

基于博弈论的安全多方计算的研究

张兴兰, 郑炜

(北京工业大学信息学部, 北京 100124)

摘要: 在经典的百万富翁协定中, 参与者其中之一获取到财产大小的结论后, 有可能不告诉另外一个参与者, 也可以不遵守这个协议, 结合博弈论可以避免这个问题, 一个参与者一定会选择做出对自己有利的决定, 因此, 可以设计一个协议, 遵循这个协议的参与者获得的利益大于背离这个协议的利益。目前, 基于博弈论的问题计算效率较低, 该协议通过引入一个二叉树大大提高了计算效率。

关键词: 博弈论; 百万富翁问题; 安全多方计算; 排序二叉树

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018010

Research on security multi-party computing based on game theory

ZHANG Xinglan, ZHENG Wei

Department of Information Science, Beijing University of Technology, Beijing 100124, China

Abstract: In the classic millionaire agreement, one party can get the final wealth comparison results, you can not tell the other party, you can not comply with this agreement, combined with game theory can avoid this problem, you can make the participants away from the agreement proceeds less than compliance with the agreement, compliance with the agreement is the optimal strategy for the participant. At present, the problem of computational efficiency based on game theory is low, and the protocol greatly improves the computational efficiency by introducing a binary tree.

Key words: game theory, millionaire problem, secure multi-party computation, binary sort tree

1 引言

多方安全计算指在一个参与者都不信赖彼此的环境中, 每位参与者通过网络共同完成各种计算任务的同时又不会泄露自己的数据^[1]。这里面的安全指既能够通过计算得到正确的结果, 又不会让别的参与者得知输入的各种隐私信息。多方安全计算在生活中随处可见, 尤其是在现在这个互联网时代, 如在网上的拍卖会, 网络上的投票

系统^[2]等。

在文献[3]中, Yao 首先提出了百万富翁比较财产多少的问题, 在 2 个人不告诉对方财产数额的前提下, 比较出谁更有钱。在文献[4,5]中, Goldreich 等设计出了一个通用性高的多方安全计算协议。在文献[6]中, 冯登国等设计了一个有半诚实第三方的两方安全比较协议。在文献[7]中, 李顺东等运用不经意传输协议, 设计出了一种有效的两方安全比较协议。在文献[8,9]中, 作者利用半诚实的

收稿日期: 2017-10-22; 修回日期: 2017-12-09

通信作者: 郑炜, sj.bill@qq.com

基金项目: 国家自然科学基金资助项目 (No.10007016201201)

Foundation Item: The National Natural Science Foundation of China (No.10007016201201)

模型，分别对数据库中的隐私数据和网络空间中认证的策略进行了深入的理论研究。综上可知，当前很多研究运用都是的半可信模型。文献[10]设计出了一个实际应用具有局限性的多方计算方案。所以，大多数人所设计的协议都有一些片面，因为一个参与者曾经也许没有背叛过协议，但是当他能够获得非常大的利益时，也许他就不会像曾经那样严格遵守协议了。因此，不从利益的角度考虑是片面的。

借助博弈论思想，可以实现在传统的协议中很难实现的公平性。文献[11]提出了一个思想，当人们无法预测何时得到计算结果时，他们会非常乐于去遵循协议。Naor等^[12]为了使参与者严格地遵守协议的约定，引入了博弈论的相关概念。但该方案设计比较复杂。在文献[13]中，Amjed设计了一个引入博弈论的方案，但是这个方案要求生成的多项式的幂次数之间的差值必须不大于1，具有局限性。文献[14,15]需要在使用的時候提供一些物理性的材料，如信件等，不利于应用。在文献[16]中，同时考虑了善意的参与者和具有攻击性的参与者，在这个基础上，设计出了一种新的理性安全多方计算的方案。

在传统密码协议中，一般会从具有攻击性的参与者和诚实参与者2个角度设计协议，这样是不够全面的，因为利益也会影响参与者的行为，因此博弈论的思想在信息安全上越来越重要。现阶段，已经有很多结合了博弈论思想的方案。

当前，已经有安全计算协议与博弈论结合的模型。但是参数过于简单单一，只考虑了参与者攻击成功与否所获得的收益，并没有考虑攻击所要耗费的各种代价，而且在所设计的密码协议中需要进行多轮计算，计算效率很低，因此分析不具有全面性和一般性，计算繁琐。

本文引入多个参数，从多个角度考虑，构建一个具有一般性和全面性的博弈模型，在此基础上，引入一个二叉树在不暴露参与者信息的同时简化计算过程，提高运算效率。

2 背景知识及博弈模型分析

2.1 背景知识

排序二叉树：一种具有特殊性质的二叉树，

它拥有如下特质。

1) 当左子树不是空的时候，左子树上的所有值都会小于该左子树的根节点的值。

2) 当右子树不是空的时候，右子树上的所有值都会大于该右子树的根节点的值。

3) 这个节点的左子树和右子树也都是排序二叉树，具有上述特质。

安全两方计算：其解决了在一个陌生环境中互相都不信赖的所有参与者之间的计算问题，在保证计算准确性的同时，又不会泄露参与者的个人秘密输入。例如，参与者A和参与者B分别输入了自己的数据X和Y，计算 $\mathcal{F}(X,Y)$ ，计算结束后，参与者A和参与者B都会得到正确的结果，并且A和B并不知道对方所输入的数据。

公平性：在进行安全两方计算时，如果其中的参与者都成功地得到了计算结果，或者全都没有成功地获得计算结果，那么这个协议就是公平的。

博弈论：其主要目的是为了深入研究参与者之间在存在利益冲突的情况下，根据对方所做出决定的不同而做出不同的决定，理性的参与者总是会做出最优的决定。

纳什均衡：当参与者之间在相互对抗相互依存的时候，形成各个参与者的当前选择都是最优选择时的一种稳定状态。

左0右1编码：是指从根节点开始，如果要编码的节点在根节点左子树上，则记下一个0，如果在根节点的右子树上，则记下一个1，然后进入要编码节点所在的子树，进行上述过程，直到子树就是该节点自己，按先后顺序组合成只含有0和1的序列，这个序列就是该节点的编码。

2.2 博弈模型分析

攻击者以概率 ε 攻击成功，这意味着攻击者可以提前知道所比较的大小而不必在履行协议。

攻击者以 $1-\varepsilon$ 概率攻击失败，但是它成功地进行了一次猜测，也增加了随后猜测成功的概率，这将鼓励攻击者继续发起下一次猜测。

在本文所设计的模型中，让不执行协议的参与者或者计划猜测正确值的参与者能得到的利益非常小，远小于一个善意的并且积极遵守协议的参与者的利益。其主要思想在于以一定概率传输无用数据来混淆能够判断出比较结果的核心元素。

如果攻击者想要发起攻击行为,从3个角度进行考虑。

1) 具有恶意参与者攻击成功的概率是 ε ,得到了 F 的回报。

2) 具有恶意的参与者攻击失败的概率是 $1-\varepsilon$,由于攻击的损耗,所以得到了 G 的回报。

3) 参与者并没有发起任何攻击,他会得到 H 作为回报。

根据情况分析, $F>H>G$ 。

之前在设计博弈论模型的时候,一般只考虑攻击者发起攻击所得到的利益,从而忽略了恶意攻击者在进行攻击的时候,准备阶段的人力物力以及攻击阶段的计算耗费等消耗,但往往在实际生活中,具有恶意的攻击者也会将攻击成本作为一个重要的参考,因此以往的博弈论模型考虑的并不全面。

本文从两名参与者相互博弈的角度考虑,全面引入了协议参与者不同情况下所获得的利益。

表1的博弈模型支付矩阵中的参数都是整数, E_A 表示参与者发送数据时的能量消耗, E_I 表示恶意参与者发起攻击时的消耗;由于恶意参与者成功发起攻击时,诚实参与者必然会有损失,损失为 C_A^+ ;假定发送数据的总个数为 N ,那么一个恶意参与者发动攻击的成功概率为 ε ,即 $\frac{1}{N}$;恶意参与者成功发起了攻击,因此不必在履行协议,因此他的收益为 U^+ ; U^- 为恶意参与者发动攻击,但是没有成功时的获益;恶意参与者严格履行协议不发动攻击时的获益为 U ,显然 $U^+>U>U^-$ 。上面提到的参数与真实应用场景相关。

表1 博弈模型

诚实参与者	攻击者	
	发起攻击	不发动攻击
传送无用数据	$U_A - E_A - \varepsilon C_A^+, \varepsilon U^+ + (1-\varepsilon)U^- - E_I$	$-E_A, U$

不具有恶意的参与者在发送数据时因为混入了大量无效值,成功将真实值隐藏在其中,导致恶意的参与者无法获知其中哪一个是真实值,所以很大程度上提高了这个协议传输时的安全性,因此将这样获得的收益设为 U_A 。但是,如果恶意参与者在此时没有去攻击,这种收益是不存在的。

这时,不具有恶意的参与者不会有这个 U_A 收益。

定义1 恶意参与者成功进行攻击的概率为 ε ,为了避免其进行攻击,则

$$\varepsilon < \frac{U - U^- + E_I}{U^+ - U^-} \quad (1)$$

证明 博弈模型的支付矩阵,攻击者选择不攻击的收益为 U 。

当一个恶意参与者发现对协议进行攻击去获取真实值节点时所要花费的代价大于获取真实值后的收益,那么从理性的角度考虑,其不会发动攻击,从而有

$$U > \varepsilon U^+ + (1-\varepsilon)U^- - E_I \quad (2)$$

化简可得

$$\varepsilon < \frac{U - U^- + E_I}{U^+ - U^-} \quad (3)$$

因此,非恶意参与者在传输节点数据时,让真实值节点在总节点中的比例应符合 ε ,从而保证了协议的安全性。

定义2 协议的节点个数 m 在满足 $m \geq \frac{U^+ - U^-}{U - U^- + E_I}$ 时,参与者不会违背协议,不会去通过猜测等手段获得真实节点值,会严格执行协议。

证明 参与者Alice和Bob不知道在对方所给予的树中的 m 个元素中哪个元素是真正的 X 和 Y 。如果参与者想在不继续履行协议的情况下提前知道 X 和 Y 的值,只能通过猜测,因此,根据定义1中的结论,当 $m \geq \frac{U^+ - U^-}{U - U^- + E_I}$ 时,遵守

协议的收益会大于不履行协议去猜测的收益,因此参与者会严格遵守协议。

3 理性的安全两方计算协议

本文给出一个具有两名参与者的计算协议,参与者都是具有理性的,他们会根据利益大小去做出能让自己利益最大化的决定,也就是说,都可以试图猜测或推算其他参与者的真实值,不履行协议,以达到在不让对方知道大小的情况下自己先知道大小。

3.1 数据准备阶段

输入 令 X 和 Y 是Alice、Bob的私有输入值。在协议进行过程中, X 和 Y 的值并不会被外界以

及对方知晓。

Alice 从有限域 F 中选取一系列随机元素 $A_1, A_2, A_3, \dots, A_{m-1}, A_m$, 选取元素的个数 m 满足 $m \geq \frac{U^+ - U^-}{U - U^- + E_l}$ (定义 1), 然后将 X 值放入这一系列随机元素中成为 $A_1, A_2, A_3, \dots, X, \dots, A_{m-1}, A_m$, 然后将这些随机元素构成二叉排序树。

构成排序二叉树 A_{tree} 后, 对树中的 X 进行左 0 右 1 的编码。例如, 在图 1 中, 如果 X 在 51 的位置, 那么编码为 001; 如果 X 在 93 的位置, 那么编码为 110; Alice 记下 X 所在位置的编码 $A_{tree}XCode$ 。

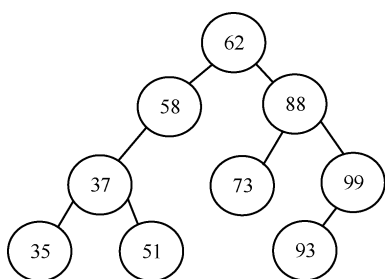


图 1 二叉排序树

Bob 对自己的随机序列 $B_1, B_2, B_3, \dots, Y, \dots, B_{m-1}, B_m$ 做相同的准备, 构成排序二叉树 B_{Tree} 记下自己的 Y 所在位置的编码 $B_{Tree}YCode$ 。

3.2 数据交互计算阶段

1) Alice 将自己的二叉排序树 A_{Tree} 上的元素按照从上到下、从左到右的顺序发送给 Bob, Bob 收到所有元素后, 还原成 A_{Tree} 树, 将自己的 Y 值添加到 A_{Tree} 中, 并进行左 0 右 1 的编码, 得到 Y 值所在位置的编码 $A_{Tree}YCode$ 。

2) Bob 将自己的二叉排序树 B_{Tree} 上的元素按照从上到下从左到右的顺序发送给 Alice, Alice 收到所有元素后, 还原成 B_{Tree} 树, 将自己的 X 值添加到 B_{Tree} 中, 并进行左 0 右 1 的编码, 得到 X 值所在位置的编码 $B_{Tree}XCode$ 。

3) Alice 将 $B_{Tree}XCode$ 编码发送给 Bob, 同时, Bob 将 $A_{Tree}YCode$ 编码发送给 Alice。Alice 通过 $A_{Tree}YCode$ 编码结合自己的 A_{Tree} 树能够判断出 X 和 Y 的值的大小。例如, Bob 发送的 $A_{Tree}YCode$ 编码是 1100, 而 Alice 自己的编码 $A_{Tree}Xcode$ 编码为 0100, 可从第一位上判断出 X 在左子树, Y 在右子树, 因此 Y 必然大于 X , 从而判断出大小。Bob 同理可以得出结论。

4 协议分析

4.1 时间复杂度和计算复杂度

本协议在数据交互阶段仅需要进行一轮交互, 时间复杂度较低。同时, 在对排序二叉树进行左 0 右 1 的编码时计算简单, 便于操作。

4.2 公平性

从数据交互阶段可以看出, Alice 和 Bob 都不会从步骤 3) 前的数据准备和数据交互阶段中提前得到大小的信息, 只有 Alice 和 Bob 在步骤 3) 中同时发送数据后, 彼此才能获得大小的信息。可见, Alice 和 Bob 要么都能成功获得正确的计算数据, 要么都不能成功获得正确的计算数据, 保证了协议的公平性。

4.3 安全性

本文可以保证 Alice 和 Bob 两方在比较 X 和 Y 大小的同时不会获取到 X 和 Y 的值。考虑到协议具有对称性交互这一特点, 只需要从其中一个参与者进行分析即可, 因此从 Alice 的角度进行分析。Alice 有 2 次从 Bob 处得到信息。

1) 在协议的数据交互阶段的步骤 2) 中, Alice 从 Bob 处得到 B_{Tree} , B_{Tree} 是含有多个随机元素的排序二叉树, Alice 想从中获取到 Bob 的秘密输入 Y 只能通过猜测, 而 Alice 结合自身利益并没有通过猜测而不去履行协议的动机 (定义 2), 因此 Alice 并不能获得 Bob 的秘密输入 Y 。

2) 协议的数据交互阶段的步骤 2) 中, Alice 从 Bob 处得到了 $A_{Tree}Y$ 编码, 仅通过编码 Alice 并不能得到 Bob 的真实秘密输入值。

由上面的说明可知, Alice 并不会从数据交互中获取到 Bob 的任何隐私性的信息。Bob 同理。

4.4 正确性

同样, 从 Alice 的角度考虑。Alice 得到 B_{Tree} 后, 把自己的值 X 添加到 B_{Tree} 上构成新的排序二叉树, 然后对 X 这个节点进行左 0 右 1 编码得到 $B_{Tree}XCode$, 然后将 $B_{Tree}XCode$ 编码告诉 Bob, 这样 Bob 就能通过 Alice 给出的编码及自己的 B_{Tree} 排序二叉树确定出 X 节点在树中的位置, 由于排序二叉树的性质, Bob 再结合 B_{Tree} 中自己的 Y 值的位置, 就能判断出 X 和 Y 的大小。

4.5 纳什均衡

在协议的第一部分数据准备阶段 (3.1 节),

各个参与者都是单独进行数据准备, 所以不会打破公平性。在数据交互阶段, 交互前双方自己并不知道比较的结果, 要想知道比较的结果, 都依赖于对方发送的编码。而不履行协议单独去猜测编码又不符合理性参与者自身的利益, 故在数据交互的整个过程中, 如果参与者出现背叛而不履行协议或者不发送最后的编码, 均不能增加收益, 因此协议双方的最佳策略是相互合作, 即所有参与者都能得到结果。

5 结束语

从博弈论的角度考虑, 对传统的多方安全计算协议进行了分析, 发现传统的安全多方计算协议一般要经过多轮的复杂计算, 实际效率很低, 将其与生活实际相结合时成本很高, 并且很多多方安全计算协议在设计的时候只从恶意参与者和非恶意参与者2个角度考虑, 而忽略了当利益巨大的时候, 即便是非恶意的参与者也会具有攻击倾向; 当攻击成本昂贵, 甚至超过攻击所能获得的利益时, 即便是恶意参与者, 也很有可能放弃攻击。通过引入二叉排序树, 大大简化了运算的复杂性, 使参与者只有极少的交互便实现了比较大小的目的, 并且协议的参与者能够正确、安全、公平地得到计算结果。

参考文献:

- [1] GOLDREICH O. Secure multi-party computation[EB/OL]. <http://theory.lcs.mit.edu/>.
- [2] CRAMER R. Introduction to secure computation[M]//Lectures on Data Security. Berlin Heidelberg: Springer. 1999:16-62.
- [3] YAO A C. Protocols for secure computation[C]//The 23rd IEEE Symposium on Foundations of Computer Science(FOCS 1982). 1982:160-164.
- [4] GOLDREICH O, MICALI S, WIGDERSON A. How to play any mental game[C]//The 19th Annual ACM Symposium on Theory of Computing(STOC 1987). 1987:218-229.
- [5] GOLDREICH O. Foundations of cryptography: basic application[M]. Cambridge: Cambridge University Press, 2004.
- [6] QIN J, ZHANG Z F, FENG D G, et al. A protocol of comparing information without leaking[J]. Journal of Software, 2004, 15(3): 421-427.
- [7] LI S D, DAI Y Q, YOU Q Y. An efficient solution to Yao's millionaires' problem[J]. Acta Electronica Sinica, 2005, 33(5): 769-773.
- [8] ZHOU S G, LI F, TAO Y F, et al. Privacy preservation in database applications: a survey[J]. Chinese Journal of Computers, 2009, 32(5): 847-861.
- [9] ZHANG F, CHANG H Y. Privacy-preserving outlier detection with oblivious third party[J]. Journal of Computer Research and Development, 2007, 44(S): 226-231.
- [10] GORDON D, HAZAY C, KATZ J, et al. Complete fairness in secure two-party computation[C]//The 40th Annual ACM Symposium on Theory of Computing (STOC 2008). 2008: 413-422.
- [11] HALPERN J, TEAGUE V. Rational secret sharing and multiparty computation[C]//The 36th Annual ACM Symposium on Theory of Computing(STOC 2004). 2004: 623-632.
- [12] KOL G, NAOR M. Cryptography and game theory: designing protocols for exchanging information[C]//The 5th Theory of Cryptography Conf (TCC 2008). 2008: 317-336.
- [13] MALEKA S, AMJED S, RANGAN C P. The deterministic protocol for rational secret sharing[C]//The 22th IEEE International Parallel and Distributed Processing. 2008: 1-7.
- [14] IZMALKOV S, MICALI S, LEPINSKI M. Rational secure computation and ideal mechanism design[C]//The 46th Annual Symposium on Foundations of Computer Science (FOCS 2005). 2005: 585-595.
- [15] FUCHSBAUER G, KATZ J, NACCACHE D. Efficient rational secret sharing in the standard communication networks[C]//Theory of Cryptography Conf (TCC 2010). 2010: 419-436.
- [16] ASHAROV G, LINDELL Y. Utility dependence in correct and fair rational secret sharing[J]. Journal of Cryptology, 2011, 24(1): 157-202.

[作者简介]



张兴兰(1970-), 女, 山西吕梁人, 博士, 北京工业大学教授, 主要研究方向为密码学和安全协议。



郑伟(1989-), 男, 河北石家庄人, 北京工业大学硕士生, 主要研究方向为密码学、博弈论及安全多方计算。