基于CPK和改进ECDH算法的可证安全的认证协议

侯惠芳 王云侠
(河南工业大学信息科学与工程学院 郑州 450001)

摘 要 针对ECDH易受中间人攻击的问题,提出在Canetti-Krawczy(CK)模型下的可证安全的改进算法,并结合CPK算法,利用CK模型的模块化方法设计出安全和高效的快速认证协议,设计并改进了一个消息传输认证器,使其所采用的对称加密算法的密钥是动态生成的。协议在实现双向认证的同时,协商并确认会话密钥。分析表明,协议具有较高的安全性和性能。

关键词 组合公钥,Canetti-Krawczy模型,消息传输认证器,认证密钥协商
中图法分类号 TP309 **文献标识码** A

Provable Secure Authentication Protocol Based on CPK and Improved ECDH Algorithm

HOU Hui-fang WANG Yun-xia
(College of Information Science and Engineering, Henan University of Technology, Zhengzhou 450001, China)

Abstract Since ECDH was easily suffered from man-in-the-middle attack, a provable secure improved ECDH in the Canetti-Krawczy(CK) model was presented. Combined with CPK, a security and efficient fast authentication protocol was devised based on the modular approach of Canetti-Krawczyk(CK) model. It also designed and improved a message transmission authenticator in which the key of symmetric encryption algorithm was dynamically generated. It realized session key association and confirmation meanwhile mutual authentication. Analysis shows it has better security and performance.

Keywords Combined public key, Canetti-Krawczy model, Message transmission authenticator, Authenticated key agreement

1 引言

在通信网络环境中,为实现安全通信,首先需要认证。认证方案是认证方案与密钥分配方案相结合方案的简称,主要实现认证与密钥协商两个目的[1]。事实上,认证和密钥协商功能通过认证协议来保障,并力争在保证安全性的前提下计算量和通信次数尽可能少,也称为快速认证协议;同时,双向认证是通信的本质要求,其不仅是各种安全技术的综合运用,也是保障其他业务的基础。认证协议的分析和设计是网络安全领域发展前沿的重大课题,也吸引了大批学者的不断关注和研究。

椭圆曲线密钥协商算法ECDH[2]是Diffie-Hellman公钥系统在椭圆曲线上的实现,算法安全性依赖于椭圆曲线上的离散对数问题(ECDLP)的困难性。ECDH算法实现了会话密钥协商功能,但与最初的Diffie-Hellman一样,通信实体在不知对方身份的情况下建立相互的密钥,缺乏对实体的认证,因而易遭受中间人攻击[3]。EAP-TLS使用临时DH和签名的密钥交换算法,不能提供双向认证,易遭受中间人攻击[4],而且开销也比较大。文献[5]通过将安全hash函数引入到Diffie-hellman中,解决了中间人攻击,但是所设计的快速相互认证协议,需要采用公钥加解密算法来实现对信息的加密和获取,这需要证书的传输与验证,而且公钥加解密算法相对于对称加解密算法计算量较大。

本文提出一种在Caneti-Krawczyk(简称CK)模型[6]下可证明安全的改进ECDH算法,并采用CK模型的模块化设计,提出一种基于CPK和改进ECDH算法的快速认证协议,在通信双方完成双向身份认证的同时实现会话密钥的协商与确认,具有较强的安全属性和较好的性能。

2 背景知识

2.1 相关的数学问题

椭圆曲线离散对数问题(ECDLP):对于定义于有限域F_q上的椭圆曲线$E(F_q)$上的任意点$Q=kP, k\in F_q$,求整数k,即为ECDLP。也可理解为由给定的k和P计算Q较容易,而给定P和Q计算k较困难。

椭圆曲线计算性Diffie-Hellman问题(ECDHP):对于未知的a和b,给定$X=aP, Y=bP$,计算出$Z=abP$是困难的。

椭圆曲线除法计算性Diffie-Hellman问题(EDC-

到稿日期:2011-04-01 返修日期:2011-07-17 本文受国家高技术研究发展计划("863"计划)基金项目(2007AA01Z434),国家自然科学基金项目(61003052/F020304)资助。

侯惠芳(1972—),女,博士,副教授,主要研究方向为信息安全,E-mail:houhf72@163.com;王云侠(1977—),女,硕士,讲师,主要研究方向为信息安全、智能算法。

DHP)[7]：对于未知的 a 和 b，给定 $X=aP, Y=bP$，计算出 $Z=\frac{a}{b}P$ 是困难的。

上述 3 个问题被视为困难性问题，文献[7]研究并证明，ECDHP 和 EDCDHP 一样困难，ECDLP 至少与 ECDHP 和 EDCDHP 一样困难。

2.2 组合公钥(Combined Public Key,CPK)算法简介

1999 年南湘浩院士提出 CPK 算法[8]，该算法是在椭圆曲线密码体制的基础上构建的，安全性基于 ECDLP 的难解性，具体算法如下。

离线的密钥管理中心(KMC)依据参数，构建 $m\times h$ 阶公钥种子矩阵 PSK(可公开)和 $m\times h$ 阶私钥种子矩阵 SSK(自己保留)，PSK 和 SSK 中的元素分别记为 $R_{i,j}$ 和 $r_{i,j}$($R_{i,j}=r_{i,j}P=(X_{i,j},Y_{i,j})$)，对应位置的 $R_{i,j}$ 与 $r_{i,j}$ 即为一公私钥对。分别从 PSK 和 SSK 中的每一列取一个因子并求和即可构造出公钥和私钥。

实体 A 根据实体 B 的标识(如姓名、IMSI、身份证、IP 地址等)计算出 B 的公钥。具体方法为：求出 B 的标识对应的 h 个标识映射函数的值($i_1,i_2,\cdots,i_h$)，用($i_1,i_2,\cdots,i_h$)作行坐标，利用 PSK，求出公钥 $PK=\sum_{l=1}^{h}R_{i_l,l} \bmod n$。由实体的公钥 PK 和椭圆曲线的参数，求出实体的私钥 SK 是 ECDLP。

CPK 算法不依赖第三方，可“当场”直接认证实体的标识，解决了直接认证和认证规模化两大课题[8]，近年来，CPK 体制在不断改进[9]，CPK 技术也得到越来越多的应用[10,11]。

2.3 Canetti-Krawczyk(CK)模型

CK 模型[6]是可证明安全方法之一，该模型给出会话密钥安全(SK-secure)的定义(即协议产生的密钥和一个独立随机值的不可区分性)以及利用该定义证明协议安全性的模块化方法。鉴于用 CK 模型证明的安全性，反映了现实通信模型系统中的安全要求，CK 模型可得到实际有效的密钥分配协议。CK 模型同时适用于对称与非对称两种密码体制，并极大简化了认证与密钥协商协议的设计与分析。

在 CK 模型中证明协议是会话密钥安全(SK-secure)的，只需证明其满足 SK-secure 的两个性质：

性质 1(一致性要求) 未被攻陷的参与者完成协议后，会话匹配，得到相同的会话密钥。

性质 2 攻击者进行测试会话查询攻击时，不能以不可区分的优势区分会话密钥和随机数。

CK 模型下的协议具有安全属性：丢失信息安全、抗密钥泄漏伪装攻击、已知会话密钥安全和未知密钥共享安全等。

CK 模型采用模块化方法[12]设计密钥协商协议，具体步骤如下：

(1)在理想环境下的认证链路攻击(AM)模型下，设计或者重用一个基本的 SK-secure 协议。

(2)对得到协议的安全性进行形式化分析。

(3)设计能被证明是有效的认证器。

(4)应用认证器将 AM 下的基本协议转换成真实网络环境下的未认证链路攻击(UM)模型中的安全认证协议。

(5)运用重用消息组合、重新排序、消除冗余的随机数等方式优化结果协议。

在实际设计协议时，除完成上述 5 个步骤外，还要对协议在降低计算成本和存储需求方面做优化。

3 快速双向认证与密钥协商协议

3.1 认证协议用到的参数和运算

ID_A：A 的身份标识；SK_A：A 的私钥；PK_A：A 的公钥；$Nounce_A$：A 生成的随机数；$hash(m)$：在 m 上的单向安全的 hash 运算；$E_K(m)$：用对称密钥 k 对 m 加密；$prf(\ )$：密钥产生函数，$F_q\rightarrow\{0,1\}^l$，$l\geqslant 128$；$sig_{SK}(m)$：用私钥 SK 对 m 签名；签名方案采用 CPK 中的方案。

3.2 改进的 ECDH 算法

本文在未增加计算量的前提下，通过引入用户公钥信息到 ECDH 算法，生成一个会话密钥安全的改进 ECDH 算法，使其能抵抗中间人攻击。具体实现过程如下：

Step1 A 产生随机数 $Nounce_A$，计算 $Q_A=(Nounce_A+SK_A)PK_B$，发送 A,Q_A 给 B；

Step2 B 产生随机数 $Nounce_B$，计算 $Q_B=(Nounce_B+SK_B)PK_A$，发送 B,Q_B 给 A；B 计算密钥：$k_{BA}=SK_B^{-1}(Nounce_B+SK_B)Q_A$；

Step3 A 计算密钥：$k_{AB}=SK_A^{-1}(Nounce_A+SK_A)Q_B$。

改进 ECDH 算法与 ECDH 算法相比，仅增加了计算量小的加法运算，计算量较大的椭圆曲线的标量乘运算并没有增加，其中，SK_A 和 SK_B 的求逆运算 SK_A^{-1} 和 SK_B^{-1} 也可以提前计算，因而改进 ECDH 算法相比于 ECDH 算法未增加计算量。

定理 在 ECDHP 假设下，改进 ECDH 算法在 AM 中是 SK-secure 的。

前提：基点 $P\in E(F_q)$，n 为阶。

目标：A 和 B 共享会话密钥 $(Nounce_A+SK_A)(Nounce_B+SK_B)P$。

证明：

首先证明改进 ECDH 算法满足 SK-secure 的条件(1)。

因为 AM 中的攻击者无法对消息进行主动攻击，所以协议参与方在未遭受到破坏的前提下，能够正确执行协议且能接收到对方用于交换的临时公共参数 Q_A 和 Q_B，进而计算出相同的会话密钥。

$$\begin{aligned}k_{AB}&=SK_A^{-1}(Nounce_A+SK_A)Q_B\\&=SK_A^{-1}(Nounce_A+SK_A)(Nounce_B+SK_B)PK_A\\&=(Nounce_A+SK_A)(Nounce_B+SK_B)P=k_{BA}\end{aligned}$$

下证改进 ECDH 算法满足 SK-secure 的条件 2。参照文献[6]的思想设计算法 PA，算法 PA 将 KE 对手 KEA 作为子程序，KEA 控制着所有通信信道；PA 代替协议交互过程中的所有实体，并执行所有的调度操作。PA 和 KEA 交替来模仿协议的执行过程，回答 KEA 的一切询问，并将协议的输出消息返回给 KEA。证明的思路是：利用反证法，假设 KEA 能以不可忽略的优势 ε 猜到测试会话中的 b，从而判断测试会话查询中的返回值是随机数还是真实的会话密钥，则算法 PA 将能够以不可忽略的优势计算出 $(Nounce_A+SK_A)(Nounce_B+SK_B)P$，显然与 ECDHP 假设相悖，因此协议是 SK-secure 的。

算法 PA 的具体描述如下：

(1)PA 随机选择编号为 m 的会话作为 KEA 的测试会话，设最大会话数目为 l，并把公共参数 q 和 P 告诉 KEA。

(2)PA 激活 KEA 和参与实体，对其进行仿真交互，除了标记为“秘密”的本地输出，KEA 知道激活结果和参与实体的

本地输出，且当会话不是第 m 个会话或接收一条信息时，PA 替代该参与方，按照协议的要求建立其他会话。

(3)若会话过期，则参与实体将会话状态及会话密钥从其存储器中擦去。

(4)若 KEA 攻陷一个参与实体或暴露出会话 m 的会话的状态后，则 PA 将攻陷的参与实体或暴露的会话的相关信息返回给 KEA。

(5)当第 m 次会话被激活时，PA 让 A 把消息(s_m,A,Q_A)发送给 B。

(6)当 B 收到消息(s_m,A,Q_A)时，PA 让 B 把消息(s_m,B,Q_B)发送给 A。

(7)若第 m 个会话(A,B,s_m)已经暴露，或选中非 m 会话作为测试会话查询，或 KEA 没有选择测试会话就停止，则 PA 随机选择 0 或 1 返回给 KEA，将值赋给 b' 后输出并停止。

(8)若 KEA 对会话 m 进行测试会话查询，则 PA 掷币 $b\in\{0,1\}$，若 $b=1$，则 PA 返回一随机数给 A；若 $b=0$，则 P 发送会话密钥 $k=(Nounce_A+SK_A)(Nounce_B+SK_B)P$ 给 KEA。之后，KEA 停止攻击，PA 停止运行。此时，KEA 猜测出正确的会话密钥的概率为 $\varepsilon+1/2$。

从上述过程可以看出，由 PA 激发的 KEA 的执行过程和 KEA 单独对抗改进算法的正常运行是一致的。KEA 对测试的会话有以下两种选择：①若 A 选中第 m 次会话作为测试会话，则 KEA 成功得到会话密钥的概率等于 PA 选择 $b=0$ 还是 $b=1$ 的概率，此时，KEA 猜中响应是真实的会话密钥还是随机数的概率是 $\varepsilon+1/2$。②当 A 没有选中第 m 次会话作为测试会话，PA 输出一个随机数 b。此时，KEA 猜中会话密钥的概率是 1/2。

KEA 选中第 m 次会话的概率是 $1/l$，对应的未选中第 m 次会话的概率是 $1-1/l$，则 KEA 正确猜测 b，获得会话密钥的概率是 $(1/2+\varepsilon)\times(1/l)+1/2\times(1-1/l)=1/2+\varepsilon/l$。

若攻击者 KEA 能以不可忽视的优势 ε 猜到测试会话中的 b，则攻击者获得会话密钥的概率 $1/2+\varepsilon/l$ 也不可忽视，与 ECDHP 假设相悖。

因此，改进 ECDH 算法在 AM 下是 SK-secure 的。

改进 ECDH 算法具有 SK-secure 满足的安全属性，而且当 A 和 B 私钥安全时，该算法实现了隐式密钥认证，能够抵挡中间人攻击，解决了 ECDH 算法易遭受中间人攻击的问题。

传递的 Q_A 和 Q_B 中分别包含对方的公钥，因此只有拥有 A 的私钥才能从 B 发来的 Q_B 计算出 $(Nounce_B+SK_B)P$ 的值，分析过程：有两种方法由 Q_B 计算 $(Nounce_B+SK_B)P$，一是通过 SK_A 计算 $SK_A^{-1}Q_B$ 得到 $(Nounce_B+SK_B)P$，而由 $PK_A=SK_AP$ 计算出 SK_A 是 ECDLP；二是求出 $(Nounce_B+SK_B)$，再计算 $(Nounce_B+SK_B)P$，而由 Q_B 计算 $(Nounce_B+SK_B)$ 也是 ECDLP。同理只有拥有 B 的私钥才能从 A 发来的 Q_A 计算出 $(Nounce_A+SK_A)P$ 的值。而且即使能把 Q_A 和 Q_B 分解，由 $(Nounce_A+SK_A)P$ 和 $(Nounce_B+SK_B)P$ 求出 $(Nounce_A+SK_A)(Nounce_B+SK_B)P$ 也是 ECDHP。因此 A 和 B 确认其他实体都得不到他们的密钥，即该算法较好地实现了隐式密钥认证。

3.3 消息传输认证器(MT-authenticator)的设计

3.3.1 改进的基于动态加密密钥和 hash 函数的消息传输认证器

本文设计基于对称加密算法和随机数的 MT-authenticator 来保护 A 向 B 传递的加密信息及相互认证，该认证器的安全性基于 EDCDHP。

设计思路：文献[13]提出一种 MT-authenticator，A 向 B 发送用对称密码算法加密的信息，B 返回 A 消息认证码，实现 A 对 B 的认证。在该认证器中，双方需要预先定义和协商对称密钥，密钥管理和更新复杂、难度大，无法满足系统扩展性的需要，因此，本文将静态预先协商的对称密钥改进为在通信时动态生成，并且确认只有对方才能计算出该密钥，提供隐式密钥认证功能。具体算法过程如下：

Step 1 A 产生随机数 $Nounce_A$ 和 $Nounce$，计算 $Q_A=(Nounce_A+SK_A)PK_B$，动态对称密钥 $ks=prf((Nounce_A+SK_A)P||Q_A)$ 和加密信息 $ENC_{ks}(Nounce)$，将 m，$ENC_{ks}(Nounce)$，Q_A 传给 B。

Step 2 B 收到消息后，计算 $Q_A/SK_B=(Nounce_A+SK_A)P$，而后求出动态对称密钥 ks，解密 $ENC_{ks}(Nounce)$ 获得 $Nounce$，最后将 m，$hash(Nounce)$ 传给 A；B 计算 ks，

$ks=prf((Nounce_A+SK_A)P||Q_A)=prf(Q_A/SK_B||Q_A)$。

Step 3 A 收到消息后，验证 $hash(Nounce)$ 正确后，认证 B。

该认证器中对 $SK_B^{-1}Q_A$ 的计算基于 EDCDHP。

证明：

$Q_A=(Nounce_A+SK_A)PK_B=(Nounce_A+SK_A)SK_BP$

且 $PK_B=SK_BP$，因此求 $\dfrac{(Nounce_A+SK_A)SK_B}{SK_B}P$ 为 EDCDHP，只有拥有与公钥 PK_B 所对应私钥 SK_B 的实体 B 才能计算出动态对称密钥。

3.3.2 基于数字签名和随机数的消息传输认证器

A 与 B 之间采用基于数字签名和随机数的认证器实现不可否认性及认证，该认证器详细证明可参见文献[13]。

Step 1 A 向 B 发送消息 m。

Step 2 B 收到消息后，随机产生 $Nounce_B$，将 m，$Nounce_B$ 传送给 A。

Step 3 A 收到消息后，计算签名信息 $sig_{SK_A}(m,Nounce_B,B)$，将 m，$sig_{SK_A}(m,Nounce_B,B)$ 传送给 B。

Step 4 B 验证签名 $sig_{SK_A}(m,Nounce_B,B)$，正确后，认证 A。

3.4 UM 下可证安全的快速双向认证与密钥协商协议

将上述 2 个认证器先应用于改进 ECDH 算法即 AM 协议中的消息流中，并经过优化组合，最后仿真得到 UM 中的协议。鉴于所用 MT-authenticator 是可证安全的，因此，根据 CK 模型模块化设计方法自动编译得到的 UM 中的协议也是可证安全的。协议的具体过程如下：

Step 1 A 根据通信方 B 的标识，利用 CPK 算法计算其公钥 PK_B，产生随机数 $Nounce_1$ 和 $Nounce$，而后计算 $Nounce_A=Nounce_1+SK_A$，$Q_A=Nounce_APK_B$，$ks=prf(Nounce_AP||Q_A)$，$W_{AB}=E_{ks}(ID_A||ID_B||Nounce||Wsig_A)$，$Wsig_A=sig_{SK_A}(ID_A||ID_B||W_{AB}||Nounce)$，然后发送消息$\langle ID_A,ID_B,Q_A,W_{AB},Wsig_A\rangle$给 B。

Step 2 B 产生随机数 $Nounce_2$，根据 A 的标识，利用 CPK 算法计算出其公钥 PK_A，计算 $Nounce_B=Nounce_2+SK_B$，$K=prf(Nounce_BQ_A/SK_B)$，$Q_B=Nounce_BPK_A$，解密 W_{AB}，验证签名 $Wsig_A$，正确后，计算 $Wsig_B=sig_{SK_B}(ID_A||$

$ID_B||Q_B||hash(Nounce))$，$W_{BA}=E_K(ID_A||ID_B||hash(Nounce))$，然后发送消息$\langle ID_A, ID_B, Q_B, W_{BA}, Wsig_B\rangle$给 A。

Step 3 A 计算 $K=prf(NounceQ_B/SK_A)$，解密 W_{BA}，验证 $hash(Nounce)$和签名 $Wsig_B$，正确后，认证 B。

4 协议的安全性和性能分析

4.1 安全性分析

4.1.1 双向认证

A 和 B 利用 CPK 算法由对方的标识计算出其公钥，而只有正确的私钥才能与公钥对应，因此，即使 A 和 B 的身份被伪造，基于 ECDLP，伪造者也得不到正确的私钥；再者，W_{AB}需要 A 利用自己的私钥计算得到，而且只有 A 才能计算出正确的签名 $Wsig_A$，易知攻击者不能假冒 A 计算出 W_{AB}和 $Wsig_A$，故而当 B 验证签名 $Wsig_A$ 并与解密 W_{AB}得到的 $Wsig_A$ 比较后，认证 A；因为只有 B 可利用其私钥计算出密钥 ks，而后解密 W_{AB}得到 $Nounce$，再利用改进 ECDH 算法计算出与 A 的会话密钥，计算出正确的签名 $Wsig_B$，因此 A 通过验证得到的 $hash(Nounce)$和 $Wsig_B$，认证 B。

4.1.2 会话密钥安全

本协议具有 CK 模型中会话密钥的安全属性，此外，协议具有的属性分析如下：

(1)密钥控制安全性

A 与 B 之间的会话密钥依赖于 A 和 B 分别产生的随机数 $Nounce_A$ 和 $Nounce_B$，任何一方均不能单独控制密钥为提前预先选择的值，即该算法保证了密钥控制安全性。

(2)前向保密性

A 与 B 之间的会话密钥与私钥及每次产生的随机数均相关，因此，即使实体的私钥泄露，攻击者由 Q_A 或 Q_B 计算出 $(Nounce_A+SK_A)P$ 或 $(Nounce_B+SK_B)P$，但是计算出 $(Nounce_A+SK_A)(Nounce_B+SK_B)P$ 仍是 ECDHP，所以即使实体的长期私钥泄露后，以前所建立的会话密钥并不受影响，即该算法保证了密钥的前向保密性。

(3)临时密钥安全

A 与 B 之间的会话密钥中包含 A 和 B 的私钥，即使 A 和 B 的临时秘密 $Nounce_A$ 和 $Nounce_B$ 被泄，攻击者由于没有 A 和 B 的私钥也无法计算出会话密钥，因此抵御了临时密钥泄露后的攻击，满足了临时密钥安全，对 A 和 B 的私钥及他们之间协商的会话密钥均无影响。

4.1.3 不可否认性

认证中 A 和 B 的数字签名可保证通信双方 A 和 B 的不可否认性。

4.2 性能分析

A 和 B 利用 CPK 算法依据双方的身份标识，计算出所需的公钥，省去了公钥证书的传输及验证，节省了带宽和证书验证时延；而且不用存储、发送或处理证书，故也减轻了实体的存储负担。

通信开销：协议的参与方仅需要 2 轮信息交互，且在实现双向认证的同时协商并确认会话密钥。

计算开销：将协议与其他文献的协议就实体 A 的运算次数和通信开销进行比较，结果如表 1 所列。

从表 1 中可以看出，本文设计的协议与 EAP-TLS 相比，信息交互次数明显减少，而且不需要公钥加解密运算，其执行速度明显提高。虽然本协议与 WAPI 和文献[5]的信息交互次数相同，但是由于采取对称密码算法代替公钥加密算法，运算速度明显得到提高，虽然其相比于文献[5]多了签名运算，但是比文献[5]增加实现了不可否认性。因此，相较于其他的协议，本协议还是高效的。

表 1 实体 A 性能比较

	公钥传输	公钥加/解密	生成签名	验证签名	验证证书	信息交换次数
EAP-TLS	需要	1/1	1	1	0	5
文献[5]	需要	1/1	0	0	1	2
WAPI[14]	需要	1/1	1	1	1	2
本文协议	不需	0/0	1	1	0	2

结束语 针对网络中通信双方的通信安全问题，本文提出一种基于 CK 模型的可证安全的双向认证和密钥协商协议。根据 CK 模型，首先构造并证明一个 AM 模型下的可证安全的改进 ECDH 算法；然后重用并改进设计现有可证安全的消息传输认证器；最后得到 UM 模型下的认证与密钥协商协议，实现了双向实体认证的功能、会话密钥的协商和确认功能。在协议中采用动态加密算法代替公钥加密算法实现了对信息的加密，并用 CPK 算法节省了对公钥的传递与验证。分析表明，该协议具有较高的安全属性，计算量和通信开销也是较低的，可广泛应用于网络通信中。

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signature schemes [C]// Advances in Cryptology-CRYPTO'84. Vol. 196 of LNCS, Springer-Verlag, 1984: 47-53

[2] Lee W, Lee J. Design and Implementation of Secure E-mail System Using Elliptic Curve Cryptosystem[J]. Future Generation Computer Systems, 2004, 20(2): 315-326

[3] Diffie W, Hellman M E. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, IT-22: 644-654

[4] 朱建民，马建峰. 无线局域网安全：方法与技术[M]. 北京：机械工业出版社，2009

[5] 朱辉，李晖，王育民，等. 新的可证明安全的快速认证协议[J]. 电子科技大学学报，2009，38(1)：55-58

[6] Canetti R, Krawczyk H. Analysis of Key-Exchange Protocols and their Use for Building Secure Channels(Full Version)[C]// Advances in Cryptology-EUROCRYPT 2001. Vol. 2045 of LNCS, Springer-Verlag, 2001: 453-474

[7] Bao Feng, Deng R H, Zhu Huafei. Variations of Diffie-Hellman problem[C]// Proceedings of ICICS 2003. China, 2003: 301-312

[8] 南湘浩. CPK 标识认证[M]. 北京：国防工业出版社，2006

[9] 南湘浩. CPK 五种版本要点[J]. 计算机安全，2010，10：1

[10] 陈永刚，贾春福，吕述望. 一个基于 CPK 的高效签密方案[J]. 电子与信息学报，2009，31(7)：1753-1757

[11] 万伟，王晋东，张恒巍. 一种基于 CPK 的传输协议[J]. 计算机工程，2010，36(4)：147-149

[12] Brown D, Menezes A. A Small Subgroup Attack on a Key Agreement Protocol of Arazi' Key Agreement Protocol[R]. Canada: University of Waterloo, 2001

[13] Tin Y S T, Vasanta H, Boyd C, et al. Protocols with security proofs for mobile applications[C]// Proceedings of the ACISP 2004. Sydney, 2004: 358-369

[14] 中华人民共和国国家标准. 国标 GB15629.11-2003 信息远程通信和信息交换局域网和城域网特定要求第 11 部分：无线局域网媒体访问控制和物理层规范[S]. 北京：中国标准出版社，2003