无线信道物理层密钥生成方法与密钥协商体系

杨 硕,侯晓赟,朱 艳
(南京邮电大学 信号处理与传输研究院,江苏 南京 210003)

摘 要:由于信道的开放性,无线通信面临着被窃听的危险,通常采用加密来增强通信的安全传输。无线物理层密钥技术利用了无线信道的时变性和互易性,不仅可以实现“一次一密”,而且无需进行密钥分发,避免了传统加密技术中因密钥分发而引起的泄密风险,因而成为信息安全领域的最新研究热点之一。为此,对基于无线信道特征的物理层密钥生成方法进行了回顾与总结,并比较了各自优缺点。针对通信双方初始生成密钥的不一致性问题,从信息调和、一致性认证、保密增强这三个方面分析研究了密钥协商体系。归纳总结了一些典型的技术和算法,并对比分析了其优缺点。未来研究方向应是充分利用信道特征,并设计出更优的量化策略,提高初始密钥的一致性,降低信息协商的程度,同时要兼顾密钥的随机性以及密钥生成速率;在信息协商阶段,应设计出更好的信道编码进行纠错。

关键词:物理层;密钥生成;密钥协商;信息调和;一致性认证;保密增强
中图分类号:TP301 **文献标识码**:A **文章编号**:1673-629X(2017)05-0123-05
doi:10.3969/j.issn.1673-629X.2017.05.026

Generation and Agreement of Secret Keys for Physical Layer Security Based on Wireless Channels

YANG Shuo, HOU Xiao-yun, ZHU Yan
(Institute of Signal Processing & Transmission, Nanjing University of Posts & Telecommunications, Nanjing 210003, China)

Abstract: Due to the openness of the channel, the wireless communication faces the danger of being eavesdropped, so it usually uses encryption to enhance the security of communication. The wireless physical layer key technology utilizes the time-varying and reciprocity of radio channel, not only to achieve "one-time pad", but also to eliminate the need for key distribution, avoiding the risk of leak caused by key distribution for the traditional encryption technology. Therefore it has become one of the latest research hotspots in the field of information security. For this reason, the physical layer key generation method based on the characteristics of the wireless channel is reviewed and summarized, and their advantages and disadvantages are compared. According to the inconsistent problem of the initial generation of the key, the key agreement protocol are analyzed in three aspects: information reconciliation, consistency authentication and privacy amplification. Some typical techniques and algorithms are summarized, and their advantages and disadvantages are compared. Further research direction is to make full use of channel characteristics, and to design better quantitative strategies, which can improve the consistency of the initial key and reduce the level of information reconciliation. At the same time, the randomness of the key and the rate of the key generation should be considered. In the key agreement phase, a better channel coding is designed to correct the error.

Key words: physical layer; secret key generation; secret key agreement; information reconciliation; consistency authentication; privacy amplification

0 引 言

随着无线网络的不断发展,无线通信在生活中起到了越来越重要的作用。然而由于无线媒介的广播性和开放性,传播的信息极易被窃听,无线通信的隐私以及安全问题已经成为广泛关注的焦点。保障通信安全的传统技术主要是在网络层以密码学为基础,其安全性依赖于计算能力,随着量子信息时代的到来,很多传统的加密方法越来越容易被破解。而物理层安全技术则可以达到信息理论意义上的安全,它通过物理层密钥与探索信道随机性的信道编码技术来保证第三方无

收稿日期:2016-05-26 **修回日期**:2016-09-08 **网络出版时间**:2017-03-07
基金项目:国家自然科学基金资助项目(61201270)
作者简介:杨 硕(1991-),男,硕士研究生,研究方向为无线物理层密钥安全。
网络出版地址:http://kns.cnki.net/kcms/detail/61.1450.TP.20170307.0921.050.html

法在无线媒介上窃听。

与传统加密技术相比,物理层密钥技术具有诸多优势。第一,密钥在认证双方直接生成,不需要密钥管理中心及密钥分发过程,降低了密钥被窃听的风险。第二,物理层密钥是基于无线信道的随机性机理,因此它独立于计算复杂度,可以简单高效地解决安全问题。第三,由于收发双方的移动和不断变化的环境,物理层密钥生成是动态的,这样可以提高共享密钥的安全。

1949 年,Shannon 给出了完美保密的定义[1],利用关于完善保密的两个定理,证明了一次一密的无条件安全性。在此基础上,Wyner 提出了窃听信道的数学模型[2],假设窃听的信道是合法接收者的退化信道。Maurer 等的研究表明相关随机性可以用来生成密钥[3-4],然而在文献[3]中 Maurer 认为 Wyner 的退化窃听信道未必现实,提出了通信双方可以安全通信的密钥协商协议。该方案的关键要素是信息调和与保密增强。此外,基于噪声信道的密钥协商方案在文献[3-4]中提出,第三方可以在认证的公开信道中窃听通信但不能破坏通信。这种方法在通信双方分享相关高斯信源的模型中被拓展[5]。在文献[6]中,在准静态衰落信道中提出了机会通信,只在通信双方信道状态好于窃听方的情况下传送信号。由于合法通信用户对于双方之间的信道估计存在不可避免的误差,提取的密钥必然不一致,在密钥提取方案中必须通过辅助方法进行密钥协商。通信双方需要通过公开信道交互一部分信息进行密钥协商,进而提高密钥一致性,而这部分信息在传输过程中存在泄漏的风险,需要进行保密增强。文献[7-8]中对无线密钥生成技术进行了总结分析,但主要集中在初始密钥提取和生成阶段。可见,基于无线信道特征的物理层密钥生成方法是值得研究的。为此,在回顾总结的基础上,比较分析了其各自优缺点。针对通信双方初始生成密钥的不一致性问题,从信息调和、一致性认证、保密增强这三个方面分析研究了密钥协商体系,归纳总结了一些典型的技术和算法,并对比分析了其优缺点。

1 密钥生成

无线物理层密钥生成是基于公共无线信道的互易特性。系统模型如图 1 所示。假设无线通信系统有两个合法节点 A 和 B 以及被动攻击者 E。A 和 B 测量物理信道的互易特性,分别用 h_{AB} 和 h_{BA} 表示。当窃听者 Eve 与合法通信用户 Alice 和 Bob 之间的距离大于 $\lambda/2$ 以上时,E 的测量 h_{AE} 和 h_{BE} 与 A 和 B 的测量几乎没有相关性。

一般地,在一个散射的环境中,两个认证实体 Alice 和 Bob 分别利用特殊的估计算法估计上行和下行信道状态,根据信道互易性特征,它们的估计在某种程度上是相关的,因此可以提取几乎相同的密钥,差异不大。运用某种量化准侧,可以将估计的样值转换成一定的比特序列,这些比特序列是初始密钥。

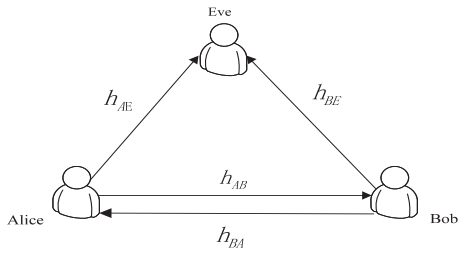

图 1 系统模型

最常见的密钥生成方法是根据接收到的信号强度量化成比特流。然而其他信道特征也可以进行密钥生成,例如信道相位、信道包络和多径下的信道特征等。文献[9]提出了一种基于接收信号强度(Received Signal Strength,RSS)的密钥提取方法。将信息论的理论研究转化为实际的密钥提取过程,提出一种有别于以前的依赖于双方鉴权的密钥提取的新算法,并利用基于 FPGA 平台的 802.11 协议进行算法验证。针对基于 RSS 生成密钥速率低以及随机性差等缺点,文献[10]探索了信道相位随机性,取得了较高的密钥生成速率,并在此基础上提出了协作密钥生成方案[11]。文献[12]提出了一种基于多径相对时延的密钥生成方法,利用相对时延与平均时延的差值产生密钥,具有一定的抗噪性能。根据基于放大转发的双向中继信道的特性,文献[13]利用时分系统无线多径信道的互易性和卷积性,采用基于压缩感知的重构算法对信道状态信息进行估计,提出了基于多径相对幅度和基于多径相对相位的密钥生成方案,均可以达到较高的密钥一致性。

很多对于密钥生成性能的改进是从信道估计和量化策略入手,例如文献[14]提出一种 ESPAR(Electronically Steerable Parasitic Array Radiator)天线的波束成型技术,可以增强信道的波动特征,并且有能力基于接收信号强度充分独立地生成密钥。这样的信道估计更加准确。同时,更优的量化策略也可以产生更好的性能效果。由于缺少信道波动,提取的比特具有很低的熵值,无法作为密钥。文献[15]提出一种自适应有损量化器结合交互式环境自适应的密钥提取方案。为了取得更好的密钥一致性,文献[16]提出一种利用 RSS 的多电平密钥提取量化方案并采用校验序列,提升了合法通信用户之间的密钥一致性,该算法在密钥一致性和密钥生成速率之间作了折衷。

密钥生成算法的性能评价指标主要有 3 个:

(1)密钥生成速率,指相干时间内生成的比特流

数目,加快信道的变化可以提高密钥生成速率;

(2)密钥不一致率,指通信双方错误比特数与总比特的比率;

(3)密钥随机性,反映 0 和 1 的均匀程度,0 和 1 均匀分布会有好的随机性,保证安全性。

2　密钥协商系统模型

图 2 表示共同信息通过公开讨论的密钥协商系统模型[17]。Alice,Bob,Eve 分别表示发送者、合法接收者和窃听者。X 为 Alice 的发送信号,Y 为 Bob 的接收信号,而 Z 是 Eve 的接收信号,P 是 X,Y 和 Z 的联合概率分布。一开始 Alice 和 Bob 不分享密钥,他们知道随机变量 X 和 Y,而 Eve 知道随机变量 Z。

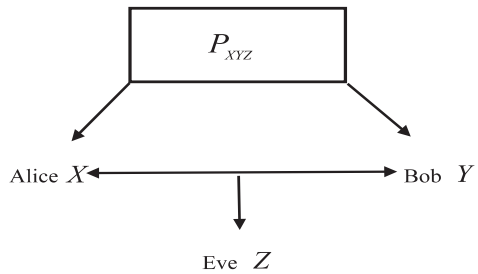

图 2　协商模型

文献[4]中给出了秘密认证信道的定义,让 U^a 和 U^b 分别表示消息 M 发出前和发出后 Eve 的全部信息。$\bar{M}$ 表示接收者收到的信息。

(1)如果 $I(M;U^a\,|U^b)=0$,就称信息是秘密的。

(2)如果 $M=\bar{M}$,就称信息是认证的。

同时也给出了密钥协商协议的定义,包括通信阶段和密钥生成阶段,假设生成的密钥取决于双方所知道的信息而不是额外的随机比特。此外,在假设通过公共信道是认证而不是秘密的情况下也给出了定义。

密钥协商是在初始密钥生成之后进行的,主要包括以下步骤:

(1)信息调和:丢弃或纠正两端生成密钥的差异。

(2)一致性确认:确定双方是否生成了完全一致的密钥。

(3)保密增强:Alice 和 Bob 从正确数据中提取秘密比特。

3　信息调和

初始密钥生成后,由于信道估计、噪声等影响,导致密钥一致性很难保证。文献[18]介绍了 BBBSC 算法,该算法的核心是利用 2 分法查找通信双方错误比特的位置。首先 Alice 和 Bob 各自检测每组数据的奇偶性,并通过公开信道进行比较。在这个环节会泄露一定的信息。若双方所对应的数组彼此奇偶性不同,就表明该组有错误比特,并且是奇数个错误。接着将这样的数组一分为二,进行奇偶性检测比较。一直重复这个步骤,知道最后一个数位,这个数位就是错误比特位。为了确保不让 Eve 获得新信息,每公开一次数组的奇偶性,就将该数组最后的数位舍弃,被发现的错误位也被舍弃。在信息协商中,BBBSC 算法是非常经典的算法,其效率较高,实现的复杂度较低,实际应用也非常广泛。Brassard 提出的 Caseade 协议[19],要求收发双方对其量化后的比特分别分成固定长度的组,并检验每一组的校验位。Alice 计算各组的奇偶性并通过公开信道告知 Bob,Bob 将 Alice 的结果与自己的进行比较。经过一轮分组纠错后只存在偶数个错误。此外,文献[20]提出了 Winnow 算法,即汉明码信息协调方法,是利用 Hamming 码通过公共信道进行纠错。以 $[n,k]$ 线性分组为例:它将比特信息扩展成 n 比特码字,利用额外 $n-k$ 比特进行纠错。文献[21]就是利用该算法,密钥序列被分隔成长度为 7 的密钥块。这些密钥块将被送入具有前向纠错能力的(7,3)汉明码的解码器中,其产生的码字用于下一步的公开密钥协商。对于公开讨论而言,4 比特的信息被发送出去用于协助密钥协商,尽管 4 比特的信息对于窃听者 Eve 是可知的,但 Alice 和 Bob 保持着 3 比特的安全性。

上述讨论的是通过一些经典算法进行密钥协商,然而由于信息调和本质上是进行纠错的过程,所以可以根据信道随机性的信道编码技术实现密钥协商。问题的关键在于带有编码的边信息译码器,在这里 Alice 提供附加信息以便 Bob 恢复 Alice 传输的序列。LDPC 码由于具有很强的纠错能力,因此应用比较广泛。文献[21]中利用 LDPC 降低了由信道噪声引起的密钥序列不一致。文献[22]采用 BCH 码,文献[23]则采用了 Reed-Muller 码实现信息调和。

4　一致性确认

单向 Hash 函数是现代密码学的核心概念,用于通信过程中的身份验证和信息完整性验证。Hash 的安全性是指它的单向性,即输出的不反映任何与输入数据有关的信息。令 Hash 算法用 Hash( )表示,则 Y = Hash(X),表示输出序列 Y 为输入序列 X 的 Hash 值。由 Hash 函数的性质可知,即使截获 Y,想反向推断 X 也十分困难。

在密钥生成的最后阶段,合法通信用户 Alice 和 Bob 在使用密钥进行安全通信之前要确认是否生成相同的密钥,为了执行这个确认,通过三个步骤进行说明。该过程将采用 AVISPA(Automated Validation of Internet Security Protocols and Applications)协议[24],如图 3 所示。

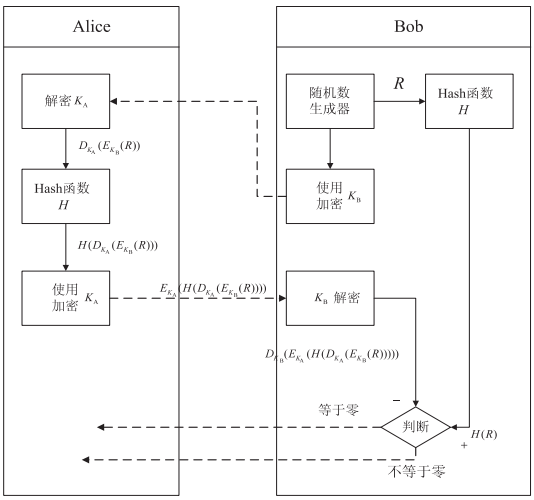

图 3 认证过程

步骤 1:Bob 选取一个真实随机数 R,使用自己的密钥 K_B 进行加密,然后通过公开信道发送加密值 $E_{K_B}(R)$ 给 Alice,$E_K(.)$ 表示的是通过密钥 K 进行的加密操作。

步骤 2:Alice 通过自己的密钥 K_A 解密接收到的数值,进行 Hash 处理后用 K_A 再进行加密。将 $E_{K_A}(H(D_{K_A}(E_{K_B}(R))))$ 通过公开信道发送给 Bob,其中 $D_K(.)$ 和 $H(.)$ 表示的是用 K 解密和哈希操作。

步骤 3:接收者 Bob 通过密钥 K_B 进行解码操作。如果解密出的结果和 $H(R)$ 相等,则 Bob 发送确认信息给 Alice,确认密钥相同。如果解密出的结果和 $H(R)$ 不相等,则 Bob 发送否认信息给 Alice,表示密钥不相同。

这里需要注意的是 $E_K(.)$、$D_K(.)$ 和 $H(.)$ 均是公开操作,并且,每次 R 都要进行更新,因为存在重复攻击对抗这个算法。

文献[25]提到基于双 Hash 函数的密钥一致性协商,主要是利用 Hash_2 函数进行密钥去相关。当信道缓慢变化时,连续多次信道估计得到的信道特征值相近,因此经过相同的密钥生成算法生成的密钥也很相近,具有很强的相干性,从而降低了密钥的动态安全性。因此需要进行密钥去相关处理。

5 保密增强

假设 Alice 和 Bob 有一样的序列 X^l,l 是其长度。Eve 有一相关序列 Z^l。保密增强的作用是通过压缩函数,将部分安全的密钥压缩为几乎不被 Eve 所利用的信息。文献[26]中 Bennett 等利用 Hash 函数,以二阶瑞利熵为工具,给出了对保密增强的完整证明。

让 Alice 和 Bob 拥有随机变量 W,例如一串随机的 n 比特序列。而窃听者 Eve 可以学习相关的随机变量 V,提供 $t < n$ 关于 W 的比特信息,$H(W|V) \geq n - t$。Alice 和 Bob 想公开选择压缩函数 $g: \{0,1\}^n \rightarrow \{0,1\}^r$,然而由于只能得到 Eve 的部分信息关于 W,以及全部的信息关于 g,所以对于 $K = g(W)$ 的信息几乎是很少的。

文献[27]中介绍了两种保密增强协议,一种是 UH(通用 Hash 函数)协议,另一种是 EX(提取器)协议。UH 协议是基于通用 Hash 函数以及部分密钥的瑞利熵研究,在窃听方看来部分密钥的长度是超过三分之二序列的部分。然后,协议提取与这长度等同的序列。UH 协议的计算非常简单。对于更长的序列,基于 EX 协议是可以使用的。它的优势是可以重复使用相同的密钥在保密增强的步骤中。

保密增强环节虽然不能增加原有密钥的随机性,但是却避免了弱密钥导致加密算法出现漏洞的几率。

6 结束语

为了更加深入、系统地研究无线物理层密钥安全技术,总结回顾了无线物理层密钥生成与协商的发展历程,从信息调和、一致性认证、保密增强三个方面讨论了密钥协商协议。在信息调和的过程中一些算法和信道编码技术值得深入研究,从而设计出更好的方法。密钥协商主要解决密钥不一致问题,因此要想进行安全通信,必须处理好这个问题,加强对密钥协商的研究。

由于噪声和估计同步等问题的影响,导致密钥提取阶段存在误差,可以考虑充分利用信道特征,以及设计出更优的量化策略,提高初始密钥的一致性,降低信息协商的程度,同时要兼顾密钥的随机性以及密钥生成速率。在信息协商阶段,设计出更好的信道编码进行纠错应该是接下来研究的重点。

参考文献:

[1] Shannon C E. Communication theory of secrecy systems[J]. Bell System Technical Journal,1949,28(4):656-715.

[2] Wyner A D. The wire-tap channel[J]. Bell System Technical Journal,1975,54(8):1355-1387.

[3] Maurer U M. Secret key agreement by public discussion from common information[J]. IEEE Transactions on Information Theory,1993,39(4):733-742.

[4] Ahlswede R,Csiszár I. Common randomness in information theory and cryptography, part I: secret sharing[J]. IEEE Transactions Information Theory,1993,39(4):1121-1132.

[5] Naito M,Watanabe S,Matsumoto R,et al. Secret key agreement by soft-decision of signals in Gaussian Maurer's model[J]. IEICE Transactions on Fundamentals, 2009, E-92(2):525-534.

[6] Bloch M,Barros J,Rodriguez M R D,et al. Wireless information-theoretic security[J]. IEEE Transactions Information Theory,2008,54(6):2515-2534.

[7] 李古月,胡爱群,石　乐. 无线信道的密钥生成方法[J]. 密码学报,2014,1(3):211-224.

[8] 隋　雷,郭渊博,姜文博,等. 基于无线信道特征的密钥生成与提取研究[J]. 计算机科学,2015,42(2):137-141.

[9] Kim H S. Measurement and model based characterization of indoor wireless channels[D]. Lowell: University of Massachusetts,1989.

[10] Wang Q, Su H, Ren K, et al. Fast and scalable secret key generation exploiting channel phase randomness in wireless networks[C]//Proceedings of In INFOCOM. [s. l.]: IEEE, 2011:1422-1430.

[11] Wang Q, Su H, Ren K. Cooperative secret generation from phase estimation in narrowband fading channels[J]. IEEE Journal on Selected Areas in Communications,2012,30(9): 1666-1674.

[12] 周百鹏,黄开枝,金　梁,等. 一种基于多径相对时延的密钥生成方法[J]. 计算机应用研究,2011,28(6):2196-2198.

[13] 魏　浩,郑宝玉,侯晓赟,等. 基于放大转发的双向中继信道密钥生成[J]. 电子与信息学报,2013,35(6):1344-1350.

[14] Aono T, Higuchi K, Ohira T, et al. Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels[J]. IEEE Transactions on Antennas and Propagation,2005,53(11):3776-3784.

[15] Jana S, Premnath S N, Clark M, et al. On the effectiveness of secret key extraction from wireless signal strength in real environments[C]//Proceedings of the 15th annual international conference on mobile computing and networking. [s. l.]: ACM,2009:321-332.

[16] Ohira T. Secret key generation exploiting antenna beam steering and wave propagation reciprocity[C]//Proceedings of EUMC. London, UK: [s. n.],2005:23-27.

[17] Maurer U, Wolf S. Secret-key agreement over unauthenticated public channels. i: definitions and a completeness result [J]. IEEE Transactions on Information Theory, 2003, 49(4):832-838.

[18] Brassard G, Salvail L. Secret-key reconciliation by public discussion[C]//EU-ROCRYPT 93. Berlin: Springer, 1994: 410-423.

[19] Bennett C H, Brassard G, Robert J M. Secret-key reconciliation by public discussion[M]. Berlin: Springer-Vering, 1986.

[20] Buttler W T, Lamoreaux S K, Torgerson J R, et al. Fast efficient error reconciliation for quantum cryptography[J]. Physical Review A,2003,67:052303.

[21] Madisek M G, McGuire M L, Nevilile S S, et al. Secret key generation and agreement in UWB communication channels [C]//IEEE global telecommunications conference. [s. l.]: IEEE,2008:1-5.

[22] Liu H, Wang Y, Yang J, et al. Collaborative secret key extraction leveraging received signal strength in mobile wireless networks[C]//IEEE international conference on computer computer communication. [s. l.]: IEEE,2012:927-935.

[23] Wilson R, Tse D, Scholtz R A. Channel identification: secret sharing using reciprocity in ultrawideband channels[J]. IEEE Transaction on Information Forensics and Security, 2007, 2(3):364-375.

[24] Armando A, Basin D, Boichut Y, et al. The AVISPA tool for the automated validation of internet security protocols and applications[C]//Proceedings of computer aided verification. [s. l.]: [s. n.],2005:281-285.

[25] 周百鹏. 基于无线信道特征提取的密钥生成技术研究[D]. 郑州:解放军信息工程大学,2011.

[26] Bennett C H, Brassard G, Crépeau C, et al. Generalized privacy amplification[J]. IEEE Transactions on Information Theory,1995,41(6):1915-1923.

[27] Maurer U, Wolf S. Secret-key agreement over unauthenticated public channels. III: privacy amplification[J]. IEEE Transactions on Information Theory,2003,49(4):839-851.

(上接第 122 页)

blind signature[J]. Science in China Series F: Information Sciences,2006,49(5):604-615.

[9] Lindell Y, Pinkas B. Privacy preserving data mining[J]. Journal of Cryptology,2002,15(3):177-206.

[10] Cachin C. Efficient private bidding and auctions with an oblivious third party[C]//Proceedings of the 6th ACM conference on computer and communications security. [s. l.]: ACM,1999:120-127.

[11] Li S D, Wu C Y, Wang D S, et al. Secure multiparty computation of solid geometric problems and their applications[J]. Information Sciences,2014,282:401-413.

[12] Du W, Atallah M J. Secure multi-party computation problems and their applications: a review and open problems [C]//Proceedings of new security paradigms workshop. New York: ACM Press,2001:13-22.

[13] 罗永龙,黄刘生,荆巍巍,等. 空间几何对象相对位置判定中的私有信息保护[J]. 计算机研究与发展,2006,43(3):410-416.

[14] 罗永龙,黄刘生,荆巍巍,等. 保护私有信息的叉积协议及其应用[J]. 计算机学报,2007,30(2):248-254.

[15] 李顺东,司天歌,戴一奇. 集合包含与几何包含的多方保密计算[J]. 计算机研究与发展,2005,42(10):1647-1653.

[16] 李顺东,戴一奇,王道顺,等. 几何相交问题的多方保密计算[J]. 清华大学学报:自然科学版,2007,47(10):1692-1695.

[17] 杨晓莉,李顺东,左祥建. 计算几何问题的多方保密计算[J]. 密码学报,2016,3(1):33-41.

[18] 罗永龙,黄刘生,徐维江,等. 一个保护私有信息的多边形相交判定协议[J]. 电子学报,2007,35(4):685-691.

[19] 李顺东,王道顺,戴一奇,等. 两个集合相等的多方保密计算[J]. 中国科学:信息科学,2009,39(3):305-310.