

一种无可信第三方的智力扑克协议

刘 镇¹, 杨晓元^{1,2}, 严波涛¹, 肖海燕¹

(1. 武警工程学院 电子技术系, 西安 710086; 2. 西安电子科技大学 计算机网络与信息安全教育部重点实验室, 西安 710071)

(lliu Zheng@163.com)

摘 要:智力扑克是一种特定场景的安全多方计算, 近些年来, 学术界对智力扑克协议的研究基本都是基于可信第三方的。利用语义安全的加密体制, 结合同步生效签名算法, 巧妙地设计了一种不安全信道下无可信第三方的智力扑克协议。该协议能很好地确保游戏双方的公平性、能有效抵抗重放攻击, 同时还具有不可否认性、不可伪造性和游戏过程可追踪性等优点。

关键词:安全多方计算; 智力扑克协议; 语义安全性; 签名

中图分类号: TP309 **文献标志码:** A

Mental poker protocol without trusted third party

LIU Zhen¹, YANG Xiao-yuan^{1,2}, YAN Bo-tao¹, XIAO Hai-yan¹

(1. Department of Electronic Technology, Engineering College of Armed Police Force, Xi'an Shaanxi 710086, China;

2. Key Laboratory of Computer Network and Information Security of the Ministry of Education, Xidian University, Xi'an Shaanxi 710071, China)

Abstract: Mental poker is a secure multi-party computation solution in specific scene. In recent years, the studies on mental poker protocol in academe are mainly based on Trusted Third Party (TTP). Using the semantic secure encrypt algorithm, combining with the signature algorithm in which the two signatures become effective at the same time, a mental poker protocol without TTP in an unreliable channel was designed. The new protocol can ensure the fairness of game participators and resist the attack of playback, with the advantages of non-repudiation, unforgeability and traceability.

Key words: secure multi-party computation; mental poker protocol; semantic security; signature

0 引言

安全多方计算是指在一个互不信任的多用户网络中, 各用户能够通过网络来协同完成可靠的计算任务, 同时又能保持各自数据的安全性。多年来安全多方计算一直是密码学理论的研究热点, 并取得了一定的成果。但将一般的安全多方计算协议直接应用于特殊情形, 效果并不理想, 因此针对实际的应用情形, 给出有效、安全的特殊安全多方计算协议, 并从理论上给出协议安全性的证明是一项有意义的工作。

扑克游戏是一种广泛流行的游戏。在现实生活中, 游戏双方可以相互监督, 以确保游戏顺利、公平的进行。计算机网络的飞速发展, 使得通过网络, 处于不同地理位置的参与者可以玩扑克游戏, 如何在网络的环境下使游戏双方遵守游戏规则, 确保游戏顺利、公平的进行, 这就是智力扑克协议所要解决的问题。智力扑克协议是一种特殊场景的安全多方计算。

文献[1]中第一次提出了智力扑克协议, 随后智力扑克协议受到了国外专家和学者的广泛关注, 然而在国内除了参考文献[2]和[3]外, 还未见其他有关对智力扑克研究的文献。文献[2]简单介绍了一个的三方智力扑克协议, 同时也指出其采用的 RSA 公钥加密算法存在着消息泄露问题, 文献[3]介绍了 shamir 的双方智力扑克协议, 同文献[3]一样, 该方案也存在着二次方程残余对消息的泄露, 从而导致游戏丧失公平性。同时还发现, 文献[2]的方案中, Alice 知道所有的 $C_i = E_A(M_i)$, 如果她解密 Bob 选给她的牌后发现牌很小, 那么她可以自己重选一张密文牌解密作为自己手中的牌, 并且

只要她选的这张牌和 Bob 手中的牌不重复, Bob 就不会发现, 从而使游戏对 Bob 丧失公平性。另外该方案也不具有不可否认性, 如果游戏一方抵赖, 由于缺乏证据, 无法解决纠纷。文献[4]首次提出利用概率加密算法解决智力扑克协议的公平性, 遗憾的是方案中依然存在着上述缺陷。文献[5]引入可信第3方(Trusted Third Party, TTP)成功解决了上述缺陷。近些年来, 智力扑克协议的研究基本上都是基于 TTP 的, 因为学术界广泛认为采用 TTP 是解决智力扑克协议公平性的最好方法。然而, 扑克作为一种娱乐、休闲游戏, 很多场景并不存在第3方, 更难确保第3方的可信。因此, 如何在无 TTP 介入时实现具有公平、不可否认和保密性质的智力扑克协议具有重要的实际意义。

本文采用语义安全的加密体制, 利用可验证的同时生效签名算法, 设计了一种具有公平、不可否认和保密性质的双方智力扑克协议, 该协议的过程具有可追踪性, 同时还能很好地防止游戏双方伪造扑克牌, 由于比赛过程引入了时间戳, 该协议还能有效抵抗重放攻击。

1 准备知识

1.1 智力扑克游戏简介

假设两个人 A 和 B 通过计算机网络进行扑克游戏比赛, 比赛过程除了扑克牌不是现实中的牌外, 其他都和现实中扑克游戏一样, 比赛中不用第三方做裁判, 发牌者可由任一方担任。为确保游戏的公平性, 发牌过程应满足以下要求:

1) 任一副牌(即发给参赛人员手中的牌)是等可能的。

收稿日期: 2009-01-12; 修回日期: 2009-03-13。 基金项目: 国家自然科学基金资助项目(60842006)。

作者简介: 刘镇(1985-), 男, 湖南衡阳人, 硕士研究生, 主要研究方向: 网络与信息安全; 杨晓元(1959-), 男, 陕西西安人, 教授, 主要研究方向: 网络与信息安全; 严波涛(1983-), 男, 陕西大荔人, 硕士, 主要研究方向: 密码学、隐秘检测; 肖海燕(1985-), 女, 甘肃兰州人, 硕士, 主要研究方向: 密码学、公平交易。

2) 发给 A, B 手中的牌没有重复的。

3) 每人都知道自己手中的牌, 但却不知对方手中的牌。

4) 比赛结束后, 每一方都能发现对方的欺骗行为(如果有欺骗)。

1.2 语义安全性

多项式时间不可区分选择明文攻击的安全性通常简称为 IND-CPA 安全性, 它是由文献[6]首次提出的, 命名为语义安全性。语义安全性意味着密文不会向任何计算能力为多项式有界的敌手泄露有关相应明文的任何有用信息(如果明文的长度不是有用信息)。它对任何已知明文先验知识的攻击者免疫, 等同于密文的不可区分性。文献[2]中对语义安全的密码体制做了深入的研究, 并给出了几种密码体制的语义安全版本, 介于篇幅的关系, 这里不再详细介绍。

1.3 同时生效签名

文献[7]利用阅下信道的思想在随机信息中隐藏了秘密信息 *keystone*, 得以成功利用可验证环签名设计了一种同时生效签名算法, 并用该签名算法构造了一个同时生效签名协议。该协议的签名具有模糊性和不可伪造性、可鉴别性、不可否认性与公平性, 达到了解决公平交换的目的。同时, 该签名协议的参与者就是交易双方, 没有引入第三方。本文仿照文献[7]中的签名协议, 将文献[7]中的签名算法用于智力扑克协议, 很好地解决了智力扑克协议的公平交换问题。签名算法的具体过程介于篇幅的原因这里就不再重述。

2 公平的智力扑克协议

2.1 协议的实现过程

设 $I = \{A, B\}$ 是环成员, 对于 $i \in I$, 有 RSA 公钥密码体制下的公钥 $P_i = (n_i, e_i)$, 私钥 r_i , 函数 $f_i(x) = x^{e_i} \pmod{n_i}$ 是一个单向门限置换, 其逆置换 f_i^{-1} 只有 i 知道, E_k 是一个对称加密算法, 对于任意长度为 l 的密钥 k , 函数 E_k 都是 b 比特长度上的一个置换。定义复合函数: $C_k(y_1, y_2) = E_k(y_1 \oplus E_k(y_2))$, H 为输出是 l 比特长度的哈希函数, sig_i 是 i 的普通签名函数, pro_i 是一个承诺函数, $keystone_i$ 是 i 私有秘密信息, ENC_{K_i} 是一个语义安全的加密算法, ENC_{K_i} 满足交换律(即对于任意消息 M , $ENC_{K_A}(ENC_{K_B}(M)) = ENC_{K_B}(ENC_{K_A}(M))$), DNC_{K_i} 是相应的解密算法, K_i 为 i 的密钥。比赛开始前 A, B 商量好用于表示一副牌(为了表述简单方便, 这里设一副牌 3 张)的消息 w_1, w_2, w_3, T 为时间戳, \parallel 为比特连接, 比赛过程给每人发 1 张牌。注意: 游戏的步骤 4 后, 由于发给双方的牌已经确定或部分确定, 并且游戏的参与方已经部分或完全知道了自己的牌, 因此主动退出游戏方视为认输。

步骤 1 A, B 分别对 $keystone_A, keystone_B$ 做出承诺 $pro_A(keystone_A), pro_B(keystone_B)$ 。对于 $i = 1, 2, 3, B$ 计算 $ENC_{K_B}(sig_B(w_i \parallel T))$, 设 $m_i = w_i \parallel ENC_{K_B}(sig_B(w_i \parallel T)) \parallel T$, 将 $(m_i, sig_B(m_i))$ 发送给 A 。

步骤 2 A 先检验时间戳 T 是否正确以及验证消息是否被篡改, 如果 T 不正确或者消息被篡改, 则通知 B 重传或者终止游戏, 否则 A 将 $(m_i, sig_B(m_i))$ 重新随机排列得到 $(m_{j_i}, sig_B(m_{j_i}))$, 其中 $1 \leq j_i \leq 3$, 对于 $i = 1, 2, 3, A$ 计算 $m_i = ENC_{K_A}(w_{j_i} \parallel sig_A(w_{j_i} \parallel T) \parallel ENC_{K_B}(sig_B(w_{j_i} \parallel T))) \parallel T$, 将 $(m_i, sig_A(m_i))$ 发送给 B 。

步骤 3 B 先检验时间戳 T 是否正确以及验证消息是否被篡改, 如果 T 不正确或者消息被篡改, 则通知 A 重传或者终止游戏, 否则 B 从 3 个 $(m_i, sig_A(m_i))$ 中随机选择 1 张密文牌

记为 $(m_j, sig_A(m_j))$, 其中 $1 \leq j \leq 3$, 并根据文献[7]中的同时生效签名算法利用 $keystone_B$ 计算 m_j 的同时生效签名 $\sigma_1 = (P_B, P_A; v; x_B, x_A)$, 并将 (m_j, σ_1) 发送给 A 。

步骤 4 A 验证签名 σ_1 是否有效, 如无效, 则要求 B 重传或者转步骤 11 解决纠纷, 否则, 对 m_j 解密, 得到 $w_j \parallel sig_A(w_j \parallel T) \parallel ENC_{K_B}(sig_B(w_j \parallel T))$, 并保存 σ_1 。

步骤 5 B 从剩下的 2 个 $(m_i, sig_A(m_i))$ 中随机选择 1 张密文牌记为 $(m_k, sig_A(m_k))$, 其中 $1 \leq k \leq 3$, 显然有 $k \neq j$, 根据 $m_k = ENC_{K_A}(w_k \parallel sig_A(w_k) \parallel ENC_{K_B}(sig_B(w_k \parallel T))) \parallel T$ 计算 $m_k' = ENC_{K_B}(ENC_{K_A}(w_k \parallel sig_A(w_k) \parallel ENC_{K_B}(sig_B(w_k \parallel T)))) \parallel T$, 并将 $(m_k', sig_B(m_k'))$ 发送给 A 。

步骤 6 A 先检验时间戳 T 是否正确以及验证消息是否被篡改, 如果 T 不正确或者消息被篡改, 则通知 B 重传或者转步骤 11 解决纠纷(注意, 此时 A 不能主动退出游戏, 否则视为认输), 否则根据 m_k' 计算 $m_k = ENC_{K_B}(w_k \parallel sig_A(w_k) \parallel ENC_{K_B}(sig_B(w_k \parallel T))) \parallel T$, 并根据文献[7]中的同时生效签名算法计算 m_k 的同时生效签名 $\sigma_2 = (P_B, P_A; v'; x_B', x_A')$, 其中 $x_B' = x_A$, 将 (m_k, σ_2) 发送给 B 。

步骤 7 B 验证时间戳 T 是否正确、签名 σ_2 是否有效以及 $x_B' = x_A$ 是否成立, 如有一项验证不通过, 则要求 A 重传或者转步骤 11 解决纠纷(注意, 此时 B 不能主动退出游戏, 否则视为认输), 否则, 对 m_k 解密, 得到 $w_k \parallel sig_A(w_k \parallel T) \parallel ENC_{K_B}(sig_B(w_k \parallel T))$, 并保存 σ_2 , 其中 $w_k \parallel sig_A(w_k \parallel T)$ 为 B 的牌, 然后 B 公开 $keystone_B$ 。

步骤 8 A 计算 $m_j = ENC_{K_A}(w_j) \parallel ENC_{K_A}(ENC_{K_B}(sig_B(w_j \parallel T))) \parallel T$, 并根据文献[3]中的同时生效签名算法利用 $keystone_A$, 计算 m_j 的同时生效签名 $\sigma_3 = (P_A, P_B; v; x_A, x_B)$, 并将 (m_j, σ_3) 发送给 B 。

步骤 9 B 验证时间戳 T 是否正确以及签名 σ_2 是否有效, 如有一项验证不通过, 则要求 A 重传或者转步骤 11 解决纠纷, 否则根据 m_j 计算 $m_j' = ENC_{K_A}(w_j) \parallel ENC_{K_A}(sig_B(w_j \parallel T)) \parallel T$, 并根据文献[3]中的同时生效签名算法计算 m_j' 的同时生效签名 $\sigma_4 = (P_A, P_B; v'; x_A', x_B')$, 其中 $x_A' = x_B$, 将 (m_j, σ_4) 发送给 A 。

步骤 10 A 验证时间戳 T 是否正确、签名 σ_4 是否有效以及 $x_A' = x_B$ 是否成立, 如有一项验证不通过, 则要求 A 重传或者转步骤 11 解决纠纷, 否则, 对 m_j' 解密, 得到 $(w_j \parallel sig_B(w_j \parallel T))$, 并保存 σ_4 , 其中 $(w_j \parallel sig_B(w_j \parallel T))$ 为 A 的牌, 然后 A 公开 $keystone_A$ 。

步骤 11 如果 A, B 发生纠纷, 则 A, B 分别公开承诺 $pro_A(keystone_A), pro_B(keystone_B)$, 并出示自己的证据 $\sigma_1, \sigma_2, \sigma_3, \sigma_4, A, B$ 或者任意第 3 者都可以验证是谁作弊。

2.2 协议分析

2.2.1 正确性

如果游戏双方都是诚实的, 根据协议的过程, A 在协议的步骤 10 可以得到自己的牌 $(w_j \parallel sig_B(w_j \parallel T))$, B 在协议的步骤 7 可以得到自己的牌 $w_k \parallel sig_A(w_k \parallel T)$, 显然该协议是正确的。

2.2.2 安全性

该协议的安全性体现在以下几点

1) 该协议能确保游戏双方的公平性。

证明 下面证明协议满足公平性的四个要求。

① 任一副牌(即发给参赛人员手中的牌)是等可能的。

协议的步骤 2, A 对 B 发过来的牌进行随机洗牌, 然后对每张牌用自己的密钥加密后发给 B , 由于加密函数是语义安全的, 密文不会泄露明文的任何信息, 所以在协议步骤 3, B 并不知道 3 张

牌的任何有用信息,所以只能随机选取一张发给A,A得到任何一张牌的概率都为 $1/3$,而B在协议的步骤5,同样只能从剩下的两张牌中任选一张发送给A作为将要发给自己的牌,他得到任何一张牌的概率也为 $(1 - 1/3) \times 1/2 = 1/3$ 。协议步骤5后,发给A,B的牌就都确定了,下面只是对发给各自手中的密文牌解密的过程,只要协议继续进行,最终,A,B得到任何一张牌的概率都为 $1/3$,即发给他们俩的牌是等可能的。

② 发给A、B手中的牌没有重复。

协议的步骤2,如果A伪造两张相同的牌加密后发送给B,由于发给他们俩的牌都是B随机选取的,因此这对他并没有什么好处,显然A不会这么做,另外,即使A想要伪造,由于他无法伪造B对牌的签名信息,伪造的结果也只能是使他自已得不到有效的牌,而协议的步骤3后,所有过程都是可追踪的,B能很容易发现他的作弊行为。

如果B在协议的步骤5选择一张和A一样的牌作为发给自己的牌,那么在玩牌过程中必然产生纠纷,在协议的步骤11解决纠纷时,A,B都公开承诺,由于协议步骤5后双方交换信息的都是带证据的不可否认交换,而在协议的步骤5,A得到了B发给他的消息的证据(普通签名),B不可否认,只要要求B将步骤5的消息解密就能发现B作弊。

协议的步骤5后发给A,B的牌就已经确定,随后进行的过程都是相互解密的过程,因此发给A,B手中的牌没有重复的。

③ 每人都知道自己手中的牌,但却不知对方手中的牌。

协议的步骤2时,A进行了洗牌,然后用自己的密钥加密发给B,确保了B在发牌时,不知道任何一张牌的有用信息,协议的步骤2后,发给A或者B的牌,始终都是以用自己的密钥加密的保密状态出现在对方面前,所以双方都不会知道对方的牌。

④ 比赛结束后,每一方都能发现对方的欺骗行为(如果存在欺骗)。

协议的步骤11,A,B都公开自己的承诺后,协议的消息交换过程变成了带证据点不可否认交换,协议的过程具有可追踪性,任何一方的欺骗行为很容易被发现。

2) 能有效地抵抗重放攻击。

证明 由于协议的每一步传输的消息上都有时间戳 T ,并附着着包含 T 的消息的数字签名,伪造或者篡改 T ,很容易被发现,并且每张有效的牌都含有时间戳 T 的数字签名,不同比赛回合的同一张牌,其后面的签名信息都不一样,因此我们的协议能很好地抵抗重放攻击。

3) 协议双方都不能伪造自己的牌而不被对方发现。

证明 协议中,每张有效的牌是由A,B事先商量好的用来表示牌的信息的 w_i 和对方对 $w_i \parallel T$ 的数字签名两部分组成,可以看出,在协议的执行过程中,对于任意一方,除了发给他的那张牌中对方的签名信息最后可以获得外,其他所有牌的签名信息始终是以密文的形式出现在他面前的,并且加密算法是语义安全的,他无法获得除发给他的那张牌以外的任何一张牌的签名信息,同时,由于签名引入了时间戳,不同回合同一张牌的签名信息不一样,他也不能根据先前的玩牌经历得到任何一张牌的签名信息,因此他不可能成功地伪造自己的牌而不被对方发现。

4) 协议具有不可否认性和保密性。

证明 保密性。协议除了步骤1,用来表示牌的信息的 w_i 是以明文的形式在链路上传输外,链路上传输的其他任何信息都是以密文的形式传输,而每张牌是由 w_i 和对 $w_i \parallel T$ 的数字签名两部分组成,仅知道 w_i 并无多大作用,如果对保密

性要求非常高,也可以在协议的步骤1中,B将 w_i 用A的公钥加密传输给A。因此该协议对链路具有保密性,而协议双方之间的保密性体现在游戏的公平性中。

5) 协议过程具有可追踪性。

证明 在协议的步骤1和步骤2,A,B之间只是在为下面的发牌做准备,他们之间并未交换有关要发给自己或者对手的牌的任何有用信息,因此我们不考虑它的可追踪性。从协议的步骤3开始,除协议的步骤5外,所有信息都以附带同时生效签名作为证据的形式传输,由参考文献[7]知,当秘密信息 $keystone$ 公开后,该签名具有可鉴别性和签名双方不可否认性,而协议中游戏的开始A,B都对自己的 $keystone$ 做出承诺,能确保 $keystone$ 被公开。而在协议的步骤5传输的消息不会泄露给接收方任何有用信息,接收方不会否认,我们采用的普通签名,确保发送方不可否认。因此协议的整个过程具有可追踪性。

2.2.3 效率

该协议共需A,B双方进行7次通信,比文献[5]多,在计算方面,消耗计算资源的主要是加解密运算和A,B对 $keystone$ 的承诺,由于该协议没有用到非常耗时的模指数运算,计算效率不会太低。由于该协议不需可信第三方介入,以较低的效率牺牲带来较高的安全性是值得的。与文献[5]比较的具体情况见表1。

表1 文献[5]方法的比较

方法	游戏 玩家	TTP	广播通 信次数	点对点 通信次数	主要耗时 的运算
本文	2	无	无	7	加解密与承诺
文献[5]	3	有	10	3	加解密

3 结语

语义安全的密码体制由于其密文不会泄露明文的任何有用信息,近些年来在密码界备受重视。本文对安全多方计算的特殊应用进行了研究,根据智力扑克游戏的安全性要求,利用语义安全的加密算法并结合同时生效签名算法,巧妙地设计了一种不安全信道下无需TTP的双方智力扑克协议,该协议能很好确保游戏双方的公平性,能有效抵抗重放攻击,同时还具有保密性、不可否认性、不可伪造性和可追踪性等优点。

参考文献:

- [1] SHAMIR A, RIVEST R, ADLEMAN L. Mental poker[EB/OL]. [2008-11-12]. <http://people.csail.mit.edu/rivest/Shamir-RivestAdleman-MentalPoker.pdf>.
- [2] MAO WENBO. Modern cryptography: Theory and practice[M]. 王继林, 伍前红, 译. 北京: 电子工业出版社, 2004: 316-323.
- [3] SCHNEIER B. Applied cryptography: Protocols, algorithms, and source code in [M]. 吴世忠, 译. 北京: 机械工业出版社, 2000: 65-66.
- [4] GOLDWASSER S, MICALI S. Probabilistic encryption and how to play mental poker keeping secret all partial information[C]// Proceedings of the 18th ACM Symposium on the Theory of Computing. New York: ACM, 1982: 270-299.
- [5] FORTUNE S, MERRITT M. Poker protocols[C]// Advances in Cryptology: Proceedings of Crypto'84. Berlin: Springer-Verlag, 1985: 454-466.
- [6] GOLDWASSER S, MICALI S. Probabilistic encryption[EB/OL]. [2008-11-10]. <http://groups.csail.mit.edu/cis/pubs/shafi/1984-jess.pdf>.
- [7] 贾仁超, 寇卫东, 刘景伟. 一种基于可验证环签名的同时生效签名[J]. 计算机工程与应用, 2006, 42(33): 56-57, 61.