密钥协商协议进展*)

秦 波[1,3] 伍前红[2] 王育民[1] 王尚平[3] 王晓峰[3]
(西安电子科大 ISN 国家重点实验室 西安 710071)[1]
(武汉大学计算机学院 武汉 430079)[2] (西安理工大学理学院数学系 西安 710048)[3]

摘 要 密钥协商协议允许两个或多个用户在公开网络中建立一个共享密钥,是最基本的密码原型和公钥密码学的基础。本文综述密钥协商协议的研究进展,包括密钥协商的安全模型、传统离散对数环境下的密钥协商协议、最近发展起来的基于双线性对的密钥协商协议以及基于口令的密钥协商协议,指出了密钥协商协议中的公开问题和未来可能的发展方向。

关键词 密钥协商,密钥分发,群密钥协商,认证密钥协商,公钥密码体制

State of Key Agreement Protocols

QIN Bo[1,3] WU Qian-hong[2] WANG Yu-min[1] WANG Shang-ping[3] WANG Xiao-feng[3]
(National Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China)[1]
(School of Computer, Wuhan University, Wuhan 430079, China)[2] (School of Science, Xi'an University of Technology, Xi'an 710048, China)[3]

Abstract Key agreement protocols allow two or more users to establish a common secret key though open networks. This notion of key agreements is one of the most fundamental cryptographic primitives and the base of public cryptography. This paper presents a survey on the state of key agreements including the security model of key agreements, the key agreement protocols in the context of conventional discrete logarithms, pairing-based key agreement protocols and password-based key agreement protocols. We also remark some open problems and the promising research lines in this area.

Keywords Key agreement, Key distribution, Group key agreement (GKA), Authenticated key agreement, Public key cryptosystem

1 引言

许多复杂的密码系统需要在用户之间有一个秘密信道。密钥协商协议的目的就是建立这样一个信道。密钥协商协议是公钥密码系统中最基本、最核心的协议,是公钥密码学的基础。

2 密钥协商安全模型

最早提出密钥协商安全性概念的是 Bellare 和 Rogaway,其主要贡献是使用了不可区分性来定义协商出来的密钥的安全性。粗略地说,在该定义中,如果在允许的攻击行为下,攻击者仍然不能区分一个密钥是由真实协议生成的,还是来自密钥空间的一个独立随机值,那么就称这个密钥协商协议是安全的。后来对这个模型也有一些扩展,包括比较有影响的 Blake-Wilson 等[11]和 Bellare 等[14]所作的研究。

在构造密钥协商协议中使用模块化设计最早是由 Bellare 等倡议的。这种方法要求先为理想的认证过的链接构造一个安全协议,然后将认证操作应用到所有的协议流,获得在标准无认证链接模型下安全的协议。Mayer 和 Yung[30]给出了一种编译器,可以将两方密钥协商协议转化成一个群密钥协商协议;他们的编译器需要调用原始协议 $O(n)$ 次。Bellare 等给出了另外一种编译器,将无认证的两方协议转化为认证协议。如果要将其扩展到群环境,需要 3 倍的通信轮数,还要求 n 次签字生成/验证,每个用户每轮增加 $O(n)$ 的带宽开销。在文献[28]中,Katz 和 Yung 提出了一种编译器,将任意抗被动攻击者的 GKA 转化为抗主动攻击者的 GKA 协议,还可以保持原始协议的前向安全性质。Katz 和 Yung 将他们的编译器应用于 Burmester-Desmedt 协议,构造了静态的三轮认证 GKA 协议。而 Kudla 和 Paterson 没有采用模块化设计,但采用了认证密钥协商协议中的模块化证明技术。

密钥协商协议往往是作为复杂密码系统的一个子协议,因此考虑在协议组合环境下的安全性是必要的。可泛组合(UC)框架就是这样的数学工具。这里对该框架作一个简短的描述,感兴趣的读者可以参考文献[15]获得完整的技术细节。粗略地说,UC 框架的安全性定义为理想函数 F,它是一个可信实体,和环境中的用户交互来计算某个已知函数 f。F 用用户提供的输入来计算 f,并返回给每个用户相应的输出。因此,在理想化环境中,协议的安全得到了内在的保证,因为对于任何攻击者来说,控制某个实体也只能获得该实体的输入和输出,而不能获得其它任何信息。我们考虑一种环境 Z,它给每个用户提供输入,目标是区分输出是由真实执行协议(涉及到所有的实体和控制某些实体和他们之间通信的攻击者 A)产生的,还是执行理想协议(只涉及与 F 交互的虚拟实体,及和 F 交互的理想攻击者 S)产生的。如果对现实世界的任何有多项式界的攻击者 A,在理想世界存在一个有多项式界的攻击者 S,使得任何有多项式界的环境 Z 都不能以显著

*)国家自然科学基金(60473027)。秦 波 博士,讲师;伍前红 博士,副教授;王育民 教授,博导;王尚平 博士,教授;王晓峰 博士,副教授。

的概率区分是在和真实协议交互还是和理想协议交互，我们就说协议 π 实现了函数 F。可泛组合定理保证即使在任意的网络环境下，协议 π 的行为也会像理想函数一样。但最初的UC定理将系统看作一个独立的单元来分析系统的安全性，如果不同的协议共享一定的状态和随机值UC定理将不再有效。因此如果协议的不同会话共享相同的随机预言机、相同的理想密码或公共参考串，UC定理将不再适用。在文献[20]中，Canetti和Rabin引入了联合状态环境下的可泛组合概念，提出了一个新的组合操作，允许不同的协议具有一些共同的状态，解决最初的UC定理不能处理不同会话或协议共享公共状态的问题。

3 传统离散对数环境下的密钥协商协议

密钥协商协议目的是使两方或多方在一个公开网络中协商出一个公共密钥。它们大多数是在离散对数环境下实现的，其中最经典的密钥协商协议可能是Diffie-Hellman协议和Burmester-Desmedt协议[7]，它们在被动攻击下安全。Burmester-Desmedt协议于2003年在假设Diffie-Hellman协议安全的条件下完成了安全性证明[28]，Diffie-Hellman协议的安全性则直接作为了密码学中的标准假设，即CDH假设和DDH假设。

基本的Diffie-Hellman协议是一个单轮两方协议。如果在每次会话中固定一方而让另一方动态改变，从Diffie-Hellman协议就得到一种公钥加密方案，即著名的ElGamal密码体制。除了在被动攻击（窃听）下安全的基本密钥协商协议外，许多工作致力于研究如何对抗主动攻击者。这个目标基本上可以使用上一节提到的认证方法或编译器来实现。另外还有一些工作致力于研究如何提高密钥协商协议在实际应用中的效率。对两方密钥协商协议的研究已经比较成熟了（如文献[17]），这些工作已经被广泛接受。

对如何在 n 方中安全建立一个秘密信道的GKA协议的研究尚不多，也有一些工作致力于研究如何将两方的Diffie-Hellman协议推广到多方的环境[7]。其中Burmester-Desmedt协议[7]是一个两轮 n 方协议，是目前效率最高的群密钥协商（GKA）协议，其轮效率不受 n 的限制。这些协议都只考虑了被动攻击下的安全性。在抗主动攻击的认证GKA协议方面具有开创性意义的工作有文献[4-6]，最早给出了GKA协议安全性在标准模型下的形式化证明。随后，文献[13,36]中分别提出了在随机预言机模型下可证明安全的常数轮的认证GKA协议。文献[4]中的安全性模型和可证明安全性协议是用于静态认证GKA的，其安全模型源于Bellare等的两方密钥协商的安全模型[BR94]。他们的方案需要 $O(n)$ 轮。在文献[36,13]中分别独立提出了具有常数轮的静态认证GKA协议。Boyd和Nieto在随机预言机模型下证明了协议[13]的安全性。Katz和Yung提出了基于两轮协议[7]的认证静态GKA协议[28]。最近，基于标准秘密共享技术，Bresson和Catalano又提出了在标准模型下只需要两轮的可证明安全的认证静态GKA协议[2]。

对于动态群，Bresson等改进了文献[6]中的协议，提出了动态GKA协议[5]。但Bresson等的协议不是常数轮的，每一个成员在中间密钥协商材料中嵌入他们的秘密，并将用这个秘密生成的最后结果提交给下一个群成员，这就使得在启动/加入算法中的轮数和群成员数目成线性关系。在文献[3]中，Bresson等提出了一个两轮的可证明安全的认证群密钥分发协议，主要解决群成员的移动设备计算效率瓶颈，可用于功率受限的设备和无线环境。Kim等人提出了一个不使用任何信任树的两轮动态认证协议[25]，这是目前适用于动态群的最有效的GKA方案。

一些文献（如文献[13,36]）声称他们的GKA协议是一轮的。我们注意到这些密钥协商协议是基于公钥加密的，不同于以上的协议，因为它们GKA协议不是从零开始的，这里我们称一个GKA协议是从零开始的，如果在执行协议之前不需要假设任何保密信道。这些方案的一般思想是非常简单的，它们首先假设所有都同意某种公钥密钥体制并拥有一个该公钥密码体制下的公钥，然后每个用户用其他用户的公钥加密一个随机串，并公布其密文。这样每个用户可以提取来自其用户的随机串，并用一个事先同意的密钥计算函数如杂凑函数将这 n 个随机串作为输入计算共享秘钥。显然，这样的协议不是从零开始的。因为在建立GKA协议之前需要一个长期的公钥来提供点对点的机密信道。注意到这些协议不是前向安全的，如果某个用户的长期秘密钥泄漏的话。为了解决这个问题，在运行该协议之前，用户必须生成一个新的公钥。这就表明这样的协议至少需要两轮。因此，构造单轮的 n 方密钥协商协议仍然是一个公开问题。

4 基于对的密钥协商协议

关于基于双线性对的密钥协商协议的研究，我们首先回顾Sakai等人[35]和Joux[24]的工作，这些结果为后来的著名Boneh-Franklin基于身份的加密方案铺平了道路。然后我们讨论文献[35,24]中的密钥协商协议是如何扩展的以及基于身份的密钥协商协议和多方密钥协商协议的研究状况。

4.1 非交互式密钥分发方案（NIKDS）

像Diffie-Hellman协议那样的交互式协议当然可以在用户之间建立共享密钥。然而双向信道并不总是可能的，比如其中一个用户处于离线状态。另外有时候即使可能建立双向信道，但其代价也会过于高昂，比如收音机或电视机可以接收卫星信号，但让它们向卫星发射信号在经济上就没有意义。密钥分发是一种特殊的密钥建立机制，其中有一个可信方为其它参与者生成密钥，它可以为上述环境中的用户建立共享密钥。Sakai等人[35]针对这个问题提出了基于双线性对的解决方案，构造了一个非交互式密钥分发方案（NIKDS）。不久Dupont和Enge重新发现了与Sakai等的NIKDS非常接近的一个版本[21]，每个实体接收两部分私钥，其安全证明需要将杂凑函数看作一个随机预言机。

上述协议是两方NIKDS协议，其中一个可信方为两个用户生成独立的密钥，而两个用户不需要发送任何消息就可以共享一个密钥。如果能够获得交互式通信，三方能否还像上述协议类似地快速地建立一个共享密钥呢？这个问题事实上在1976年的Diffie-Hellman协议之后一直是一个公开问题，直到2000年，几乎在Sakai等人提出他们的两方NIKDS的同时，Joux[24]提出了一个新颖的三方密钥协商协议，其中每一方只需要广播一次消息就能实现密钥协商。因此，Joux协议只需要一轮通信就能在三方中共享一个密钥，而在椭圆曲线上Diffie-Hellman协议的朴素扩展需要两轮，两者形成了鲜明的对比。

Sakai等人的方案一个重要且吸引人的特点是该协议是基于身份的。基于身份的密码体制的概念可以追溯到Shamir[35]的工作，他的想法是不要公钥和笨拙的公钥证书，

而在密码方案和协议中只用实体的身份(或者其它的标识信息)来生成他们的公钥,由一个可信机构 TA 来代替证书机构 CA,负责分发实体的私钥和维护系统参数。尽管 Shamir 和许多作者都构造出了基于身份的签字方案,但是在基于双线性对的密码学出现之前,构造可证明安全的基于身份加密(IBE)的实用方案一直是一个公开的问题。2001 年,Boneh 和 Franklin 提出第一个这样的 IBE 方案[10]。考察文献[35,24,10]可以发现,在解决这个存在近 20 年的公开问题的过程中,Sakai 等人和 Joux 的工作为著名的 Boneh-Franklin IBE 方案[10]提供了关键的思想。

4.2 基于身份的密钥协商

Smart 最早提出双线性对可能用于设计基于身份的认证密钥协商协议,他的协议使用 Boneh-FranklinIBE 方案同样的密钥生成机制,该协议还考虑提供密钥证实,使每个实体相信其他实体实际上也计算出了共享密钥。尽管没有给出形式化的安全分析,目前为止还没发现对该方案的攻击。

在 Smart 协议里每个参与者需要计算两个对,Chen 和 Kudla[19]给出了另外一个协议只需要计算一个对。在公钥环境下 Bellare-Rogaway 模型由 Blake 和 Wilson 等所作的扩展[11]是适用于这类协议的一种有用的安全模型,在文献[18]中证明了上述协议在这个模型下是安全的认证密钥协商协议。这个结果的最初证明有缺陷,在文献[19]中给出的更正需要对攻击者行为进行一个很严格的限制。Chen 和 Kudla 还考虑了他们协议的一些修改,提供前向保密性,反托管以及支持多 TA 等功能。

还有其他一些作者试图改进 Smart 协议。在文献[34]中证明 Shim 的改进协议在中间人攻击下是很脆弱的。Yi 的协议[38]利用了一种点压缩形式,只需 Smart 协议一半的带宽。Boyd 等在文献[12]中提出另外一种基于身份密钥协商的方法,所得协议在 BCK 模型下可证明是安全的,该协议的一个有趣特征是提供可否认服务,这是由于任何一方都可以计算出协议执行中的所有消息,因此两方都可以否认参与了协议。文献[12]的作者尝试把基于身份加密用作一种会话密钥传输机制,用以提高系统的效率。在文献[9]中研究了在"秘密握手"中使用 Smart 协议,还考虑将这些协议集成到 SSL/TLS 协议套装中。

4.3 基于对的多方认证密钥协商协议

由于 Joux 协议是非认证的,因此容易遭到中间人攻击。强化协议安全性的一种显然方法是对瞬息消息加上签字,在文献[1]中却描述了一种无需签字的高效方法来保证 Joux 协议的安全性。也许有点令人意外,和 Diffie-Hellman 协议在非广播环境下带密钥证实的三方认证协议的简单扩展相比,文献[1]中证明上述认证 Joux 协议并没有什么优势,因为此种环境下任何安全的协议都至少需要六个消息。Galbraith 等研究了 BDH 问题的比特安全性,他们的结果可以用于文献[1]中的协议,证明根据这些协议交换的原始密钥材料使用有限域的迹运算来计算会话密钥也是安全的。

对文献[1]中协议的攻击表明在三方协议中加上认证是一件微妙的工作。Zhang 和 Liu 研究了 Joux 协议基于身份的认证版,Nalla 和 Reddy[31]也提出了基于身份的三方密钥协商协议,但都被攻破了[16],同时攻破[34]的还有 Shim 的三方协议。一些作者[33,8]考虑了用 Joux 协议构造多于三方的协议,然而对多于三方的情形,Joux 协议并不能提供多少帮助,在这种环境下实现单轮密钥协商是一个更有挑战性的公开问题。

5 基于口令的密钥协商协议

与熵很高的随机密钥不同,口令的熵通常很低,容易记忆,不必使用可信硬件产生或存储随机密钥。当然,从另一方面讲,低熵的口令容易遭到穷举搜索。如何在两方或多方中使用提前共享的由低熵口令组成的秘密信息来认证生成高质量的密钥,这是基于口令的密钥协商要解决的主要问题。在这种环境中,攻击者可以穷举整个口令空间,借助在线字典攻击来选择正确的口令,冒充一方使用每一个可能的共享秘密。因为这样的攻击是不可避免的,这个领域的工作就集中在如何防止离线字典攻击,保证在线穷举攻击是最有效的攻击,也就是说,为了验证每一个猜测的口令,攻击者必须模仿一个合法用户。除了攻击者的猜测是否正确,这种交互不会泄漏其它任何有用的信息。

最早的基于口令的会话密钥生成协议是由 Bellovin 和 Merritt 提出的。这个协议影响很大,是这个领域后面许多工作[32,37]的基础。不使用任何附加的启动程序就可获得安全性的协议最早是由 Goldreich 和 Lindell[22]提出的。最近,Katz 等[26]提出了在公共参考串模型下基于口令的高效认证密钥协商协议。在文献[23]中,Gennaro 和 Lindell 提出了在公共参考串模型中基于口令的认证密钥协商协议的一般框架。大多数协议不能解决适应性环境下的强勾结问题,但也有几个例外,包括两方的 HMQV 协议和 NAXOS[29]协议,以及 Katz 和 Shin[27]在群 AKE 下的工作,但是他们都假设存在公钥基础设施,不是真正的基于口令的密钥协商协议。

结束语 就像 Joux[24]评论的那样,在一些情况下,两轮密钥协商协议比较麻烦,单轮协议要方便得多。例如在一个群中协商出一个电子邮箱的密钥,使用两轮协议就要求所有用户都在线,这对成员较多的群来说很不现实。另一个例子是群中互相信任的用户希望在不安全的 Internet 上共享他们的私人文件,单轮 GKA 协议可以轻松解决这个问题,每个用户只需广播一次消息,不需要第三方,用户也不必一直保持在线。但是如果采用两轮协议,所有的用户必须都同时在线才能生成一个共享密钥。遗憾的是,到目前为止如何实现一个单轮 GKA 协议仍然是一个公开问题,其解决方案不仅具有理论重要性,而且也具有非常重要的实用价值。

认证密钥协商允许用户在存在主动攻击者的公开网络建立共享密钥,但我们应注意到这里的主动攻击者不包括参与协议的成员,因此在这种模型里的攻击者都是外部攻击者。最近,Katz 和 Shin[27]形式化了存在内部攻击者的认证群密钥协商协议的安全模型与定义,但 Katz 和 Shin 并没有给出达到此种安全性的协议,也没有证明现有协议在他们的模型下是安全的,因此实现这些可证明的安全协议将是很有意义的工作。还可以进一步强化 Katz 和 Shin 的模型,考虑如何实现在群密钥协商协议中实现内部攻击者的追踪,尤其是追踪恶意泄漏群成员协商的密钥的内部成员,这类似于在广播系统中的叛徒追踪。然而由于群密钥协商协议后群成员共享的是同一个密钥,因此在群密钥协商中合理地给出叛徒追踪的模型与安全定义也是颇有挑战性的。

参 考 文 献

[1] Al-Riyami S S, Paterson K G. Authenticated three party key agreement protocols from pairings // Cryptography and Coding

2003, LNCS 2898. Springer-Verlag, 2003: 332-359

[2] Bresson E, Catalano D. Constant round authenticated group key agreement via distributed computation // PKC 2004, LNCS 2947. Springer- Verlag, 2004: 115-129

[3] Bresson E, Chevassut O, Essiari A, et al. Mutual authentication and group key agreement for low-power mobile devices. Computer Communication, 2004, 27(17): 1730-1737

[4] Bresson E, Chevassut O, Pointcheval D. Provably authenticated group Diffie- Hellman key exchange -the dynamic case // Asiacrypt'01, LNCS 2248. Springer- Verlag, 2001: 290-309

[5] Bresson E, Chevassut O, Pointcheval D. Dynamic group Diffie-Hellman key exchange under standard assumptions // Eurocrpt'02, LNCS 2332. Springer-Verlag, 2002: 321-336

[6] Bresson E, Chevassut O, Pointcheval D, et al. Provably authenticated group Diffie-Hellman key exchange. ACM CCCS'01, ACM, 2001: 255-264

[7] Burmester M, Desmedt Y. A secure and efficient conference key distribution system // Eurocrypt'94, LNCS 950. Springer-Verlag, 1994: 275-286

[8] Barua R, Dutta R, Sarkar P. Extending Joux's protocol to multi-party key agreement // Indocrypt'03, LNCS 2551. Springer-Verlag, 2003: 205-217

[9] Balfanz D, Durfee G, Shankar N, et al. Secret handshakes from pairing-based key agreements // Proc. of S&P'03. IEEE Press, 2003: 180-196

[10] Boneh D, Franklin M. Identity based encryption from the Weil pairing // Crypto'2001, LNCS 2139. Springer-Verlag, 2001: 213-229

[11] Blake-Wilson S, Johnson D, Menezes A. Key agreement protocols and their security analysis // Cryptography and Coding, LNCS 1355. Springer-Verlag, 1997: 30-45

[12] Boyd C, Mao W, Paterson K G. Deniable authenticated key establishment for Internet protocols // Proc. of Workshop on Security Protocols 2003, LNCS 3364. Springer-Verlag, 2003: 255-271

[13] Boyd C, Nieto J M G. Round-optimal contributory conference key agreement // PKC'03, LNCS 2567. Springer-Verlag, 2003: 161-174

[14] Bellare M, Pointcheval D, Rogaway P. Authenticated key exchange secure against dictionary attacks // Eurocrypt'00, LNCS 1807. Springer-Verlag, 2000: 139-155

[15] Canetti R. Universally composable security: A new paradigm for cryptographic protocols // FOCS'01. IEEE Computer Society, 2001: 136-145

[16] Chen Z. Security analysis of Nalla-Reddy's ID-based tripartite authenticated key agreement protocols. In IACR e-print archive. http://eprint.iacr.org/., # 2003/103, 2003

[17] Canetti R, Krawczyk H. Analysis of key-exchange protocols and their use for building secure channels // B. Pfitzmann, ed. Advances in Cryptology - EUROCRYPT 2001, LNCS 2045. Springer-Verlag, 2001: 453-474

[18] Chen L, Kudla C. Identity based authenticated key agreement protocols from pairings. In IACR e-print archive. Available at: http://eprint.iacr.org/., #2002/184, 2002

[19] Chen L, Kudla C. Identity based authenticated key agreement protocols from pairings // IEEE Computer Security Foundations Workshop. IEEE Computer Society Press, 2003: 219-233

[20] Canetti R, Rabin T. Universal composition with joint state // Crypto'03, LNCS 2729. Springer-Verlag, 2003: 265-281

[21] Dupont R, Enge A. Practical non-interactive key distribution based on pairings. In IACR e-print archive. Available at: http://eprint.iacr.org/., # 2002/136, 2002

[22] Goldreich O, Lindell Y. Session key generation using human passwords only // Crypto'01, LNCS 2139. Springer-Verlag, 2001: 408-432

[23] Gennaro R, Lindell Y. A framework for password-based authenticated key exchange // Eurocrypt'03, LNCS 2656. Springer-Verlag, 2003: 524-543

[24] Joux A. A one round protocol for tripartite Diffie-Hellman // ANTS IV, LNCS 1838. Springer-Verlag, 2000: 385-394

[25] Kim H-J, Lee S-M, Lee D H. Constant-round authenticated group key exchange for dynamic groups // Asiacrypt'04, LNCS 3329. Springer-Verlag, 2004: 245-259

[26] Katz J, Ostrovsky R, Yung M. Practical password-authenticated key exchange provably secure under standard assumptions // Eurocrypt'01, LNCS 2045. Springer-Verlag, 2001: 475-494

[27] Katz J, Shin J. Modeling insider attacks on group key-exchange protocols // ACM Conference on Computer and Communications Security. 2005: 180-189

[28] Katz J, Yung M. Scalable Protocols for Authenticated Group Key Exchange // Crypto'03, LNCS 2729. Springer-Verlag, 2003: 110-125

[29] LaMacchia B, Lauter K, Mityagin A. Stronger security of authenticated key exchange. Cryptology ePrint Archive, Report 2006/73. 2006. http://eprint.iacr.org/

[30] Mayer A, Yung M. Secure protocol transformation via "expansion": from two-party to groups // ACM-CCS'99, ACM. 1999: 83-92

[31] Nalla D, Reddy K C. ID-based tripartite authenticated key agreement protocols from pairings. In IACR e-print archive. Available at: http://eprint.iacr.org/., #2003/04, 2003

[32] Patel S. Number theoretic attacks on secure password schemes // Proc. of the 1997 IEEE Symposium on Security and Privacy. IEEE Computer Society, 1997: 236-247

[33] Reddy K C, Nalla D. Identity based authenticated group key agreement protocol // A. Menezes and P. Sarkar, eds. Indocrypt'02, LNCS 2551. Springer-Verlag, 2002: 215-233

[34] Sun H-M, Hsieh B-T. Security analysis of Shim's authenticated key agreement protocols from pairings. In IACR e-print archive. Available at: http://eprint.iacr.org/., # 2003/113, 2003

[35] Shamir A. Identity based cryptosystems and signature schemes // Crypto'84, LNCS 196. Springer-Verlag, 1985: 47-53

[35] Sakai R, Ohgishi K, Kasahara M. Cryptosystem based on pairing // Symposium on Cryptography and Information Security—SCIS 2000. Okinawa, Japan, 2000

[36] Tzeng W-G, Tzeng Z-J. Round efficient conference key agreement protocols with provable security // Asiacrypt'00, LNCS 1976. Springer-Verlag, 2000: 614-627

[37] Wu T. The Secure Remote Password Protocol // 1998 Internet Society Symposium on Network and Distributed System Security. 1998: 97-111

[38] Yi X. Efficient ID-based key agreement from Weil pairing. Electronics Letters, 2003, 39: 206-208