用于多媒体加密的基于身份的密钥协商协议的安全性

刘永亮[①] 高 文[①②] 姚鸿勋[①] 黄铁军[②]
[①](哈尔滨工业大学计算机科学与技术学院 哈尔滨 150001)
[②](中国科学院计算技术研究所 北京 100080)

摘 要：最近 Yi 等(2002)提出了一个用于多媒体加密的基于身份的密钥协商协议。协议建立在 Diffie-Hellman 密钥交换协议和 RSA 公钥密码体系之上。Yi 等分析了协议的安全性，并认为该协议对于恶意攻击是鲁棒的。然而，本文证明该协议对于某些攻击如伪造秘密信息和篡改交换消息是脆弱的，并分析了该协议受到这些攻击的原因。本文指出由于该协议内在的缺陷，该协议可能难于改善。

关键词：安全性；基于身份的密钥协商；恶意攻击
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2007)04-0892-03

Security on ID-Based Key Agreement for Multimedia Encryption

Liu Yong-liang[①] Gao Wen[①②] Yao Hong-xun[①] Huang Tie-jun[②]
[①](*School of Computer Science and Technology*, *Harbin Institute of Technology*, *Harbin* 150001, *China*)
[②](*Institute of Computing Technology*, *Chinese Academy of Sciences*, *Beijing* 100080, *China*)

Abstract: Recently, Yi *et al.*.(2002) proposed an ID-based key agreement protocol for multimedia encryption. The protocol was built on both the Diffie-Hellman key exchange protocol and the RSA public key cryptosystem. Yi *et al.* analyzed the security of the protocol, and understood that the protocol is robust to the malicious attacks. However, this paper shows that the protocol is vulnerable to certain malicious attacks such as forging secret information and tampering exchanging messages and analyzes the reasons that the protocol suffers these attacks. This paper points out that it may be hard to improve the protocol due to the inherent flaw of the protocol.

Key words: Security; ID-based key agreement; Malicious attack

1 引言

在文献[1]中，Yi 等提出了一个用于多媒体加密的基于身份的密钥协商协议。该密钥协商协议建立在 Diffie-Hellman 密钥交换协议和 RSA 公钥密码系统之上。在该密钥协商协议中，身份信息如姓名、社会保险号、网络地址或者电话号码被用作用户的公钥，同时，可信的密钥分配中心对身份信息的签名作为用户的私钥。Yi 等分析了协议的安全性，并认为该协议能够抵抗恶意攻击，包括主动攻击和被动攻击。然而，在研究中发现该协议中存在严重的安全缺陷。本文证明该协议对于某些攻击如伪造秘密信息和篡改交换消息是脆弱的。而且，分析了协议受到这些攻击的原因。

本文组织如下：第 2 节给出安全协议的简单介绍。第 3 节回顾了 Yi 等的基于身份的密钥协商协议。第 4 节描述了对 Yi 等协议的攻击。第 5 节给出了一个结论。

2 安全的协议

本节简要介绍安全协议的定义和基本的安全目标。这些内容将用于分析 Yi 等协议的安全性。

2005-08-28 收到，2006-04-06 改回
国家 863 计划(2004AA119010)和国家自然科学基金(60472043)资助课题

2.1 安全协议的定义

在文献[2–9]中讨论了安全协议的定义。特别地，Diffie 等给出了下面的安全协议的定义。

定义 1 一个协议的一个特定的执行是一个不安全的执行，如果协议中涉及的任何方，比如说 Alice，如实地执行了协议并接受了另一方的身份，下面的条件之一满足：

(1)在 Alice 接受另一方的身份时，另一方的部分或全部执行记录与 Alice 的记录不匹配。

(2)Alice 接受的交换密钥被 Alice 接受身份方以外的其它方知道。

定义 2 一个安全的协议是这样的一个协议，在一方 Alice 如实地执行协议并接受另一方的身份的情况下，下面的条件满足：

(1)在 Alice 接受另一方的身份时，另一方的部分或全部记录完全匹配 Alice 的记录。

(2)除了 Alice 和 Alice 接受身份方以外的其它方获得 Alice 接受的交换密钥是计算不可能的。

以上的定义在确定一个给定的协议是否安全不是特别有帮助。然而，这些定义可以直接用于确定一个给定的可能的攻击是否是一个真正的攻击。

2.2 基本的安全目标

下面描述的基本的安全目标被认为在任何应用中都是至关重要的[6–9]。其它的安全属性在某些环境下是重要的，但是在其它环境下可能不太重要。

(1)隐式密钥认证(implicit key authentication) 一个密钥协商协议被称为提供 Bob 向 Alice 的隐式密钥认证，如果 Alice 确信除了 Bob 之外其它方不可能知道特定的密钥值。

(2)密钥确认(key confirmation)一个密钥协商协议被称为提供 Bob 向 Alice 的密钥确认，如果 Alice 确信 Bob 实际上计算了协商的密钥。

(3)明确密钥认证(explicit key authentication) 一个密钥协商协议被称为提供 Bob 向 Alice 的明确密钥认证，如果协议同时提供了隐式密钥认证和密钥确认。

在实际应用中，非常希望密钥协商协议提供明确密钥认证，因为明确密钥认证可能提供隐式密钥认证中不存在的安全属性。

3 Yi 等的基于身份的密钥协商协议

Yi 等的基于身份密钥协商协议需要一个可靠的密钥分配中心 TC。TC 负责计算和发布秘密密钥给授权的用户。协议可简要地描述为 3 个阶段：初始化阶段、密钥生成阶段和密钥协商阶段。

3.1 初始化阶段

TC 首先产生两个大素数 p 和 q，满足 $p=q=3(\mathrm{mod}\ 4)$，计算乘积 $n=pq$ 和 $\phi(n)=(p-1)(q-1)$，确定一对数(e,d)，满足$ed\equiv 1(\mathrm{mod}\,\phi(n))$，其中$e$ 是从 1 和 $\phi(n)$之间随机选择的，且e与$\phi(n)$互素，即e和$\phi(n)$的最大公约数是 1。e和d 被分别作为 TC 的公钥和私钥。然后，TC 确定有限域$\mathrm{GF}(p)$和 $\mathrm{GF}(q)$一个的生成元g。参数 p，q和d 是 TC 的秘密信息， 参数n， e 和g对于所有用户都是公开的。

3.2 密钥生成

对于一个授权的用户 A，其身份信息为id_A，TC 为其计算相应的秘密信息 $s_A=\mathrm{id}_A^{-d}(\mathrm{mod}\,n)$。然后，TC 把$(n,g,e,s_A)$存储到一张智能卡中，并把卡发给用户 A。如果s_A是根据公式$s_A=\mathrm{id}_A^{-d}(\mathrm{mod}\,n)$计算得出，那么容易得出$s_A^e=(\mathrm{id}_A^{-d})^e(\mathrm{mod}\,n)=\mathrm{id}_A^{-1}(\mathrm{mod}\,n)$。

根据 RSA 签名算法的安全性，如果不知道 TC 的私钥d，即使知道id_A，e和n，也很难计算出s_A。如果知道n的因子p和q，那么d可以使用欧基里德算法或其它方法从等式$ed\equiv 1(\mathrm{mod}\,\phi(n))$计算出。然而，分解$n$是计算不可行的，因为 n的长度是 1024bit。

3.3 密钥协商

假定 A 和 B 是两个授权的用户，他们都有一张智能卡，其中存储有 TC 发给他们的私钥。A 和 B 可以通过如下的方式建立一个共享的会话密钥k：

步骤 1　A 随机地选择一个数r_A，并计算$x_A=s_A\cdot g^{r_A+\mathrm{id}_B}(\mathrm{mod}\,n)$。$B$ 也随机地选择一个随机数 r_B，并计算$x_B=s_B\cdot g^{r_B+\mathrm{id}_A}(\mathrm{mod}\,n)$。

步骤 2　A和B交换消息$(\mathrm{id}_A,\ x_A)$和(id_B,x_B)。

步骤 3　A 计算公共的会话密钥k：

$$k=((g^{-\mathrm{id}_A}x_B)^e\mathrm{id}_B)^{r_A}=((g^{r_B}s_B)^e\mathrm{id}_B)^{r_A}=(g^{er_B}s_B^e\mathrm{id}_B)^{r_A}$$
$$=g^{er_Br_A}(\mathrm{mod}\ n)$$

B计算公共的会话密钥k：

$$k=(g^{-\mathrm{id}_B}x_A)^e\mathrm{id}_A)^{r_B}=((g^{r_A}s_A)^e\mathrm{id}_A)^{r_B}=(g^{er_A}s_A^e\mathrm{id}_A)^{r_B}$$
$$=g^{er_Ar_B}(\mathrm{mod}\ n)$$

执行完上面的 3 步之后，A 和 B 获得了共享的会话密钥k。注意，实际当中k只是 A 和 B 共享的一个秘密，为了获得共享的会话密钥，还需要使用一个双方协商的密钥导出函数来计算得出会话密钥。

这个协议乍看起来是安全的。不幸的是，协议中存在着一些安全缺陷使得该协议会遭受一些恶意攻击。下一节给出对该协议的恶意攻击。

4 对 Yi 等协议的恶意攻击

4.1 伪造秘密信息

恶意攻击者可以伪造秘密信息。恶意攻击者可以是一个授权的内部用户，也可以是一个没有获得授权的外部攻击者。在描述攻击之前，首先证明下面的两个性质。

性质 1　g模n的逆元$g^{-1}(\mathrm{mod}\,n)$存在。

证明　因为g是有限域$\mathrm{GF}(p)$和 $\mathrm{GF}(q)$的生成元，所以等式 $\gcd(g,p)=1$ 和 $\gcd(g,q)=1$ 成立，其中 $\gcd(u,v)=1$ 表示 u 和 v 的最大公约数是 1。因为 $n=pq$，所以$\gcd(g,n)=1$。因此，$g^{-1}(\mathrm{mod}\,n)$存在[10]。

性质 2　对于任意 $R\in[1,n-1]$，g^R 模 n 的逆元$(g^R)^{-1}(\mathrm{mod}\,n)$存在。

证明　在性质 1 的证明中已经证明$\gcd(g,n)=1$，所以$\gcd(g^R,n)=1$。因此，$(g^R)^{-1}(\mathrm{mod}\,n)$存在[10]。

4.1.1 *来自内部用户的攻击*　假定攻击者 M是一个授权的用户。因为参数g，n和e对所有用户都是公开的，M 可以选择一个随机数r，计算$g^{er}(\mathrm{mod}\,n)$。让$\mathrm{id}_E=\mathrm{id}_Mg^{er}(\mathrm{mod}\,n)$，$\mathrm{id}_E$可能等于或不等于某个授权用户的身份信息数值。进一步，M可以伪造秘密签名信息s_E，因为

$$s_E=(\mathrm{id}_E)^{-d}=(\mathrm{id}_Mg^{er})^{-d}=\mathrm{id}_M^{-d}g^{-edr}=s_Mg^{-r}(\mathrm{mod}\,n)$$

而其中s_M对于 M 是已知的，g^{-r}可计算得出(由性质 2，$g^{-r}(\mathrm{mod}\,n)$存在)。在成功地伪造秘密信息后，M 可以使用伪造的信息(id_E,s_E)来冒充为一个授权的用户 E(E 可能是也可能不是一个授权的用户)同一个授权的用户 A 执行 Yi 等的协议。此过程描述如图 1：

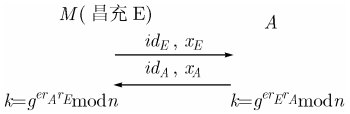

图 1

攻击开始于 M 产生一个随机数 r_E，计算 $x_E = s_E \cdot g^{r_E+\mathrm{id}_A} (\mathrm{mod}\, n)$，发送消息 id_E 和 x_E 给 A。一旦收到消息后，A 产生一个随机数 r_A，计算 $x_A = s_A \cdot g^{r_A+\mathrm{id}_E} (\mathrm{mod}\, n)$，向 M 返回消息 id_A 和 x_A。然后，M 和 A 分别计算公共的会话密钥 $k = g^{er_Ar_E} (\mathrm{mod}\, n)$。执行协议后，$M$ 成功地冒充了用户 E，并使得用户 A 错误地认为密钥是在 A 和 E 之间共享的。

4.1.2 *来自外部攻击者的攻击* 假定 M 是一个未获得授权的外部攻击者。M 可以采用如下的方式伪造秘密信息：

M 选择一个随机数 $r \in [1, n-1]$，计算 $h = g^r (\mathrm{mod}\, n)$，$\mathrm{id} = h^e (\mathrm{mod}\ n)$ 和 $s = h^{-1} = g^{-r} (\mathrm{mod}\, n)$。根据上面的数值关系，下面的等式成立

$$s = \mathrm{id}^{-d} (\mathrm{mod}\ n)$$

因此，M 以上面的方式成功地伪造了身份信息 id 和相应的秘密信息 s。在这样的情况下，M 可以使用消息对 (id, s) 冒充一个授权的用户和其它授权的用户进行通信执行 Yi 等的协议。

上述的两个伪造秘密信息攻击是非常微妙的，需要非常少的计算花费。但是它们可能引起严重的后果。在协议中被这两个攻击利用到的弱点是身份信息和秘密信息之间潜在的代数结构关系。尽管可以通过 TC 定期发布所有合法用户身份信息列表的方式部分防止上述的伪造攻击，但是潜在的威胁依然存在。因此，协议的这个缺陷可能是内在的，难以克服。

4.2 篡改交换的消息

这个攻击描述如图 2：

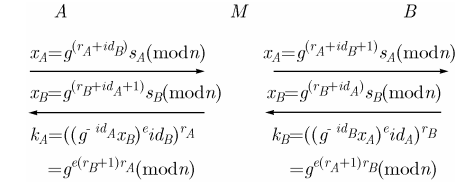

图 2

在此攻击中，M分别使用 $\overline{x}_A = g^{(r_A+\mathrm{id}_B+1)} s_A (\mathrm{mod}\, n)$ 和 $\overline{x}_B = g^{(r_B+\mathrm{id}_A+1)} s_B (\mathrm{mod}\, n)$ 替换 $x_A = g^{(r_A+\mathrm{id}_B)} s_A (\mathrm{mod}\, n)$ 和 $x_B = g^{(r_B+\mathrm{id}_A)} s_B (\mathrm{mod}\, n)$（注意，这里 M 把 $x_A = g^{(r_A+\mathrm{id}_B)} s_A (\mathrm{mod}\, n)$ 篡改为 $\overline{x}_A = g^{(r_A+\mathrm{id}_B+1)} s_A (\mathrm{mod}\, n)$ 仅是一种可能的情况，只是为了表述和理解简单）。在这种情况下，A计算会话密钥 $k_A = g^{er_A(r_B+1)}$，B计算会话密钥 $k_B = g^{er_B(r_A+1)}$。然而，在协议执行的过程中A和B不能够检测到他们所计算的密钥是不同的，尽管他们都如实地执行了协议。

这个攻击看起来可能不是一个严重的攻击，因为M不知道密钥值。然而，这的确表示一个攻击，因为它使得A/B错误地认为接收到的消息来自于B/A，并且执行完协议后与B/A共享了一个会话密钥。而且，A/B的执行记录明显不匹配。根据第2节的定义，这的确表示一个攻击。

这个攻击有效的原因是交换的消息没有被签名并且协议没有提供密钥确认。尽管协议提供了隐式密钥认证(只有意向消息接收方能够计算会话密钥)，但协议对于上面的攻击是脆弱的。

5 结束语

本文提出了对 Yi 等协议的伪造秘密信息攻击和篡改交换消息攻击，并分析了该协议受到这些攻击的原因。本文指出由于该协议的内在的缺陷，改善该协议防止伪造秘密签名信息可能是困难的。

参 考 文 献

[1] Yi X, Tan C H, and Siew C K, *et al*.. ID-based key agreement for multimedia encryption. *IEEE Trans. on Consumer Electronics*, 2002, 48 (2): 298–303.

[2] Bird R, Gopal I, and Herzberg A, *et al*.. Systematic design of two-party authentication protocols. Advances in Cryptology——CRYPTO'91, Santa Barbara, 1991: 44–61.

[3] Diffie W, Oorschot P, and Wiener M. Authentication and authenticated key exchanges. *Designs, Codes and Cryptography*, 1992 2(2): 107–125.

[4] Bellare M and Rogaway P. Provably secure session key distribution. Advances in Cryptology——CRYPTO'93, Santa Barbara, 1993: 232–249.

[5] 毛文波. 现代密码学: 理论与实践. 北京: 电子工业出版社, 2004: 1–477.

[6] Wilson S B and Menezes A. Authenticated Diffie-Hellman key agreement protocols. Fifth Annual Workshop on Selected Areas in Cryptography, Ontario, 1998: 339–361.

[7] 卿斯汉. 安全协议 20 年研究进展. 软件学报, 2003, 14 (10): 1740–1752.
Qing Si-han. Twenty years development of security protocols research. *Journal of Software*, 2003, 14 (10): 1740–1752.

[8] 卿斯汉. 安全协议的设计与逻辑分析. 软件学报, 2003, 14(7): 1300–1309.
Qing Si-han. Design and logical analysis of security protocols. *Journal of Software*, 2003, 14(7): 1300–1309.

[9] 范红, 冯登国. 安全协议理论与方法. 北京: 科学出版社, 2003: 13–46.

[10] Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. New York: John Wiley & Sons, Inc. 1996: 246–246.

刘永亮： 男，1973 年生，博士生，研究方向为数字权利管理(DRM).

高 文： 男，1956 年生，教授，博士生导师，研究方向为多媒体数据压缩、图像处理、人工智能等.

姚鸿勋： 女，1965年生，教授，博士生导师，研究方向为模式识别、数字水印等.

黄铁军： 男，1970年生，研究员，研究方向为数字媒体、数字图书馆、模式识别与图像处理.