第 44 卷第 1 期
2012 年 2 月

南 京 航 空 航 天 大 学 学 报
Journal of Nanjing University of Aeronautics & Astronautics

Vol. 44 No. 1
Feb. 2012

防范秘密攻击的安全计算的博弈论实现

罗喜召[1]　钱陪德[1]　朱艳琴[1]　刘建伟[2]

(1. 苏州大学计算机科学与技术学院，苏州，215006；
2. 北京航空航天大学电子信息工程学院，北京，100191)

摘要：在博弈论中，惩罚博弈模拟了参与者试图欺骗但又不想被抓住，即安全计算中秘密攻击者的情形。针对密码学的计算博弈模型，本文对 Halpern 与 Rafael 提出的能否在计算具有成本的惩罚博弈与具有一定威慑度的防范秘密攻击的安全计算之间建立联系的问题给出肯定的回答，提出威慑度为 1/2 的防范秘密攻击的安全是计算博弈中错误可忽略的调解人的通用实现。

关键词：纳什均衡；安全计算；通用实现；计算博弈

中图分类号：TP305　　**文献标识码**：A　　**文章编号**：1005-2615(2012)01-0070-05

Secure Computation Against Convert Adversaries Based on Game Theory

Luo Xizhao[1], *Qian Peide*[1], *Zhu Yanqin*[1], *Liu Jianwei*[2]

(1. School of Computer Science and Technology, Soochow University, Suzhou, 215006, China;
2. Department of Electronic and Information Engineering, Beihang University, Beijing, 100191, China)

Abstract: Punish game in game theory models a situation in which players try to cheat, but not to be caught, i.e., the case in secure computation involving convert adversaries. Based on the computational game model for cryptography, the problem proposed by Halpern and Rafael is solved. The result suggests that secure computation with deterrent 1/2 is a universal implementation of the mediator with negligible error in the computational game theory.

Key words: Nash equilibrium; secure computation; universal implementation; computational game

理性密码学主要研究利用密码学中不存在可信第三方的安全协议取代博弈论中理性参与者之间的可信第三方等问题[1-6]。传统安全计算[7]要求：(1)保密性。除了输出之外，攻击者不能从协议中获取任何其他信息；(2)正确性。输出结果根据指定的设计功能进行分发。传统博弈论[8]没有明确考虑保密性与正确性，而仅要求其保持存在激励时的纳什均衡。博弈论考虑在理性参与者存在的情况下如何保持参与者之间的纳什均衡，而密码学主要考虑如何防范某些攻击，例如半诚实攻击、恶意攻击或者秘密攻击。尽管密码学没有考虑激励措施，它仍是比博弈论更强的概念。

为了模拟计算共有成本的博弈，文献[1]引入了结合密码学的计算博弈。在该框架内，参与者效用不仅与其输入类型相关，而且还依赖于其策略的复杂度；不仅确保参与者具有适当的激励措施利用其输入执行协议，同时还保证其保密性和正确性。

在安全计算环境中防范半诚实攻击并不充分，然而达到防范恶意攻击的代价又太大。因此，文献[9]提出试图欺骗，但又不想被抓住的秘密攻击者概念，而这正对应惩罚博弈中参与者企图获取其他参与者信息但又不想被抓住的行为。因此本文利用

基金项目：国家自然科学基金(61070170)资助项目；江苏省高校自然科学研究计划(08KJB520011)资助项目；苏州市应用基础研究计划(SYJ09024)资助项目；苏州市融合通信重点实验室(SZS0805)；江苏省政府留学基金资助项目及江苏省博士后科研计划(11021135C)资助项目。

收稿日期：2010-10-09；**修订日期**：2010-12-23

通讯作者：钱陪德，男，教授，博士生导师，E-mail：pdqian@suda.edu.cn。

文献[1]提出的针对密码学的计算博弈模型，在计算具有成本的惩罚博弈与具有一定威慑度防范秘密攻击的安全计算之间建立肯定关联，提出威慑度为 1/2 的防范秘密攻击的安全计算是计算博弈中错误可忽略的调解人的通用实现。

1　贝叶斯机器博弈

贝叶斯博弈是不完全信息博弈，指至少存在一个参与者不能确定其他某个参与者的类型，从而也不能确定其效用函数。然而贝叶斯博弈并没有考虑计算成本。当考虑计算成本时，则其称为贝叶斯机器博弈[1]，此时策略被机器代替。

定义 1　贝叶斯机器博弈　贝叶斯机器博弈 G 为$([m],\mathscr{M},T,\Pr,\mathscr{L}_1,\cdots,\mathscr{L}_m,u_1,\cdots,u_m)$，其中 $[m]=\{1,\cdots,m\}$ 为参与者集合，$\mathscr{M}$ 为机器集合，$T\subseteq(\{0,1\}^*)^{m+1}$ 为类型集，其中第 $(m+1)$ 元素为自然的类型，$\Pr$ 为在 T 上的概率分布，$\mathscr{L}_i$ 为复杂度函数，$u_i:T\times(\{0,1\}^*)^m\times\mathbf{N}^m\to\mathbf{R}$ 为参与者 i 的效用函数。

给定贝叶斯机器博弈 G，则在 $T\times(\{0,1\}^\infty)^m$ 上的随机变量 $u_i^{G,\vec{M}}$ 表示如下：

$$u_i^{G,\vec{M}}(\vec{t},\vec{r})=u_i(\vec{t},M_1(t_1;r_1),\cdots,M_m(t_m;r_m),\mathscr{L}_1(M_1,t_1;r_1),\cdots,\mathscr{L}_m(M_m,t_m;r_m))$$

设 $\Pr_U$ 为在 $(\{0,1\}^\infty)^k$ 上的均匀分布。给定空间 X 上的任意分布 $\Pr_X$，用 $\Pr_X^+$ 表示 $X\times(\{0,1\}^\infty)^k$ 上的分布 $\Pr_X\times\Pr_U$。给定 T 上的概率分布 $\Pr$，则参与者 i 关于 $\Pr^+$ 的期望效用为随机变量 $u_i^{G,\vec{M}}$ 的期望，即 $u_i^G(\vec{M})=\boldsymbol{E}_{\Pr^+}[u_i^{G,\vec{M}}]$。因此有以下定义。

定义 2　机器博弈中的纳什均衡[1]　假定贝叶斯机器博弈 G，机器概要为 $\vec{M}\in\mathscr{M}$ 及 $\epsilon\geqslant 0$，若对$\forall\ M'_i\in\mathscr{M}$

$$U_i^G[M_i,\vec{M}_{-i}]\geqslant U_i^G[M'_i,\vec{M}_{-i}]-\epsilon$$

则称 M_i 是对 $\vec{M}_{-i}$ 的 ϵ-最好响应。对$\forall\ i\in[m]$，若 M_i 是 $\vec{M}_{-i}$ 的 ϵ-最好响应，则 $\vec{M}$ 是 G 的 ϵ-纳什均衡。

2　计算博弈的密码学框架

计算博弈的效用涉及到计算的复杂度，参与者的效用函数可能不同并发生改变，因此要求即使参与者效用发生变化，所产生的结果仍然是纳什均衡，即保持其健壮性。

定义 3　计算健壮纳什均衡[1]　设函数 $p:\mathbf{N}\to\mathbf{N}$。若对所有的机器 M 和视图 v 均有：

$$\mathscr{L}'(M,v)<\mathscr{L}(M,v)\leqslant p(\mathscr{L}'(M,v))$$

则称复杂度函数 $\mathscr{L}$ 最多是 $\mathscr{L}$ 的 p-加速。若 $\mathscr{L}'_i$ 最多是 $\mathscr{L}_i$ 的 p-加速，其他保持不变，则 G' 最多是 G 的 p-加速。对任一最多是 G 的 p-加速的博弈 $\widetilde{G}$ 来讲，若 M_i 是 $\vec{M}_{-i}$ 的 ϵ-最好响应，则称 M_i 最多是 G 中 $\vec{M}_{-i}$ 的 p-健壮的 ϵ-最好响应。对$\forall\ i\in[m]$，若 M_i 是 $\vec{M}_{-i}$ 的 p-健壮的 ϵ-最好响应。则称 $\vec{M}$ 是 G 的 p-健壮的 ϵ-均衡。

2.1　联合机器博弈

在多个参与者执行博弈时，存在参与者合谋，即联合博弈的情形。设参与者集合子集$[m]$组成的集合为 $\mathscr{Z}$，对于所有的 $Z\in\mathscr{Z}$，若控制 Z 的参与者以期望获取效用优势但仍不想偏离协议，则称 $\vec{M}$ 为 G 的 $\mathscr{Z}$-安全纳什均衡。机器 M_Z^b 为 Z 中参与者 i 提供真实输入以及 M_i 的输出。在联合机器博弈中，根据联合效用函数，任何合谋都不会比使用 M_Z^b 获得更好的效用。

定义 4　联合机器博弈的纳什均衡[1]　给定多方联合机器博弈 G，机器概要 $\vec{M}$，$Z\in[m]$ 及 $\epsilon\geqslant 0$，若任一联合机器 $M'_Z\in\mathscr{M}$ 均有：

$$U_Z^G[(M_Z^b,\vec{M}_{-Z})]\geqslant U_Z^G[(M'_Z,\vec{M}_{-Z})]-\epsilon$$

则称 M_Z^b 为 $\vec{M}_{-Z}$ 的 ϵ-最好响应。对$\forall\ Z\in\mathscr{Z}$ 均有 M_Z^b 是 $\vec{M}_{-Z}$ 的 ϵ-最好响应，则称 $\vec{M}$ 为 G 是 $\mathscr{Z}$-安全 ϵ-纳什均衡。

2.2　具有调解人的机器博弈

参与者之间的通信还可通过调解人转发信息。具有调解人的贝叶斯机器博弈为$(G,\mathscr{F})$，其中 G 为交互式的贝叶斯机器博弈，$\mathscr{F}$ 为交互式图灵机。为了满足安全计算的博弈论实现，需把传统博弈论的调解人推广到计算博弈情形。参与者诚实提供其输入给 $\mathscr{F}$，若其也愿意使用同样的输入运行 $\vec{M}$，则称 $\vec{M}$ 实现了 $\mathscr{F}$，并称其为标准联合博弈，每个参与者输入时形如 $x_i;z_i$ 的类型 t_i，其中 x_i 表示其输入，z_i 由其所拥有的其他信息组成。若输入均有固定长度 n，则称该博弈为长度为 n 的标准联合博弈。

设 $\Lambda^{\mathscr{F}}$ 为发送 $t=x;z$ 给 $\mathscr{F}$ 并输出 $\mathscr{F}$ 接收到的消息，然后停止的机器。为了满足参与者无论何时使用 $\mathscr{F}$ 也希望使用 $\vec{M}$，则要求：若 $\vec{\Lambda}^{\mathscr{F}}$ 在$(G,\mathscr{F})$中是纳什均衡，则在同样的输入下，运行 $\vec{M}$ 也是纳什均衡。一般来讲，对于任一 $G\in\mathscr{G}$，若 $\vec{\Lambda}^F$ 是$(G,\mathscr{F})$的纳什均衡，则 $\vec{M}$ 也是$(G,\mathscr{F}')$的纳什均衡。

定义 5　通用实现[1]　设 $\mathscr{G}$ 为联合博弈组成，Z 为$[m]$的子集组成。$\mathscr{F}$ 与 $\mathscr{F}'$ 为调解人，$M_1,\cdots,M_m$ 为交互式图灵机，精确度函数 $p:\mathbf{N}\times\mathbf{N}$ 与可忽略函数 $\epsilon:\mathbf{N}\times\mathbf{R}$。对$\forall\ n\in\mathbf{N}$ 任一输入长度为 n 的博

弈 $G\in\mathscr{G}$ 及 $\forall\ \mathscr{Z}'\in\mathscr{Z}$，若 $\vec{\Lambda}^{\mathscr{T}}$ 是 $(G,\boldsymbol{F})$ 中 $p(\cdot)$-健壮的 $\mathscr{Z}'$-安全纳什均衡，且(1)$\vec{M}$ 是 $(G,\mathscr{T}')$ 中的 $\mathscr{Z}'$-安全 ϵ-纳什均衡；(2)对每个类型概要 $\vec{t}$，由 $(G,\mathscr{T})$ 中的 $\vec{\Lambda}^{\mathscr{T}}$ 所确定的行动概要与由 $(G,\mathscr{T}')$ 中的 $\vec{M}$ 所确定的行动概要具有同一分布，则称 $(\vec{M},\mathscr{T}')$ 为 $\mathscr{T}$ 的具有可忽略错误 ϵ 的 $(\mathscr{G},\mathscr{Z},p)$ 的通用实现。

2.3 计算情形

设 $\mathscr{G}^{\vec{\mathscr{T}},\mathrm{poly}}$ 为对所有多项式函数 T 的 $\mathscr{G}^{\vec{\mathscr{T}},T}$ 的并集。若 $\mathscr{L}_Z((\vec{\Lambda}^{\mathscr{T}})^b_Z,\cdot)=\mathscr{L}_Z((M)^b_Z,\cdot)=c_0$，则称 $\mathscr{L}$ 为 $\vec{M}$-可接受的。正如传统安全计算中参与者可能放弃一样，若参与者的输出与 $f(\lambda_Z,\vec{x}_{-Z})$ 保持一致分布(λ 为放弃参与者的输入)，则称 $\vec{M}$ 为 f 的放弃保持计算。

3 具有惩罚的博弈

现实环境中许多情形可描述为参与者选择一些行动惩罚某些参与者欺骗的博弈。文献[9]提出如何防范更加实际的，即试图欺骗但又不想被抓住的秘密攻击者的两方安全协议，在理想模型中不同与一般的两方安全计算[10]主要为：设参与者集合为 $\{P_1,P_2\}$，其中 P_i 表示被攻击者控制。

(1)发送输入给可信方(用 TP 表示)：P_j 总是发送其输入 x_j 给 TP：被 A 控制的参与者或者放弃(此时用特殊的消息 abort_i 代替其输入)或者发送与其输入等长的其他值给 TP(其依赖于 P_i 的真实输入以及 A 辅助输入)。用 $\bar{\omega}$ 表示发送给 TP 的输入。若 TP 收到 P_i 形如 abort_i 的输入，则其发送 abort_i 给 P_j 并停止；若 P_i 发送 $w_i=\mathrm{corrupted}_i$ 给 TP 作为其输入，则 TP 发送 $\mathrm{corrupted}_i$ 给诚实参与者 P_j 并停止；若 TP 接收到上述两种类型的输入，则其忽略 $\mathrm{corrupted}_i$ 消息。

(2)若 P_i 发送 $w_i=\mathrm{cheat}_i$ 给 TP 作为其输入，则①TP 以 ϵ 的概率发送 $\mathrm{corrupted}_i$ 给 A 和 P_j；②TP 以 $1-\epsilon$ 的概率发送 undetected 以及 P_j 的输入给 A。A 依据从 T 所接收到的输出为 P_j 选择输出 y_j 并发送给 TP；TP 接收到 y_j 后，把其发送给 P_j。若 w_j 不为 abort_i，$\mathrm{corrupted}_i$ 或者 cheat_i，则继续。

理想模型中诚实参与者与 A 的输出表示为 $\mathrm{IDEAL}^{\epsilon}_{f,S_{(z)}}(\bar{x},n)$。设 $f:\{0,1\}^*\times\{0,1\}^*\to\{0,1\}^*\times\{0,1\}^*\to$，其中 $f=(f_1,f_2)$，A 为非均匀 PPT 算法，$I\subset\{1,2\}$ 是被 A 控制，π 为计算 f 的两方协议。在参与者输入为 $\bar{x}$，A 的辅助输入为 z 以及安全参数为 n 时，用 $\mathrm{REAL}_{\pi,A_{(z)},I}(\bar{x},n)$ 表示 π 在现实情形中诚实参与者与 A 的输出。

定义 6 设 f 与 π 如上所述，$\epsilon:\mathbf{N}\to[0,1]$ 为可忽略函数，在存在秘密攻击者情况下，若现实模型中的每个非均匀 PPT A，在理想模型中都存在非均匀的 PPT $\boldsymbol{S}$，使得对每个 $I\subset\{0,1\}$ 有：

$$\{\mathrm{IDEALSC}^{\epsilon}_{f,S_{(z)},I}(\bar{x},n)\}_{\bar{x},z\in(\{0,1\}^3),n\in\mathbf{N}}\overset{c}{\equiv}\{\mathrm{REAL}_{\pi,A_{(z)},I}(\bar{x},n)\}_{\bar{x},z\in(\{0,1\}^3),n\in\mathbf{N}}$$

则称 π 以 ϵ 的威慑度安全计算 f。

正如安全计算中可信第三方几乎是不存在的一样，为了参与者之间互相直接交互，需要一个对应于安全信道或者廉价磋商情形下特殊的调解人 comm，其策略是转发消息以及发送者身份给目的接收者。结合上述计算博弈的密码学框架与防范秘密攻击者的两方安全计算协议，有如下结论。

定理 1 假定 f 为两方功能函数，$\mathscr{T}$ 为计算 f 的调节人，$2\vec{M}$ 为计算 f 的机器概要，$\mathscr{Z}$ 为参与者 $\{0,1\}$ 子集组成集合，$\mathscr{L}$ 为有效的复杂度函数以及 p 为精确度函数。若 $\vec{M}$ 是关于秘密攻击者放弃保持且威慑度为 1/2 的 f 的 $\mathscr{Z}$-安全计算且 $\mathscr{L}$ 是 $\vec{M}$-可接受的，则称 $(\vec{M},\mathrm{comm})$ 为 $\mathscr{T}$ 的错误可忽略的 $(\mathscr{G}^{\mathrm{punish}},\mathscr{Z},p)$-通用实现。

4 证 明

本节主要根据上述针对密码学的计算博弈模型对定理 1 进行证明，即威慑度为 1/2 的防范秘密攻击的安全计算是计算惩罚博弈中错误可忽略的调解人通用实现。为了简单化，仅考虑两方博弈 G；同时把其有效用函数划分为没有考虑计算成本的标准博弈 G' 的效用函数以及在每个参与者的复杂度概要上的复杂度函数 u_i^C，即 $u_i(\vec{t},\vec{a},\vec{c})=u_i^{G'}(\vec{t},\vec{a})+u_i^C(\vec{c})$，并称 G' 为嵌入到 G 的标准博弈。

证明：假设 $\vec{M}$ 为 $\mathscr{L}$-精确为 p 的 f 弱 $\mathscr{Z}$-安全计算。因 $\vec{M}$ 计算 f，因此对每个多项式 T 及 $G\in\mathscr{G}^{\vec{\mathscr{T}}}$，在 (G,comm) 中由 $\vec{M}$ 得到的行动概要与由 $(G,\mathscr{T})$ 中 $\vec{\Lambda}$ 所执行得到的行动概要具有一致的概率分布。现在只需对任一多项式 T，证明 $(\vec{M},\mathrm{comm})$ 是 $\mathscr{T}$ 的错误为 ϵ 的 $(\mathscr{G}^{\mathrm{publish}},\mathscr{Z},p)$ 的通用实现。

引理 1 对任一多项式 T，均存在一个可忽略函数 ϵ 满足：$(\vec{M},\mathrm{comm})$ 为 $\mathscr{T}$ 的错误为 ϵ 的 $(\mathscr{G}^{\mathrm{publish}},\mathscr{Z},p)$ 的通用实现。

证明：假定存在输入长度为 n 的博弈 $G\in\mathscr{G}^{\mathrm{publish}}$ 满足：$(G,\mathscr{T})$ 中 $\vec{\Lambda}^F$ 是 $p(n,\cdot)$ 健壮的 $\mathscr{Z}$-安全纳什均衡。接下来证明 $\mathscr{M}$ 在 (G,comm) 是 $\mathbf{Z}$-安全纳什均衡，即对 $\forall\ \mathbf{Z}\in\mathscr{Z}$ 以及 M'_Z，有

$$U_Z^{(G,\mathrm{comm})}(M'_Z,M_{-Z}) \leqslant U_Z^{(G,\mathrm{comm})}(M_Z^b,M_{-Z})+\epsilon(n)$$

采用反证法来进行证明。假定存在多项式 T 以及 $n\in\mathbf{N}$ 使得存在 $M'_Z\in\mathscr{M}^{T(n)}$ 满足:

$$U_Z^{(G,\mathrm{comm})}(M'_Z,M_{-Z}) > U_Z^{(G,\mathrm{comm})}(M_Z^b,M_{-Z})+\epsilon(n) \quad (1)$$

通过构建一个最多是 G 的 $p(n,\cdot)$-加速的博弈 $\widetilde{G}$ 与机器 $\widetilde{M}_Z$ 满足:

$$U_Z^{(\widetilde{G},\mathscr{F})}(\widetilde{M}_Z,\Lambda_{-Z}^{\mathscr{F}}) > U_Z^{(\widetilde{G},\mathscr{F})}((\Lambda^{\mathscr{F}})_Z^b,\Lambda^{\mathscr{F}})_{-Z})$$

从而得出与 Λ^F 是 p-健壮均衡的假设矛盾。

对在廉价磋商中的任何策略 M',在$(\widetilde{G},\mathscr{F})$中构建与其至少具有同样效用的策略 $\widetilde{M}$。

引理 2　对具有策略 M' 的廉价磋商$(G,\mathscr{F})$,存在一个与其效用至少一样的博弈$(\widetilde{G},\mathscr{F})$。

证明:定义调解人博弈$(\hat{G},\hat{F})$($\hat{F}$ 是定义 6 中 TP 的变体),其复杂度函数 $\hat{\mathscr{L}}$ 除 $\mathrm{precise}_{Z,M'_Z,M_Z}(n,\hat{v})=1$ 与 $\mathscr{L}(\hat{M}_Z,\hat{v})\geqslant\mathscr{L}(M'_Z,v)$时 $\hat{\mathscr{L}}_Z(\hat{M}_Z,\hat{v})=\mathscr{L}(M'_Z,v)$之外,都与 $\vec{\mathscr{L}}$ 保持一致。

显然 $\hat{\vec{\mathscr{L}}}$ 弥补了模拟器 $\hat{M}_Z$ 模拟 M'_Z 时产生的负载,即 $\hat{\vec{\mathscr{L}}}$ 使多项式 $\vec{\mathscr{L}}$ 的多项式加速。因除了复杂度函数 $\hat{\vec{\mathscr{L}}}$,外 $\hat{G}$ 与 G 保持一致,因此 $\hat{G}$ 最多是 G 的多项式加速。

下面把 $\hat{M}$ 转换为从未输出特殊消息 corrupted 以及 cheat 的 $\widetilde{M}$。首先,$\widetilde{M}$ 运行 $\hat{M}$;若 $\hat{M}$ 试图输出特殊消息,则 $\hat{M}$ 输出被贿赂参与者的输入。根据定义,提供真实输入获得效用为 1/2;然而,提供 corrupted 的效用为 0,提供 cheat 最多获得 $1/2\times1+1/2\times0$ 的效用,因此 $\widetilde{M}$ 与 $\hat{M}$ 具有至少一样的效用。根据 $\widetilde{G}$ 的构建,因此对任何策略 M'_Z,存在 G 的多项式加速的博弈$(\widetilde{G},\mathscr{F})$,其中 $\widetilde{G}$ 具有与 M' 至少一样的效用。

因 $\vec{\mathscr{L}}$ 为有效的复杂度函数以及 $\vec{u}$ 为被 $T(\cdot)$ 模拟电路计算,可知 D 能够被有效构建。若 $G\in\mathscr{G}$ 是输入长度为 n 的标准博弈且其类型为 $x;z$,需把 $x;z$ 变换为适合 $\Lambda_i^{\mathscr{F}}$ 的 x。若 $i\in Z$,则 $\vec{t}^D=x_i;z_i$,否则 $\vec{t}^D=x_i$。若存在 $\vec{t}\in T$,使得 $z=t_1^D;t_2^D$ 及 $\vec{x}=(2t_1^D;t_2^D)$,则$(\vec{x},z)$为可接受的;若$(\vec{x},z)$是可接受的,则假定 $\vec{t}_{(\vec{x},z)}$为以上述方式确定的 T 元素。若 $\Pr_G$ 为类型概要上的概率分布及$(\vec{x},z)$是可接受的,则 $\Pr(\vec{x},z)=\Pr_G(\vec{t}_{(\vec{x},z)})$;否则 $\Pr(\vec{x},z)=0$。

因 D 与效用函数输出不同,定义概率 D:若 $\mathrm{precise}=0$ 或者$(\vec{x},z))$为不可接受,则 $D(z,(\vec{x},\vec{y},\mathrm{view}),\mathrm{precise})=0$;否则以 $u_Z(\vec{t}_{\vec{x},z},\vec{y},\vec{\mathscr{L}}_Z(M'_Z,\mathrm{view}),\vec{c}_{0-Z})$的概率得 $D(z,(\vec{x},\vec{y},\mathrm{view}),\mathrm{precise})=1$。

因 M'_Z 作为控制 Z 中参与者的攻击者,则由弱精度安全计算可知对上述区分者 D 以及分布 $\Pr$,存在模拟器 $\widetilde{M}_Z$ 满足:

$$\overset{+}{\Pr}(\{(\vec{x},z);D(z,\mathrm{REAL}_{\vec{M},M'_Z}(\vec{x},z),1)\}) - \overset{-}{\Pr}(\{(\vec{x},z);D(z,\mathrm{IDEAL}_{f,\widetilde{M}_Z}(\vec{x},z),\ \mathrm{precise}(n,\mathrm{view}_{f,\widetilde{M}_Z}(\vec{x},z))=1)\}) < \epsilon(n) \quad (2)$$

引理 3　由区分者 D 定义可知

$$U_Z^{(\widetilde{G},\mathscr{F})}(\widetilde{M}_Z,\Lambda_{-Z}^{\mathscr{F}}) \geqslant \overset{+}{\Pr}(\{(\vec{x},z):D(z,\mathrm{IDEAL}_{f,\widetilde{M}_Z}(\vec{x},z),\ \mathrm{precise}(n,\mathrm{view}_{f,\widetilde{M}_Z}(\vec{x},z))=1)\}) \quad (3)$$

证明　首先,设 $a_Z(\vec{t},\vec{r})$与 $a_i(\vec{t},\vec{r})$分别为在给定策略概要,类型概要以及随机串时 Z 以及 Z 中参与者的输出;类似地,设 $\mathrm{view}_{\widetilde{M}_Z}(\vec{t},\vec{r})$与 $\mathrm{view}_{\Lambda_i^{\mathscr{F}}}(\vec{t},\vec{r})$分别为攻击者的视图与不在 Z 中的参与者的视图。

根据上述讨论,对某输入$(\vec{x},z)$,若 $\vec{t}\in T$ 则 $\Pr_G(\vec{t}_{(\vec{x},z)})=\Pr(\vec{t}_{(\vec{x},z)})$;又因 $\mathscr{L}$ 是 $\vec{M}$-可接受的,则对 $i\notin Z$,假定 $\widetilde{\mathscr{L}}_i(\Lambda_i^{\mathscr{F}},\mathrm{view}_i(\vec{t},\vec{r})=\mathscr{L}_i(\Lambda_i^{\mathscr{F}},\mathrm{view}_i(\vec{t},\vec{r})=c_0$,因此:

$$U_Z^{(\widetilde{G},\mathscr{F})}(\widetilde{M}_Z,\Lambda_{-Z}^{\mathscr{F}} = \sum^{\vec{t},r}\overset{+}{\Pr_G}(\vec{t},\vec{r})u_Z(\vec{t},a_Z(\vec{t},\vec{r}),a_{-Z}(\vec{t},\vec{r})),(\widetilde{\mathscr{L}}(\widetilde{M},\mathrm{view}_{\widetilde{M}_Z}(\vec{t},\vec{r}))),\widetilde{\mathscr{L}}(\Lambda_{-Z}^{\mathscr{F}},\mathrm{view}_{\Lambda_{-Z}^{\mathscr{F}}}(\vec{t},\vec{r}))) = \sum^{\vec{x},z,\vec{r}}\overset{+}{\Pr}(\vec{x},z,\vec{r})u_Z(\vec{t}_{(\vec{x},z)},(a_Z(\vec{t}_{(\vec{x},z)},\vec{r}),a_{-Z}(\vec{t}_{(\vec{x},z)},\vec{r})),(\widetilde{\mathscr{L}}(\widetilde{M},\mathrm{view}_{\widetilde{M}_Z}(\vec{t}_{(\vec{x},z)},\vec{r}),c_{0-Z})) \quad (4)$$

因此只需表明对所有的 $\vec{x},z$ 以及 $\vec{r}$,

$$u_Z(\vec{t}_{\vec{x},z},(a_Z(\vec{t}_{\vec{x},z},\vec{r}),a_{-Z}(\vec{t}_{\vec{x},z},\vec{r})),(\widetilde{\mathscr{L}}(\widetilde{M}_Z,\mathrm{view}_{\widetilde{M}_Z}(\vec{t}_{(\vec{x},z)},\vec{r}))),c_{0-Z}) \geqslant \Pr_U(D(z,\mathrm{IDEAL}_{f,\widetilde{M}_Z}(\vec{x},z,\vec{r}),\ \mathrm{precise}(n,\mathrm{view}_{f,\widetilde{M}_Z}(\vec{x},z,\vec{r}))=1)) \quad (5)$$

即可。

若 $\mathrm{precise}(n,\mathrm{view}_{f,\widetilde{M}_Z}(\vec{x},z,\vec{r}))=0$ 时,显然(5)成立;然而,当 $\mathrm{precise}(n,\mathrm{view}_{f,\widetilde{M}_Z}(\vec{x},z,\vec{r}))=1$ 根据区分者 D 的定义,(5)的右边为 $u_Z(\vec{t}_{(\vec{x},z)},(a_Z(\vec{t}_{\vec{x},z},\vec{r}),a_{-Z}(\vec{t}_{\vec{x},z},\vec{r})),(\widetilde{\mathscr{L}}(\widetilde{M},v_Z(\vec{t}_{\vec{x},z},\vec{r}),c_{0-Z}))$,其中 $v_Z(\vec{t}_{\vec{x},z},\vec{r})=\mathrm{view}_{\widetilde{M}_Z}(\vec{x},z,\vec{r})$。因 $\widetilde{\mathscr{L}}$ 是 $\mathscr{L}$ 的多项式加速,当$(\mathscr{L}_Z(\widetilde{M}_Z,\mathrm{view}_{\widetilde{M}_Z}(\vec{t}_{(\vec{x},z)},\vec{r}))\geqslant(\mathscr{L}_Z(M'_Z,v_Z(\vec{t}_{(\vec{x},z)},\vec{r}))$以及 $\mathrm{precise}(n,\mathrm{view}_{f,\widetilde{M}_Z}(\vec{x},z,\vec{r}))=1$ 时,有$(\widetilde{\mathscr{L}}_Z(\widetilde{M}_Z,\mathrm{view}_{\widetilde{M}_Z}(\vec{t}_{(\vec{x},z)},\vec{r}))=(\mathscr{L}_Z(M'_Z,v_Z(\vec{t}_{(\vec{x},z)},\vec{r}))$。因此,式(5)中等式成立。另外,若$(\mathscr{L}_Z$

$(\widetilde{M}_Z, \text{view}_{\widetilde{M}_Z}(\vec{t}_{(\vec{x},z)}, \vec{r})) < (\mathscr{L}_Z(M'_Z \underset{\sim}{,} v_Z(\vec{t}_{(\vec{x},z)}, \vec{r}))$ 时，则有 $(\mathscr{L}_Z(M'_Z, v_Z(\vec{t}_{(\vec{x},z)}, \vec{r})) > (\mathscr{L}_Z(\widetilde{M}_Z, \text{view}_{\widetilde{M}_Z}(\vec{t}_{(\vec{x},z)}, \vec{r}))$。因此由 u_Z 的单调性可知，式(5)成立。

由式(4,5)可知，该引理成立。

同理可得

$$\overset{+}{\Pr}(\{(\vec{x},z): D(z, \text{REAL}_{\vec{M},M'_Z}(\vec{x},z),1)\}) = U_Z^{(G,\text{comm})}(M'_Z, M_{-Z}) \quad (6)$$

由式(2,3,6)可知

$$U_Z^{(\tilde{G},\mathscr{F})}(\widetilde{M}_Z, \Lambda^{\mathscr{F}}_{-Z}) \geqslant U_Z^{(G,\text{comm})}(M'_Z, M_{-Z}) - \epsilon(n) \quad (7)$$

与式(1)联合可知

$$U_Z^{(\tilde{G},\mathscr{F})}(\widetilde{M}_Z, \Lambda^{\mathscr{F}}_{-Z}) > U_Z^{(G,\text{comm})}(M^b_Z, M_{-Z}) \quad (8)$$

因 $\vec{M}$ 与 $\mathscr{F}$ 均完成 f 的计算，因此有

$$U_Z^{(G,\text{comm})}(M^b_Z, \vec{M}_{-Z}) = U_Z^{(G,\mathscr{F})}((\Lambda^{\mathscr{F}})^b_Z, \vec{\Lambda}^{\mathscr{F}}_{-Z} = U_Z^{(\tilde{G},\mathscr{F})}((\Lambda^{\mathscr{F}})^b_Z, \vec{\Lambda}^{\mathscr{F}}_{-Z} \quad (9)$$

由式(8,9)可知

$$U_Z^{(\tilde{G},\mathscr{F})}(\widetilde{M}_Z, \Lambda^{\mathscr{F}}_{-Z}) > U_Z^{(\tilde{G},\mathscr{F})}((\Lambda^{\mathscr{F}})^b_Z, \vec{\Lambda}^{\mathscr{F}}_{-Z} \quad (10)$$

然而(10)与已知 $\Lambda^{\mathscr{F}}$ 是 p-健壮的纳什均衡前提相矛盾，故(1)中假设不成立。则 $\vec{M}$ 在 (G,comm) 中是 $\mathscr{L}$-安全纳什均衡。

由上述论证过程可知定理1成立。

5 结束语

理性密码学的研究问题之一即为可信第三方或调解人在什么情形下被替换或者实现。然而，传统博弈论中并没有考虑计算成本，因此如何建立它们之间的联系是近期密码学与博弈论交叉领域的研究热点。在具有调解人的计算博弈的密码学框架基础上，本文对防范秘密攻击的两方安全计算进行形式化并证明其是计算博弈中错误可忽略的调解人的通用实现。正如文献[1]所提到的，通过考虑关于计算成本的博弈的通用实现，公平性就能够比较容易的获得。因此，在本文工作的基础上对博弈论和密码学的交叉领域继续研究将是主要研究工作之一。

参考文献：

[1] Halpern J, Rafael P. Game theory with costly computation: Formulation and application to protocol security[C]//Editor: Yao A. Proceedings of 1st Innovation in Computer Science. China: Tsinghua University Press, 2010:120-142.

[2] Pass P, Shelat A. Renegotiation-safe protocols [C]//Editor: Chazelle B. Proceedings of 2nd Innovation in Computer Science. China: Tsinghua University Press, 2011:61-78.

[3] Halpern J, Pass R. Algorithmic rationality: adding cost of computation to game theory[J]. SIGecom Exchanges, 2011,10(2):9-15.

[4] Gradwohl R, Livne N, Rosen A. Sequential rationality in cryptographic protocols[C]//Proceeding of 51th Annual IEEE Symposium on Foundations of Computer Science. USA: IEEE Computer Society, 2010:623-632.

[5] Abraham I, Dolev D, Gonen R, et al. Distributed computing meets game theory: robust mechanisms for rational secret sharing and multiparty computation[C]//Proceedings of 25th Annual IEEE Symposium on Principals of Distributed Computing. USA: ACM, 2006:53-62.

[6] Zhang Z, Liu L. Unconditionally secure rational secret sharing in standard communication networks [C]//Editor: Rhee K, Nyang D. Proceedings of the 13th International Conference of Information Security and Cryptography. Koera: Lecture Notes in Computer Science, Springer, 2010:355-369.

[7] Goldreich O, Micali S, Wigderson A. How to play any mental game—a completeness theorem for protocols with honest majority[C]//Proceedings of the 19th Annual ACM Symposium on Theory of Computing. USA: ACM, 1987:218-229.

[8] Forges F. Universal mechanisms[J]. Econometrica, 1990,58(6):1341-1364.

[9] Aumann Y, Lindell Y. Security against covert adversaries: Efficient protocols for realistic adversaries [J]. Journal of Cryptology, 2010,23(2):281-343.

[10] Goldreich O. Foundations of cryptography-volume 1, basic techniques[M]. UK: Cambridge University Press, 2001.