基于CPK的TLS握手协议的设计与研究

程克非，贾廷强

(重庆邮电大学计算机科学与技术学院 重庆 南岸区 400065)

【摘要】TLS协议作为当今应用最广泛的传输层安全协议，受到了人们的极大关注，但是其自身存在证书管理复杂、握手交互过多和安全缺陷等诸多问题。对TLS握手协议分析和研究，并结合基于身份的组合公钥密码体制(CPK)的特点，提出了基于CPK的握手协议方案。通过对其安全性分析和基于串空间模型理论的形式化证明，证明了该方案的安全可靠性高。在相同安全条件下进行仿真，实验结果显示与原方案对比该方案具有握手交互次数少、鉴别简捷、建立可信连接过程简单、高效等明显优点。

关 键 词 组合公钥; 握手协议; 安全分析; 串空间模型; TLS

中图分类号 TP393.08 **文献标志码** A doi:10.3969/j.issn.1001-0548.2013.03.020

Design and Research of CPK-Based TLS Handshake Protocol

CHENG Ke-fei and JIA Ting-qiang

(College of Computer Science and Technology, Chongqing University of Posts and Telecommunications Nanan Chongqing 400065)

Abstract As one of the most widely applied transport layer security protocols, the transport layer security (TLS) protocol has caused widespread attention, but it still has a lot of problems, such as complex certificate management, too much times of interactive shake hands, safety defects, and so on. Through the analysis and research on the shake hands protocol of the TLS, and combining the features of the identity-based combined public key (CPK) cryptosystems, a new CPK-based handshake protocol is proposed. The new scheme is much better in security and reliability proved by the security analysis and the formal analysis based on the strand space theory. The simulation experiment and comparison with original protocol with equivalent security show that the CPK-based handshake protocol has some obvious advantages, such as more less number of shake hands interaction, more simple identification, and the higher security and reliability.

Key words combined public key; handshake protocol; security analysis; strand space model; TLS

TLS协议作为当今最流行的安全传输协议，被广泛应用在各种网络服务中。但其在实际应用中并非无懈可击，依然存在被攻击的可能性。文献[1-2]分析了TLS握手的缺陷并验证了TLS攻击的可能，即利用中间人攻击中的劫持会话的方法，欺骗客户端实现攻击。文献[3]提出了一种新的重协商攻击，攻击者能够干扰客户端和服务器之间的TLS会话，并插入其任意选区的数据，这一攻击可能导致多种潜在的安全威胁。而且TLS协议基于PKI(public key infrastructure)，但PKI以众多的CA(certificate authentication)为基础，存在交互次数多、认证复杂、效率低等问题。针对上述缺陷和不足，文献[2,4]分别提出了不同的改进TLS协议方案，但均无法从根本上解决TLS协议自身存在的缺陷。文献[5]根据TLS协议设计原理，提出了基于IBC(identity-based cryptograph)的改进方案，但因IBC自身仍存在安全缺陷，故该方案难以应用到实践中。

因此本文在分析TLS握手协议的基础上，结合基于身份的组合公钥密码体制和认证技术，提出了基于CPK的TLS握手协议方案CPK-TLS，并在串空间模型下证明协议的安全可靠性。

1 TLS握手协议原理及其分析

1.1 TLS握手协议原理[6]

TLS协议主要由两层协议组成，底层的记录协议为更高层协议提供基本的安全服务。上层的握手协议是TLS协议的核心部分，用于通信双方建立会话的安全参数，是通信双方建立可信连接的前提。其消息流程如图1所示，其中将发起连接的一方称为客户端C，接受连接的一方称为服务器S，图中带*

收稿日期：2011－08－29；修回日期：2012－03－21
基金项目：重庆市自然科学基金重点项目(CSTC-BA2043)；重庆市科技攻关计划(CSTC2010AB)
作者简介：程克非(1974－)，男，博士，教授，主要从事网络及信息安全、嵌入式、高性能计算方面的研究.

的消息表示可选。

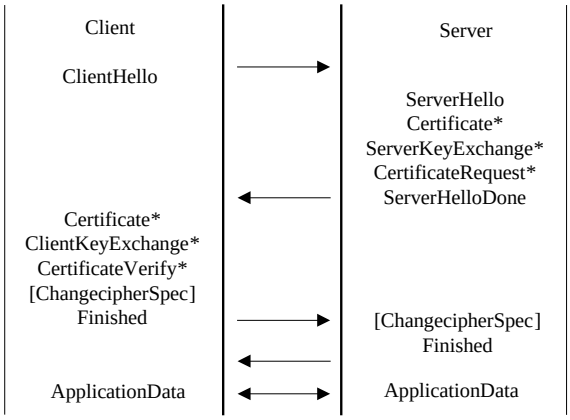

图1　TLS握手协议消息流程图

1.2　TLS握手协议分析

为了实现客户端和服务器的双向认证，当前TLS协议采用了基于证书的公钥密码体制，即通过PKI颁发的公钥证书实现认证和密钥交换。但由于PKI是基于CA证书和在线第三方认证，且其自身存在诸多缺陷，导致基于PKI的TLS协议在实际应用中存在资源开销大、效率低、易被攻击等诸多不足[7]。分析如下：

1) TLS握手协议前半阶段报文以明文传输，因此可通过监听即可获得客户端报文并进行篡改，使得TLS的会话劫持攻击成为可能。

2) TLS握手协议基于PKI密码体制，没有解决超大规模的通信标识的认证问题，而且其认证过程中需要获得大量公钥证书，这必然会消耗网络中的大量带宽资源，并增加计算的复杂度。

3) 其过程中使用了大量证书，这就要求系统支持证书的管理和分发功能，极大地增加了系统的管理复杂度。

4) 交互次数过多，过程比较复杂，效率低，实现成本较高。

2　基于CPK的TLS握手协议

为了克服PKI体制的弊端，文献[8]提出了基于身份标识的CPK技术，极好地解决了海量公钥的管理问题。该技术可以在本地一次性查找用户公钥，满足了验证的简便性和管理的有效性，其安全性基于离散对数的数学难解性，可信度高，且不需在线第三方的证明，只要少量参数就能管理大量密钥，整个认证过程可以在芯片级实现，极大地提高了运行效率，并降低了成本。

2.1　CPK密码体制原理

CPK密码体制[7]是离散对数难题型的基于标识的密钥生成与管理体制。它依据椭圆曲线上离散对数难题的数学原理构建密钥生成基，即公私钥种子矩阵；然后采用杂凑函数与密钥交换将实体标识映射为种子矩阵的行坐标和列坐标序列，用以对矩阵元素进行选取和组合，生成数量庞大的实体密钥——公私钥对，从而实现基于标识的超大规模的密钥生成与分发。私钥由实体分散保存，而公钥矩阵公开，使任意实体均能根据对方标识计算出其公钥。

CPK体制基于实体的标识生成证书解决了实体和公钥的“捆绑”，无需在线第三方认证，私钥集中生产和分发，便于管理和建立网络上的秩序，且可以实现端到端的互相认证，有着很好的安全性，为通信标识的可信性证明提供了技术基础。因此，可以设计一种基于CPK的TLS握手协议，解决当前TLS握手协议存在的不足和缺陷。

2.2　基于CPK的TLS握手协议方案

基于CPK的TLS握手协议方案的主要思想是根据握手实体双方的标识，如IP地址、MAC地址等，通过可信的密钥管理中心(KMC)生成其相应的公私钥对，以更有效的方式实现握手实体双方标识和密钥的绑定，对握手实体双方标识进行认证，提供了真实性、直接性证明。其流程如图2所示。

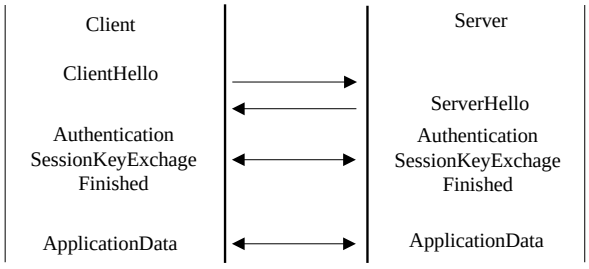

图2　基于CPK的TLS握手协议消息流程图

假设方案中CPK密码体制是建立在给定椭圆曲线 $T=(a,b,G,n,p)$ 基础上，方案如下：

1) 客户端C发送 ClientHello消息，服务器S发送ServerHello消息，完成安全参数的建立。

2) 客户端C和服务器S完成双方身份认证、会话密钥交换和验证等，以实现安全连接的建立。具体步骤如下：

① 客户端C向服务器S发起握手连接请求报文。

$$\mathrm{C}\rightarrow\mathrm{S}:\{\mathrm{ID_C}\,|\,RC\,|\,\mathrm{SIG}_{\mathrm{SK_C}}(\mathrm{data})\,|\,r(\mathrm{PK_S})\}\qquad(1)$$

式中，$\mathrm{data}=\{\mathrm{ID_C},\mathrm{ID_S}\}$；$\mathrm{ID_C}$ 表示客户端标识，$\mathrm{ID_S}$ 表示服务器标识；$\mathrm{SK_C}$ 表示客户端C的私钥；$\mathrm{PK_S}$ 表示服务器的公钥；$r(\mathrm{PK_S})$ 表示利用服务器公钥加密的对称密钥；随机数R表示报文的新鲜性，签名操作 $\mathrm{SIG}_{\mathrm{SK_C}}(\mathrm{data})$ 表示客户端用其私钥对 data 签名，作为

标识鉴别码。

详细说明如下：客户端中的CPK系统首先产此次会话的随机数 R_C，用自己的私钥对 data 进行签名得到 $\mathrm{SIG}_{\mathrm{SK_C}}(\mathrm{data})$，生成本次会话对称密钥 $\mathrm{key}=rG$；然后根据服务器标识通过系统中的公钥矩阵单元，计算出服务器的公钥，利用该公钥加密由客户端生成的对称密钥 key；最后客户端将随机数、加密密钥、标识鉴别码报文发送给服务器。

② 服务器S首先判断客户端C发来的握手连接请求报文是否可信，以验证客户端C是否可信，即实现对客户端C的认证，然后向客户端C发送验证报文。其中 T 表示服务器S产生的时间戳。

$$\mathrm{S}\rightarrow\mathrm{C}:\{\mathrm{ID_S}\,|\,R_S\,|\,E_{\mathrm{key}}(\mathrm{SIG}_{\mathrm{SK_S}}(T))\} \tag{2}$$

详细说明如下：服务器收到握手连接请求报文后，首先通过 R_C 检验消息的新鲜性，读取客户端的标识 $\mathrm{ID_C}$，通过服务器中的CPK系统中的公钥矩阵计算出客户端的公钥，然后利用客户端的公钥对 $\mathrm{SIG}_{\mathrm{SK_C}}(\mathrm{data})$ 进行解密，得到客户端和服务器的标识 $\mathrm{ID_C}$ 和 $\mathrm{ID_S}$，判断其标识的真伪，以验证客户端C是否可信，即实现对客户端C的认证，进而决定是否接收该连接请求。

如果是合法可信请求，服务器中CPK系统则利用自己的私钥解密 $r(\mathrm{PK_S})$，得到本次会话的对称密钥 key；接着服务器生成时间戳 T，通过对称密钥 key 对时间戳 T 进行加密得到 $E_{\mathrm{key}}(T)$，然后服务器通过自己的私钥对 $E_{\mathrm{key}}(T)$ 进行签名，作为验证信息；最后服务器向客户端发送验证信息。

③ 客户端C对服务器S发送来的验证报文，首先利用 R_S 检验消息的新鲜性，读取服务器标识 $\mathrm{ID_S}$ 后通过其CPK系统计算出服务器的公钥；然后利用该公钥和已选择的对称密钥 key 对收到的验证报文进行解密，得到时间戳 T^*，同时实现对服务器S的认证，接着客户端将通过协商的会话密钥加密的时间戳 T^* 发送给服务器，服务器用协商的会话密钥对该信息进行验证，判断 $T=T^*$ 是否成立，以确定安全连接是否建立，接下来，客户端和服务器之间即可开始安全可信通信。

$$\mathrm{C}\rightarrow\mathrm{S}:\{E_{\mathrm{key}}(T^*)\} \tag{3}$$

3 基于CPK的TLS握手协议安全性分析及证明

3.1 基于CPK的TLS握手协议安全性分析

协议中，在通信双方握手之前，均已从可信的KMC中获得了各自的公私钥对。在进行握手阶段时，通信实体如果能够用自身私钥正确地解密用自己公钥加密的数据，或用通信双方的会话密钥解密用对称算法加密的数据，则在通信实体的密钥没有泄露的情况下能够证实通信实体的身份，即满足认证性的要求。在通信过程中，通信双方协商会话密钥之后，使用会话密钥来加密二者之间的通信。该会话密钥只有通信的双方能够得到，因此能够保证通信的机密性。TLS握手协议的完整性可以通过自身的散列函数和消息认证码实现。另外，通过选择带有不可否认性的基于标识的数字签密方案，可以使发送方或接收方不能否认发送或接收过信息，从而达到不可否认性的安全需求。

综上分析可知，基于CPK的TLS握手协议不仅能够满足安全协议认证性、保密性、完整性和不可否认性等基本安全要求，而且由于协议中，通信双方握手之前，均可获得各自的公私钥对和对方的公钥，在通信双方握手一开始就直接用标识签名来证明连接的可信性，同时实现了通信双方双向身份认证，故该协议方案能够克服原协议包括在握手起始阶段存在明文方式传输等带来的安全缺陷，即该方案明显增强了协议的安全性。

3.2 基于串空间模型的安全性证明

形式化分析方法是对安全协议进行验证和证明的有效工具。文献[9]中提出的串空间模型，将安全协议的形式化分析技术推向一个新的高度。串空间模型是一种结合定理证明和协议迹的混合形式化分析方法，由于它具有高效、严谨、直观、简洁等特点，受到了研究人员的广泛关注[10]。

下面结合文献[9]和文献[11-12]给出的串空间模型理论和基于串空间模型的认证性测试方法对协议进行安全性证明。

3.3 协议的串空间模型

定义 ID 为身份标识集合，Ver 为实体支持的协议版本号，Suite 为实体支持的密钥算法套件，R 为随机数集合，K 为协议使用的密钥集合，key_p 表示入侵者掌握的密钥，D 为协议执行过程中主体传递的其他数据。其中，$K\cap(\mathrm{ID}\cup R\cup D)=\varnothing$，$\mathrm{ID}\cap R=\varnothing$，设 $Y=\mathrm{ID}\cup R\cup D$。

定理1 若 C 是串空间 $\sum$ 上的一个丛，$S\subseteq Y\cup K$，$k\subseteq K$，且 **错误！未定义书签。** $K\subseteq S\cup k^{-1}$，那么 $I_K[S]$ 是诚实的。

基于CPK的TLS握手协议的抽象描述如下：

$$\mathrm{C}\rightarrow\mathrm{S}:\{\mathrm{ID_C}\,|\,R_C\,|\,\mathrm{SIG}_{\mathrm{SK_C}}(\mathrm{data})\,|\,r(\mathrm{PK_S})\}$$

$$\mathrm{S}\rightarrow\mathrm{C}:\{\mathrm{ID_S}\,|\,R_S\,|\,E_{\mathrm{key}}(\mathrm{SIG}_{\mathrm{SK_S}}(T))\}$$

$$\mathrm{C}\to\mathrm{S}:\{E_{\mathrm{key}}(T^*)\}$$

定义协议3种类型的串如下：

1) 攻击者串 $S_p\in P$。

2) 发起串者 $S_i\in \mathrm{Init}[\mathrm{ID_C},\mathrm{ID_S},R_\mathrm{C},R_\mathrm{S},T,T^*,r]$，且其有如下轨迹：

$$\langle +\{\mathrm{ID_C}\,|\,R_\mathrm{C}\,|\,\mathrm{SIG}_{\mathrm{SK_C}}(\mathrm{data})\,|\,r(\mathrm{PK_S})\},$$

$$-\{\mathrm{ID_S}\,|\,R_\mathrm{S}\,|\,E_{\mathrm{key}}(\mathrm{SIG}_{\mathrm{SK_S}}(T))\},+\{E_{\mathrm{key}}(T^*)\}\rangle$$

3) 响应者串 $S_r\in \mathrm{Re}\,sp[\mathrm{ID_C},\mathrm{ID_S},R_\mathrm{C},R_\mathrm{S},T,T^*,r]$，且其有如下轨迹：

$$\langle -\{\mathrm{ID_C}\,|\,R_\mathrm{C}\,|\,\mathrm{SIG}_{\mathrm{SK_C}}(\mathrm{data})\,|\,r(\mathrm{PK_S})\},$$

$$+\{\mathrm{ID_S}\,|\,R_\mathrm{S}\,|\,E_{\mathrm{key}}(\mathrm{SIG}_{\mathrm{SK_S}}(T))\},-\{E_{\mathrm{key}}(T^*)\}\rangle$$

由定义可知，当给定一个串时，可以唯一确定它是那类串，且有集合 Init 和 Resp 不相交。协议的串空间 $\sum = p\cup \mathrm{Init}\cup \mathrm{Re}\,sp$。协议的丛示意图如图3所示。

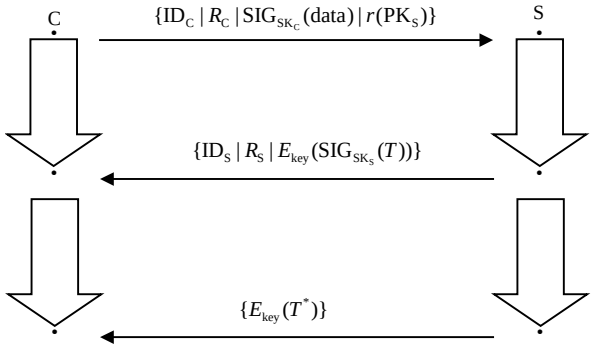

图3　协议的丛示意图

3.3.1　认证属性分析

设：1) $\mathrm{SK_C},\mathrm{SK_S}\notin \mathrm{key}_p$；2) $\mathrm{ID_C}$ 和 $\mathrm{ID_S}$ 唯一产生，二者不等；3) R_C 和 R_S 唯一产生，且二者也不等。

首先，证明响应者成功认证发起者。设 C 为丛，$S_r\in \mathrm{Re}\,sp[\mathrm{ID_C},\mathrm{ID_S},R_\mathrm{C},R_\mathrm{S},T,T^*,r]$ 且 $C-\mathrm{hight}(S_r)=3$。由于 $\mathrm{SK_C}\notin \mathrm{key}_p$，$R_\mathrm{S}$ 唯一产生在 $\langle S_r,2\rangle$，边 $\langle S_r,2\rangle\Rightarrow^+\langle S_r,3\rangle$ 是 $\{\mathrm{ID_S}\,|\,R_\mathrm{S}\,|\,E_{\mathrm{key}}(\mathrm{SIG}_{\mathrm{SK_S}}(T))\}$ 中 R_S 出测试。根据文献[9]中的测试理论，存在正常节点 $m,m'\in C$，使得 $\{\mathrm{ID_S}\,|\,R_\mathrm{S}\,|\,E_{\mathrm{key}}(\mathrm{SIG}_{\mathrm{SK_S}}(T))\}$ 是 m 的分量，且 $m\Rightarrow^+ m'$ 是 R_S 的转换边。这 m 只可能为 $\langle S_i,2\rangle$，其中 $S_i\in \mathrm{Init}[\mathrm{ID_C},\mathrm{ID_S},R_\mathrm{C},R_\mathrm{S},T,T^*,r]$。于是变换边 $m\Rightarrow^+ m'$ 必为 $\langle S_i,2\rangle\Rightarrow^+\langle S_i,3\rangle$，且 $C-\mathrm{hight}(S_i)=3$。因此证明了协议中响应者成功地认证了发起者。

其次，证明发起者成功认证响应者。设 C 为丛，且 $C-\mathrm{hight}(S_i)=3$。由于 R_C 唯一产生在 $\langle S_i,1\rangle$，边 $\langle S_i,1\rangle\Rightarrow^+\langle S_i,2\rangle$ 是 $\{\mathrm{ID_C}\,|\,R_\mathrm{C}\,|\,\mathrm{SIG}_{\mathrm{SK_C}}(\mathrm{data})\,|\,r(\mathrm{PK_S})\}$ 中 R_C 的出测试。同理，也可证明了协议中发起者成功地认证了响应者。

同时结合自发测试定理[12]，可得协议实体双方是相互认证的。

3.3.2　秘密性与新鲜性分析

命题1　C 是串空间 $\sum$ 上的一个丛，R_C、$r(\mathrm{PK_S})$ 和 T 均是唯一最初生产的，而且 $\mathrm{SK_C}\notin \mathrm{key}_p$，则 $r(\mathrm{PK_S})$ 和 T 是秘密和新鲜的。

证明：在丛 C 中，令 $S=\{R_\mathrm{C},r(\mathrm{PK_S}),T,\mathrm{SK_S}\}$，$k=K\setminus \mathrm{PK_S}$，则 $S\subseteq Y\cup K$，$k\subseteq K$，$K\subseteq S\cup k^{-1}$，满足定理1，即 $I_K[S]$ 是诚实的。则不存在正常节点 $n\in C$，n 是理想 $I_K[S]$ 的入口点。于是，对任何节点 $n\in C$，可得 $\mathrm{term}(n)\notin S$，这样就可以保证 $r(\mathrm{PK_S})$ 和 T 的秘密性。

对于节点 $-\{\mathrm{ID_C}\,|\,R_\mathrm{C}\,|\,\mathrm{SIG}_{\mathrm{SK_C}}(\mathrm{data})\,|\,r(\mathrm{PK_S})\}$，由自发测试定理可知，存在正常节点 $+\{\mathrm{ID_C}\,|\,R_\mathrm{C}\,|\,\mathrm{SIG}_{\mathrm{SK_C}}(\mathrm{data})\,|\,r(\mathrm{PK_S})\}\in C$，又 R_C 唯一最初生成于正常节点，易知存在正常节点满足串空间模型新鲜性的定义，所以 $r(\mathrm{PK_S})$ 和 T 是新鲜的。

综上论述，协议的安全性得到证明。

4　基于CPK的TLS握手协议性能分析

4.1　定性分析

1) 计算开销上：在整个通信过程中，终端用户只需2次对称密钥加解密和1次非对称加解密，由此可知终端计算开销很小。

2) 通信开销上：协议传输的认证消息中仅包含加密的随机数、会话密钥和标识，而且握手交互次数大为减少，因此其通信开销很小。

3) 存储开销上：在CPK体制中，终端只需存储自己的私钥和公钥矩阵，而公钥矩阵很小，$m\times h$ 矩阵可以组合出 m^h 对公钥，而其存储空间仅需 $(m\times h)\times 24$ Byte。

4.2　实验分析

在局域网由配置Inter Pentium 2.80 GHz处理器和2.0 GB内存，并安装了内核版本为2.6.33的Fedora13 OS的PC机搭建的C/S仿真实验环境中，对两种握手方案进行性能比较。两种握手协议选择相同的密钥算法，且均实现双向认证的实验环境中对两种协议握手成功所消耗时间进行多次统计，其平均处理时间如图4所示。

在相同安全条件下，利用ssldump协议分析工具对该两种握手协议方案抓包分析，可知其握手次数

分别为13次和6次，同时分析其各自握手过程，得出二者在证书数量、签名/验证签名和公钥加解密次数等方面对比，如表1所示。

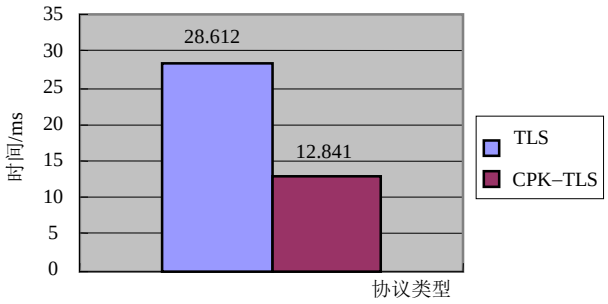

图4 两种协议握手成功所消耗平均时间对比

表1 TLS与CPK-TLS的握手协议对比

	握手次数	证书数	签名/验证签名	公钥加/解密
TLS	13	2	4	3
CPK-TLS	6	0	2	1

从图4和表1中，可知CPK-TLS协议利用CPK体制明显减少了通信连接的握手次数，节省了传递证书和验证证书的过程，在签名、验证签名、加密和解密的计算量上都有明显减少，显著减小了握手延迟，因此该方案具有鉴别简捷、资源开销小、建立可信连接过程简单、快捷和高效等优点。

5 结 束 语

基于身份的组合公钥算法能够很好地解决密钥管理的两个关键问题，与数字签名协议共同组成规模化认证算法。基于CPK的TLS握手协议方案从密钥算法、密钥管理机制等方面对现有协议进行了改进，通过串空间模型理论安全性证明和仿真实验分析证明了其能够克服原方案存在的安全缺陷和证书管理带来的存储、计算和通信开销等弊端，在保证安全性的同时降低了握手延迟，减少了通信开销，提高了协议性能，为网络世界的安全提供了一种更安全、高效的解决方案。

参 考 文 献

[1] PETER B. SSL man-in-the-middle attacks[R]. [S.l.]: SANS Institue InfoSec Reading, 2003.

[2] CHENG Ke-fei, JIA Ting-qiang, GAO Meng. Research and implementation of three HTTPS attacks[J]. Journal of Networks, 2011, 6(5): 757-764.

[3] RAY M, DISPENSA S. Renegotiating TLS[EB/OL]. [2011-06-29]. http://wenku.baidu.com/view/51ac6529647d27284b735123.html.

[4] 孙林红, 叶顶锋, 吕述望, 等. 传输层安全协议的安全性分析及改进[J]. 软件学报, 2003, 14(3): 518-523.
SUN Lin-hong, YE Ding-feng, LÜ Shu-wang, et al. Security analysis and improvement of TLS[J]. Journal of Software, 2003, 14(3): 518-523.

[5] PENG Chang-yan, ZHANG Quan, TANG Chao-jing. Improved TLS handshake protocols using identity-based cryptography[C]//International Symposium on Information Engineering and Electronic Commerce. Changsha: IEEE Press, 2009:135-139.

[6] DIERKS T, RESCORLA E. The transport layer security (TLS) protocol version 1.2[EB/OL]. [2011-06-29]. http://tools.ietf. org/html/rfc5246# section-7.4.1, 2008.

[7] 南湘浩. CPK密码体制与网际安全[M]. 北京: 国防工业出版社, 2008.
NAN Xiang-hao. CPK-cryptosystem and cyber security[M]. Beijing: National Defense Industry Press, 2008.

[8] 南湘浩, 陈中. 网络安全技术概论[M]. 北京: 国防工业出版社, 2003.
NAN Xiang-hao, CHEN Zhong. Profile to network security techniques[M]. Beijing: National Defense Industry Press, 2003.

[9] THAYER F J, HERZOG J C, GUTTMAN J D. Strand space: why is a security protocol correct?[C]//Proceeding of the 1998 IEEE Symposium on Security and Privacy. Oakland: IEEE Society Press, 1998: 160-171.

[10] CARLSEN I. Cryptographic protocol flaws[C]// Proceeding of the 7th IEEE Computer Security Foundations Workshop. MA: IEEE Computer Society Press, 1994: 192-200.

[11] GUTTMAN J D, THAYER F J. Authentication tests[C]//Proceedings of IEEE Symposium on Security and Privacy. Oaklaud CA: IEEE Press , 2000: 96-109.

[12] GUTTMAN J D. Security protocol design via authentication tests[C]//Proceeding of the 15th IEEE Computer Security Foundations Workshop. [S.l.]: IEEE Computer Society Press, 2002: 92-103.

编 辑 张 俊