots,n)$ 来表示参与者集合，可见理性分发者 P_0 与参与者 P_i 之间是由一个分发者对应一个参与者的 n 对二人博弈。

3.1.1 密钥生成机制分析

下面从博弈的三要素入手来分析分发者和参与者之间的博弈，详细分析如下。

1) 参与者： P_0 和 $P_i(i=1,\cdots,n)$。

2) 策略：理性分发者 P_0 的策略有 2 个，即发

送正确的子密钥和错误的子密钥，分别用 $\{S_{01},S_{02}\}$ 表示；同样参与者 P_i 的策略也有 2 个，即接受子密钥和拒绝子密钥，分别用 $\{S_{i1},S_{i2}\}$ 表示。

3) 效用：对于理性分发者 P_0，用 w_1,w_2,w_3 和 w_4 表示 4 种不同的收益。即 w_1：P_0 发送错误的子密钥 P_i 接收；w_2：P_0 发送正确的子密钥 P_i 接收；w_3：P_0 发送错误的子密钥 P_i 拒绝；w_4：P_0 发送正确的子密钥 P_i 拒绝，由于分发者 P_0 总是希望自己的收益最大，显然有 $w_1>w_2>w_3>w_4$。对于每一个理性参与者 $P_i(i=1,\cdots,n)$ 来说，总是希望收到正确的子密钥而不是错误的子密钥，因此为了防止分发者的欺骗，他需要通过验证协议来验证其子密钥的正确性。对于参与者 P_i，用 v_1,v_2,v_3 和 v_4 来表示相应的收益。即：v_1：P_i 接收正确的子密钥；v_2：P_i 拒绝正确的子密钥；v_3：P_i 拒绝错误的子密钥；v_4：P_i 接收错误的子密钥，显然有 $v_1>v_2>v_3>v_4$。

这种情况和博弈论中经典的“囚徒困境”问题非常类似，通过求解可知 (S_{02},S_{i2}) 是博弈唯一的纳什均衡点，此时的收益为 (w_3,v_3)，因此可得出结论在分发者 P_0 和参与者 P_i 都是理性的条件下，子密钥不能成功分发。因为 P_0 总是倾向于发送错误的子密钥，而参与者 P_i 总是拒绝。显然，对于理性分发者和各参与者来说其最大收益为 (w_2,v_1)，纳什均衡所产生的并不是他们最大收益。下面给出解决该问题的具体机制。

3.1.2 理性密钥分发机制

设 $(G_1,+)$ 和 $(G_1,\cdot)$ 分别为 p 阶加法循环群和乘法循环群，其中 p 为素数;令 P 为 G_1 的生成元，$e:G_1\times G_1\to G_2$ 为双线性对。理性分发者 P_0 想在 n 位参与者间分发签名密钥 $Sig\in Z_q^*$，记理性密钥分发机制 $\Delta=\{\Delta_1,\cdots,\Delta_n\}$：密钥分发者将 $Sig_i=(f(i)=Sig+a_1i+\cdots+a_{t-1}i^{t-1})$ 发送给 P_i，其中 $a_i\in Z_q^*$。具体机制如下。

该机制分为 3 个阶段：理性分发者承诺阶段，理性分发者与参与者交互阶段及理性分发者与参与者间的策略执行阶段。

1) 理性分发者承诺阶段

该阶段分 3 步。

Step1　P_0 随机选取 $Q_0,\cdots,Q_{t-1}\in G_1$ 并保密 $Q_0,\cdots,Q_{t-1}$。

Step2　P_0 计算 $C_0=e(P,Q_0)^{sig}$

$C_1=e(P,Q_1)^{a_1},\cdots,C_{t-1}=e(P,Q_{t-1})^{a_{t-1}}$

Step3　P_0 向各位参与者广播 $C_i(i=1,\cdots,t-1)$。

2) 理性分发者与参与者交互阶段

说明：该阶段通过 P_0 和 P_i 的讨价还价，为他们之间的博弈产生更为有利的博弈结果。在该阶段的讨价还价机制如下。

P_i 做如下讨价还价。

Step1　P_i 告诉 P_0，若 P_0 选择策略 S_{02}，则 P_i 必选择策略 S_{i2}；如果该情况发生，则输出 $flag_i$=0。

Step2　P_i 告诉 P_0，若 P_0 选择策略 S_{01}，则 P_i 必选择策略 S_{i1}；如果该情况发生，则输出 $flag_i$=1。

P_0 做如下讨价还价。

Step3　P_0 告诉 P_i，若 P_i 选择策略 S_{i2}，则 P_0 必选择策略 S_{02}；如果该情况发生，则输出 $flag$=0。

Step4　P_0 告诉 P_i，若 P_i 选择策略 S_{i1}，则 P_0 选择策略 S_{01}；如果该情况发生，则输出 $flag$=1。

3) 理性分发者与参与者间的策略执行阶段

该阶段协议由以下 4 步组成。

Step1　如果 $flag_i$=1，则 P_0 选择执行策略 S_{01}，即 P_0 选择发送正确的子密钥给 P_i。此时，执行如下 2 步。

a) P_0 计算 $Sig_i=(f(i)=Sig+a_1i+\cdots+a_{t-1}i^{t-1})$ 和 $R_i=(G(i)=Q_0+iQ_1+\cdots+i^{t-1}Q_{t-1})$;

b) P_0 秘密发送 (Sig_i,R_i) 给 P_i。

Step2　否则，P_0 执行策略 S_{02}，即 P_0 发送错误的子密钥 (Sig',R') 给 P_i，其中，$Sig'\in Z_q,R'\in G_1$ 被 P_0 随机选取的。

Step3　$flag$=1，则 P_i 执行如下 2 步。

a) 验证

$$e(Sig_i\cdot P,R_i)=\prod_{j=0}^{t-1}C_j^{i2j} \tag{3}$$

是否成立。

b) 若成立，则选择策略 S_{i1}；否则，选择策略 S_{i2}。

Step4　$flag$=0，则 P_i 直接拒觉接收子密钥，选择执行策略 S_{i2}。

由此可得出如下结论。

定理 1　如果分发者和各参与者是理性的，在 BDH 假设下，上述理性密钥分发机制 $\Delta=\{\Delta_1,\cdots,\Delta_n\}$ 能达到最优均衡结果 (w_2,v_1)。

证明　根据理性密钥分发机制的描述，在理性分发者承诺阶段，其承诺 $C_i=e(P,Q_i)^{a_i}$ 保证分发者存在欺骗而获得更大收益的可能。这是因为 $Q_i\in G_1$ 是随机选取的，P 与 Q_i 间的离散对数任何人均不知

道，则理性分发者不可能用 2 种方式打开承诺 C_i，在 BDH 困难假设下，理性分发者若发送一份不合法的子密钥给参与者 P_i，则通过验证的概率是可以忽略的。因此，在该阶段理性分发者以欺骗的方式发送错误子密钥而获得更大的效用概率是可以忽略的。

在讨价还价阶段，理性分发者 P_0 可能存在说假话的可能性。在这种情况下，即 $flag$=1，而他选择策略 S_{02}，根据理性分发者 P_0 与参与者 P_i 间策略执行阶段的协议描述可知，理性分发者 P_0 所发送的子密钥能通过验证的概率是可以忽略的。因此，在该阶段就算理性分发者 P_0 说了假话，他也不可能获得更大的收益，而且说真话导致的收益大于其说假话的收益。因此，一位理性的密钥分发者 P_0 在此阶段的最佳策略是说真话。另一方面，一位理性的参与者 P_i 说真话的收益大于说假话的收益。所以，在该阶段，参与者 P_i 不可能通过说假话获得更大的收益。

综上所述，在该理性密钥分发机制中，对于理性的密钥分发者 P_0 和理性的参与者 P_i 来说，他们的最佳策略是(S_{01}, S_{i1})，从而得到最优的均衡结果 (w_2, v_1)。

3.2 签名合成博弈论分析

在 (t,n) 门限签名方案中，就是将签名的责任被一个由多个签名者组成签名集合分享，至少要有 t 个参与者提供自己的子签名才能生成一份信息的合法签名，而在现实生活对于每个理性参与者来说，他们一般希望行使签名的权利（即可以得到其他参与者代表群体的合成签名），但是不愿意承担由于签名信息所带来的责任（即自己不提供签名信息）。所以，签名合成可以看作一个 n 个参与者之间的博弈。

3.2.1 签名合成机制分析

本节从博弈论的观点来分析门限签名的合成机制，主要从每个参与者在签名合成过程中需要承担的“责任”和及享有的“权利”两方面来分析。首先从博弈的三要素入手，分析参与签名的理性参与者之间的博弈，具体分析如下。

1) 参与者：所有参与签名者 $p_i(i=1,\cdots,n)$。

2) 策略：参与者 P_i 的策略有 2 个，即合作和不合作，用 $\{B,S\}$ 表示，B 表示 P_i 是合作的，提供正确的子签名，S 表示 P_i 不合作，不提供或者提供错误的子签名，因为所有的子签名都可以被公开验证，那么提供错误的子签名将会以很大概率被检测到，因此将这种行为等同于不提供进行处理。

3)效用：在签名合成阶段，与理性秘密共享最后的秘密重构阶段类似，每位理性的参与者都希望自己不出示子秘密而得到秘密，同样对于理性的参与签名的参与者来说，第 1 种情况是，希望在自己不签名的情况下得到其他人代表群体的合成签名，第 2 种情况是，自己提供子签名后得到合成签名；第 3 种情况是，自己不提供签名，最终也不能得到合成签名；第 4 种情况是最坏的情况，自己提供了子签名，而其他参与者未提供导致自己不能得到合成签名。分别用 u_1,u_2,u_3 和 u_4 表示以上 4 种情况下的相应收益，显然有 $u_1>u_2>u_3>u_4$。

针对每个参与者 P_i 的 2 个策略，即合作 B 和不合作 S，下面分别讨论 (t,n) 门限签名体制下，各参与者之间博弈的纳什均衡。

1) 当 P_i 选择 B 时：当有大于等于 $t-1$ 位参与者选择策略 B 时，无论余下参与者选择 B 还是 S，其参与者都能得到合成签名，此时 P_i 的收益是 u_2，其他参与者的收益可能是 u_1 或 u_2；当有小于 $t-1$ 位参与者选择策略 B 时，无论余下参与者选择 B 还是 S，其参与者都不能得到合成签名，此时 P_i 的收益是 u_4，其他参与者的收益是 u_3 或 u_4。

2) 当 P_i 选择 S 时：当有大于等于 t 位参与者选择策略 B 时，无论余下参与者选择 B 还是 S，其参与者都能得到合成签名，此时 P_i 的收益是 u_1，其他参与者的收益可能是 u_1 或 u_2；当有小于 t 位参与者选择策略 B 时，无论余下参与者选择 B 还是 S，其参与者都不能得到合成签名，此时 P_i 的收益是 u_3，其他参与者的收益可能是 u_3 或 u_4。

通过上面的分析很容易看出，当参与者 P_i 选择发送策略 B 时，无论最终能不能得到合成签名，他的收益总是小于等于其他参与者的，而当参与者 P_i 选择不发送策略 S 时，无论最终能不能得到合成签名，他的收益总是大于等于其他参与者的。由此可见，对于理性的签名者来说，他们一定会选择自己收益最大的行为，因此该合成签名博弈达到的纳什均衡将是 $(S,\cdots,S)$，也就是说在签名合成阶段，没有任何一位参与者有动机发送自己的子签名，人人都会等待其他参与者发送子签名，从而自己获得唯一的合法签名，这样导致对消息的签名无法完成，所以传统的门限签名方案在理性环境中并不适用。下面给出解决该问题的方法。

3.2.2 理性门限签名合成机制

基于以上博弈分析，本节从各位参与者认为参

与签名既是一种“权利”，同时也需要从承担相应的“责任”的角度出发，在本文所提出的理性密钥分发方案基础上，构造理性门限签名机制，记为RTSig。

设在该签名合成机制 RTSig 中，共有 l 位理性参与者参与合成签名，其中，$t-1<l<n+1$ 为门限值。该机制是基于 BLS 短签名[19]的门限签名方案，其假设也与该文类似，但该文重点在于论述该理性门限签名合成机制问题。相关假设同基础知识部分，现设需要签名的消息为 m，$H(\cdot)$ 是散列函数，$H(\cdot):\{0,1\}^{*}\to G_1$。每位参与者 P_i 有签名的私钥 Sig_i 及相应的公钥 Pub_i，$0<l<n+1$。在开始合成算法前，每位参与者 P_i 仅拥有自己对消息 m 的签名 $\rho_i=Sig_iH(m)$。

理性门限签名合成机制包括：部分签名分组转发算法和剩余部分签名随机公开算法，具体如下。

1) 部分签名分组转发算法

Step1　随机将 l 位参与签名合成的参与者分成 3 个组，分别记为 A、B 和 C(这里 3 个组的成员要么相同，要么相差一位)。

Step2　A 组的成员向 B 组成员广播他们的签名 $\rho_i, j\in A$。

Step3　B 组的成员通过式(4)验证收到 A 组成员部分签名 $\rho_j, j\in A$ 的合法性。

$$\mathrm{e}(H(m),Pub_i)=\mathrm{e}(\rho_j,P),\forall j\in A \tag{4}$$

如果通过验证，则协议继续；否则，则向 l 位参与者广播“P_i 是欺骗者，不愿承担签名责任，建议剔除 P_i”，重新运行共有剩余 l–1 位参与者执行的部分签名分组转发算法。

Step4　B 组的成员向 C 组成员广播他们的签名 $\rho_j, j\in B$。

Step5　C 组的成员通过如下等式验证收到 B 组成员部分签名 $\rho_j, j\in B$ 的合法性。

$$\mathrm{e}(H(m),Pub_i)=\mathrm{e}(\rho_j,P),\forall j\in B \tag{5}$$

如果通过验证，则协议继续；否则，则向 l 位参与者广播“P_i 是欺骗者，不愿承担签名责任，建议剔除 P_i”，重新运行共有剩余 l–1 位参与者执行的部分签名分组转发算法。

Step6　C 组的成员向 A 组成员广播他们的签名 $\rho_j, j\in A$。

Step7　A 组的成员通过式(6)验证收到 C 组成员部分签名 $\rho_j, j\in C$ 的合法性。

$$\mathrm{e}(\mathrm{H}(\mathrm{m}),Pub_i)=\mathrm{e}(\rho_j,P),\forall j\in C \tag{6}$$

如果通过验证，则协议继续；否则，则向 l 位参与者广播“P_i 是欺骗者，不愿承担签名责任，建议剔除 P_i”，重新运行共有剩余 l–1 位参与者执行的部分签名分组转发算法。

Step8　转发协议结束。

2) 剩余部分签名随机公开算法

Step1　根据在部分签名分组转发算法中 Step1 的分组情况，分别均匀地在 A、B 和 C 3 个组中随机选取 $t-\frac{n}{3}-1$ 位参与者，记 A 组中 a 位，B 组中 b 位和 C 组中 c 位，满足 $t-\frac{n}{3}-1=a+b+c$，并且若 $t-\frac{n}{3}-1/3=0$，则 $a=b=c$；否则，a,b,c 的数量关系满足：若 $|A|-|B|=2$，则 $a-b=1$；其他关系依此类推。

Step2　要求随机选取的 $t-\frac{n}{3}-1$ 位参与者同时向 l 位参与者同时广播他们的子签名。

Step3　收到这些子签名的参与者通过式(4)验证其子签名的合法性。若通过验证，则各位参与者通过拉格朗日插值多项式方法计算合成其签名，协议结束。

Step4　上一步被检查出的欺骗者，各位参与者向全体参与签名合成人员广播“P_i 是欺骗者，不愿承担签名责任，建议剔除 P_i”。

Step5　要求收到上一步中广播错误子签名的签名者的正确子签名人员向大家广播其正确的子签名。

Step6　各参与者计算其合成签名后结束协议。

由此可得到如下结论。

定理 2　如果各参与者是理性的，在 BDH 假设下，上述理性门限签名合成机制 RTSig 能达到最优纳什均衡 $u_2,u_2,\cdots,u_2$。

证明　根据协议机制描述，在部分签名分组转发算法阶段，每位参与者 P_i 将能成功收到 $\frac{n}{3}$ 份部分签名，它共拥有 $\frac{n}{3}+1$ 份部分签名。否则，在这个阶段如果存在参与者 P_i 发送非法的部分签名，在 BDH 困难假设下，P_i 肯定被其他参与者通过式(4)~式(6)中的一个等式不成立检测到。根据方案的设计规则，则 P_i 将被剔除出局。此时，P_i 的最好收益最多

是 u_3，甚至有非常大的可能性是 u_4。因此，对于理性的参与者来说，在该阶段的最佳策略是选择合作，执行策略 B，即给相应分组广播其部分签名。

在剩余部分签名随机公开算法阶段，对于随机选取的参与者 P_i，如果不向所有参与部分签名合成的其他参与者通过广播公开他的部分签名，根据方案设计规则，P_i 将被剔除出局，接下来要求在部分签名分组转发阶段，要求收到其签名的参与者公开 P_i 的部分签名，方案执行结束后，P_i 将得不到最后合成的签名，而其他参与者则能够成功合成最后的签名。因此，在该阶段，如果理性 P_i 采取不合作策略，则他的收益将是 u_4，是所有可能收益中最差的情况。

综述所述，如果 BDH 假设成立，一位理性的参与者 P_i 在 RTSig 机制下，其最佳策略是选择合作，即在协议的 2 个阶段均向相应的参与者集合广播他的部分签名。在这种情况下，参与门限签名合成的参与者的收益均为 u_2。

4 方案性能分析

本节对提出的签名密钥分发机制和签名合成机制的性能进行分析，主要从方案的存储开销、计算开销和通信开销方面与文献[15]进行对比分析。

4.1 理性密钥分发机制性能分析

在计算开销方面，签名密钥分发者主要计算子密钥及其承诺，其计算量与门限签名方案的参与者 n 及其门限 t 有关，计算子密钥的开销主要是 Z_q^* 和 G_1 上的 2 个多项式($f(i)=Sig + a_1 i + \cdots + a_{t-1} i^{t-1}$)和 $R_i=(G(i)=Q_0 + i\,Q_1 + \cdots + i^{t-1} Q_{t-1})$，其计算量包括 t 次乘法运算、t 次数乘运算。其承诺的计算量包括 t 个 G_1 上的对运算。可见，其计算开销与参与者数 n 及其门限 t 成线性关系。这方面与文献[15]相当（因文献[15]未具体实现数学工具，其计算量与相应的实现工具有关）。但是，在文献[15]中需要签名密钥分发者 P_0 与 P_i 间执行安全多方计算协议，因此，本机制的计算量将优于文献[15]中机制的计算量。

在存储开销方面，主要包括公开参数和 2 个多项式系数，公开参数存储量包括 $2t$ 个群 G_1 中元素及 t 个 Z_q^* 中元素的存储量，共为 $5tq$，其中 q 为群的阶。多项式系数的存储量包括 t 个 Z_q^* 中元素存储量及 t 个 G_1 中元素存储量，其存储量为 $3tq$。因此，该方案的总存储开销为 $8tq$，其量均与 n 和 t 成线性关系，并且与具体的实现方法有关，因此，这方面可以认为与文献[15]相当。

在通信量方面，与文献[15]相比较，本文方法增加了讨价还价机制的通信复杂度，该交互需要两轮。文献[15]有执行安全多方计算的通信开销，其交互次数也为 2 轮。因此，从这个角度来说，其通信开销也相当。

综上所述，本文的理性密钥分发机制与文献[15]相比，在存储开销与通信开销不增加的情况下，降低了计算开销。

4.2 理性门限签名合成机制性能分析

本节主要分析签名合成机制中对性能影响最大的通信开销，并与文献[15]进行比较。

在理性门限签名合成机制中，其部分签名分组转发阶段，共需要 3 轮广播通信；其剩余部分签名公开算法阶段，至多需要 2 轮广播通信。因此本文的签名合成机制最多仅需要 5 轮广播通信。而在文献[15]中，在密钥轮分发阶段，共需要 $(n-1)(n-2)$ 轮点对点通信；在其最后阶段，需要 n 轮健忘传输协议。

可见，本文中的方案其通信开销远远优于文献[15]中的通信开销。

5 结束语

本文首先对传统门限签名体制下理性参与者的行为进行了分析，指出在传统的门限签名密钥分发阶段，密钥不能成功分发；在门限签名合成阶段，理性的参与者没有动机合作，即没有动机提供自己的子签名来合成最终的门限签名，或者说他们希望享有签名“权利”，但不愿意承担相应的“责任”，导致所有的参与者均不作为。其次针对以上问题，基于讨价还价模型构造了理性签名密钥分发机制，解决了理性参与者之间的不合作行为；基于随机均匀分组的方法构造了理性门限签名合成机制，该机制能有效保证各参与者在享有签名“权利”的同时，也能承担相应的“责任”。最后对所提机制的安全性和纳什均衡进行了分析。另外，本文的设计思想能为理性密码协议设计提供一种新的构造思路和方法，更加符合实际的应用场景。

参考文献：

[1] DESMEDT Y, FRANKEL Y. Shared generation of authenticators and signatures[A]. Proceeding of Advances in Cryptology-CRYPTO’91[C]. Springer-verlag,1991. 457-469.

[2] HARN L. Group-oriented (*t*, *n*) threshold signature and digital multi signature[J]. IEEE Proceedings Computers and Digital Techniques, 1994, 141(5):307-313.

[3] LI Z C, ZHANG J M, LUO J. Group-oriented (*t*, *n*) threshold digital signature schemes with traceable signers[A]. Electronic Commerce Techniques, the Second International Symposium, ISEC2001[C]. 2001.57-69.

[4] HWANG M, LU E. A practical (*t*, *n*) threshold proxy signature scheme based on the RSA cryptosystem[J]. IEEE Transactions on Knowledge and Data Engineering, 2003, 15(16):1552-1560.

[5] HWANG M S, CHANG T Y. Threshold signatures: current status and key issues[J]. International Journal of Network Security, 2005, 1(3): 123-137.

[6] ALMANSA J, DAMGARD I, NIELSEN J. Simplified threshold RSA with adaptive and proactive security[A]. EUROCRYPT 2006[C]. Petersburg, Russia, 2006. 593-611.

[7] GENARO R, HALEVI S, KRAWCZYK H, *et al*. Threshold RSA for dynamic and ad-hoc group[A]. EUROCRYPT 2008[C]. Istanbul, Turkey, 2008. 88-107.

[8] 芦殿军, 张秉儒, 赵海兴. 基于多项式秘密共享的前向安全门限数字签名[J]. 通信学报, 2009,30(l):45-49.
LU D J, ZHANG B R, ZHAO H X. Forward-secure threshold signature scheme based on polynomial secret sharing[J]. Journal on Communications, 2009,30(1):45-49.

[9] 石贤芝, 林昌露, 张胜元等. 无可信中心下基于身份的门限签名方案[J]. 武汉大学学报(理学版), 2013, 59(2):137-142.
SHI X Z, LIN C L, ZHANG S Y, *et al*. Identity-based threshold signature scheme with non-trusted dealer[J]. Journal of Wuhan University (Science Edition) , 2013,59(2):137-142.

[10] 杨小东,李春梅,徐婷等.无双线性对的基于身份的在线/离线门限签名方案[J]. 通信学报,2013,(8):185-190.
YANG X D, LI C M, XU T, *et al*.ID-based on-line/off-line threshold signature scheme without bilinear pairing[J]. Journal on Communications, 2013,34(8):185-190.

[11] HALPERN J, TEAGUE V. Rational secret sharing and multiparty computation[A]. Proceedings of the 36th Annual ACM Symposium on Theory of Computing[C]. New York: ACM Press, 2004. 623-632.

[12] GORDON D, KATZ J. Rational secret sharing, revisited[A]. Proceedings of SCN 2006[C]. LNCS 4116. Heidelberg: Springer, 2006. 229-241.

[13] ABRAHARN D, DOLEV R, GONEN. Distributed computing meets game theory: robust mechanisms for rational secret sharing and multiparty computation[A]. Proceedings of the 25th ACM Symposium on Principles of Distributed Computing[C]. 2006.53-62.

[14] MALEKA S, AMJED S, PAUDU C. Rational secret sharing with repeated games [A]. Proceedings of ISPEC 2008[C]. LNCS 4991. Heidelberg: Springer, 2008. 334-346.

[15] 田有亮, 马建峰, 彭长根等. 秘密共享的博弈论体制分析[J]. 电子学报, 2011, 39(12): 2790-2795.
TIAN Y L, MA J F, PENG C G, *et al*. Game-theoretic analysis for the secret sharing scheme[J]. Acta Electronica Sinica, 2011, 39(12): 2790-2795.

[16] 张恩, 蔡永泉. 基于双线性对的可验证的理性秘密共享方案[J]. 电子学报, 2012, 40(5): 1050-1054.
ZHANG E, CAI Y Q. A verifiable rational secret sharing scheme based on bilinear pairing[J]. Acta Electronica Sinica, 2012, 40(5): 1050-1054.

[17] 王伊蕾, 郑志华, 王皓等. 满足可计算序贯均衡的理性公平计算[J]. 计算机研究与发展, 2014, 51(7):1527-1537.
WANG Y L, ZHENG Z H, WANG H, *et al*. Rational Fair computation with computational sequential equilibrium[J]. Journal of Computer Research and Development, 2014,51(7):1527-1537.

[18] BONEH D, FRANKLIN M. Identity based encryption from the weil pairing[J]. Extended Abstract in Crypto, 2001, 586-615.

[19] BONEH D, LYNN B, SHACHAM H. Short signatures from weil pairing[J]. Journal of Cryptography, 2004, 17(4): 277-290.

作者简介：

王洁（1977-），女，山西霍州人，北京工业大学博士生，山西师范大学副教授，主要研究方向为信息安全、算法博弈论。

蔡永泉（1956-），男，安徽肥东人，北京工业大学教授、博士生导师，主要研究方向为信息安全、密码学理论与应用。

田有亮（1982-），男，贵州盘县人，博士，贵州大学副教授、硕士生导师，主要研究方向为算法博弈论、密码学与安全协议等。