第36卷 第14期 计 算 机 工 程 2010年7月
Vol.36 No.14 Computer Engineering July 2010
·安全技术· 文章编号：1000—3428(2010)14—0141—03 文献标识码：A 中图分类号：TP309.2

强安全三方认证密钥交换协议

王元元，曹珍富，黄 海
(上海交通大学计算机科学与工程系，上海 200240)

摘 要：针对现有的三方认证密钥交换协议缺乏严格安全证明的问题，研究三方密钥交换协议的安全模型。将两方认证密钥交换协议的强安全模型eCK模型推广至三方，同时考虑内部人攻击，定义强三方认证密钥交换协议安全模型，提出一个具体三方认证密钥交换协议并给出其在强安全模型中的安全性证明。

关键词：三方认证密钥交换协议；eCK安全模型；GBDH问题；内部人攻击

Stronger Security Tripartite Authenticated Key Exchange Protocol

WANG Yuan-yuan, CAO Zhen-fu, HUANG Hai
(Dept. of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai 200240)

【Abstract】 Currently there are few tripartite Authenticated Key Exchange(AKE) protocols which have a formal security proof. Aiming at this problem, this paper investigates the security model for the tripartite AKE protocols. A strong security model named enhanced Canetti-Krawczyk(eCK) model for two-party AKE protocols is proposed. A strong security model for three-party AKE protocols is introduced which generalizes the eCK model for two-party setting, and the insider attack is taken into account. It presents a new tripartite AKE protocol and shows that the protocol is provably secure in the strong security model.

【Key words】 tripartite Authenticated Key Exchange(AKE) protocol; enhanced Canetti-Krawczyk(eCK) security model; GBDH problem; insider attack

1 概述

密钥交换协议是一个重要的密码学原语，可以让两方或者多方在不安全的信道上协商一个会话密钥，从而建立一个安全的通信信道。三方或多方参与的密钥交换协议称为群密钥交换协议，其中三方是一种重要的情形，三方是比较常见的通信情形，比如手机漫游时需要涉及到终端，远程服务器，本地服务器三方的交互，在传统的两方密钥交换协议中引入第三方可以为通信的双方提供各种服务，比如现在电子交易中，引入支付宝等第三方提供支付功能为交易双方提供了巨大的方便。

DH协议是第一个密钥交换协议[1]，它使协议双方能在不安全的信道上协商会话密钥，攻击者无法利用窃听到的信息得到会话密钥。由于DH协议缺乏消息认证，不能抵抗中间人攻击，以后的学者们致力于如何给DH协议添加各种认证，提出了大量的认证密钥交换(Authenticated Key Exchange, AKE)协议。文献[2]总结了认证密钥交换协议应该满足的各种安全属性：已知会话密钥安全，前向安全，抵抗未知密钥共享攻击，抗密钥泄漏伪装攻击，密钥确认和相互认证。

现有的很多三方密钥交换协议[3-4]都没有严格的安全证明。文献[5]推广了两方的CK模型至三方情形。文献[6]提出了一个两方扩展CK(eCK)模型，在模型中，增强了攻击者的能力，由于攻击者可以同时查询各方的临时私钥或者长期私钥，或者其他不能使攻击者简单的获得会话密钥的组合，eCK模型不仅包含了CK模型所定义的安全属性，同时还包含了抗密钥泄漏伪装(KCI)攻击。抗密钥泄漏伪装攻击是指假设被攻击者A的长期私钥泄漏，这时敌手肯定可以假冒A和任何人通信，但仍然可以保证即使这个时候攻击者也无法假冒其他方和A通信。

现有大部分三方认证密钥交换协议假设所有参与方均为诚实的，该假设过于苛刻。文献[7]考虑了存在恶意参与方时协议的安全问题，即考虑了内部人(Insider)攻击。Insider攻击者有2个目标：(1)攻击者冒充某一个诚实的参与方参与会话；(2)攻击者能使2个诚实的参与方计算出不同的会话密钥。抗Insider攻击对三方和多方密钥交换协议有着重要的意义。现有的抗Insider攻击的三方AKE协议[4]只考虑了情形(1)，没有考虑到情形(2)的攻击。

本文所做工作如下：(1)推广两方情形的eCK模型，提出三方认证密钥交换协议的强安全模型，使之具备eCK模型所具有的安全属性。相比文献[5]中的CK模型，eCK模型能够更好地支持临时私钥查询，并且能够抗密钥泄漏伪装攻击。(2)考虑到协议存在恶意参与方的情形，使本文的安全模型能够抗Insider攻击。(3)提出一个具体的三方认证密钥交换协议，给出其在本文定义的强安全模型中安全证明。

2 预备知识

令G是一个加法群，G_T是一个素数阶q的乘法群。令P是群G的生成元，$e:G\times G\to G_T$是一个双线性映射。

2.1 双线性BDH问题

给定了一组$\langle P,aP,bP,cP\rangle$，其中，$P$是$G$的生成元，$a,b,c\in_R \mathbb{Z}_q^*$，求$e(P,P)^{abc}$。

基金项目：国家自然科学基金资助项目(60673079, 60773086)
作者简介：王元元(1986－)，男，硕士研究生，主研方向：密钥交换协议；曹珍富，教授、博士生导师；黄 海，博士研究生
收稿日期：2010-01-20 **E-mail：**wangyuanjnu@tom.com

BDH 假设：任意的概率多项式时间(*PPT*)攻击者解决 BDH 问题的优势都是可忽略的。

2.2 Gap 问题

DBDH 预言机：输入 $\langle U,V,W,K\rangle$，其中，$U=uP, V=vP, W=wP, P\in G$，如果 $K=e(P,P)^{uvw}$ 则返回真，否则返回假。

GBDH 假设：在存在 DBDH 预言机的条件下，对于任意的 *PPT* 攻击者来说解决 BDH 问题的优势是可忽略的。

3 强三方认证密钥交换协议安全模型

本文推广两方 eCK 安全模型至三方情形，并考虑 Insider 攻击，定义了强三方安全模型。

(1)参与方：设 P 为确定个数的参与者集合，每一个参与者 $ID_i\in P$ 是一个 *PPT* 的图灵机。每一个参与者 ID_i 可以并行的执行多项式个协议的实例，称 ID_i 的第 t 次协议实例为 $\prod_i^t(i,j,k)$ (一次会话)，其中，ID_i 为 $\prod_i^t$ 的发起者，ID_j, ID_k 为 ID_i 指定的参与者。

(2)攻击者模型：设攻击者 M 是一个 *PPT* 的图灵机，完全控制了参与方的通信信道，能够任意窃听、延迟、重放、修改和插入消息。本文通过定义各种预言机供攻击者查询以模拟攻击者的能力。

1) EmphemeralKeyReveal($\prod_i^t$)：攻击者得到会话 $\prod_i^t$ 的临时私钥。

2) SessionKeyReveal($\prod_i^t$)：如果会话 $\prod_i^t$ 完成，协商出会话密钥 sk，则攻击者能够获得会话密钥 sk。

3) StaticKeyReveal(ID_i)：攻击者获得 ID_i 的长期私钥。

4) EstablishParty(ID_i)：攻击者能够任意代表 ID_i 注册公钥，攻击者将完全控制 ID_i，称被攻击者控制的参与方为不诚实的参与方。

5) Send($\prod_i^t, m$)：攻击者向会话 $\prod_i^t(i,j,k)$ 发送消息 m，攻击者获得相应响应。

6) Test($\prod_i^t$)：该查询攻击者只能够执行一次。假设会话 $\prod_i^t$ 已经完成，攻击者能在任何时候执行该查询。随机选择 $b\in\{0,1\}$, 若 b=0，则返回 $\prod_i^t$ 的会话密钥；如果 b=1，则返回一个随机数 $\varsigma\in\{0,1\}^k$。

定义 1(匹配对话) 设 $\prod_i^t$ 为一个完成的会话，其公共的输出为 $sid_i^t=(X,Y,Z), pid_i^t=(ID_i,ID_j,ID_k)$，$ID_i$ 是会话的发起者，ID_j, ID_k 是 ID_i 指定的参与方。X 是 ID_i 的输出，Y 是 ID_j 的输出，Z 是 ID_k 的输出。如果存在另一完成的会话 $\prod_j^{t'}$，其公共输出 $sid_j^{t'}, pid_j^{t'}$ 有 $sid_j^{t'}=sid_i^t, pid_j^{t'}=pid_i^t$ 成立，则称 $\prod_j^{t'}$ 是 $\prod_i^t$ 的匹配会话。

定义 2(新鲜性) 设 $\prod_i^t$ 为一个完成的会话，ID_i 是会话的发起者，ID_j，ID_k 是 ID_i 指定的参与方。以下情形中攻击者可以轻易获得 $\prod_i^t$ 的会话密钥：

(1)攻击者查询 $\prod_i^t$ 或者其匹配会话(如果存在)的会话密钥；

(2) $\prod_i^t$ 存在匹配会话 $\prod_j^{t'}$，$\prod_k^{t'}$，攻击者做了以下 3 组中任何一组查询：

StaticKeyReveal(ID_i), EmphemeralKeyReveal($\prod_i^t$)

StaticKeyReveal(ID_j), EmphemeralKeyReveal($\prod_j^t$)

StaticKeyReveal(ID_k), EmphemeralKeyReveal($\prod_k^{t'}$)

(3) $\prod_i^t$ 的匹配会话不存在，攻击者做了以下 3 组中任何一组查询：

StaticKeyReveal(ID_i), EmphemeralKeyReveal($\prod_i^t$)

StaticKeyReveal(ID_j)

StaticKeyReveal(ID_k)

如果攻击者没有做以上任何查询，则称 $\prod_i^t$ 是新鲜的。

定义 3(AKE 安全) 定义概率多项式时间攻击者 M 攻击协议Σ的优势函数为安全参数 k 的函数：

$$Adv_{M,\Sigma}^{AKE}(k)=|Succ_{M,\Sigma}^{AKE}(k)-1/2|$$

这里 $Succ_{M,\Sigma}^{AKE}(k)$ 为攻击者对新鲜的会话 $\prod_i^t$ 查询 Test 预言机后，输出 b'，使 $b'=b$(b 为 Test 预言机使用的一位比特数)成立的概率。如果对任意的概率多项式时间攻击者 M，该概率都是可忽略的，则称该认证密钥交换协议Σ是 AKE 安全的。

定义 4(相互认证安全) 设Σ是一个密钥交换协议，攻击者 M 可以查询第 3 节中定义的各种预言机。如果存在两个诚实的参与方 ID_i, ID_m (攻击者没有查询 ID_m 的长期私钥)，攻击者(可以是合法的内部人)使得 ID_i 的某一个会话 $\prod_i^t$ 没有匹配会话 $\prod_m^{t'}$；或 $\prod_i^t$ 有匹配会话 $\prod_m^{t'}$，但 $sk_m^{t'}\neq sk_i^t$，就称 M 成功。定义 M 成功的概率为 $Succ_{M,\Sigma}^{MA}(k)$，如果对任意概率多项式时间攻击者 M，该概率都是可忽略的，则称该认证密钥交换协议Σ是相互认证安全的。

4 方案描述

4.1 参数生成

设 k 为安全参数，令 $e:G\times G\to G_T$ 是一个双线性配对，G, G_T 为素数阶 q 的循环群，P 是 G 的生成元；$H:\{0,1\}^*\to G$, $H_1:\{0,1\}^*\to\{0,1\}^k$ 为哈希函数；参与方 $\hat{A}$ 的长期私钥是 $a\in\mathbb{Z}_q^*$，公钥为 $A=aP\in G$，类似 $\hat{B}$ 和 $\hat{C}$ 的公私钥对为 $(B=bP,b)$ 和 $(C=cP,c)$。

4.2 协议描述

第 1 轮：

(1) $\hat{A}$ 选择随机数 $x\in\mathbb{Z}_q^*$，计算 $X=xP$，发送 X；

(2) $\hat{B}$ 选择随机数 $y\in\mathbb{Z}_q^*$，计算 $Y=yP$，发送 Y；

(3) $\hat{C}$ 选择随机数 $c\in\mathbb{Z}_q^*$，计算 $Z=zP$，发送 Z。

第 2 轮：

(1) $\hat{A}$ 取 $sid=(X\|Y\|Z\|\hat{A}\|\hat{B}\|\hat{C})$，计算 $\delta_A=aH(sid)$，发送 δ_A；

(2) $\hat{B}$ 取 $sid=(X\|Y\|Z\|\hat{A}\|\hat{B}\|\hat{C})$，计算 $\delta_B=bH(sid)$，发送 δ_B；

(3) $\hat{C}$ 取 $sid=(X\|Y\|Z\|\hat{A}\|\hat{B}\|\hat{C})$，计算 $\delta_C=cH(sid)$，发送 δ_c。

消息认证和密钥协商的步骤如下：

(1) $\hat{A}$ 接收到消息 δ_B, δ_c，$\hat{A}$ 检查是否有

$$e(\delta_B,P)=e(H(sid),B), e(\delta_C,P)=e(H(sid),C)$$

成立。如果不成立，$\hat{A}$ 终止协议，否则，$\hat{A}$ 计算:

$$K=e(B+Y,C+Z)^{a+x}=e(P,P)^{(a+x)(b+y)(c+z)}$$

(2) $\hat{B}$ 接收到消息 δ_A, δ_c，$\hat{B}$ 检查是否有

$$e(\delta_A,P)=e(H(sid),A), e(\delta_C,P)=e(H(sid),C)$$

成立。如果不成立，$\hat{B}$ 终止协议，否则，$\hat{B}$ 计算:

$$K=e(A+X,C+Z)^{b+y}=e(P,P)^{(a+x)(b+y)(c+z)}$$

(3) $\hat{C}$ 接收到消息 δ_A,δ_B， $\hat{C}$ 检查是否有

$e(\delta_A,P)=e(H(sid),A),e(\delta_B,P)=e(H(sid),B)$

成立。如果不成立， $\hat{C}$ 终止协议，否则， $\hat{C}$ 计算:

$K=e(A+X,B+Y)^{c+z}=e(P,P)^{(a+x)(b+y)(c+z)}$

(4) $\hat{A},\hat{B},\hat{C}$ 计算会话密钥 $sk=H_1(K,sid)$。

5 安全证明

定理 如果 GBDH 假设成立，则提出的协议是 AKE 安全(定义 3)和相互认证安全(定义 4)的。

证明如下：

(1)相互认证安全：首先证明 $\prod_i^t$ 存在匹配会话 $\prod_m^{t'}$ 时，$sk_m^{t'}\neq sk_i^t$ 的概率是可忽略的。根据匹配会话的定义，$\prod_i^t$ 和 $\prod_m^{t'}$ 有相同的 sid 和 pid，由于 $K=e(P,P)^{(a+x)(b+y)(c+z)}$，$sk=H_1(K,sid)$，显然 $\prod_i^t$ 和 $\prod_m^{t'}$ 有相同的 sk。其次证明 $\prod_i^t$ 不存在匹配会话的概率是可忽略的。由于 $\prod_i^t$ 已经被接受，即 ID_i 验证了 $e(\delta_m,P)=e(H(sid),M)$ （$\delta_m=mH(sid),M=mP$）成立，根据定义，攻击者没有查询用户 ID_m 的长期私钥 m，攻击者自己无法生成合适的 δ_m (相当于求解 CDH 问题)使得 ID_i 能够通过验证，所以 $\prod_i^t$ 必然存在匹配会话 $\Pi_m^{t'}$。

(2)AKE 安全

已知 Test 会话生成的会话密钥为 $sk=H_1(K,sid)$，攻击者有 2 种情况获得优势：

情况 1 伪造攻击：攻击者 M 向随机预言机 H_1 查询了相同的 (K,sid)。

情况 2 密钥复制攻击：攻击者建立另一不与 Test 会话匹配的会话，该会话与 Test 会话有相同的会话密钥。

根据定义 1，2 个不匹配的会话的参与方相同并且有相同的临时公钥的概率是可忽略的，即 K,sid 是不同的，又由于 H_1 是随机预言机，所以情况 2 出现的概率是可忽略的。

考虑情况 1，分为以下 2 种情况：

情况 1.1：Test 会话有匹配的诚实用户的会话。

情况 1.2：Test 会话不存在匹配的诚实用户的会话。

在 MA 安全的证明中，已经证明了情况 1.2 发生的概率是可忽略的，下面考虑情况 1.1：记 $\hat{A}$ 的长期私钥为 a，临时私钥为 x；$\hat{B}$ 的长期私钥为 b，临时私钥为 y；$\hat{C}$ 的长期私钥为 c，临时私钥为 z。根据定义 2 中新鲜性的定义，攻击者不能同时查询某一用户的长期私钥和临时私钥，则攻击者还有 8 种途径进行攻击：

1.1.1 攻击者查询 x,y,z；1.1.2 攻击者查询 x,y,c；

1.1.3 攻击者查询 x,b,z；1.1.4 攻击者查询 x,b,c；

1.1.5 攻击者查询 a,y,z；1.1.6 攻击者查询 a,y,c；

1.1.7 攻击者查询 a,b,z；1.1.8 攻击者查询 a,b,c。

方案中 a 与 x，b 与 y，c 与 z 的位置对称，8 种情况证明是一致的。现在以情况 1.1.1 为例证明攻击者获得优势的概率是可忽略的。本文将证明如果存在一个攻击者在 1.1.1 的情况下成功获得优势，便能够找到 BDH 问题的解。

设模拟者 S 的输入为 $U,V,W\in G$，其中 $U=uP,V=vP,W=wP$，S 建立与攻击者的游戏，目标是利用攻击者的攻击能力构造 BDH 问题的解 $e(P,P)^{uvw}$。设游戏的参与者集合为 $P=\{ID_1,ID_2,\cdots,ID_n\}$，设 Test 会话为 $\prod_{\hat{A}}^t(\hat{A},\hat{B},\hat{C})$，其匹配会话为 $\prod_{\hat{B}}^{t'},\prod_{\hat{C}}^{t'}$ $(\hat{A},\hat{B},\hat{C}\in P)$，$\hat{A},\hat{B},\hat{C}$ 的长期公钥为 $A,B,C\in G$，S 设置 $A=U,B=V,C=W$，S 不知道 U,V,W 对应的 u,v,w，即不知道 $\hat{A},\hat{B},\hat{C}$ 的长期私钥。

在模拟过程中，如果攻击者控制某一方 $\hat{D}\in P$（$\hat{D}$ 可以是攻击者自己注册的用户，长期公钥为 D，S 不知道 $\hat{D}$ 的长期私钥)和 $\hat{A},\hat{B},\hat{C}$ 中 2 个开始会话，会话结束之后攻击者将可以算出此次会话的会话密钥，由于模拟者不知道 $\hat{A},\hat{B},\hat{C}$ 的长期私钥，无法产生正确的会话密钥。从本质上来说，模拟的难度在于攻击者可以对同一次会话同时查询随机预言机 H_1 和 SessionKeyReveal，2 种查询的结果都是该次会话的会话密钥，但如果没有所有参与方的私钥，S 无法保证回答的一致性。为解决该难题，分别给 H_1 查询和 SessionKeyReveal 维护 2 张表：H_1^{List} 和 SK^{List}，在攻击者查询 H_1 时先扫描 SK^{List}，利用 DBDH 预言机查找之前有没有过回答过相应的会话密钥；攻击者查询 SessionKeyReveal 时先扫描 H_1^{List}，利用 DBDH 预言机查找之前有没有回答过相应的 H_1 查询。总之，S 利用 DBDH 预言机保持回答 2 种查询的一致性，使攻击者对模拟和实际情况不可区分。

下面将只考虑在 S 不知道参与者长期私钥的情形下模拟回答攻击者的各类查询，设 $\hat{D},\hat{E}$ 是攻击者注册的 2 个用户，其长期公钥为 D,E，攻击者控制 $\hat{D},\hat{E}$ 与 $\hat{A}$ 交互，S 回答攻击者的各种预言机查询。

(1) $H(X,Y,Z,\hat{A},\hat{D},\hat{E})$: S 维护一张表 H^{List}，表项为 (X,Z,ID_i,ID_j,ID_k,l,h)。如果 H^{List} 中找到 $(X,Y,Z,\hat{A},\hat{D},\hat{E})$ 返回对应的 h；否则任意选择 $l_x\in\{0,1\}^k$，计算 $h_x=l_xP$，返回 h，并将 $(X,Y,Z,\hat{A},\hat{D},\hat{E},l_x,h_x)$ 插入到 H^{List} 中。

(2)$H_1(K,X,Y,Z,\hat{A},\hat{D},\hat{E})$：$S$ 维护一张表 H_1^{List}，表项为 $(K,X,Y,Z,\hat{A},\hat{D},\hat{E},h)$。如果在 H_1^{List} 中找到 $(K,X,Y,Z,\hat{A},\hat{D},\hat{E},\cdot)$，$S$ 返回对应的 h；否则，S 查询 SK^{List}（SessionKeyReveal 查询中维护的表）。如果找到 $(X,Y,Z,\hat{A},\hat{D},\hat{E},)$，$S$ 查询 DBDH $(X+A,Y+D,Z+E,K)$。如果返回真，S 将返回 SK^{List} 存储的对应 SK。并将 $(K,X,Y,Z,\hat{A},\hat{D},\hat{E},SK)$ 插入 H_1^{List} 中；如果返回假，S 随机选择 $h^*\in\{0,1\}^k$，返回给攻击者，并将 $(K,X,Y,Z,\hat{A},\hat{D},\hat{E},h^*)$ 插入到 H_1^{List} 中。

(3)Send$(\Pi_{\hat{A}}^{t^*},m)$：如果询问发生在第 1 轮，随机选择 $x\in Z_q$，返回 $X=xP$。注意这里的 x 即为临时私钥，S 可以在攻击者进行临时私钥查询时将该值返回。

如果询问发生在第 2 轮，s 查询 H 预言机得到 $H(m)=l_iP$，计算 $\delta_A=l_iA$，返回 δ_A。攻击者验证 $e(\delta_A,P)=e(l_iA,P)=e(l_iaP,P)=e(l_iP,aP)=e(H(sid),A)$ 成立。

(4) SessionKeyReveal $(\Pi_{\hat{A}}^{t^*}(\hat{A},\hat{D},\hat{E}))$: S 维护一张表 SK^{List}，表项为 $(X,Y,Z,\hat{A},\hat{D},\hat{E},SK)$。如果在 SK^{List} 中能找到 $(X,Y,Z,\hat{A},\hat{D},\hat{E},\cdot)$，则返回对应的 SK；否则查询 H_1^{List}（H_1 查询维护的一张表)，如果找到 $(K,X,Y,Z,\hat{A},\hat{D},\hat{E},h)$，查询 DBDH 预言机 $(X+A,Y+D,Z+E,K)$，如果为真，则返回 H_1^{List} 该表项对应的 h 并将 $(X,Y,Z,\hat{A},\hat{D},\hat{E},h)$ 插入到 SK^{List} 中，否则，随机选择 $SK^*=\{0,1\}^k$，返回 SK^*，并将 $(X,Y,Z,\hat{A},\hat{D},\hat{E},SK*)$ 插入 SK^{List} 中。

(下转第 146 页)