安全多方计算 调研报告

王傲

15300240004

保密技术概论

COMP130116.01

指导教师：吴杰

目录

内容摘要：

本文调研了安全多方计算的相关概念、相关协议和应用场景，并给出了具体的例子，了解了安全多方计算的整体情况和研究现状，进一步加深了对安全多方计算的认识和了解。

关键字：同态加密 零知识证明 交换加密函数 不经意传输

1. 绪论

随着网络和分布式计算的飞速发展，多方协同计算的计算方式越来越引起人们的注意。而合作计算过程中对数据隐私的保护也是不得不考虑的问题，安全多方计算由此而来。安全多方计算主要研究参与方在保持自己的输入隐私的情况下如何共同完成某个计算任务，使得各方除了得到计算的结果外不会泄露自己的隐私数据信息。

安全多方计算最早由图灵奖得主姚期智于上世纪八十年代提出。本文则对安全多方计算进行了进一步的调研。

2. 相关概念

2.1 同态加密

同态加密体制允许在不知道解密后的数据的情况下直接对加密数据进行运算，且解密后的结果等于直接对未加密数据进行运算得到的结果。同态加密算法满足同态性质，而且属于非对称公钥加密体制的范畴。

设 E(m)表示明文消息 m 的密文。若加密方案对操作⊗和⊕，消息 a 和 b 的加密消息 E(a)和 E(b)满足：

$$E_k(a) \otimes E_k(b) \equiv E_k(a \oplus b)$$

则称这个加密方案为同态加密方案。其中 k 为密钥。如果同态加密方案满足：

$$E_k(a) \cdot E_k(b) \equiv E_k(a \times b)$$

则称为乘同态加密，例如 GM 算法和 ElGamal 加密方案。如果同态加密方案满足：

$$E_k(a) \cdot E_k(b) \equiv E_k(a + b)$$

则称为加同态加密，例如 Paillier 加密方案。

由于同态加密良好的性质，可以被应用于安全多方计算中。比如，针对姚氏百万富翁问题，有人提出了基于同态加密的解决方案。

2.2 零知识证明

设有 P 与 V 两方，P 代表证明方，V 代表验证方。P 需要向 V 证明某个命题为真，但是又不想让 V 知道他证明这个命题所用到的关键信息。或者说 P 知道某个消息，他需要向 V 证明自己知道这个消息，但是又不向 V 泄漏这个消息的内容。V 可以验证 P 是否真的知道这个消息。这样的证明就是零知识证明，相应的证明规则称为零知识证明协议。零知识交互证明协议必须满足完备性、合理性和零知识三个特性。

2.3 交换加密函数

交换加密函数是将一对加密函数 f 和 g 组合起来加密消息 x 的协议，满足 $f(g(x)) = g(f(x))$。参与方各自持有一个加密函数，通过组合加密函数 $f(g(x))$加密信息 x，可保证参与的一方在没有另一方的帮助下是不可能还原出信息 x 的。尽管这种加密函数是两个函数的组合，但是每一个参与方都可以利用自己的函数先加密，最后得到相同的结果。也就是说，交换加密函数最终加密得到的结果与加密函数加密的顺序无关。

2.4 不经意传输

不经意传输又称茫然传输，是密码学的一个基本协议，也是解决安全多方计算问题的一个基本工具。理论上讲，任何半诚实模型下的安全多方计算问题都可以通过不经意传输协议得到解决。不经意传输最早由 Rabin 提出，实现“2 选 1”的不经意传输方案。随着研究的深入，其他不经意传输的协议相继被提出。

安全多方计算中使用的其他理论和技术还有很多，也很复杂，这里不一一列出。

3. 相关协议

安全多方计算的应用有很多，这里举出几个协议的例子。

3.1 基于同态加密的比较协议

Paillier 加密算法有比较好的同态属性：

$$E(m_1, r_1) \cdot E(m_2, r_2) = E(m_1+m_2, r_1+r_2)$$

$$E(m, r)^c = E(m \cdot C, r \cdot C)$$

基于 Paillier 加密算法的比较协议如下（设 Alice 财富为 a，Bob 财富为 b）：

1. Bob 生成两个非常大的随机正整数 x 和 y，但是并不公开

2. Alice 生成一对属于自己的密钥，公钥为 pub，私钥为 pri，用公钥加密自己的财富得到 E(a)，连同自己的公钥一起公布出去

3. Bob 得到 Alice 公布的数据后，首先用 Alice 的公钥计算 $E(b\cdot x+y)$，然后用 Paillier 算法的同态属性计算出 $E(a\cdot x+y)=E(a)^x\cdot E(y)$,并将这两个结果公布出去

4. Alice 得到 Bob 公布出来的结果后，用自己的私钥反解出 $A= a\cdot x+y$ 和 $B= b\cdot x+y$ 的值。Alice 虽然对 x、y 和 b 一无所知，但她只要比较 A 和 B 的大小就可以了。而对 Bob 来说，他对 A、B 和 a 也是一无所知，如果他想知道比较结果，只需要 Alice 告诉他结果或者角色对换重新执行一次协议。

可以看出，这个协议巧妙的利用了 Paillier 算法的同态性，实现起来非常简单，而且复杂度远远小于姚期智给出的原始方案，是百万富翁问题的一个更好的解决方案。

3.2 保护私有信息的两方整数排序协议

这里给出一个能够保护私有信息的两方整数排序协议。在该协议基础上，可以完成保护私有信息的多方排序协议。

协议流程如下（设 Alice 的数据为 a，Bob 的数据为 b）：

1. Alice 生成一组满足同态加密性的公钥和私钥，公开自己的公钥 E，加密自己的数据得到 $c=E(a)$并将结果发送给 Bob

2. Bob 随机选择整数 u_1，v_1，w_1，满足$|v_1-w_1|<u_1$ 且 $u_1>0$，并计算

$X_1=c^{u1}\,E(v_1)$，$Y_1=E(u_1b+w_1)$，将结果发送给 Alice

3. Alice 解密 $D(X_1)=u_1a+v_1$，$D(Y_1)=u_1b+w_1$。如果 $D(X_1)>D(Y_1)$,则 a>=b；如果 $D(X_1)<D(Y_1)$, 则 a<=b

4. Bob 随机选择整数 u_2，v_2，w_2，满足$|v_2-w_2|<u_2$，$u_2>0$ 且$(v_2-w_2)(v_1-w_1)<0$，计算 $X_2=c^{u2}\,E(v_2)$，$Y_2=E(u_2b+w_2)$并发送给 Alice

5. Alice 解密 $D(X_2)$，$D(Y_2)$。如果 $D(X_2)>D(Y_2)$,则 a>=b；如果 $D(X_2)<D(Y_2)$, 则 a<=b

6. Alice 分析两次比较的结果，如果 $D(X_1)>D(Y_1)$且 $D(X_2)>D(Y_2)$,则 a>b；如果 $D(X_1)<D(Y_1)$且 $D(X_2)<D(Y_2)$，则 a<b；否则，a=b。最后，Alice 将结果告诉 Bob。

这个协议通过两次重复的过程判别出了等于的情况，并且复杂度为 O(1)，有着很好的效果。在该协议基础上，可以完成保护私有信息的多方排序协议。

4. 应用场景

安全多方计算涉及到了很多相关的应用场景，这里给出几个安全多方计算在实际应用场景中的例子。

4.1 安全多方集合计算问题

安全多方集合计算问题可以描述如下：n 个参与方 $P_1, P_2, ..., P_n$ 各有一个数据集，在不泄漏各自数据集信息的情况下，参与方进行集合的相关操作计算。目前经常涉及到的集合计算问题主要有计算并集以及并集的势、计算交集以及交集的势、判断集合是否相交、判断集合是否存在包含关系等。

4.2 电子拍卖

电子拍卖是安全多方计算应用的典型案例,实现安全电子拍卖涉及许多高级密码协议的研究,对其它电子商务活动的安全性研究具有重要的理论意义和实用价值。现有的电子拍卖协议基本上都是有拍卖行的,这使得竞标者的身份和竞标价存在着泄露的隐患,降低了整个拍卖系统的安全性；而少数没有拍卖行的拍卖协议计算又非常复杂,实用性不强。在安全多方计算的基础理论及关键技术的基础上,可以设计出既能满足现实拍卖的实际需要,又实现了竞拍者匿名、竞拍价保密和可验证性等密封式电子拍卖所要求的安全特性的协议,并且能较容易的计算出中标结果。

4.3 保护私有信息的数据挖掘问题

数据挖掘是一个融合数据库、人工智能和统计学的交叉的新兴研究方向。当今信息社会储存着海量的信息和各类数据，而数据挖掘在对数据的分析中发挥了十分重要的作用。考虑到某些数据信息的隐私性，需要研究如何在保护私有信息的情况下更好的进行数据挖掘工作。基于安全多方计算的理论和技术，可以对相关数据实现保护，在不泄漏私有信息的情况下进行数据挖掘，在保证信息安全的同时获得相关结果。

5. 总结

本文调研了安全多方计算的相关概念、相关协议和应用场景，并给出了具体的例子，了解了安全多方计算的整体情况和研究现状，进一步加深了对安全多方计算的认识和了解。

6. 参考文献

[1]蒋瀚,徐秋亮.实用安全多方计算协议关键技术研究进展[J].计算机研究与发展,2015,52(10):2247-2257.

[2]刘明洁,王安.全同态加密研究动态及其应用概述[J].计算机研究与发展,2014,51(12):2593-2603.

[3]孙茂华. 安全多方计算及其应用研究[D].北京邮电大学,2013.

[4]耿涛. 安全多方计算若干问题以及应用研究[D].北京邮电大学,2012.