第32卷 第20期 计 算 机 工 程 2006年10月
Vol.32 № 20 Computer Engineering October 2006
·安全技术· 文章编号：1000—3428(2006)20—0168—02 文献标识码：A 中图分类号：TP393.08

DSS签字标准在密钥交换协议中的应用研究

程 辉[1]，欧阳旦[2]
(1. 解放军信息工程大学电子技术学院，郑州 450004；2. 空军电子技术研究所，北京 100089)

摘 要：密钥的安全分配是采用密码技术保证通信安全的重要环节，文章介绍了一种将DSS签字标准与Diffie-Hellman协议相结合的密钥交换协议，指出其在前向安全性上的不足。在此基础上，提出了一种密钥交换协议设计方案，并对其安全和计算量作了简要分析。
关键词：密钥交换；数字签名；数字签字标准；离散对数

Research on Application of Digital Signature Standard to the Key Exchange Protocols

CHENG Hui[1], OUYANG Dan [2]
(1. Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004;
2. Research Institute of Electronic Technology, Air Force, Beijing 100089)

【Abstract】The secure distribution of the key is an important process of keeping the security of communication by using cryptographic technology. This paper introduces a protocol integrating Diffie-Hellman protocol into the digital signature standard, points out its weakness in perfect forward secrecy, proposes a new key exchange protocol and analyses its security and efficiency briefly.
【Key words】Key exchange; Digital signature; Digital signature standard(DSS); Discrete logarithm

现代密码学认为：采用密码技术对重要信息的保护取决于密钥的安全性，而不是对密码算法本身的保护。因此，密钥的管理在信息保密系统中非常重要。现有的密钥管理协议主要包括具有管理中心的密钥分配协议和不具有管理中心的密钥协商协议。不具有管理中心的密钥协商协议以DH(Diffie-Hellman)协议为代表，它是第1个双钥算法，它的安全性来自于有限域上计算离散对数的困难性。协议的原理十分简单，但由于缺少认证机制，因此协议容易受到中间人攻击。1993年Arazi第1次将DH协议结合到DSS签字标准中[1]，使进行密钥交换的双方可以对对方的身份进行认证。但该协议的弱点在1994年由Nyberg和Rueppel发现[2]，被定义为已知密钥攻击。文献[3]也给出了一种将DH协议与DSS相结合的方案，本文对其安全性进行了分析，指出其在前向安全性上的不足，提出了一种密钥交换协议，并对其安全性作了简要分析。

1 DSS签字标准

DSS(Digital Signature Standard)签字标准是在1991年8月由美国国家标准与技术研究所(NIST)公布的，1994年5月19日正式公布，1994年12月1日正式采用为美国联邦信息处理标准。DSS中所采用的算法简记为DSA(Digital Signature Algorithm)，其安全性基于有限域上求解离散对数的困难性，它是在ElGamal和Schnorr两个签字方案基础上设计的。它的算法可描述为：

(1)全局公钥 (p,q,g)，p 是 $2^{L-1}<p<2^L$ 中的大素数，$512\leq L\leq 1024$，按64bit递增；q 是 $(p-1)$ 的素因子，且 $2^{159}<q<2^{160}$，即字长160bit；$g=h^{p-1}\bmod p$，且 $1<h<(p-1)$，使 $h^{(p-1)/q}\bmod p>1$。

(2)用户密钥 x 是在 $0<x<q$ 内的随机或拟随机数。

(3)用户公钥 q，$Q=g^x \bmod p$。

(4)用户为每个签字消息选取的秘密随机数 k(是在 $0<k<q$ 内的随机或拟随机数)。

(5)签字过程：给定消息 M，其签字为：

$S=Sig_k(M,k)=(r,s)$，

其中：

$r\equiv(g^k \bmod p)\bmod q$，

$s\equiv[k^{-1}(H(M)+xr)]\bmod q$（$H(M)$为计算 M 的杂凑值)。

(6)验证过程：计算 $w=s^{-1}\bmod q$，$u_1=[H(M)w]\bmod q$，$u_2=rw \bmod q$，$v=[(g^{u_1}Q^{u_2})\bmod p]\bmod q$，$Ver(M,r,s)$＝真 $\Leftrightarrow v=r$。

2 相关研究

2.1 协议内容

文献[3]提出了一种新的将DSS签字标准与DH协议相结合的密钥交换协议，具体内容为：

系统参数 (p,q,g) (如DSS标准中定义)，A、B的私钥分别是 a 和 b，公钥分别是 Q_A 和 Q_B。

(1)A选择秘密随机数 $x\in[1,q-1]$，计算：$R_A=g^x \bmod p$，并将 R_A 传给B；

(2)B选择秘密随机数 $y\in[1,q-1]$，计算 $K_{BA}=(Q_A)^y \bmod p$，$K_{AB}=(R_A)^b \bmod p$，$R_B=g^y \bmod p$，$r_B=R_B \bmod p$，

作者简介：程 辉(1981－)，男，硕士生，主研方向：网络安全技术；欧阳旦，高工
收稿日期：2005-10-14 **E-mail：**chui8101@163.com

$s_B=(y^{-1}(H(R_B\|K_{BA}\|K_{AB})+br_B))\bmod q$，把 (R_B,s_B) 传给 A；

(3)A 计算：

$K_{AB}=(Q_B)^x \bmod p$， $K_{BA}=(R_B)^a \bmod p$， $r_B=R_B \bmod p$，$w=s_B^{-1}\bmod q$，$u_1=[H(R_B\|K_{BA}\|K_{AB})w]\bmod q$，$u_2=r_Bw\bmod q$，$v=[(g^{u_1}Q_B^{u_2})\bmod p]\bmod q$；验证 $v=r_B$ 是否成立，若不成立则终止协议，若成立则接着计算：$r_A=R_A \bmod p$，$s_A=(x^{-1}(H(R_A\|K_{AB}\|K_{BA})+ar_A))\bmod q$，把 s_A 传给 B；

(4)B 计算：

$r_A=R_A \bmod p$，$w=s_A^{-1}\bmod q$，$u_1=[H(R_A\|K_{AB}\|K_{BA})w]\bmod q$，$u_2=r_Aw\bmod q$，$v=[(g^{u_1}Q_A^{u_2})\bmod p]\bmod q$；验证 $v=r_A$ 是否成立，如果成立，则 A、B 之间成功建立共享秘密参数 K_{AB} 和 K_{BA}，A 和 B 分别把 K_{AB} 和 K_{BA} 作为与对方通信时的密钥。

2.2 协议安全性分析

(1)在分析密钥交换协议时很重要的一点是看协议能否抵抗已知密钥攻击(known key attack)，该攻击方法由 Nyberg 和 Rueppel 在文献[2]中提出，基本思想是：如果攻击者 C 知道 A、B 之间一个或多个时间段的密钥，那么 C 可根据 A、B 间的公开信息计算出 A、B 间其它秘密，从而推算出 A、B 间其它时间段的密钥。对该协议抵抗已知密钥攻击分析如下：

A、B之间交换的信息S_A, S_B可表示为：

$$s_Ax=(H(R_A\|K_{AB}\|K_{BA})+ar_A)\bmod q$$
$$s_By=(H(R_B\|K_{BA}\|K_{AB})+br_B)\bmod q$$

两式交叉相乘得到

$$s_Axbr_B+s_AxH(R_B\|K_{BA}\|K_{AB})=s_Byar_A+s_ByH(R_A\|K_{AB}\|K_{BA})\bmod q$$

取 g 为底数

$g^{s_Axbr_B+s_AxH(R_B\|K_{BA}\|K_{AB})}=g^{s_Byar_A+s_ByH(R_A\|K_{AB}\|K_{BA})\bmod q}$，即

$$(K_{AB})^{s_Ar_B}(R_A)^{s_AH(R_B\|K_{BA}\|K_{AB})}=(K_{BA})^{s_Br_A}(R_B)^{s_BH(R_A\|K_{AB}\|K_{BA})} \bmod p$$

如文献[4]指出，如果攻击者 C 掌握了 K_{AB} 和 K_{BA} 中的一个，要计算出另一个其难度相当于解离散对数。再由 $s_Ax=(H(R_A\|K_{AB}\|K_{BA})+ar_A)\bmod q$ 得

$$g^{s_Axb}=g^{bH(R_A\|K_{AB}\|K_{BA})+abr_A} \bmod p$$

即 $(K_{AB})^{s_A}=(Q_B)^{H(R_A\|K_{AB}\|K_{BA})}(g^{ab})^{r_A} \bmod p$，假设 C 同时掌握了某个时间段的 K_{AB} 和 K_{BA}，那么就可以计算出 g^{ab}，但要通过 g^{ab} 计算出 A、B 间另一个时间段的 K_{AB} (或 K_{BA})其难度相当于求解离散对数。再假设 C 掌握了 g^{ab} 和某一时间段的 K_{AB}，要通过它们计算出 K_{BA}，其难度仍相当于求解离散对数。因此，该协议可以较好地抵抗已知密钥攻击。

(2)密钥交换协议中还有一种攻击方法被称作未知密钥共享攻击(unknown key-share attack)，基本内容是：攻击者 C 能强迫通信双方 A、B 建立密钥，但 A、B 至少有一方并不知道该密钥已被 C 共享。文献[5]论述了具有密钥证实(key confirmation)的可认证密钥交换协议能抵抗未知密钥共享攻击。在上述协议中，A 收到 B 的签字信息 $s_B=(y^{-1}(H(R_B\|K_{BA}\|K_{AB})+br_B))\bmod q$，该签字中包含已生成的密钥 $K_{AB}=g^{xb} \bmod p$，x 是由 A 选择的秘密随机数，因此 A 可完成对 K_{AB} 的密钥证实。同理，B 也可完成对 K_{BA} 的密钥证实。所以协议可通过密钥证实抵抗未知密钥共享攻击。

(3)为了增强密钥交换协议的安全性，协议还要具备的一个性质是前向保密性(perfect forward secrecy)，这就是要求即使在 A、B 中一方或双方的长期使用的私钥泄漏情况下，之前 A、B 确定的通信密钥仍然是安全的，通信的内容仍然不可破译。而上述协议显然不能满足这一点。例如，如果 A 的私钥 a 暴露，由于 R_B 是公开传递的参数，因此攻击者可轻易计算出 $K_{BA}=(R_B)^a \bmod p$。

3 本文提出的密钥交换协议

3.1 协议内容

系统参数 (p,q,g) (如 DSS 标准中定义)，A、B 的私钥分别是 a 和 b，公钥分别是 Q_A 和 Q_B。

(1)A 选择秘密随机数 $x_1,x_2\in[1,q-1]$，计算：$R_A=g^{x_1} \bmod p$，$R_A^{'}=g^{x_2} \bmod p$，将 $(R_A,R_A^{'})$ 传给 B。

(2)B 选择秘密随机数 $y_1,y_2\in[1,q-1]$，计算共享密钥 $K=(R_A^{'})^{y_2} \bmod p$；计算：$R_B=g^{y_1} \bmod p$，$R_B^{'}=g^{y_2} \bmod p$，$r_B=R_B \bmod q$，$s_B=y_1^{-1}(H(R_B\|R_B^{'}\|R_A\|R_A^{'}\|K)+br_B)\bmod q$；将 $(R_B,R_B^{'},s_B)$ 传给 A；

(3)A 计算共享密钥 $K=(R_B^{'})^{x_2} \bmod p$，然后计算：$r_B=R_B \bmod q$，$w=s_B^{-1}\bmod q$，$u_1=H(R_B\|R_B^{'}\|R_A\|R_A^{'}\|K)w\bmod q$，$u_2=r_Bw\bmod q$，$v=g^{u_1}Q_B^{u_2} \bmod p$，验证 $v=r_B$ 是否成立，如果不成立则终止协议，若成立则计算 $s_A=x_1^{-1}(H(R_A\|R_A^{'}\|R_B\|R_B^{'}\|K)+ar_A)\bmod q$，把 s_A 传给 B。

(4)B 计算：$r_A=R_A \bmod q$， $w=s_A^{-1}\bmod q$，$u_1=H(R_A\|R_A^{'}\|R_B\|R_B^{'}\|K)w\bmod q$，$u_2=r_Aw\bmod q$，$v=g^{u_1}Q_A^{u_2} \bmod p$，验证 $v=r_A$ 是否成立，如果不成立则终止协议，若成立那么 $K=g^{x_2y_2} \bmod p$ 就是 A、B 建立的密钥。

3.2 协议安全性分析

(1)根据 s_A、s_B 的表达式可得

$$x_1y_1s_As_B=H(X)H(Y)+H(X)br_B+H(Y)ar_A+abr_Ar_B \bmod q$$

其中，$X=R_A\|R_A^{'}\|R_B\|R_B^{'}\|K$，$Y=R_B\|R_B^{'}\|R_A\|R_A^{'}\|K$

取 g 为底数得

$$(g^{x_1y_1})^{s_As_B}=g^{H(X)H(Y)}(Q_B)^{r_BH(X)}(Q_A)^{r_AH(Y)}(g^{ab})^{r_Ar_B} \bmod p$$

在协议中A、B双方计算出的共享密钥为 $K=g^{x_2y_2} \bmod p$，而参与计算 s_A 和 s_B 的参数为 x_1 和 y_1，所以攻击者即使掌握了某个时间段的 K，也无法使用上面的等式来计算 A、B 的长期秘密 g^{ab}。因此协议可抵抗类似文献[2]中提出的已知密钥攻击方法。

(2)在 A 对 B 的认证过程中，A 收到 B 的签字消息 $s_B=y_1^{-1}(H(R_B\|R_B^{'}\|R_A\|R_A^{'}\|K)+br_B)\bmod q$，$s_B$ 的计算中包括 K，而 $K=g^{x_2y_2} \bmod p$，参数 x_2 由 A 随机选定，因此通过双方在计算杂凑函数时加入协商的密钥 K，A 可完成对 K 的密钥证实，同理，B 也可完成对 K 的密钥证实。那么协议可通过密钥证实来抵抗未知密钥共享攻击。

(3)如果 A、B 的私钥泄露，因为 $K=g^{x_2y_2} \bmod p$，所以无法由 a、b 直接计算出 K。另外，根据签名信息：$s_A=x_1^{-1}(H(R_A\|R_A^{'}\|R_B\|R_B^{'}\|K)+ar_A)\bmod q$，在知道 a 的情况下，因为 K 存在于杂凑值中，且等式中并不含参数 x_2 和 y_2，所以也无法由 s_A 计算出 K。同理根据等式 (下转第 172 页)