文章编号:1009-3087(2015)04-0125-07 DOI:10.15961/j.jsuese.2015.04.018

基于身份的跨自治域认证密钥协商协议

张 雪[1],李光松[1],韩文报[1],冀会芳[1],胡洪宇[2]
(1.信息工程大学 数学工程与先进计算国家重点实验室,河南 郑州 450002;2.驻成飞公司军代表室,四川 成都 610000)

摘 要:当前的跨信任域认证密钥协商协议都对系统参数做了限制假设,这种假设无法满足实际网络需要,为此提出了一种基于身份的跨自治域密钥协商方案,在该方案中各个PKG可以使用完全不同的公开参数以及各自不同的PKG主密钥。在eCK模型下给出了该密钥协商方案的形式化证明,表明该方案在满足基本安全属性的基础上,还具有弱的完美前向安全性、PKG前向安全性、抗密钥泄露伪装攻击以及抗临时密钥泄露攻击等属性。与几种典型的基于身份的跨域认证密钥协商方案性能对比分析表明,提出的方案更加安全高效。

关键词:基于身份;密钥协商;跨信任域;eCK模型
中图分类号:TP309 **文献标志码**:A

Identity-based Authenticated Key Agreement Protocol Cross Autonomous Domains

ZHANG Xue[1], *LI Guangsong*[1], *HAN Wenbao*[1], *JI Huifang*[1], *HU Hongyu*[2]
(1. State Key Lab. of Mathematical Eng. and Advanced Computing, Info. Eng. Univ., Zhengzhou 450002, China;
2. Military Representative Office for Chengdu Aircraft Co., Chengdu 610000, China)

Abstract: Current identity-based authenticated key agreement schemes still have restriction on PKG system parameters. The assumption limits the application in real network environment. In order to solve these problems, an identity-based cross-domain authenticated key agreement protocol was proposed. There is no restriction on PKG system parameters so that public system parameters, system master keys and system public keys can be totally different. The security of this scheme was analyzed under the eCK model, and the result showed that this protocol satisfies the basic security requirements, perfect forward secrecy and PKG forward secrecy. Moreover, this protocol is robust to the existing attacks such as key compromise impersonation attack and ephemeral key compromise impersonation attack. Comparison with some typical identity-based multi-domain authenticated key agreement protocols showed that this scheme is more secure and efficient.

Key words: identity-based; authenticated key agreement; cross-domains; eCK model

基于身份的密码体制中,用户公钥即是用户的身份信息,而用户的私钥则由权威可信方私钥生成器(private key generator, PKG)通过用户的身份信息计算得出。基于身份的密码体制避免了对称密码体制繁重的密钥管理问题,同时也避免了传统PKI公钥证书存储和管理维护开销大的问题。Shamir[1]于1984年提出基于身份的公钥体制,给出了一种基于身份的签名体制,直到2001年才由Boneh和Franklin[2]给出了第一个实用的基于身份的加密方案,该方案是基于双线性对构造的。2002年,Smart[3]结合Boneh和Franklin的设计思想提出第一个基于身份的密钥协商协议,该协议不具备PKG前向保密性。2003年,Chen和Kudla[4]第一次提出在不同PKG下的用户密钥协商协议。2004年McCullagh和Barreto[5]提出一个不同PKG环境下具有密钥托管和不托管2种模式的密钥协商协议,但随后被指出无法抵抗KCI攻击。近年来一些基于身份的密钥协商方案[6-12]以及无证书认证密钥协商方案[13-14]被陆续提出,但都无法满足不同信任域之间的密钥协商需求。石亚宾[15]、夏松[16]、尤娟[17]等先后给出了多信任域密钥协商协议,但都假设各PKG使用相同的系统公开参数,仅有系统主密钥和

收稿日期:2014-10-28
基金项目:国家自然科学基金资助项目(61201220)
作者简介:张 雪(1984—),女,博士生.研究方向:无线网络安全;信息安全.E-mail:whity_zhang@163.com

相应公钥不同,且石亚宾的方案不能抵抗临时密钥泄露攻击。当前的多信任域环境下的密钥协商方案研究大多都是基于这个假设。但实际的网络环境中,尤其是未来异构网络融合应用中,各个信任域大多都是独立的自治域,使用不同的系统参数,因此以上的方案大都难以满足实际的认证密钥协商需求。

为此,提出一种新的适用范围更广的跨信任域密钥协商方案,在该方案中各个 PKG 可以使用完全不同的系统公开参数,并且使用不同的 PKG 主密钥和公钥。

1 预备知识

1.1 双线性映射

设 G_1、G_2 分别是阶为素数 q 的加法循环群和乘法循环群,P 为群 G_1 的生成元。称映射 $e:G_1 \times G_1 \rightarrow G_2$ 为一个双线性对,若下列性质成立:

1) 双线性性:$e(aP,bQ) = e(P,Q)^{ab}$,对 $\forall P,Q \in G_1, a,b \in Z_q^*$ 均成立。

2) 非退化性:存在 $\forall P,Q \in G_1$,使得 $e(P,Q) \neq 1_{G_2}$,其中,1_{G_2} 为 G_2 的单位元。

3) 可计算性:对于 $\forall P,Q \in G_1$,存在有效算法来计算 $e(P,Q)$,即可在多项式时间内完成对 $e(P,Q)$ 的计算。

提出的方案的安全性基于以下假设:

1)CDH 假设:设 P 为 G_1 的一个生成元,给定 P、aP、bP,其中,$\forall a,b \in Z_q^*$,计算 abP 是困难的。

2)BDH 假设:设 P 为 G_1 的一个生成元,e 为定义在 (G_1,G_2) 上的双线性对,给定 P、aP、bP、cP,其中,$\forall a,b,c \in Z_q^*$,计算 $e(P,P)^{abc}$ 是困难的。

1.2 安全模型

LaMacchia 等在 CK 模型[18]的基础上进行扩展,提出了 eCK 模型[19]。倪亮等[20]指出 eCK 模型是目前为止安全性较强的两方认证密钥协商协议的形式化模型,在该模型下可证明安全的方案几乎涵盖所有基本的良好安全性质,包括抗基本的假冒攻击、已知会话密钥安全、弱的完美前向保密性、抗密钥泄漏伪装攻击、抗未知密钥共享攻击、抗临时密钥泄露攻击。采用基于身份扩展后的 eCK 安全模型对提出的跨信任域密钥协商协议进行分析,该模型描述如下。

协议参与者:每个参与者都被视为一个概率多项式时间图灵机,可以执行多项式次数的会话。假设协议中的 2 个参与者 i 和 j,其身份标识分别为 ID_i 和 ID_j,$\Pi_{i,j}^s$ 表示 i 与 j 交互的第 s 个会话实例。

敌手模型:敌手 M 也被视为一个概率多项式时间图灵机,可以完全控制网络进行窃听、延迟、重放、篡改消息等操作。通过一个挑战者和敌手之间的游戏定义认证密钥协商协议的安全性。游戏分为 2 个阶段进行。

第 1 阶段,敌手 M 被允许以任何顺序进行如下的预言机查询:

Establish Party(ID_i):敌手 M 通过此查询可以代表 ID_i 向 PKG 注册,得到 ID_i 的长期密钥并完全控制 ID_i。而不是由敌手注册的用户称为合法用户。

Long-term key Reveal(ID_i):敌手 M 通过此查询可以获得参与者 ID_i 的长期私钥。

Ephemeral-term key Reveal($\Pi_{i,j}^s$):敌手 M 通过此查询可以获得会话实例 $\Pi_{i,j}^s$ 中的临时密钥。

Session-key Reveal($\Pi_{i,j}^s$):敌手 M 通过此查询可以获得会话实例 $\Pi_{i,j}^s$ 的会话密钥。

PKG-Private key Reveal(PKG_i):敌手 M 通过此查询可以获得 ID_i 所属 PKG 的主密钥。

Send($\Pi_{i,j}^s,m$):敌手 M 发送消息 m 给会话实例 $\Pi_{i,j}^s$,$\Pi_{i,j}^s$ 按照协议的真实执行进行应答。如果成功,则敌手 M 可以控制参与会话双方的所有通信,可以进行篡改,否则只能被动窃听。

一旦敌手 M 决定游戏的第 1 阶段结束,它通过选取一个新鲜会话 $\Pi_{i,j}^s$ 发起一个 Test($\Pi_{i,j}^s$) 查询以开始游戏的第 2 阶段。

Test($\Pi_{i,j}^s$):敌手 M 选择一个新鲜会话 $\Pi_{i,j}^s$,随机选择比特数 $b \in \{0,1\}$,如果 $b = 0$,则将 $\Pi_{i,j}^s$ 真正的会话密钥返回给敌手 M,否则从有效的会话密钥分布域中随机选择一个值返回给敌手 M。敌手 M 只被允许执行一次该查询。

在 Test($\Pi_{i,j}^s$) 查询之后的游戏第2阶段,敌手M可以继续进行其他各种查询,但测试会话 $\Pi_{i,j}^s$ 应保持新鲜。最终敌手 M 输出一个比特数 b' 作为对 b 的猜测,游戏结束。如果 $b' = b$,则敌手 M 赢得游戏,其优势定义为:$Adv(k) = |\Pr[b = b'] - \frac{1}{2}|$,其中,$k$ 为系统安全参数。

定义 1(匹配会话) 如果会话实例 $\Pi_{i,j}^s$ 发出的每条消息都相继被发送给实例 $\Pi_{j,i}^s$,并且 $\Pi_{j,i}^s$ 的应答消息也被传回 $\Pi_{i,j}^s$ 作为 $\Pi_{i,j}^s$ 相应的下一条消息,那么这 2 个会话实例就是匹配的。

定义 2(新鲜会话) 设会话实例 $\Pi_{i,j}^s$ 是一个由

诚实用户 ID_i 和 ID_j 完成的会话,如果以下 3 个条件都不成立,则称 $\Pi_{i,j}^s$ 是新鲜会话。

1) 敌手 M 进行了 Session-key Reveal($\Pi_{i,j}^s$) 查询和 Session-key Reveal($\Pi_{j,i}^s$)(如果 $\Pi_{j,i}^s$ 存在)。

2) 如果存在 $\Pi_{i,j}^s$ 的匹配会话 $\Pi_{j,i}^s$,敌手 M 进行了以下询问之一:

Long-term key Reveal(ID_i) 和 Ephemeral-term key Reveal($\Pi_{i,j}^s$);

Long-term key Reveal(ID_j) 和 Ephemeral-term key Reveal($\Pi_{j,i}^s$)。

3) 如果 $\Pi_{i,j}^s$ 的匹配会话不存在,敌手 M 进行了以下询问之一:

Long-term key Reveal(ID_i) 和 Ephemeral-term key Reveal($\Pi_{i,j}^s$);

Long-term key Reveal(ID_j)。

定义 3(安全的认证密钥协商协议)　如果基于 eCK 模型的协议满足以下条件,则该协议时安全的认证密钥协商协议。

1) $\Pi_{i,j}^s$ 和 $\Pi_{j,i}^s$ 为匹配会话,计算得到相同的会话密钥,且该会话密钥是均匀分布的。

2) 对于任意的敌手 M,赢得以上游戏的优势 $Adv_M(k) = \left| \Pr[b = b'] - \frac{1}{2} \right|$ 是可忽略的。

2　基于身份的跨信任域认证密钥协商

网络中存在多个独立、自治的信任域,每个信任域拥有自己信任的 PKG 提供密钥分发服务。假设所有信任域的各个 PKG 是可信的,每个 PKG 使用不同的公开参数$\langle G_1, G_2, e, P, H_1, H_2\rangle$,使用的主密钥 s 和公钥 $Pub = sP$ 均不同。

2.1　系统建立

在信任域 A 中,假设 PKG_A 选择了如下的系统参数。G_1^A、G_2^A 分别是阶为素数 q_A 的加法循环群和乘法循环群,P_A 为群 G_1^A 的生成元,G_1^A、G_2^A 满足双线性映射:$e_A: G_1^A \times G_1^A \to G_2^A$。$H_1^A: \{0,1\}^* \to G_1^A$,$H_2^A: \{0,1\}^* \times G_1^A \to Z_{q_A}^*$。随机选取 $s_A \in Z_{q_A}^*$ 作为 PKG_A 的主密钥,相应的系统公钥为 $Pub_A = s_A P_A$。公开的系统参数为:$\langle G_1^A, G_2^A, q_A, P_A, Pub_A, e_A, H_1^A, H_2^A\rangle$。

在信任域 B 中,假设 PKG_B 选择了如下的系统参数。G_1^B、G_2^B 分别是阶为素数 q_B 的加法循环群和乘法循环群,P_B 为群 G_2^B 的生成元,G_1^B、G_2^B 满足双线性映射 $e_B: G_1^B \times G_1^B \to G_2^B$。$H_1^B: \{0,1\}^* \to G_1^B$,$H_2^B: \{0,1\}^* \times G_1^B \to Z_{q_B}^*$。随机选取 $s_B \in Z_{q_B}^*$ 作为 PKG_B 的主密钥,相应的系统公钥为 $Pub_B = s_B P_B$。公开的系统参数为:$\langle G_1^B, G_2^B, q_B, P_B, Pub_B, e_B, H_1^B, H_2^B\rangle$。

2.2　用户密钥对生成

假设 Alice 属于 PKG_A,身份标识 $ID_{Alice} \in \{0,1\}^*$,对应的公私钥分别为 $Q_{Alice} = H_1^A(ID_{Alice})$ 和 $S_{Alice} = s_A Q_{Alice}$。

假设 Bob 属于 PKG_B,身份标识 $ID_{Bob} \in \{0,1\}^*$,对应的公私钥分别为 $Q_{Bob} = H_1^B(ID_{Bob})$ 和 $S_{Bob} = s_B Q_{Bob}$。

2.3　密钥协商

Alice 随机选取临时密钥 $r_1^{Alice\prime}, r_2^{Alice\prime} \in \{0,1\}^*$,计算 $r_1^{Alice} = H_2^A(r_1^{Alice\prime}, S_{Alice})$,$r_2^{Alice} = H_2^B(r_2^{Alice\prime}, S_{Alice})$,则 $r_1^{Alice} \in Z_{q_A}^*$,$r_2^{Alice} \in Z_{q_B}^*$,然后计算临时公钥:$R_1^{Alice} = r_1^{Alice} P_A$,$R_2^{Alice} = r_2^{Alice} P_B$。

Bob 随机选取临时密钥 $r_1^{Bob\prime}, r_2^{Bob\prime} \in \{0,1\}^*$,计算 $r_1^{Bob} = H_2^B(r_1^{Bob\prime}, S_{Bob})$,$r_2^{Bob} = H_2^A(r_2^{Bob\prime}, S_{Bob})$,则 $r_1^{Bob} \in Z_{q_B}^*$,$r_2^{Bob} \in Z_{q_A}^*$,然后计算临时公钥:$R_1^{Bob} = r_1^{Bob} P_B$,$R_2^{Bob} = r_2^{Bob} P_A$。

然后 Alice 和 Bob 相互交换临时公钥,即:R_1^{Alice}、R_2^{Alice} 和 R_1^{Bob}、R_2^{Bob}。那么上述消息传递完成后,Alice 和 Bob 可以计算得到会话密钥。

Alice 和 Bob 密钥协商过程如下所示:

1) Alice 和 Bob 分别计算 $K_{Alice,Bob}$、$K_{Bob,Alice}$。

$$K_{Alice,Bob} = e_A(S_{Alice}, R_2^{Bob}) e_B(Q_{Bob}, r_2^{Alice} Pub_B),$$

$$K_{Bob,Alice} = e_B(S_{Bob}, R_2^{Alice}) e_A(Q_{Alice}, r_2^{Bob} Pub_A),$$

$$K_{Alice,Bob} = e_A(S_{Alice}, R_2^{Bob}) e_B(Q_{Bob}, r_2^{Alice} Pub_B) = e_A(s_A Q_{Alice}, r_2^{Bob} P_A) e_B(Q_{Bob}, r_2^{Alice} s_B P_B) = e_A(Q_{Alice}, P_A)^{s_A r_2^{Bob}} e_B(Q_{Bob}, P_B)^{r_2^{Alice} s_B},$$

$$K_{Bob,Alice} = e_B(S_{Bob}, R_2^{Alice}) e_A(Q_{Alice}, r_2^{Bob} Pub_A) = e_B(s_B Q_{Bob}, r_2^{Alice} P_B) e_A(Q_{Alice}, r_2^{Bob} s_A P_A) = e_B(Q_{Bob}, P_B)^{s_B r_2^{Alice}} e_A(Q_{Alice}, P_A)^{r_2^{Bob} s_A}。$$

显然,$K_{Alice,Bob} = K_{Bob,Alice}$。令 $K_{AB} = K_{Alice,Bob} = K_{Bob,Alice}$。

2) Alice 计算 $K_1^{Alice} = r_1^{Alice} R_2^{Bob}$,$K_2^{Alice} = r_2^{Alice} R_1^{Bob}$,Bob 计算 $K_1^{Bob} = r_2^{Bob} R_1^{Alice}$,$K_2^{Bob} = r_1^{Bob} R_2^{Alice}$。

显然 $K_1^{Alice} = K_1^{Bob} = r_1^{Alice} r_2^{Bob} P_A$,$K_2^{Alice} = K_2^{Bob} = r_2^{Alice} r_1^{Bob} P_B$。令 $K_1 = K_1^{Alice} = K_1^{Bob}$,$K_2 = K_2^{Alice} = K_2^{Bob}$。

3) Alice 和 Bob 分别计算会话密钥 $sk = H(K_{AB}, K_1, K_2, R_1^{Alice}, R_2^{Alice}, R_1^{Bob}, R_2^{Bob}, ID_{Alice}, ID_{Bob})$,$H: \{0,1\}^* \to \{0,1\}^k$,其中,$k$ 表示会话密钥长度。

3 安全性证明

采用基于身份扩展后的 eCK 安全模型对提出的跨信任域密钥协商协议进行分析。

定 理 如果 CDH 假设对于(G_1,P)成立,BDH 假设对于(G_1,G_2,P,e)成立,H_1^{A}、H_2^{A}、H_1^{B}、H_2^{B}、H是随机预言机,则该认证密钥协商方案在 eCK 模型下是可证明安全的。

证明:在 2.3 节中已经对该认证密钥协商方案的正确性进行了验证,且H是随机预言机,则表明该协议满足定义 3 的第一个条件,即匹配会话计算得到相同的会话密钥,且该会话密钥是均匀分布的。接下来证明该协议也满足定义3的第2个条件,即敌手 M 不能够以不可忽略的优势赢得游戏。

设k是系统安全参数,敌手 M 最多可以激活$n(k)$个诚实的用户实体,每个用户实体最多可以激活$s(k)$个并行会话。如果敌手 M 在 eCK 模型中能以不可忽略的优势获得测试会话的会话密钥,由于H是随机预言机,所以敌手 M 在发出测试查询后,只有在 3 种情况下来区分会话密钥和随机数。

1) 猜测攻击

敌手正确地猜出了会话密钥。由于H是随机预言机,敌手M猜中H输出值的概率为$O(\frac{1}{2^k})$,显然是可忽略不计的。

2) 密钥复制攻击

敌手 M 强迫一个非匹配会话与测试会话具有相同的会话密钥,这种情况下敌手 M 就可以通过查询这个非匹配会话得到测试会话密钥。由于H是随机预言机,不同的会话中H的输入不同的情况下,不可能输出相同的会话密钥。因而敌手 M 试图通过密钥复制攻击成功的概率可以忽略不计。

3) 伪造攻击

在某一时刻敌手 M 查询测试会话中通信双方H所使用的$\langle K_{\mathrm{AB}},K_1,K_2,ID_{\mathrm{Alice}},ID_{\mathrm{Bob}}\rangle$,由于$H$是随机预言机,敌手 M 自己计算出正确的值$K_{\mathrm{AB}}$、$K_1$、$K_2$。如果敌手M不向$H$查询会话密钥就无法获取优势赢得游戏。使用标准的归约式证明方法将敌手 M 攻击协议的优势与 CDH 假设及 BDH 假设关联起来。如果敌手 M 以不可忽略的优势赢得游戏,那么可以利用敌手M构造一个挑战者S以不可忽略优势解决CDH问题或 BDH 问题。为了利用敌手 M 来解决 CDH 问题,挑战者 S 受理一个 CDH 实例(aP,bP),其中,$\forall a,b\in Z_q^*$,要求S利用敌手M计算abP。为了利用敌手M来解决BDH问题,挑战者S受理一个BDH实例(aP,bP,cP),其中,$a,b,c\in Z_q^*$,要求S利用敌手M计算$e(P,P)^{abc}$。将挑战者S在给定安全参数k和利用敌手M的情况下解决CDH问题和BDH问题的优势分别记为$Adv_{\mathrm{S}}^{\mathrm{CDH}}(k)$和$Adv_{\mathrm{S}}^{\mathrm{BDH}}(k)$。S猜中M选择测试会话发起者为 Alice 而响应者为 Bob 的概率至少为$\frac{1}{n^2(k)}$,猜中 M 选择测试会话的概率至少为$\frac{1}{s(k)}$,则 S 猜测正确的概率大于$\frac{1}{s(k)n^2(k)}$。

挑战者 S 执行模拟游戏,随机选择Pub_{A}为$\mathrm{PKG_A}$的公钥,Pub_{B}为$\mathrm{PKG_B}$的公钥,为实体随机分配公/私钥对。维护以下几个表来应对敌手对随机言机的查询,每个表记录相应条目(输入值/输出值)。S利用这些表来进行H_1^{A}、H_2^{A}、H_1^{B}、H_2^{B}、H的模拟。如果敌手 M 的随机预言机查询与记录在相应表中的已有的一个输入值匹配,则 S 返回相应匹配条目的输出值;否则 S 随机产生一个值并将其返回给敌手 M,并将敌手 M 查询的输入值与此次产生的输出值记录与该表中形成一个新的条目。

$H_1^{\mathrm{A}}(ID_i)$:S 记录一个初始为空的列表$List^{H_1^{\mathrm{A}}}$,记录格式为(ID_i,l_i,Q_{ID_i})。若ID_i在列表中,S返回相应的Q_{ID_i};若ID_i不在列表中,S 随机选取$l_i\in Z_{q_{\mathrm{A}}}^*$,令$Q_{ID_i}=l_iP_{\mathrm{A}}$,并将$(ID_i,l_i,Q_{ID_i})$插入列表$List^{H_1^{\mathrm{A}}}$。

$H_1^{\mathrm{B}}(ID_i)$:S 记录一个初始为空的列表$List^{H_1^{\mathrm{B}}}$,记录格式为(ID_i,l_i,Q_{ID_i})。若ID_i在列表中,S返回响应的Q_{ID_i};若ID_i不在列表中,S 随机选取$l_i\in Z_{q_{\mathrm{B}}}^*$,令$Q_{ID_i}=l_iP_{\mathrm{B}}$,并将$(ID_i,l_i,Q_{ID_i})$插入列表$List^{H_1^{\mathrm{B}}}$。

$H(K,K_1,K_2,R_1^i,R_2^i,R_1^j,R_1^j,ID_i,ID_j)$:S 记录一个初始为空的列表$List^H$,记录格式为$(K,K_1,K_2,R_1^i,R_2^i,R_1^j,R_1^j,ID_i,ID_j,h)$。为了成功模拟游戏,S 必须保持$H(K,K_1,K_2,R_1^i,R_2^i,R_1^j,R_1^j,ID_i,ID_j)$预言机查询与 Session-key Reveal$(\Pi_{i,j}^s)$查询的一致性。如果$(K,K_1,K_2,R_1^i,R_2^i,R_1^j,R_1^j,ID_i,ID_j,h)$请求已经在$List^H$列表中,则S返回相应的$h$值;若$(K,K_1,K_2,R_1^i,R_2^i,R_1^j,R_1^j,ID_i,ID_j,h)$请求不在列表中,S 在列表$List^{\mathrm{Send}}$中查找$(R_1^i,R_2^i,R_1^j,R_1^j,ID_i,ID_j)$,如果$(R_1^i,R_2^i,R_1^j,R_1^j,ID_i,ID_j)$存在,则从$List^{\mathrm{Send}}$中返回相应的值,并将其作为新条目存入$List^H$列表,如果不存在,则 S 随机选取$h\in\{0,1\}^k$作为返回值返回给敌手$M$,并将条目$(K,K_1,K_2,R_1^i,R_2^i,R_1^j,R_1^j,ID_i,ID_j,h)$存入$List^H$中。

Establish Party(ID_i):S 代替敌手 M 注册 ID_i,即用 ID_i 询问 $List^{H_1^A}$ 或 $List^{H_1^B}$。若 $ID_i \in \mathrm{PKG_A}$,返回私钥 $S_{ID_i} = l_i P_A$ 给 M,若 $ID_i \in \mathrm{PKG_B}$,返回私钥 $S_{ID_i} = l_i P_B$ 给 M。

Long-term key Reveal(ID_i):S 返回 ID_i 相应的私钥 S_{ID_i}。

Ephemeral-term key Reveal($\Pi_{i,j}^s$):S 返回 ID_i 相应的临时密钥 $r_1^{ID_i}{}'$ 和 $r_2^{ID_i}{}'$。

Send($\Pi_{i,j}^s, m$):S 记录一个初始为空的列表 $List^{\mathrm{Send}}$,记录格式为($R_1^i, R_2^i, R_1^j, R_1^j, ID_i, ID_j, sk$)。S 查询 $List^H$ 列表中的($K, K_1, K_2, R_1^i, R_2^i, R_1^j, R_1^j, ID_i, ID_j, h$),如果存在,则在 $List^{\mathrm{Send}}$ 中存储新的条目($R_1^i, R_2^i, R_1^j, R_1^j, ID_i, ID_j, h$),否则 S 随机选择 $sk \in \{0,1\}^k$,并将($R_1^i, R_2^i, R_1^j, R_1^j, ID_i, ID_j, sk$) 存入 $List^{\mathrm{Send}}$。

Session-key Reveal($\Pi_{i,j}^s$):S 返回 $List^{\mathrm{Send}}$ 中存储的 sk。

Test($\Pi_{i,j}^s$):如果 $\Pi_{i,j}^s$ 是测试会话,S 随机选择比特数 $b \in \{0,1\}$,如果 $b = 0$,则将 $\Pi_{i,j}^s$ 真正的会话密钥返回给敌手 M,否则从有效的会话密钥分布域中随机选择一个值返回给敌手 M。

S 依据自己的猜测来进行游戏的模拟,在游戏期间,S 观察敌手 M 的查询,只要发现与实现的猜测不符随时中止游戏,否则游戏继续进行。

生成会话密钥 sk 需要向 H 预言机查询($K_{AB}, K_1, K_2, R_1^{\mathrm{Alice}}, R_2^{\mathrm{Alice}}, R_1^{\mathrm{Bob}}, R_2^{\mathrm{Bob}}, ID_{\mathrm{Alice}}, ID_{\mathrm{Bob}}$),其中,$K_{AB}$、$K_1$、$K_2$ 分别取值如下:

$$K_{AB} = e_A(S_{\mathrm{Alice}}, R_2^{\mathrm{Bob}}) e_B(Q_{\mathrm{Bob}}, r_2^{\mathrm{Alice}} Pub_B) = e_B(S_{\mathrm{Bob}}, R_2^{\mathrm{Alice}}) e_A(Q_{\mathrm{Alice}}, r_2^{\mathrm{Bob}} Pub_A),$$

$$K_1 = r_1^{\mathrm{Alice}} r_2^{\mathrm{Bob}} P_A, K_2 = r_2^{\mathrm{Alice}} r_1^{\mathrm{Bob}} P_B。$$

根据新鲜会话的定义不能同时暴露长期密钥和临时密钥,仅有以下几种情况:

1) 测试会话的匹配会话不存在,M 可以得到实体 Alice 的长期密钥,但不能得到测试会话中 Alice 的临时密钥。在这种攻击情况下,S 模拟情况同上述,仅有以下不同:

Long-term key Reveal(ID_i):如果 $ID_i = ID_{\mathrm{Bob}}$,S 退出游戏,因为此种情况下 S 不知道 Bob 的长期密钥;否则 S 返回 ID_i 相应的私钥 S_{ID_i}。

Ephemeral-term key Reveal($\Pi_{i,j}^s$):如果 $ID_i = ID_{\mathrm{Alice}}$ 且 $\Pi_{i,j}^s$ 是测试会话,S 退出游戏;否则 S 返回 ID_i 相应的临时密钥 $r_1^{ID_i}{}'$ 和 $r_2^{ID_i}{}'$。

Send($\Pi_{i,j}^s, m$):如果 $ID_i = ID_{\mathrm{Alice}}$ 且 $\Pi_{i,j}^s$ 是测试会话,则 S 返回 ID_i 的临时公钥给 M。

Session-key Reveal($\Pi_{i,j}^s$):如果 $\Pi_{i,j}^s$ 是测试会话,则 S 退出游戏;否则 S 返回 $List^{\mathrm{Send}}$ 中存储的 sk。

Test($\Pi_{i,j}^s$):如果 $\Pi_{i,j}^s$ 是测试会话,S 终止,否则从有效的会话密钥分布域中随机选择一个值返回给 M。

在这种攻击情况下,如果 S 赢得游戏,则 M 以不可忽略优势攻击成功并向 H 询问过测试会话,即 M 必须访问 $H(K, K_1, K_2, R_1^i, R_2^i, R_1^j, R_1^j, ID_i, ID_j)$ 中的 $K = e_A(S_{\mathrm{Alice}}, R_2^{\mathrm{Bob}}) e_B(Q_{\mathrm{Bob}}, r_2^{\mathrm{Alice}} Pub_B)$。由于 $r_2^{\mathrm{Alice}}{}'$、r_2^{Alice} 是未知的,而 $r_1^{\mathrm{Alice}} = H_2^A(r_1^{\mathrm{Alice}}{}', S_{\mathrm{Alice}})$,$r_2^{\mathrm{Alice}} = H_2^B(r_2^{\mathrm{Alice}}{}', S_{\mathrm{Alice}})$,因此 r_1^{Alice}、r_2^{Alice} 是未知的,要使挑战者 S 赢得游戏则敌手 M 必须能够计算出 $e_B(Q_{\mathrm{Bob}}, r_2^{\mathrm{Alice}} Pub_B)$。因此,S 赢得游戏的优势为:$Adv_S^{\mathrm{BDH}}(k) \geq \frac{1}{s(k) n^2(k)} Adv_M^1(k)$,其中,$Adv_M^1(k)$ 表示情况 1) 出现时敌手 M 攻击成功的优势。若 $Adv_M^1(k)$ 是不可忽略的,则 $Adv_S^{\mathrm{BDH}}(k)$ 也是不可忽略的,这与 BDH 假设矛盾。

2) 测试会话的匹配会话不存在,M 可以得到测试会话中 Alice 的临时密钥,但不能得到实体 Alice 的长期密钥。

在这种攻击情况下,S 模拟情况同上述,仅有以下不同:

Long-term key Reveal(ID_i):如果 $ID_i = ID_{\mathrm{Alice}}$,S 退出游戏,因为此种情况下 S 不知道 Alice 的长期密钥;否则 S 返回 ID_i 相应的私钥 S_{ID_i}。

Session-key Reveal($\Pi_{i,j}^s$):如果 $\Pi_{i,j}^s$ 是测试会话,则 S 退出游戏;否则 S 返回 $List^{\mathrm{Send}}$ 中存储的 sk。

在这种攻击情况下,由于 S_{Alice} 是未知的,要使挑战者 S 赢得游戏则敌手 M 必须能够计算出 $e_A(S_{\mathrm{Alice}}, R_2^{\mathrm{Bob}})$。因此,S 赢得游戏的优势为:$Adv_S^{\mathrm{BDH}}(k) \geq \frac{1}{s(k) n^2(k)} Adv_M^2(k)$,其中,$Adv_M^2(k)$ 表示情况 2) 出现时 M 攻击成功的优势。若 $Adv_M^2(k)$ 是不可忽略的,则 $Adv_S^{\mathrm{BDH}}(k)$ 也是不可忽略的,这与 BDH 假设矛盾。

3) 测试会话的匹配会话存在的情况,M 可以得到 Alice 和 Bob 的长期密钥,但不能得到 Alice 和 Bob 的临时密钥。

在这种攻击情况下,S 猜中 M 选择测试会话及其匹配会话存在的概率不小于 $\frac{2}{s^2(k)}$。M 如果成功实施攻击,由于 Alice 和 Bob 的临时密钥 $r_1^{\mathrm{Alice}}{}'$、$r_2^{\mathrm{Alice}}{}'$、

$r_1^{\text{Bob}\prime}$、$r_2^{\text{Bob}\prime}$未知,从而r_1^{Alice}、r_2^{Alice}、r_1^{Bob}、r_2^{Bob}未知,要使挑战者S赢得游戏则敌手M必须能够计算出$K_1 = r_1^{\text{Alice}} r_2^{\text{Bob}} P_{\text{A}}$,$K_2 = r_2^{\text{Alice}} r_1^{\text{Bob}} P_{\text{B}}$。因此,S赢得游戏的优势为:$Adv_{\text{S}}^{\text{CDH}}(k) \geq \frac{2}{s^2(k)} Adv_{\text{M}}^3(k)$,其中,$Adv_{\text{M}}^3(k)$表示情况3)出现时敌手M攻击成功的优势。若$Adv_{\text{M}}^3(k)$是不可忽略的,则$Adv_{\text{S}}^{\text{CDH}}(k)$也是不可忽略的,这与CDH假设矛盾。

4)测试会话的匹配会话存在的情况,M可以得到Alice和Bob的临时密钥,但不能得到Alice和Bob的长期密钥。

在这种攻击情况下,虽然$r_2^{\text{Alice}\prime}$、r_2^{Alice}、$r_2^{\text{Bob}\prime}$、$r_2^{\text{Bob}\prime}$是已知的,但$r_1^{\text{Alice}} = H_2^{\text{A}}(r_1^{\text{Alice}\prime}, S_{\text{Alice}})$,$r_2^{\text{Alice}} = H_2^{\text{B}}(r_2^{\text{Alice}\prime}, S_{\text{Alice}})$,$r_1^{\text{Bob}} = H_2^{\text{B}}(r_1^{\text{Bob}\prime}, S_{\text{Bob}})$,$r_2^{\text{Bob}} = H_2^{\text{A}}(r_2^{\text{Bob}\prime}, S_{\text{Bob}})$,由于Alice和Bob的长期密钥$S_{\text{Alice}}$和$S_{\text{Bob}}$是未知的,因此$r_1^{\text{Alice}}$、$r_2^{\text{Alice}}$、$r_1^{\text{Bob}}$、$r_2^{\text{Bob}}$是未知的,要使挑战者S赢得游戏则敌手M必须能够计算出$K_1 = r_1^{\text{Alice}} r_2^{\text{Bob}} P_{\text{A}}$,$K_2 = r_2^{\text{Alice}} r_1^{\text{Bob}} P_{\text{B}}$。因此,S赢得游戏的优势为:$Adv_{\text{S}}^{\text{CDH}}(k) \geq \frac{2}{s(k)n^2(k)} Adv_{\text{M}}^4(k)$,其中,$Adv_{\text{M}}^4(k)$表示情况4)出现时M攻击成功的优势。若$Adv_{\text{M}}^4(k)$是不可忽略的,则$Adv_{\text{S}}^{\text{CDH}}(k)$也是不可忽略的,这与CDH假设矛盾。

5)测试会话的匹配会话存在的情况,M可以得到Alice的长期密钥与Bob的临时密钥。

6)测试会话的匹配会话存在的情况,M可以得到Alice的临时密钥与Bob的长期密钥。

情况5)、6)与1)、2)类似,这里不再赘述。

$$Adv_{\text{S}}^{\text{BDH}}(k) \geq \frac{1}{s(k)n^2(k)} Adv_{\text{M}}^5(k),$$

$$Adv_{\text{S}}^{\text{BDH}}(k) \geq \frac{1}{s(k)n^2(k)} Adv_{\text{M}}^6(k),$$

其中,$Adv_{\text{M}}^5(k)$、$Adv_{\text{M}}^6(k)$分别表示情况5)、6)出现时敌手M攻击成功的优势。若$Adv_{\text{M}}^5(k)$、$Adv_{\text{M}}^6(k)$是不可忽略的,则$Adv_{\text{S}}^{\text{BDH}}(k)$也是不可忽略的,这与BDH假设矛盾。

另外,协议方案中如果PKG的主密钥暴露,则相应PKG用户的私钥也会泄露,但是根据会话新鲜性定义,如果用户的长期私钥暴露则其临时密钥就不能暴露,与情况3)类似,因此该方案具有PKG前向保密性。

若敌手M在上述的任意一种情况下能够以不可忽略的优势赢得游戏,那么挑战者S就能够利用M以不可忽略的优势来解决BDH或CDH难题,这与协议所基于的安全假设相矛盾。因而满足eCK模型中关于密钥协商协议安全定义的第2个条件。

4 性能分析

这里将从安全性能、计算开销、适用范围3个方面,对典型的几种含双线性对的跨信任域密钥协商协议进行对比分析,如表1和2所示。其中:Weak-FS表示弱的完美前向安全性,PKG-FS表示PKG前向安全性,KCI表示抗密钥泄露伪装攻击,EKCI表示抗临时密钥泄露攻击;P表示双线性对运算,E表示指数运算,S表示点乘运算;√表示满足属性,×表示不满足属性。计算开销仅统计运行一次的单方运算开销。

表1 几种基于身份的跨信任域密钥协商协议安全性能分析

Tab. 1 Security comparison of typical identity-based cross-domain authentication schemes

协议	安全性能			
	Weak-FS	PKG-FS	KCI	EKCI
文献[15]	√	√	√	×
文献[16]	√	√	√	√
提出的方案	√	√	√	√

表2 基于身份的跨信任域密钥协商协议性能分析

Tab. 2 Performance comparison of typical identity-based cross-domain authentication schemes

协议	计算开销			适用范围	
	P	E	S	多PKG环境	无参数限制
文献[15]	2	0	3	√	×
文献[16]	4	3	0	√	×
提出的方案	2	0	5	√	√

根据比较可知,虽然提出的方案计算开销较文献[15]的方案有所增加,但弥补了一些安全漏洞。而提出的方案与文献[16]的方案相比较,在具备同等安全性能的情况下,减少了2次双线性对运算。在适用范围方面,虽然这几种方案都适用于多PKG环境,但只有提出的方案无PKG参数限制,即对参数一致不作限制。

5 结束语

提出一种基于身份的跨信任域认证密钥协商协议,可使处于不同PKG管理域中的实体完成认证密钥协商,该协议假设所有信任域的各PKG使用完全不同的公开参数、不同的系统主密钥和公钥。该协议在基于身份的扩展后的eCK模型下是可证明安全的,在满足基本安全属性的基础上,还具有弱的完

美前向安全性、PKG 前向安全性、抗密钥泄露伪装攻击以及抗临时密钥泄露攻击等属性。由于该方案中对 PKG 系统参数不作限制,更适用于现实多信任域网络环境,更可扩展应用到异构网络融合中节点的认证密钥协商方案中去。

参考文献:

[1] Shamir A. Identity-based cryptosystems and signature schemes[C]//Proceedings of Crypto'84. Berlin: Springer-Verlag, 1984:47 – 53.

[2] Boneh D, Franklin M. Identity basedencryption from the Weil paring[C]//Proceedings of Crypto'01. Berlin: Springer-Verlag, 2001:213 – 229.

[3] Smart N P. Identity based authenticated key agreement protocol based on the Weil paring[J]. Eleetroniest Letters, 2002, 38(13):630 – 632.

[4] Chen L, Kudla C. Identity based authenticated key agreement protocols from pairing[C]//Proceeding of 16th IEEE Security Foundations Workshop. New York: IEEE Computer Society Press, 2003:219 – 233.

[5] McCullagh N, Barreto P S L M. A new two-party identity-based authenticated key agreement[C]//Proceedings of CT-RSA 2005. Berlin: Springer, 2005. Berlin: Springer, 2005, 3376:262 – 274.

[6] Gorantla M C, Boyd C, Manuel J. ID-based one-pass autenticated key establishment[C]//Proceedings of Australasian Information Security Conference. Sydney: Australian Computer Society, 2008, 81:39 – 46.

[7] Yasmin R, Ritter E, Wang Guilin. A pairing-free ID-based one-pass authenticated key establishment protocol for wireless sensor networks[C]//Proceedings of 5th International Conference on Sensor Technologies and Applications. Paris: IARIA, 2011:340 – 347.

[8] Gao Haiying. Provable secure ID-based authenticated key agreement protocol[J]. Journal of Computer Research and Development, 2012, 49(8):1685 – 1689. [高海英. 可证明安全的基于身份的认证密钥协商协议[J]. 计算机研究与发展, 2012, 49(8):1685 – 1689.]

[9] Chen Ming. Extended identity-based authenticated key greement in standard model[J]. Application Research of Computers, 2014, 31(6):1869 – 1873. [陈明. 标准模型下增强的身份基认证密钥协商[J]. 计算机应用研究, 2014, 31(6):1869 – 1873.]

[10] Liu Xiumei, Gao Kening, Xue Lifang, et al. Authenticated key exchange in eCK model[J]. Computer Science, 2014, 41(8):172 – 177. [柳秀梅, 高克宁, 薛丽芳, 等. eCK 模型下的密钥协商[J]. 计算机科学, 2014, 41(8):172 – 177.]

[11] Huang Chaoyang, Tang Biyu. Two-party authenticated key exchange protocol based on bilinear parings[J]. Computer Engineering and Design, 2014, 35(8):2671 – 2684. [黄朝阳, 汤碧玉. 基于双线性对的双向认证密钥交换协议[J]. 计算机工程与设计, 2014, 35(8):2671 – 2684.]

[12] Liu Zhiyuan. Secure identity-based authenticated key agreement protocol[J]. Journal of Hunan University of Science & Technology: Natural Science Edition, 2014, 29(10):64 – 67. [刘志远. 安全的基于身份认证密钥协商协议[J]. 湖南科技大学学报: 自然科学版, 2014, 29(10):64 – 67.]

[13] Swanson C, Jao D. A study of two-party certificateless authenticated key agreement protocols[C]//Proceedings of INDOCRYPT 2009. Berlin: Springer, 2009:57 – 71.

[14] Zhang Yanhong, Chen Ming. Strongly secure certificateless authenticated key agreement protocol in standard model[J]. Journal of Sichuan University: Engineering Science Edition, 2013, 45(1):125 – 132. [张延红, 陈明. 标准模型下强安全的无证书认证密钥协商协议[J]. 四川大学学报: 工程科学版, 2013, 45(1):125 – 132.]

[15] Shi Yabin, Huang Kaizhi, Yang Peng. Identity-based security provable two parties authentication key agreement[J]. Application Research of Computers, 2009, 26(9):3519 – 3522. [石亚宾, 黄开枝, 杨鹏. 基于身份证明安全的双方密钥协商协议[J]. 计算机应用研究, 2009, 26(9):3519 – 3522.]

[16] Xia Song, Quan Jianxiao, Han Wenbao. Provably secureIdentity-based authenticated key agreement protocols in multiple PKG environment[J]. Journal of Electronics & Information Technology, 2010, 32(10):2393 – 2399. [夏松, 权建校, 韩文报. 不同 PKG 环境下可证安全的基于身份 AKA 协议[J]. 电子与信息学报, 2010, 32(10):2393 – 2399.]

[17] You Juan, Xia Song, Li Junquan. Identity-based authentication key agreement protocols without bilinear paring in multiple PKG environments[J]. Journal of Shandong University: Natural Science Edition, 2012, 48(2):223 – 230. [尤娟, 夏松, 李俊全. 多 PKG 环境下无双线性对的基于身份 AKA 协议[J]. 北京大学学报, 2012, 48(2):223 – 230]

[18] Canetti R, Krawczyk H. Analysis of key-exchange protocols and their use for building secure channels[C]//Proceedings of EUROCRYPT 2001. Berlin: Springer-Verlag, 2001, 2045:453 – 474.

[19] LaMacchia A B, Lauter K, Mityagin A. Stronger security of authenticated key exchange[C]//Proceedings of PROVSEC 2007. Berlin: Springer-Verlag, 2007:4784:1 – 16.

[20] Ni Liang, Chen Gongliang, Li Jianhua. Security analysis of the eCK model[J]. Journal of Shandong University: Natural Science, 2013, 48(7):46 – 67. [倪亮, 陈恭亮, 李建华. eCK 模型的安全性分析[J]. 山东大学学报: 理学版, 2013, 48(7):46 – 67.]

(编辑　杨　蓓)