第 39 卷 第 1 期 计 算 机 工 程 2013 年 1 月
Vol.39 No.1 Computer Engineering January 2013

·安全技术· 文章编号：1000—3428(2013)01—0140—04 文献标识码：A 中图分类号：TP309.2

一种三方认证密钥协商协议的分析与改进

唐祚波，缪祥华

(昆明理工大学信息工程与自动化学院，昆明 650500)

摘 要：大多数三方认证密钥协商协议不能抵抗中间人攻击。为此，对 Tan 提出的三方认证密钥协商协议(Journal of Communications, 2010, No.5)进行分析，证明其不能抵抗发起者假冒攻击、响应者假冒攻击及中间人攻击，并利用单向哈希函数和椭圆曲线密码学技术对协议进行改进。理论分析与形式化证明结果表明，改进协议继承了原协议的安全性，并能抵抗假冒攻击及中间人攻击。

关键词：三方认证密钥协商协议；假冒攻击；中间人攻击；椭圆曲线；单向哈希函数；CDH 假设

Analysis and Improvement of a Three-party Authenticated Key Agreement Protocol

TANG Zuo-bo, MIAO Xiang-hua

(College of Information Engineering & Automation, Kunming University of Science and Technology, Kunming 650500, China)

【Abstract】 Most Three-party Authenticated Key Agreement(3PAKA) protocols are susceptible to man-in-the-middle attack. This paper analyzes security of the 3PAKA protocol presented by Tan, and proves that it can not withstand counterfeit attacks and man-in-the-middle attack. To enhance its security, an improved protocol is proposed by one-way hash function and elliptic curve cryptography. Security analysis and formal proof results show that the improved protocol inherits the security of the original protocol, and is able to resist counterfeit attack and man-in-the-middle attack.

【Key words】 Three-party Authenticated Key Agreement(3PAKA) protocol; counterfeit attack; man-in-the-middle attack; elliptic curve; one-way hash function; Computational Diffie-Hellman(CDH) assumption

DOI: 10.3969/j.issn.1000-3428.2013.01.030

1 概述

随着移动通信技术的发展，通信系统中的安全问题越来越受到重视，通过认证密钥协商协议来确认网络运营商和用户的身份，已成为一个重要的研究课题。认证密钥协商协议是密钥协商协议和实体认证协议的两者结合，能够在不安全的网络中，使通信双方相互认证，并能协商出会话密钥[1]。

目前已有许多认证密钥协商协议，其中大多数都不能抵抗中间人攻击。中间人攻击是指攻击者 E 截取用户 A 和 B 之间的交互信息，并用自己的消息替换这些消息，以此假冒 B(或 A)与 A(或 B)完成一次协议[1]。文献[2]基于椭圆曲线提出了一个三方认证密钥协商协议。文献[3]对该协议进行分析后，提出一个用于移动通信的三方认证密钥协商协议。文献[4]分析发现，文献[3]的协议不能抵抗假冒攻击和中间人攻击。文献[5]在文献[3]的基础上提出了一种改进协议，但该协议不能抵抗重放攻击[6]，原因是无法保证信息的新鲜性。另外，文献[5]中应用的双线性对技术无法保证安全性，例如攻击者 X 任意选择 r_X，都能通过验证：$\hat{e}(R_X,Q)=\hat{e}(U_X,Y_X)$。

本文针对文献[3]协议存在的问题，利用椭圆曲线密码学和哈希函数技术[7-9]进行改进，使其既继承了原协议的安全性，又能抵抗中间人攻击。

2 文献[3]的三方认证密钥协商协议

参与协议的实体有 3 个，分别是可信服务器 S、发起者 A、响应者 B。协议分为 2 个阶段：初始化阶段和认证密钥协商阶段。

2.1 初始化阶段

设有限域 F_q 上的椭圆曲线：

作者简介：唐祚波(1988－)，男，硕士研究生，主研方向：信息安全；缪祥华(通讯作者)，副教授、博士后

收稿日期：2012-03-19 **修回日期**：2012-05-06 **E-mail**：xianghuamiao@126.com

$E_q(a,b):y^2\equiv x^3+ax+b(\mathrm{mod}\ q)$

是一个由点 P 产生的大群，阶为 n。选择一对安全的对称加解密算法 $E_k()$、$D_k()$并公布给用户。每个用户 U 产生一个私钥 u 并计算对应的公钥 $U=uP$，服务器 S 选择一个私钥 s 并计算其公钥 $S=sP$。

2.2 认证密钥协商阶段

在服务器 S 的帮助下，用户 A 和用户 B 相互认证。然后产生 A 和 B 的一个会话密钥。这阶段细分成如下 3 轮：

在第 1 轮，A 执行以下步骤：

A: $r_A, w_A\in {}_RZ_q^*$

A: $R_A=r_AA$, $W_A=w_AP$

A: $K_A=ar_AS=(k_{Ax},k_{Ay})$

A: $t_A=timestamp()$

A: $C_{AS}=E_{kAx}(R_A,W_A,ID_A,ID_B,t_A)$

$A\rightarrow B$: ID_A,*Request*

$A\rightarrow S$: ID_A,C_{AS},R_A,t_A

在第 2 轮，B 执行以下步骤：

B: $r_B,w_B\in {}_RZ_q^*$

B: $R_B=r_BB,W_B=w_BP$

B: $K_B=br_BS=(k_{Bx},k_{By})$

B: $t_B=timestamp()$

B: $C_{BS}=E_{kBx}(R_B,W_B,ID_B,ID_A,t_B)$

$B\rightarrow A$: ID_B,*Response*

$B\rightarrow S$: ID_B,C_{BS},R_B,t_B

在第 3 轮，S 收到来自 A 的消息(ID_A, C_{AS}, R_A, t_A)和来自 B 的消息(ID_B, C_{BS},R_B, t_B)后，执行以下步骤：

S: *verify*(t_A, t_B)

S: $K_A=sR_A=(k_{Ax},k_{Ay})$

S: $K_B=sR_B=(k_{Bx},k_{By})$

S: $(R'_A,W_A,ID'_A,ID'_B,t'_A)=D_{kAx}(C_{AS})$

S: $(R'_B,W_B,ID''_B,ID''_A,t'_B)=D_{kBx}(C_{BS})$

S: $t'_A?=t_A$, $t'_B?=t_B$

S: $ID''_A?=ID'_A?=ID_A$, $ID''_B?=ID'_B?=ID_B$

S: $R'_A?=R_A$, $R'_B?=R_B$

S: $t_S=timestamp()$

$S\rightarrow A$: $C_{SA}=E_{kAx}(R_A,W_B,ID_A,t_S,ID_S)$

$S\rightarrow B$: $C_{SB}=E_{kBx}(R_B,W_A,ID_B,t_S,ID_S)$

最后，A 收到 C_{SA}，检查 R''_A 与第 1 轮的 R_A，并计算会话密钥 SK。具体过程如下：

A: $(R''_A,W_B,ID_A,t_S,ID_S)=D_{kAx}(C_{SA})$

A: *verify*(t_S)

A: $R''_A?=R_A$

A: $SK=w_AW_B$

类似地，B 收到 C_{SB}，检查 R''_B 与第 2 轮的 R_B，并计算会话密钥 SK。具体过程如下：

B: $(R''_B,W_A,ID_B,t_S,ID_S)=D_{kBx}(C_{SB})$

B: *verify*(t_S)

B: $R''_B?=R_B$

B: $SK=w_BW_A$

3 针对文献[3]协议的攻击

3.1 发起者假冒攻击

任何攻击者都能假冒协议发起者 A 与 B 进行协议。攻击者 X 选择 $r_X, w_X\in {}_RZ_q^*$，并计算：

$R_X=r_XP$

$W_X=w_XP$

$K_X=r_XS=(k_{Xx},k_{Xy})$

然后，X 使用 k_{Xx} 加密：

$C_{XS}=E_{kXx}(R_X,W_X,ID_A,ID_B,t_X)$

并发送(ID_A, *Request*)给 B，发送(ID_A,C_{XS},R_X, t_X)给 S。

当 B 收到 X 的请求后，运行协议，并发送(ID_B, *Response*)至 X，发送(ID_B,C_{BS},R_B, t_B)至 S。

之后 S 运行协议，发送 C_{SX} 给 X，发送 C_{SB} 给 B。

B 收到 C_{SB} 后，使用 k_{Bx} 作为解密密钥解密 C_{SB}，获得(R''_B, W_X, ID_B, t_S, ID_S)以及会话密钥 $SK= w_BW_X$。

同样，X 计算会话密钥 $SK =w_XW_B$。

在攻击过程中，X 和 S 的共享秘密密钥 $K_X=r_XsP$。因为 X 知道 r_X 的值和公钥 $S=sP$，所以他能计算共享秘密密钥 K_X。他在第 1 轮发送 $R_X =r_XP$ 给 S，S 就可以计算同样的秘密密钥 $K_X=sR_X$。很明显，S 缺乏认证功能，S 和 B 都被 X 欺骗，认为 X 就是 A。

3.2 响应者假冒攻击

文献[3]的协议受响应者假冒攻击的过程和原因与发起者假冒攻击类似。

3.3 中间人攻击

任何可以实施发起者假冒攻击和响应者假冒攻击的人都可以实现中间人攻击。实施那 2 种攻击后，用户 A、B 都被欺骗，A 认为他与 B 协议，B 认为他与 A 协议，事实上它们各自都与 X 协议。因为 X 知道 2 个会话密钥(A 与 X 的会话密钥以及 X 与 B 的会话密钥)，它可以加密和解密所有 A 和 B 之间传输的信息，所以文献[3]的协议不具备认证功能，不能抵抗中间人攻击。

4 文献[3]协议的改进

文献[3]的协议受中间人攻击的原因是任何用户 U 可以与 S 共享秘密密钥 $K_U=ur_US=usr_UP=sR_U$，S 没有检查 U 是否知道临时密钥 r_U 和长期私钥 u。解决此问题，可以使用身份标识符或公私钥对在 S 和 U 之间建立认证关系。

在文献[3]协议的基础上，本文利用单向哈希函数把用户的私钥融入到协议中，并加上一些变量 t_U、Y_U，使得每次协议时 T_U 不同。这不仅可以认证用户，

而且安全性更高。另外，协议的最后使用了哈希函数，从而使会话密钥更安全，可以抵抗中间人攻击。协议分为 2 个阶段：第 1 阶段与文献[3]协议的第 1 阶段类似；第 2 阶段细分以下 3 轮：

在第 1 轮，A 执行以下步骤：

A: $r_A \in_R Z_q^*$

A: $Y_A=r_AP$, $R_A=r_AA$, $W_A=aS$

A: $K_A=r_AW_A=(k_{Ax},k_{Ay})$

A: $t_A=timestamp()$

A: $T_A=H(t_A,W_A,Y_A)$

A: $C_{AS}=E_{kAx}(Y_A,ID_A,ID_B)$

$A\rightarrow B$: ID_A,*Request*

$A\rightarrow S$: ID_A, C_{AS}, Y_A, R_A, T_A, t_A

在第 2 轮，B 执行以下步骤：

B: $r_B \in_R Z_q^*$

B: $Y_B=r_BP$, $R_B=r_BB$, $W_B=bS$

B: $K_B=r_BW_B=(k_{Bx},k_{By})$

B: $t_B=timestamp()$

B: $T_B=H(t_B,W_B,Y_B)$

B: $C_{BS}=E_{kBx}(Y_B,ID_B,ID_A)$

$B\rightarrow A$: ID_B,*Response*

$B\rightarrow S$: ID_B, C_{BS}, Y_B, R_B, T_B, t_B

在第 3 轮，S 收到来自 A 的$(ID_A,C_{AS},Y_A,R_A,T_A,t_A)$和来自 B 的$(ID_B,C_{BS},Y_B,R_B,T_B,t_B)$后，执行以下步骤：

S: *verify*(t_A, t_B)

S: $T_A?=H(t_A, sA,Y_A)$

S: $T_B?=H(t_B, sB,Y_B)$

S: $K_A=sR_A=(k_{Ax},k_{Ay})$

S: $K_B=sR_B=(k_{Bx},k_{By})$

S: $(Y'_A,ID'_A,ID'_B)=D_{kAx}(C_{AS})$

S: $(Y'_B,ID''_B,ID''_A)=D_{kBx}(C_{BS})$

S: $ID''_A?=ID'_A?=ID_A$, $ID''_B?=ID'_B?=ID_B$

S: $Y'_A?=Y_A$, $Y'_B?=Y_B$

S: $t_S=timestamp()$

$S\rightarrow A$: $C_{SA}=E_{kAx}(Y_A,Y_B,ID_A,t_S,ID_S)$

$S\rightarrow B$: $C_{SB}=E_{kBx}(Y_B,Y_A,ID_B,t_S,ID_S)$

最后，A 收到 C_{SA}，解密出 Y''_A，检查 Y''_A 与第 1 轮的 Y_A 是否同一点。如果两者相同，那么 A 确信 B 已被 S 认证，并计算会话密钥 SK。具体过程如下：

A: $(Y''_A,Y_B,ID_A,t_S,ID_S)=D_{kAx}(C_{SA})$

A: *verify*(t_S)

A: $Y''_A?=Y_A$

A: $SK=H(r_AY_B)$

类似地，B 收到 C_{SB}，解密出 Y''_B，检查 Y''_B 与第 2 轮的 Y_B 是否是同一点。如果两者相同，那么 B 确信 A 已被 S 认证，并计算会话密钥 SK。具体过程如下：

B: $(Y''_B,Y_A,ID_B,t_S,ID_S)=D_{kBx}(C_{SB})$

B: *verify*(t_S)

B: $Y''_B?=Y_B$

B: $SK=H(r_BY_A)$

5 安全性分析与证明

改进后的协议不仅继承了原协议的安全属性，而且可以抵抗发起者、响应者假冒攻击和中间人攻击。下面给出非形式化分析和形式化证明。

5.1 非形式化分析

假设攻击者 X 假冒 A 与 B 通信。X 随机选择 r_X, $w_X \in_R Z_q^*$，并计算：

$Y_X=r_XP$

$R_X=r_XA$

$W_X=w_XS$

$K_X=r_XW_X=(k_{Xx},k_{Xy})$

$T_X=H(t_X,W_X,Y_X)$

然后，X 用 k_{Xx} 加密：

$C_{XS}=E_{kXx}(Y_X,ID_A,ID_B)$

并发送$(ID_A,Request)$给 B，发送$(ID_A,C_{XS},Y_X,R_X,T_X,t_X)$给 S。

B 收到来自 X 的$(ID_A, Request)$，运行协议，发送$(ID_B, Response)$至 X，发送$(ID_B, C_{BS}, Y_B, R_B, T_B, t_B)$至 S。

S 收到信息后运行协议，首先验证(t_X, t_B)是否有效。接着判断：

$T_X=H(t_X,sA,Y_X)$

是否成立，由于不成立，协议停止。原因是 X 不知道 A 的私钥 a，无法计算 $W_A=aS$，从而不能通过服务器的验证。要想通过验证，只有通过 P 和 A 求出 a，但已知椭圆曲线上 2 点 P、A 求出整数 a 是非常困难的。因此，改进的协议具有认证功能，可以抵抗发起者假冒攻击。

类似地，改进的协议也可以抵抗响应者假冒攻击，原因是 X 不知道响应者的私钥。

因此，改进的协议可以抵抗发起者和响应者假冒攻击以及中间人攻击。另外，改进的协议还具备了原协议所具有的安全性。例如，假冒者想延时重发 T_A，其伪造的一个新鲜 t_X 可以通过 *verify*(t_X,t_B)，但是 T_A 与 $H(t_X,sA,Y_A)$不等，能被检验出，因此，协议可以抵抗重放攻击。

5.2 形式化证明

定理 在标准模型下，如果 CDH(Computational Diffie-Hellman)假设[10]成立，那么改进的协议是安全的认证密钥协商协议。

证明：首先，若 2 个协议参与者都遵循协议规范并未被腐化，攻击者是良性的，那么参与者都能正确地收到对方发来的协议消息，最终参与者接受

$SK=K_{AB}=K_{BA}$。

其次，把攻击者对协议的攻击规约到解决 CDH 问题[10]的方法来证明改进协议的安全性。在此采用反证法。假设 $Adv_F^{3PAKA}(k)$ 是不可忽略的，那么可以使用攻击者 F 构造一个算法 E 去解决 CDH 问题，且成功效率是不可忽略的，这一过程如下，其中，$Adv_F^{3PAKA}(k)$ 是攻击者 F 在询问多项式次数后的成功优势：

(1)攻击者输入：

$(R_x,R_y)=(xP,yP)$

其中，$x,y\in_R Z^*_q$；P 是阶为 q 的群 G_1 的生成元。

(2)仿真

仿真器可以回答 *Execution* 查询、*Send* 查询、*Reveal* 查询、*Corrupt* 查询、*Test* 查询。另外，允许攻击者 F 进行 *Hash* 查询。

(3)*Execution* 查询：这种查询模仿被动攻击。

仿真器任意选择 $r_A\in_R Z_q^*$，计算：

$Y_A=r_AR_x$

$R_A=aY_A$

$W_A=aS$

$K_A=r_AW_A$

$T_A=H(t_A,W_A,Y_A)$

$C_{AS}=E_{kAx}(Y_A,ID_A,ID_B)$

并发送$(ID_A,C_{AS},Y_A,R_A,T_A,t_A)$给 S。

同时，仿真器任意选择 $r_B\in_R Z^*_q$，计算：

$Y_B=r_BR_y$

$R_B=bY_B$

$W_B=bS$

$K_B=r_BW_B$

$T_B=H(t_B,W_B,Y_B)$

$C_{BS}=E_{kBx}(Y_B,ID_B,ID_A)$

并发送$(ID_B, C_{BS},Y_B,R_B,T_B,t_B)$给 S。

类似地，仿真器计算：

$C_{SA}=E_{kAx}(Y_A,Y_B,ID_A,t_S,ID_S)$

$C_{SB}= E_{kBx}(Y_B,Y_A,ID_B,t_S,ID_S)$

并发送 C_{SA} 给参与者 A，发送 C_{SB} 给参与者 B。

(4)*Send* 查询：这种查询模仿主动攻击。

仿真器回答对服务器的 *Send* 查询过程如下：

仿真器计算对称密钥(k_{Ax},k_{Bx})，加密：

$C_{SA} =E_{kAx}(Y_A,Y_B,ID_A,t_S,ID_S)$

$C_{SB} =E_{kBx}(Y_B,Y_A,ID_B,t_S,ID_S)$

并发送 C_{SA} 至参与者 A，发送 C_{SB} 至参与者 B。

仿真器回答对用户的 *Send* 查询的过程如下：

仿真器任意选择 $r_A\in_R Z_q^*$，计算：

$Y_A=r_AR_x$

$R_A=aY_A$

$W_A=aS$

$K_A=r_AW_A$

$T_A=H(t_A,W_A,Y_A)$

并使用 k_{Ax} 加密：

$C_{AS}=E_{kAx}(Y_A,ID_A,ID_B)$

之后返回$(ID_A,C_{AS},Y_A,R_A,T_A,t_A)$。

类似地，仿真器返回$(ID_B,C_{BS},Y_B,R_B,T_B,t_B)$。

(5)*Reveal* 查询：这种查询是模仿某个实例中会话密钥的泄漏。查询时，如果会话密钥已被定义，返回 SK，否则，报错退出。

(6)*Corrupt* 查询：该查询要求被查询的实例返回它所拥有的长期私钥。

(7)*Test* 查询

仿真器首先通过 *Reveal* 查询获得 SK，然后协议随机选择一个比特 b(1 或 0)。如果 b=1，仿真器返回 SK，否则，返回随机值。

(8)*Hash* 查询：该查询用于仿真器保存(SK,Y)，返回 $Y(r_BY_A$ 或 $r_AY_B)$。

(9)通过算法 E 输出：

$yR_X=r_A^{-1}r_B^{-1}Y$

或：

$xR_y=r_A^{-1}r_B^{-1}Y\ (yR_X=xR_Y=xyP)$

其中，Y 是一个计算会话密钥 $SK=H(Y)$的值。

攻击者 F 在仿真和真实协议运行中是不可区分的，只要能 *Hash* 查询 Y，E 将成功计算 yR_X 或者 xR_y，进一步说，E 将有一个不可忽略的概率：

$Succ_{F,G1}^{CDH}\geqslant Adv_F^{3PAKA}(k)$

所以，改进的协议是安全的。

6 结束语

本文提出了一种新的三方认证密钥协商协议，通过新增的哈希函数来实现用户的认证。随后，给出了非形式化分析与形式化证明，新协议不仅具有原协议的安全性，而且可以抵抗假冒攻击和中间人攻击。如何在安全假设和安全目标不变的情况下，提出效率更高的三方认证密钥协商协议是下一步值得研究的问题。

参考文献

[1] 邱卫东, 黄 征, 李祥学, 等. 密码协议基础[M]. 北京: 高等教育出版社, 2009.

[2] Yang Jen-Ho, Chang Chin-Chen. An Efficient Three-party Authenticated Key Exchange Protocol Using Elliptic Curve Cryptography for Mobile-commerce Environments[J]. The Journal of Systems and Software, 2009, 82(9): 1497-1502.

(下转第 148 页)