

标准模型下可证安全的身份基认证密钥协商协议

王圣宝^{1),2)} 曹珍富¹⁾ 董晓蕾¹⁾

¹⁾(上海交通大学计算机科学与工程系 上海 200240)

²⁾(中国人民解放军炮兵学院计算中心 合肥 230031)

摘 要 提出一个在标准模型下可证安全的双方身份基密钥协商协议. 新协议的设计思想来源于 Gentry 的身份基加密方案. 提出的新协议可工作于托管或者无托管两种模式. 在标准模型下(即不利用随机预言假设),文中给出了该协议的安全性证明. 新提出的协议与目前现有仅在随机预言模型中证明安全的协议相比,在计算和通信效率方面相当.

关键词 身份基密码学;认证密钥协商;双线性配对;标准模型

中图法分类号 TP309

Provably Secure Identity-Based Authenticated Key Agreement Protocols in the Standard Model

WANG Sheng-Bao^{1),2)} CAO Zhen-Fu¹⁾ DONG Xiao-Lei¹⁾

¹⁾(Department of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai 200240)

²⁾(Computing Center, Artillery Academy of PLA of China, Hefei 230031)

Abstract This paper presents an identity-based key agreement protocols that are provably secure without random oracles (namely, in the standard model). It is inspired by a new identity-based encryption scheme first proposed by Gentry. This paper details how this key agreement can be used in either escrowed or escrowless mode. All the proposed protocols are compared performance (with respect to computational and communication efficiencies) to all known protocols that are only proven secure in the random oracle model.

Keywords identity-based cryptography; authenticated key agreement; bilinear pairings; standard model

1 引 言

在安全通信领域,密钥协商协议具有重要的基础性作用. 大致地说,双方认证密钥协商协议不仅能够使得两个通过不安全信道通信的用户能够协商达成一个共享的会话密钥(session key),还能让这两个用户彼此认证对方的身份^[1]. 协商得到的会话密

钥可以为后续的通信会话提供保密、认证或者完整性等安全服务.

1976年,Diffie和Hellman^[2]开创性地提出了公钥密码学的概念. 同时,文献[2]也提出了第一个密钥协商协议——Diffie-Hellman协议. 若在一个密钥协商协议中,协议的某一参与方A确信除了他的意定伙伴B之外,没有其他任何别的一方能够与他计算获得相同的某个会话密钥,那么我们就说该

协议提供了(从 B 到 A 的)隐式密钥认证(Implicit Key Authentication, IKA). 认证密钥协商协议能够同时提供协议参与方之间的双向隐式密钥认证. 进而, 若一个认证密钥协议能够使得协议的某一参与方 A 确信协议的另一参与方 B 确实拥有了某个会话密钥, 那么我们说该认证密钥协商协议提供了密钥确认(key confirmation)属性. 能提供双向密钥确认的认证密钥协商协议, 叫做带密钥确认的认证密钥协商协议. 密钥协商协议可以使用对称密码学或者公钥密码学技术, 本文我们只考虑使用公钥密码学技术的双方密钥协商协议.

身份基密码学(Identity-Based Cryptography, IBC)的概念最早由 Shamir 于 1984 年提出^[3], 它的基本思想是: 终端用户可以选取任意一个字符串(例如, 电子邮件地址或其它在线身份标识)来作为他们的公钥. 这一做法大大地降低了密码系统中密钥管理的复杂度^[4]. 2001 年, Boneh 和 Franklin^[5] 利用双线性配对(bilinear pairing)给出了第一个可行的身份基加密(Identity-Based Encryption, IBE)方案, 该方案是 ElGamal 加密方案^[6]的一个变体. 紧接着在 2002 年, Smart^[7] 利用 Boneh-Franklin 身份基加密方案的思想, 设计了第一个基于双线性配对的身份基认证密钥协商协议. 从那以后, 大量使用双线性配对的身份基认证密钥协商协议被许多学者陆续提出(例如, 文献[4, 7-15]).

本文研究的出发点. 随机预言模型(Random Oracle Model, ROM)自从于 1993 年被 Bellare 和 Rogaway^[16] 提出以来, 就成为可证安全(provable security)领域的一项主要技术手段. 据我们所知, 现有文献中所有安全的身份基密钥协商协议, 无论使用双线性配对与否, 其安全性都只在随机预言模型下得到证明(例如, 文献[4, 9, 11, 13-15]等). 然而, 众所周知, 随机预言模型下的安全并不代表真实世界的安全, 因为它依赖于现实世界无法实现的随机预言(Random Oracle, RO)假设. 而另一方面, 不需要随机预言假设的证明(即, 在标准模型下的证明)能够清楚地表明, 除非其所基于的底层难题被破解, 否则一个可证安全的密码方案不可能被攻破. 因此, 如果我们在方案的安全证明过程中不依赖理想化的函数(例如, 随机预言机 RO), 那么该方案的安全性证明将能够提供更充分的保障. 简而言之, 设计在标准模型(standard model)下可证安全的身份基认证密钥协商协议, 是本文研究工作的基本出发点.

另外, 大多数现有身份基认证密钥协商协议

都具有会话密钥托管(session key escrow)的属性, 也就是说私钥生成中心(Private Key Generator, PKG)能够通过被动窃听的方式, 计算获得它的所有用户生成的会话密钥. 正如文献[4]所指出的那样, 在不同的应用场合, 这一属性可能是可容许的, 或者是不可接受的, 亦或又是理想的. 例如, 在某些应用场合(比如医疗、卫生行业), 机密性与审计追踪都是法律规定所必须满足的条件, 因此会话密钥托管是一个理想的属性. 然而在另外一些场合, 例如个人通信领域, 尽管每个用户都需信赖 PKG 不会泄漏他们的长期私钥(因为所有用户的长期私钥都是由他们的 PKG 负责生成和分发的), 但是, 为了最大程度地保护用户的隐私, 会话密钥托管的属性最好还是能够被去除或关闭^[4].

利用 Gentry 在 2006 年欧密会(Eurocrypt 2006)上提出的一个全新身份基加密方案^[17], 本文提出一个安全的双方身份基认证密钥协商协议, 它可以工作于托管或者无托管两种模式, 在应用上具有很好的灵活性. 并且, 新协议不使用任何加密或者签名方案, 因此具有较高的运行效率. 最重要的是, 我们在标准模型下, 给出新提出协议的严格形式化安全证明.

协议设计策略. 从运行效率角度来看, 不使用任何签名和加密方案的密钥协商协议具有很多优点. 因此, 这样的协议更适合于移动或无线通信领域^[18]. 利用 ElGamal^[6] 类型公钥加密方案来设计双方认证密钥协商协议的思想, 最初是由三位日本学者 Matsumoto, Takashima 及 Imai 于 1986 年提出的. 在文献[19]中, 他们给出了一系列认证 Diffie-Hellman 密钥协商协议, 也就是说, 这些协议在原始 Diffie-Hellman 协议的基础上引入了认证功能. 这些认证密钥协商协议, 就是著名的 MTI 协议族^[19]. 特别的, 其中的 MTI/A0 协议的设计思想完全基于 ElGamal 加密方案. 其具体设计思路为: (1) 首先, 协议的两个参与方分别利用 ElGmal 加密方案中的单向密钥传输(one-way authenticated key transpot)思想, 向对方秘密地传输一个会话密钥; (2) 接着, 双方分别“解密”得到对方传输来的密钥; (3) 最后, 双方分别将自己产生的密钥和解密得到的密钥相乘, 即得到最终的会话密钥. 我们把这一协商过程形象地称作“加密-解密”密钥协商. 但是注意, 这里所谓的“加密”和“解密”只是利用了 ElGamal 加密方案中的单向密钥传输的思想, 实际上并没有真正对某个明文消息的加密或者解密操作. 因此, 这样得到

的密钥协商协议具有较高的运行效率. 利用这一设计思想的后续类似协议有 Goss 协议^[20]、美国国家安全局 NSA 于 1994 年设计的 KEA 协议^①以及 Blake-Wilson 等学者在文献[21]中所提出的第四个协议.

我们指出, 上述认证 Diffie-Hellman 协议设计的思想, 可以被扩展到身份基密码学领域. 2002 年, Smart^[7]正是利用了该设计思想, 给出了第一个来自于双线性配对的身份基认证密钥协商协议(尽管 Smart 本人并没有明确地提到这一设计思想). 本文中, 我们再次利用这一杰出设计思想, 给出一个新的身份基认证密钥协商协议. 同 Smart 的协议一样, 我们的新协议也使用双线性配对作为基本工具.

本文第 2 节, 我们给出一些相关背景知识与定义; 第 3 节简要回顾 Gentry 的身份基加密方案; 接着在第 4 节, 我们提出新协议, 并简要分析其运行效率; 在第 5 节, 我们在标准模型下, 证明所提新协议的安全性; 最后, 第 6 节总结全文.

2 背景知识及定义

2.1 安全属性

文献[1,9,22-23]等定义了(身份基)认证密钥协商协议的安全属性. 我们简要总结如下(更详细描述参见文献[1,22]):

(1) 已知密钥安全(known-key secrecy). 当两个协议参与者之间共享的某个会话密钥泄露之后, 要求获得该密钥的攻击者(adversary)无法根据已获得的会话密钥求出其它会话密钥.

(2) 完美前向安全(Perfect Forward Secrecy, PFS). 若两个协议参与者的长期私钥都泄露, 攻击者不能由此求出他们在私钥泄露之前协商获得的会话密钥.

(3) PKG 前向安全(PKG Forward Secrecy, PKG-FS). 对于身份基密钥协商协议, 若在某一时刻, PKG 的主私钥(master key)泄露, 获得该主私钥的攻击者仍然不能够求出该 PKG 的用户之前协商获得的会话密钥. 注意, PKG 前向安全性同时意味着 PKG 不能被动地托管(escrow)其用户之间协商达成的会话密钥.

(4) 抗密钥泄漏伪装攻击(Key-Compromise Impersonation (K-CI) resilience). 假设实体 A 和 B 是两个协议参与者, 则当实体 A 的长期私钥泄漏之后, 很显然, 一个获得该私钥的攻击者能够向其他用

户(例如 B)来冒充 A. 然而, 我们还希望这一密钥泄漏不能够使得攻击者反过来向实体 A 冒充为其他用户(例如 B).

(5) 抗未知密钥共享(Unknown Key-Share (UK-S) resilience). 实体 A 不会在其不知对方身份的情况下, 与某个实体 B 协商达成一个共享会话密钥. 也就是说, 当实体 A 与 B 之间协商达成一个会话密钥之后, 要求 A 不会错误地认为该密钥是和另外某个实体(比如 C)共享的.

(6) 无密钥控制(No key control). 无论是两个诚实的协议参与者(A 和 B), 还是某个攻击者, 都不能将 A 和 B 之间正在协商的会话密钥的全部或部分设置成某个其预先选定的值.

认证密钥协商协议的运行性能指标主要包括计算负荷、消息传递次数及通信带宽(或通信数据量).

2.2 形式化安全模型

本小节我们简要回顾 Chen 等学者在文献[14]中定义的身份基密钥协商协议的形式化安全模型. 他们的模型是 Blake-Wilson 等学者提出的公钥环境(public-key setting)下密钥协商协议安全模型^[22]向身份基密码学领域的扩展, 而后者来源于对称密码环境(symetric-key setting)下 Bellare-Rogaway 模型^[24].

这一模型包括了一个协议参与者集合 U , 每个参与者被模拟为一组预言机(oracle), 例如, 预言机 $\Pi_{I,J}^n$ 模拟协议参与者 I 正在同它的意定伙伴(intended partner) J 进行第 n 次密钥协商, 也即 I 与 J 之间的第 n 次协议运行(run). 每个协议参与者都拥有一个长期的公/私钥对. 其中, 公钥可根据他们的身份信息 ID 求得, 而私钥则由 PKG 负责秘密生成和分发.

模型中还包括一个主动攻击者(用 E 表示), 它被定义为一个概率多项式时间图灵机, 并且它能够访问模型中的所有预言机. 协议参与者的所有预言机只能被动地回答攻击者 E 对它们进行的各种查询(query), 预言机之间并不进行直接的通信. 也就是说, 模型中至少存在一个良性(benign)攻击者, 它唯一的动作就是忠实地传递预言机之间的协议消息.

定义 1. 匹配对话(matching conversation). 如果某个预言机 $\Pi_{I,J}^n$ 发出的每条消息都相继被传送

① NIST, SKIPJACK and KEA Algorithm Specification. <http://csrc.nist.gov/encryption/skipjack/skipjack.pdf>, 1998

到另外一个预言机 $\Pi'_{j,l}$, 并且 $\Pi'_{j,l}$ 的应答消息也被传回到 $\Pi_{i,j}$, 作为其会话脚本记录 (transcript, $T_{\Pi_{i,j}}$) 的相应的下一条消息, 那么我们说这两个预言机之间拥有了匹配对话。自然地, 拥有匹配对话的两个预言机互称为匹配预言机 (matching oracle)。

我们通过一个在挑战者 (Challenger, \mathcal{C}) 和攻击者 E 之间的游戏 (game) 来定义密钥协商协议的安全性。这一游戏被划分为两个阶段。在第一个阶段, 攻击者 E 被允许进行下面的预言机查询 (oracle query), 并且这些查询可以是无序和自适应的。

Send 查询。 E 可以向预言机 $\Pi_{i,j}$ 发送消息 M 。该预言机按照协议规范应答一个响应消息 m 。预言机将每个收到和发出的消息都记入它的运行脚步记录 $T_{\Pi_{i,j}}$ 中。若预言机收到的第一条消息 $M = \emptyset$, 那么该预言机作为发起者 (initiator) 发起一次会话。否则, 它担任响应者 (responder) 的角色。

Corrupt 查询。 此查询要求被询问的协议参与者返回它拥有的长期私钥。相应地, 回答过 Corrupt 查询的实体的状态被称为“已腐化” (corrupted)。

Reveal 查询。 收到此查询的预言机, 返回它协商得到的会话密钥。如果该预言机的状态还不是“已接受” (accepted), 那么它返回一个符号 \perp 表示终止。

Test 查询。 在游戏的某个时刻, E 可以向一个“新鲜” (fresh, 见定义 2) 的预言机发出 Test 查询。 E 将收到该预言机所拥有的会话密钥或者一个随机值。具体来说, 该新鲜预言机通过投掷一枚公平硬币 $b \in \{0, 1\}$ 来回答此查询: 若投币结果为 0, 那么它返回自己协商获得的会话密钥; 否则, 它返回会话密钥空间 $\{0, 1\}^k$ 上的一个随机值。这里, k 表示会话密钥的比特长度。

在游戏的第二阶段, E 可以继续针对预言机进行 Send, Reveal 和 Corrupt 查询。 E 所受到的限制为: 它不能对它所选被测试 (Tested) 的预言机及其匹配预言机 (若匹配预言机存在的话) 进行 Reveal 查询。另外, E 也不能对被测试参与者的意定伙伴进行 Corrupt 查询。

输出。 最后, E 输出一个对 b 的判断 (记为 b')。若 $b' = b$, 那么我们称 E 赢得了此游戏。我们定义 E 的获胜优势如下 (其中, l 为安全参数):

$$\text{Advantage}^E(l) = |\Pr[b' = b] - 1/2|.$$

定义 2. 新鲜 Oracle. 若预言机 $\Pi_{i,j}$ 的状态是“已接受” (即它计算获得了一个会话密钥 sk_i), 且它满足: (1) 没有被询问过 Reveal 查询; (2) J 没有被腐化 (uncorrupted); (3) 它的匹配预言机 $\Pi'_{j,l}$ (如果

存在的话) 也没有被询问过 Reveal 查询, 那么我们称该预言机 $\Pi_{i,j}$ 是新鲜的。

定义 3. 安全密钥协商协议^[24]. 若一个密钥协商协议满足如下 3 个条件:

(1) 在只存在一个忠实地转发协议消息的良性攻击者的情况下, 预言机 $\Pi_{i,j}$ 和它的匹配预言机 $\Pi'_{j,l}$ 总能计算获得一个相同的会话密钥, 且该会话密钥均匀随机分布在会话密钥空间 $\{0, 1\}^k$ 上;

(2) 对于任何恶性攻击者 E : 任何匹配预言机 $\Pi_{i,j}$ 和 $\Pi'_{j,l}$ 总能计算获得一个相同的会话密钥;

(3) $\text{Advantage}^E(l)$ 是可忽略的。

那么, 我们称该协议是一个安全的密钥协商协议。

文献[14]分析表明, 上述形式化安全性定义涵盖了本文第 2.1 节给出的已知密钥安全、抗密钥泄漏伪装攻击 (K-CI) 以及抗未知密钥共享等基本安全属性。

2.3 双线性配对

这里我们简要介绍双线性配对的基本定义和它需满足的性质, 更详细的介绍请参考文献[5, 17]。

令 \mathbb{G}_1 和 \mathbb{G}_2 分别表示一个阶为素数 p 的乘法交换群, 且 g 是群 \mathbb{G}_1 的一个生成元。设群 \mathbb{G}_1 及 \mathbb{G}_2 上的离散对数问题 (Discrete Logarithm Problem, DLP) 都是难解的。

定义 4. 双线性配对. 一个可接受的双线性配对 (admissible pairing) e 是一个映射 $e: \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, 它满足下列 3 条性质:

(1) 双线性. 若 $u, v \in \mathbb{G}_1$ 且 $a, b \in \mathbb{Z}_p^*$, 则 $e(u^a, v^b) = e(u, v)^{ab}$;

(2) 非退化性. $e(g, g) \neq 1_{\mathbb{G}_2}$;

(3) 可计算性. 若 $u, v \in \mathbb{G}_1$, 存在多项式时间算法计算配对 $e(u, v) \in \mathbb{G}_2$ 。

2.4 计算复杂性假设

Gentry 身份基加密方案^[17] 的安全性基于一个被称为“短式增强型双线性 Diffie-Hellman 指数” (the truncated Augmented Bilinear Diffie-Hellman Exponent assumption, 或简称为 q -ABDHE) 的计算复杂性假设。下面我们简要描述判定性 (decisional) q -ABDHE 问题如下, 更详细的说明请参考文献[17]。

判定性 q -ABDHE 问题. 给定一个含 $q+3$ 个元素的向量指下面表达式左侧

$$(g', g'^{a^{q+2}}, g, g^a, g^{a^2}, \dots, g^{a^q}) \in \mathbb{G}_1^{q+3}$$

作为输入 (这里 $a \in \mathbb{Z}_p$), 一个输出为 $b \in \{0, 1\}$ 的算法 \mathcal{B} 若满足下列不等式

$|\Pr[\mathcal{B}(g', g'^{a^{q+2}}, g, g^a, g^{a^2}, \dots, g^{a^q}, e(g^{a^{q+1}}, g')) = 0 - \Pr[\mathcal{B}(g', g'^{a^{q+2}}, g, g^a, g^{a^2}, \dots, g^{a^q}, Z) = 0]| \geq \epsilon$, 那么,我们称算法 \mathcal{B} 以优势 ϵ 解决判定性 q -ABDHE 问题. 这里的概率同 g, g' 在群 \mathbb{G}_1 中的随机选取、 α 在 \mathbb{Z}_p 中的随机选取、 Z 在 \mathbb{G}_2 中的随机选取以及算法 \mathcal{B} 使用的随机比特有关.

定义 5. 判定性 (t, ϵ, q) -ABDHE 假设. 若没有 t -时间算法以最小优势 ϵ 解决 \mathbb{G}_1 中的判定性 q -ABDHE 问题,那么我们称判定性 (t, ϵ, q) -ABDHE 假设对于群 \mathbb{G}_1 及 \mathbb{G}_2 成立.

3 Gentry 身份基加密方案回顾

在这一节,我们简要回顾 Gentry 在文献[17]中给出的两个身份基加密方案中的第一个方案——在标准模型下被证明达到抗选择明文攻击(Chosen-Plaintext Attack, CPA)的 ElGamal 类型^[6]加密方案.

设群 \mathbb{G}_1 及 \mathbb{G}_2 的阶皆为素数 p , 且 $e: \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ 是一个可接受的双线性配对(定义参见第 2.3 节). Gentry 的身份基加密方案的主要步骤描述如下:

系统建立阶段(Setup). 私钥生成中心 PKG 随机选取两个生成元 $g, h \in \mathbb{G}_1$ 以及一个整数 $\alpha \in \mathbb{Z}_p$, 计算 $g_1 = g^\alpha \in \mathbb{G}_1$. 它将系统公共参数 params 设置为 $\langle g, g_1, h \rangle$, 从而,系统主私钥为 α .

私钥生成阶段(Key-Gen). 在替身份为 $ID \in \mathbb{Z}_p$ 的用户生成长期私钥之前, PKG 首先随机选取 $r_{ID} \in \mathbb{Z}_p$, 然后输出该用户的长期私钥 $d_{ID} = \langle r_{ID}, h_{ID} \rangle$, 这里 $h_{ID} = (hg^{-r_{ID}})^{1/(\alpha-ID)}$. 并且, PKG 确保 $ID \neq \alpha$ 且对每个给定的身份 ID 都赋予固定的 r_{ID} .

加密阶段(Encryption). 发送者首先随机选取 $s \in \mathbb{Z}_p$, 然后根据接收者的身份 ID , 将密文设置为(设 $m \in \mathbb{G}_2$ 为要加密的明文消息):

$$C = (g_1^s g^{-s \cdot ID}, e(g, g)^s, m \cdot e(g, h)^{-s}).$$

解密阶段(Decryption). 在收到密文 $C = (u, v, w)$ 之后, 身份为 ID 的解密者(即接收者)计算

$$m = w \cdot e(u, h_{ID}) \cdot v^{r_{ID}}.$$

一致性条件. 接收者能够从密文 C 中正确地解密获得明文消息 m , 因为

$$\begin{aligned} & e(u, h_{ID}) \cdot v^{r_{ID}} \\ &= e(g^{s(\alpha-ID)}, h^{1/(\alpha-ID)} g^{-r_{ID}/(\alpha-ID)}) \cdot e(g, g)^{sr_{ID}} \\ &= e(g, h)^s. \end{aligned}$$

4 新的身份基认证密钥协商协议

本节我们提出一个新的身份基认证密钥协商协议的两个版本, 它们分别工作于托管和无托管模式. 新协议的设计思想来源于 Gentry 的身份基加密体制(参见第 3 节).

4.1 带密钥托管的身份基密钥协商协议

我们给出的第一个协议版本(命名为 IBAK-1)不提供 PKG 前向安全(或者说主私钥前向安全). 即, 当 PKG 的主私钥 α 泄露后, 获得该私钥的攻击者能够恢复所有用户生成的会话密钥. 这一属性也意味着 PKG 能够被动地托管其所有用户协商获得的会话密钥. 很显然, 由于利用主私钥可以求得所有用户的长期私钥, 因此 PKG 前向安全也意味着完美前向安全(PFS). 然而, 我们给出的第二个协议版本(被称为 IBAK-2)能够去除 PKG 对会话密钥的托管, 也即提供了 PKG 前向安全性. 本文提出的所有协议都是两次传递(two-pass)密钥协商协议, 都只能提供双向隐式密钥认证. 这里我们指出, 上述两个协议版本都可以按照文献[9, 21]中的通用方法, 直接增强为一个能够提供双向密钥确认的三次传递(three-pass)协议.

同所有其它身份基认证密钥协商协议一样, 我们假设系统内存在一个私钥生成中心 PKG 负责为其所辖用户生成和安全分发长期私钥.

协议 IBAK-1 由 3 个阶段组成, 分别是: 系统建立阶段 Setup、私钥生成阶段 Key-Gen 和密钥协商 Key-Agreement 阶段. 其中, Setup 及 Key-Gen 阶段完全同 Gentry 身份基加密方案^[17](参见第 3 节). 因此, 这里不再赘述.

假设两个用户 Alice 和 Bob 希望通过 IBAK-1 来协商达成一个共享会话密钥(用 A 和 B 来分别代表他们的身份). 我们沿用本文先前部分的符号标记, 且分别令 $g_A = g_1 g^{-ID_A}$, $g_B = g_1 g^{-ID_B}$ 以及 $g_T = e(g, g)$. 两个协议参与者的长期私钥分别用 $\langle r_A, h_A \rangle$ 及 $\langle r_B, h_B \rangle$ 表示. 协议 IBAK-1 的密钥协商阶段 Key-Agreement 如下:

密钥协商阶段(Key-Agreement). Alice 和 Bob 首先分别随机选取一个临时私钥(分别记为 $x, y \in \mathbb{Z}_p$), 并分别计算相应的临时公钥 $T_{A1} = g_A^x$, $T_{A2} = g_T^x$ 和 $T_{B1} = g_A^y$, $T_{B2} = g_T^y$. 然后, 他们相互交换协议数据 $T_A = T_{A1} \parallel T_{A2}$ 和 $T_B = T_{B1} \parallel T_{B2}$, 如图 1 所示(其中, 符号“ \parallel ”表示比特串联接):

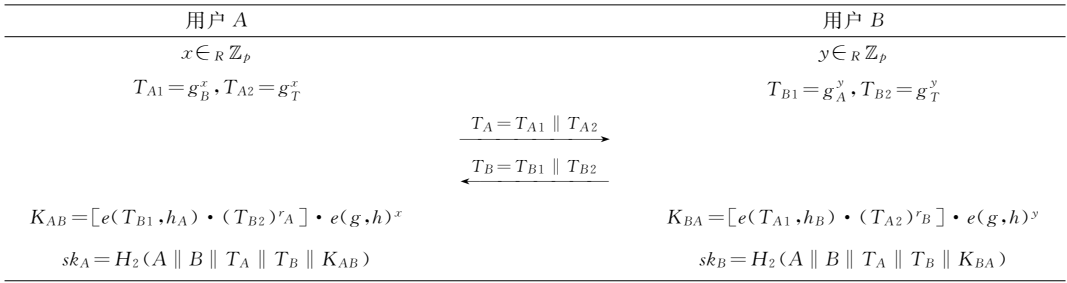


图 1 协议 IBAK-1

上述两次消息传递完成后,用户 A 和 B 分别执行如下步骤:

(1) A 计算共享秘密(shared secret) K_{AB} 如下:

$$K_{AB} = [e(T_{B1}, h_A) \cdot (T_{B2})^{r_A}] \cdot e(g, h)^x.$$

(2) B 计算共享秘密 K_{BA} 如下:

$$K_{BA} = [e(T_{A1}, h_B) \cdot (T_{A2})^{r_B}] \cdot e(g, h)^y.$$

协议正确性. 根据配对的双线性性质,我们很容易得到如下等式:

$$\begin{aligned}
 K_{AB} &= e(T_{B1}, h_A) \cdot (T_{B2})^{r_A} \cdot e(g, h)^x \\
 &= e(g_A^y, (g^{-r_A} h)^{1/(a-ID_A)}) \cdot (g_T^y)^{r_A} \cdot e(g, h)^x \\
 &= e(g^{y(a-ID_A)}, (g^{-r_A} h)^{1/(a-ID_A)}) \cdot (g_T^y)^{r_A} \cdot e(g, h)^x \\
 &= e(g^y, g^{-r_A} h) \cdot (g_T^y)^{r_A} \cdot e(g, h)^x \\
 &= e(g^y, g^{-r_A} h) \cdot e(g, g)^{y r_A} \cdot e(g, h)^x \\
 &= e(g^y, g^{-r_A} h) \cdot e(g^y, g^{r_A}) \cdot e(g, h)^x \\
 &= e(g^y, g^{-r_A} h g^{r_A}) \cdot e(g, h)^x \\
 &= e(g^y, h) \cdot e(g, h)^x \\
 &= e(g, h)^{x+y}.
 \end{aligned}$$

类似地,我们可知 Bob 计算得到的共享秘密 $K_{BA} = e(g, h)^{x+y}$. 因此,用户 Alice 和 Bob 各自独立计算的两个秘密值(即 K_{AB} 与 K_{BA})相等. 这意味着,通过运行一次协议,他们成功地协商获得了一个共享秘密 $K = K_{AB} = K_{BA}$. 他们最终的会话密钥(session key)为 $sk = H_2(A \parallel B \parallel T_A \parallel T_B \parallel K)$, 其中,Hash 函数 $H_2: \{0, 1\}^* \rightarrow \{0, 1\}^k$ 被用作密钥抽取函数(key derivation function), k 表示会话密钥的长度,即 $k = |sk|$. 注意,此处我们将协议的脚本记录(即协议中用户交换的数据 T_A 和 T_B)也作为密钥抽取函数的输入. 这样做的目的是为了防止文献[25]提到的所谓密钥复制(key replicating)攻击. 通过密钥复制攻击,攻击者 E 能够利用自己的输入来部分地影响诚实用户之间正在协商的共享秘密的最终值,尽管 E 并不会获知该共享秘密值. 这种攻击从表面上看,并没有影响最终会话密钥的保密性,似乎并不能构成什么危害. 但是,它却破坏了认证密

钥协商协议的一个基本安全属性:无密钥控制(参见第 2.1 节的相关定义).

效率分析. 协议 IBAK-1 满足角色对称(role symmetric)的性质,即协议的每一个参与者的所有操作步骤都完全相同. 同文献[4, 9]中给出的协议(这些协议都只在随机预言模型下被证明安全)相比,我们提出的新协议具有同等级别的运行效率. 在协议 IBAK-1 中,每个参与者都必须生成一个随机数,计算一个群 \mathbb{G}_1 上的指数运算(假设 g_A 与 g_B 预先计算),3 个 \mathbb{G}_2 上的指数运算以及两个配对计算. 其中,配对值 $e(g, h)$ 可以预先计算. 这样,各参与者的在线配对计算数目就减小到一个. 我们忽略 \mathbb{G}_1 及 \mathbb{G}_2 上的乘法及 Hash 函数运算,因为同其它主要运算相比,它们的计算速度要快许多.

Chen-Kudla 协议^[9]要求每个参与者生成一个随机数、计算群 \mathbb{G}_1 上的两个指数运算以及两个配对计算. 同 Chen-Kudla 协议相比,协议 IBAK-1 在计算负荷上要少计算群 \mathbb{G}_1 上的一个指数运算,只需多计算两个 \mathbb{G}_2 上的指数运算.

McCullagh-Barreto 协议^[4]要求每个参与者生成一个随机数,计算一个群 \mathbb{G}_1 上的指数运算、一个群 \mathbb{G}_2 上的指数运算以及两个配对计算. 其中的一个配对也可以预先计算. 同 McCullagh-Barreto 协议相比,协议 IBAK-1 在计算负荷上只需多计算两个 \mathbb{G}_2 上的指数运算.

在通信效率方面,协议 IBAK-1 与文献[4, 9]中的两个协议相比,传递的数据量要多出群 \mathbb{G}_1 上的一个成员. 然而我们强调,这三个协议都不能提供 PKG 前向安全性. 而在本文第 4.2 节,我们给出协议 IBAK-1 的改进版本(命名为 IBAK-2),它不增加任何通信量,却能够提供 PKG 前向安全. 协议 IBAK-2 与文献[9]中给出的 Chen-Kudla 协议的改进版本(达到 PKG 前向安全)相比,具有完全相同的通信效率.

综上所述,我们的新协议 IBAK-1 与现有协议

相比,拥有同等级别的计算和通信效率.然而,在本文第 5 节,我们将在标准模型下,证明协议 IBK-1 的安全性.也就是说,新协议与文献[4,9]中的所有协议相比,在安全性上更有保障.

会话密钥托管. 协议 IBK-1 具有会话密钥托管属性来自于以下事实:PKG 能够利用自己掌握的主私钥,恢复出系统所有用户的会话密钥.具体来说,PKG 能够计算所有用户的长期私钥,因此它也能够通过公开信道上截获的消息,计算 $e(g, h)^x$ 和 $e(g, h)^y$,从而计算获得最终的会话密钥.

4.2 无会话密钥托管的身份基密钥协商协议

正如在本文第 1 节指出的那样,在某些应用场合,会话密钥托管这一属性可能是无法让人接受的.因此在这一小节,我们通过对协议 IBK-1 的系统建立阶段 Setup 及私钥生成阶段 Key-Gen 进行小的改动,来使其改进版本——IBK-2 协议去除会话密钥托管的属性.同文献[9]中的方法类似,我们利用两个协议参与者发出的数据计算一个额外的 Diffie-Hellman 共享秘密.然而,与文献[9]中的 Chen-Kudla 协议不同,协议 IBK-2 并不增加任何额外的通信量.下面,我们详细给出协议 IBK-2 的描述,然后说明它去除了 PKG 的会话密钥托管属性.

系统建立阶段 (Setup). 与协议 IBK-1 中的 Setup 相比,这里我们要求 PKG 多选取一个 \mathbb{G}_1 的生

成元(用 t 表示). 于是,PKG 首先随机选择 3 个生成元 $g, h, t \in \mathbb{G}_1$ 以及一个随机整数 $\alpha \in \mathbb{Z}_p$,然后计算 $g_1 = g^\alpha \in \mathbb{G}_1$. PKG 将系统公共参数 params 设置为 $\langle g, g_1, h, t \rangle$,主私钥设置为 α .

私钥生成阶段 (Key-Gen). 同协议 IBK-1 中的私钥生成算法相比,IBK-2 的私钥生成过程稍微有所不同.在替身份为 $ID \in \mathbb{Z}_p$ 的用户生成长期私钥之前,PKG 首先随机选取 $r_{ID} \in \mathbb{Z}_p$,然后输出该用户的长期私钥 $d_{ID} = \langle r_{ID}, h_{ID} \rangle$,不同之处在于,这里 $h_{ID} = (ht^{-r_{ID}})^{1/(\alpha-ID)}$. 同样,PKG 确保 $ID \neq \alpha$ 且对每个给定的身份 ID 都赋予固定的 r_{ID} .

设有两个用户 Alice 和 Bob 希望利用协议 IBK-2 来协商获得他们之间的一个共享会话密钥. 同样,我们分别用 A 和 B 来表示他们的身份. 分别令 $g_A = g_1 g^{-ID_A}$, $g_B = g_1 g^{-ID_B}$ 以及 $t_T = e(g, t)^{\textcircled{1}}$. 再次,两个协议参与者的长期私钥分别用 $\langle r_A, h_A \rangle$ 及 $\langle r_B, h_B \rangle$ 表示. 协议 IBK-2 的密钥协商阶段 Key-Agreement 如下:

密钥协商阶段 (Key-Agreement). 与协议 IBK-1 类似, Alice 和 Bob 首先分别随机选取一个临时私钥(分别记为 $x, y \in \mathbb{Z}_p$),并分别计算相应的临时公钥 $T_{A_1} = g_B^x, T_{A_2} = g_T^x$ 和 $T_{B_1} = g_A^y, T_{B_2} = g_T^y$. 然后,他们相互交换数据 $T_A = T_{A_1} \parallel T_{A_2}$ 和 $T_B = T_{B_1} \parallel T_{B_2}$,如图 2 所示.

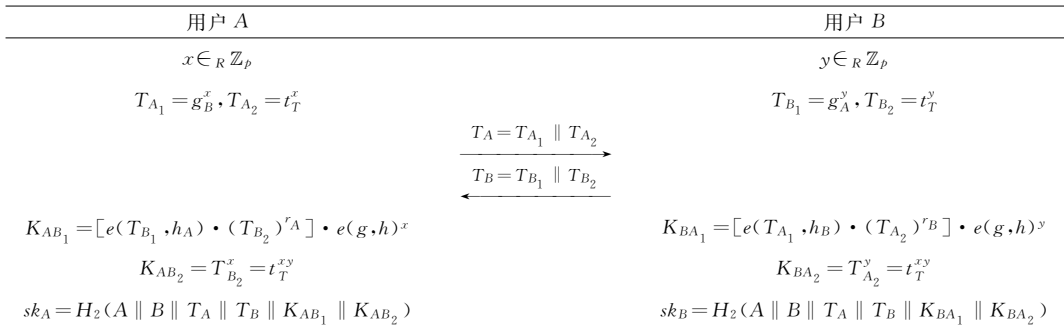


图 2 协议 IBK-2

协议正确性. 协议参与者 Alice 和 Bob 将计算获得相同的会话密钥,因为我们有如下等式:

$$\begin{aligned}
 K_{AB_1} &= e(T_{B_1}, h_A) \cdot (T_{B_2})^{r_A} \cdot e(g, h)^x \\
 &= e(g_A^y, (ht^{-r_A})^{1/(\alpha-ID_A)}) \cdot (t_T^y)^{r_A} \cdot e(g, h)^x \\
 &= e(g^{y(\alpha-ID_A)}, (ht^{-r_A})^{1/(\alpha-ID_A)}) \cdot (t_T^y)^{r_A} \cdot e(g, h)^x \\
 &= e(g^y, ht^{-r_A}) \cdot (g_T^y)^{r_A} \cdot e(g, h)^x \\
 &= e(g^y, ht^{-r_A}) \cdot e(g, t)^{yr_A} \cdot e(g, h)^x \\
 &= e(g^y, ht^{-r_A}) \cdot e(g^y, t^{r_A}) \cdot e(g, h)^x
 \end{aligned}$$

$$\begin{aligned}
 &= e(g^y, ht^{-r_A} t^{r_A}) \cdot e(g, h)^x \\
 &= e(g^y, h) \cdot e(g, h)^x \\
 &= e(g, h)^{x+y} \\
 &= K_{BA_1},
 \end{aligned}$$

$$\begin{aligned}
 K_{AB_2} &= T_{B_2}^x \\
 &= e(g, t)^{xy} \\
 &= K_{BA_2}.
 \end{aligned}$$

① 注意,在协议 IBK-1 中,我们将 g_T 记为 $e(g, g) \in \mathbb{G}_2$.

效率分析. 协议 IBAK-2 同样也满足角色对称的属性. 显然, 与其前身 IBAK-1 相比, 协议 IBAK-2 只要求每个用户多计算一个群 \mathbb{G}_2 上的指数运算.

正如前面已经指出的一样, 协议 IBAK-2 与 IBAK-1 具有完全相同的通信效率, 即通信量为群 \mathbb{G}_1 中的两个成员.

无会话密钥托管. 由于 PKG 拥有主私钥 α , 因此它能够利用 $T_{A1} = g^{x(\alpha - ID_B)}$ (相应地, $T_{B1} = g^{y(\alpha - ID_A)}$) 计算出 g^x (相应地, g^y). 从而, PKG 能够计算获得配对值 $e(g, g)^{xy}$. 但是, 它却无法计算获得 $t_T^{xy} = e(g, t)^{xy}$. 这表明 PKG 无法计算获得用户 Alice 和 Bob 之间的共享会话密钥, 也就是说, 协议 IBAK-2 去除了会话密钥托管的属性. 我们指出, 根据 t_T, t_T^x 和 t_T^y 来计算共享秘密数据 t_T^{xy} 正好是群 \mathbb{G}_2 上的难题——计算性 Diffie-Hellman (Computational Diffie-Hellman, CDH) 问题.

5 安全性证明

在本节, 我们在标准模型下 (即不利用随机预言假设) 来证明协议 IBAK-1 的安全性. 我们指出, 协议 IBAK-2 的基本安全属性可以用相同的方法得到证明, 不同之处仅在于它的安全性基于一个稍微不同的复杂性假设. 限于篇幅, 我们这里只给出协议 IBAK-1 的详细证明过程.

根据本文第 2.2 节给出的身份基密钥协商协议的安全模型及定义, 我们给出如下定理.

定理 1. 若判定性 q -ABDHE 假设对于群 \mathbb{G}_1 及 \mathbb{G}_2 成立, 那么协议 IBAK-1 是一个安全的认证密钥协商协议.

证明. 我们证明的主要思路基于文献[17].

我们首先说明条件 1 是满足的: 因为若两个协议参与者遵循协议规范, 并且攻击者 E 是良性的, 那么两个参与者都能正确地收到对方发来的协议消息. 又据协议正确性分析, 我们有 $K_{AB} = K_{BA}$, 且他们的对话是匹配的. 所以, 他们会计算获得相同的会话密钥 sk . 并且, 该密钥均匀随机分布于会话密钥空间.

其次, 条件 2 也是满足的: 若两个协议参与者都没有被腐化 (uncorrupted), 那么他们不可能被攻击者冒充; 若他们的对话是匹配的, 则意味着他们正确地收到了对方发来的协议消息, 因此他们能够计算获得相同的会话密钥 sk . 下面, 我们证明条件 3 也是满足的.

我们采用反证法. 假设存在一个攻击者 E 能够以不可忽略的优势 ϵ 在 t 时间内赢得我们定义的攻击游戏 (参见第 2.2 节), 即 E 在 Test 查询过后, 正确猜对 b 的值. 我们来说明如何构造一个模拟器 (一个被称为 simulator 的算法) S , 如何利用 E 作为预言机以另一个不可忽略的优势 ϵ' 解决判定性 q -ABDHE 问题.

给定输入. 两个群 $\mathbb{G}_1, \mathbb{G}_2$, 双线性配对 e 及一个随机的判定性 q -ABDHE 挑战 $(g', g'^{a^{q+2}}, g, g^a, g^{a^2}, \dots, g^{a^q}, Z)$, 模拟器 S 的任务是区分 Z 等于 $e(g^{a^{q+1}}, g')$ 或者只是 \mathbb{G}_2 中的一个随机成员.

模拟器算法 S 为攻击者 E 模拟攻击游戏, 它们之间的交互过程如下:

初始化阶段. 这一阶段与文献[17]中的相应初始化阶段相同. S 首先随机生成一个阶为 q 的秘密多项式 $f(x) \in \mathbb{Z}_p[x]$, 然后它设置 $h = g^{f(a)}$, 并根据 $(g, g^a, g^{a^2}, \dots, g^{a^q})$ 计算得出 h 的值. 最后, S 将系统公钥设置为 $(g, g_1 = g^a, h)$ 并把它们发送给攻击者 E , 从而系统主私钥为 α . 显然, 这一公钥与真实系统内的公钥具有相同的分布. 注意, 模拟器 S 并不知道主私钥 α 的值.

为了保证多项式 $f(x)$ 的机密性, 我们限制攻击者 E 所能进行的 Corrupt 查询的次数最多为 $q-1$ (q 为 $f(x)$ 的阶). 另外, 我们假设 E 最多发起 q_s 次协议会话 (sessions), 也就是说, 对于任意预言机 Π_{AB}^s , 都有 $s \in \{1, 2, \dots, q_s\}$. S 随机选取 3 个整数 $i, j \in \{1, 2, \dots, q\}$ 及 $n \in \{1, 2, \dots, q_s\}$, 并猜测预言机 Π_{IJ}^n 将被 E 选中来进行 Test 查询. 其中, I 和 J 分别表示 S 创建的第 i 个和第 j 个协议参与者.

Corrupt 查询. S 模拟 E 的第 u 次, 即针对 ID_u 的 Corrupt 查询如下:

若 $g^{ID_u} = g_1$ (此时 $ID_u = \alpha$), 那么 S 直接利用 α 来解决它所面临的判定性 q -ABDHE 问题. 否则, 令 $F_{ID}(x)$ 表示一个 $(q-1)$ 阶多项式 $(f(x) - f(ID_u)) / (x - ID_u)$, S 设置私钥 $\langle r_{ID_u}, h_{ID_u} \rangle$ 为 $(f(ID_u), g^{F_{ID_u}(a)})$. 这是一个关于 ID_u 的有效私钥, 因为根据要求 $g^{F_{ID_u}(a)} = g^{(f(a) - f(ID_u)) / (a - ID_u)} = (hg^{-f(ID_u)})^{1/(a - ID_u)}$. 由于 $f(x)$ 是一个均匀随机多项式, 因此这一私钥对于攻击者 E 来说是有效的, 即它满足正确的分布. 当 E 针对协议参与者 J 发出 Corrupt 查询时, S 退出游戏并报错.

Send 查询. S 诚实回答对除 Π_{IJ}^n 之外的普通预言机的 Send 查询, 即对于第一个 Send 查询, S 随机

选取一个 \mathbb{Z}_p 中的随机数来生成它的协议消息. 令 $f_2(x) = x^{q+2}$, $F_{2, ID_J}(x) = (f_2(x) - f_2(ID_J)) / (x - ID_J)$ 为一个阶为 $q+1$ 的多项式. 当攻击者 E 对预言机 $\Pi_{I,J}^n$ 发出一个 Send 查询后, S 以下面的方式为预言机 $\Pi_{I,J}^n$ 计算协议消息 T_{I1} 和 T_{I2} :

$$T_{I1} = g^{f_2(a) - f_2(ID_J)},$$

$$T_{I2} = Z \cdot e(g', \prod_{l=0}^q (g^{a^l})^{F_{2, ID_J}(l)}).$$

这里, $F_{2, ID_J, l}$ 表示 $F_{2, ID_J}(x)$ 中 x^l 的系数.

记预言机 $\Pi_{I,J}^n$ 收到的协议消息为 T_{J1} 和 T_{J2} , S 计算共享秘密 K_{IJ} 如下:

$$K_{IJ} = [e(T_{I1}, h_J) \cdot T_{I2}^{r_{J1}}] \cdot [e(T_{J1}, h_I) \cdot T_{J2}^{r_{I1}}].$$

根据协议规范, S 为预言机 $\Pi_{I,J}^n$ 计算会话密钥 sk_I 如下:

$$sk_I = H_2(I \parallel J \parallel T_{I1} \parallel T_{I2} \parallel T_{J1} \parallel T_{J2} \parallel K_{IJ}).$$

令 $\lambda = (\log_g g') F_{2, ID_J}(a)$. 若 $Z = e(g^{a^{q+1}}, g')$, 那么 $T_{I1} = g^{\lambda(a - ID_J)}$, $T_{I2} = e(g, g)^\lambda$, 且 $e(T_{I1}, h_J) \cdot T_{I2}^{r_{J1}} = e(g, h)^\lambda$. 所以, $K_{IJ} = e(g, h)^\lambda \cdot [e(T_{J1}, h_I) \cdot T_{J2}^{r_{I1}}]$ 是对应于参与者 I 在选择随机值 λ 来生成其协议消息的情况下的合法会话秘密(用于生成会话密钥 sk_I). 由于 $\log_g g'$ 和 λ 都是均匀随机分布的, 因此共享会话密钥 sk_I 对于攻击者 E 来说是有效且恰当分布的挑战.

Reveal 查询. 若攻击者 E 对预言机 $\Pi_{I,J}^n$ 或其匹配预言机 $\Pi_{J,I}^s$ (如果存在的话) 进行 Reveal 查询, 那么 S 退出游戏并报错. 否则, 它将被提出 Reveal 查询的预言机所拥有的会话密钥返回给 E .

Test 查询. 在模拟过程的某个时刻, E 将针对某个预言机进行一次 Test 查询. 若 E 没有选择 S 事先所猜测的预言机 $\Pi_{J,I}^s$ 来提出 Test 查询, 那么 S 退出游戏并报错. 然而, 若 E 恰好选择了预言机 $\Pi_{I,J}^n$ 来进行 Test 查询, S 将会话密钥 sk_I 返回给 E .

输出. 在进行过 Test 查询之后, 攻击者 E 输出它对 b 的猜测 $b' \in \{0, 1\}$.

注意, 若模拟器 S 在整个模拟过程中都没有退出, 那么攻击者 E 在该模拟游戏中的视角(view)与其在现实攻击场景中的视角完全相同. 也就是说, S 对攻击游戏的模拟是完美且让攻击者 E 无法区分的. 从而, 若 S 一直没有退出, 那么根据假设 E 是一个成功的攻击者, 我们得到 $|\Pr[b' = b] - 1/2| > \epsilon$. 这里的概率与 S 和 E 选择使用的随机比特有关.

解决判定性 q -ABDHE 问题. S 直接将 E 的输出 b' 作为回答返回给它的 q -ABDHE 问题挑战者.

若 $Z = e(g^{a^{q+1}}, g')$, 则模拟是完美的, E 将以 $\epsilon + 1/2$ 的概率猜对比特 b . 否则, 若 Z 是均匀随机的, 那么 T_{I1} 和 T_{I2} 分别是 \mathbb{G}_1 与 \mathbb{G}_2 中的独立且均匀随机成员. 因此, K_{IJ} 及 sk_I 皆均匀随机地独立于 E 的视角. 在这种情况下, E 没有任何优势猜对比特 b , 即它猜对 b 的概率只能是 $1/2$.

现在, 我们来计算 S 解决判定性 q -ABDHE 问题的优势 ϵ' . 首先, 若 S 一直没有退出模拟游戏, 我们有

$$|\Pr[\mathcal{B}(g', g'^{a^{q+2}}, g, g^a, g^{a^2}, \dots, g^{a^q}, e(g^{a^{q+1}}, g')) = 0] - \Pr[\mathcal{B}(g', g'^{a^{q+2}}, g, g^a, g^{a^2}, \dots, g^{a^q}, Z) = 0]| \geq 1/2 + \epsilon - 1/2 = \epsilon.$$

其次, S 不退出游戏的概率至少为 $1/(q^2 q_S)$. 综合上述两个结果, 我们有 $\epsilon' = \epsilon / (q^2 q_S)$.

S 的时间复杂度完全与文献[17]中的证明相同. 在上述模拟游戏中, 模拟器 S 的主要操作是计算 $g^{F_{ID}(a)}$ 以回答 E 对 ID 进行的 Corrupt 查询. 由于 $F_{ID}(x)$ 是一个 $q-1$ 阶的多项式, 因此每一次计算需要 $O(q)$ 群 \mathbb{G}_1 中的指数运算. 所以, S 的时间复杂度为 $t + O(t_{\text{exp}} \cdot q^2)$. 证毕.

6 结论与下一步工作

本文利用 Gentry 的身份基加密方案^[17], 提出了一个新的身份基认证密钥协商协议. 我们的新协议可以工作于托管或者无托管模式, 具有很强的灵活性. 并且, 我们在标准模型下, 证明了新协议的安全性基于判定性 q -ABDHE 假设. 我们的新协议是第一种能在标准模型下可证安全的身份基认证密钥协商协议.

下一步工作包括详细证明文中给出的无托管协议的安全性, 特别是它的 PKG 前向安全(也即无托管)这一属性. 另外, 我们注意到, 文中给出的托管模式下工作的协议不具有完美前向安全性. 所以, 如何在不影响其可托管这一属性的前提下引入完美前向安全, 也值得进一步研究.

致谢 匿名审稿人对本文进行了仔细阅读并提出了宝贵的修改意见, 作者在此表示衷心感谢!

参 考 文 献

[1] Blake-Wilson S, Menezes A. Authenticated Diffie-Hellman key agreement protocols//Proceedings of the SAC'98, Lecture Notes in Computer Science 1556. Berlin: Springer-Verlag, 1999: 339-361

- [2] Diffie W, Hellman M E. New directions in cryptography. *IEEE Transactions on Information Theory*, 1976, 22(6): 644-654
- [3] Shamir A. Identity-based cryptosystems and signature schemes//*Proceedings of the CRYPTO'84, Lecture Notes in Computer Science* 196. Berlin: Springer-Verlag, 1984: 47-53
- [4] McCullagh N, Barreto P S L M. A new two-party identity-based authenticated key agreement//*Proceedings of the CT-RSA'05, Lecture Notes in Computer Science* 3376. Berlin: Springer-Verlag, 2005: 262-274
- [5] Boneh D, Franklin M. Identity-based encryption from the Weil pairing//*Proceedings of the CRYPTO'01, Lecture Notes in Computer Science* 2139. Berlin: Springer-Verlag, 2001: 213-229
- [6] ElGamal T. A public key cryptosystem and signature scheme based on discrete logarithms. *IEEE Transaction on Information Theory*, 1985, 31(4): 469-472
- [7] Smart N. An ID-based authenticated key agreement protocol based on the Weil pairing. *Electronic Letters*, 2002, 38(13): 630-632
- [8] Shim K. Efficient ID-based authenticated key agreement protocol based on Weil pairing. *Electronic Letters*, 2003, 39(8): 653-654
- [9] Chen L, Kudla C. Identity based key agreement protocols from pairings//*Proceedings of the 16th IEEE Computer Security Foundations Workshop*. Los Alamitos, California: IEEE Computer Society, 2002: 219-213
- [10] Ryu E K, Yoon E J, Yoo K Y. An efficient ID-based authenticated key agreement protocol from pairings//*Proceedings of the NETWORKING'04, Lecture Notes in Computer Science* 3042. Berlin: Springer-Verlag, 2004: 1458-1463
- [11] Boyd C, Mao W, Paterson K. Key agreement using statically keyed authenticators//*Proceedings of ACNS'04, Lecture Notes in Computer Science* 3089. Berlin: Springer-Verlag, 2004: 248-262
- [12] Choie Y J, Jeong E, Lee E. Efficient identity-based authenticated key agreement protocol from pairings. *Journal of Applied Mathematics and Computation*, 2005, 162(1): 179-188
- [13] Xie G. An ID-based key agreement scheme from pairing. *Cryptology ePrint Archive, Report* 2005/093, 2005
- [14] Chen L, Cheng Z, Smart N P. Identity-based key agreement protocols from pairings. *Cryptology ePrint Archive, Report* 2006/199, 2006
- [15] Wang Y. Efficient identity-based and authenticated key agreement protocol. *Cryptology ePrint Archive, Report* 2005/108, 2005
- [16] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols//*Proceedings of the First ACM Conference on Computer and Communications Security*. New York, USA: ACM Press, 1993: 62-73
- [17] Gentry C. Practical identity-based encryption without random oracles//*Proceedings of the EUROCRYPT'06, Lecture Notes in Computer Science* 4004. Berlin: Springer-Verlag, 2006: 445-464
- [18] Kunz-Jacques S, Pointcheval D. About the Security of MTI/C0 and MQV//*Proceedings of the SCN'06, Lecture Notes in Computer Science* 4116. Berlin: Springer-Verlag, 2006: 156-172
- [19] Matsumoto T, Takashima Y, Imai H. On seeking smart public-key distribution systems. *Transaction of IEICE of Japan*, 1986, E69: 99-106
- [20] Goss K C. Cryptographic method and apparatus for public key exchange with authentication. *US Patent* 4956863, September 1990
- [21] Blake-Wilson S, Johnson D, Menezes A. Key agreement protocols and their security analysis//*Proceedings of the 6th IMA International Conference on Cryptography and Coding, Lecture Notes in Computer Science* 1355. Berlin: Springer-Verlag, 1997: 30-45
- [22] Menezes A, van Oorschot P, Vanstone S. *Handbook of applied cryptography*. Boca Raton, FL, USA: CRC Press, 1997
- [23] Boyd C, Mathuria A. *Protocols for Authentication and Key Establishment*. Berlin: Springer-Verlag, 2003
- [24] Bellare M, Rogaway P. Entity authentication and key distribution//*Proceedings of the CRYPTO'93, Lecture Notes in Computer Science* 773. Berlin: Springer-Verlag, 1994: 110-125
- [25] Choo K-K R, Boyd C, Hitchcock Y. On session key construction in provably secure protocols//*Proceedings of the MYCRYPT'05, Lecture Notes in Computer Science* 3715. Berlin: Springer-Verlag, 2005: 116-131



WANG Sheng-Bao, born in 1978, Ph.D. candidate. His research interests include applied cryptography and network information security.

CAO Zhen-Fu, born in 1962, professor, Ph.D. supervisor. His current research interests include cryptography, information security and computational number theory etc.

DONG Xiao-Lei, born in 1971, Ph.D., associate professor. Her current research interests include cryptography and number theory etc.

Background

Key agreement protocols are fundamental for establishing communications between two parties over an insecure network. The random oracle has been a popular technique in provable security since its formalization by Bellare and Rogaway in 1993. Although some have argued that a proof in the random oracle model is more of a heuristic proof than a real one, existing provably-secure identity-based authenticated key agreement protocols are usually proven secure in the random oracle model. It is generally acknowledged that security in the random oracle model does not, however, imply security in the real world.

In this work, the identity-based authenticated key agreement protocol proposed by the authors is proven secure in the standard model (i. e. , it does not use ideal functions such as random oracles). To the best of our knowledge, this is the first such protocol.

This work was supported in part by the National High Technology Research and Development Program (863 Program) of China under grant No. 2006AA01Z424 and the National Natural Science Foundation of China under grant Nos. 60673079, 60572155 and 60773086.