基于PKI的通用无线认证协议研究

谌双双 陈泽茂 王 浩
(海军工程大学电子工程学院 武汉 430033)

摘 要 基于PKI的WTLS协议涉及复杂的证书操作,需耗费较大的通信和计算开销,且缺乏对服务器证书的有效性检查。引入可信证书验证代理(TCVP)和证书有效性凭据(CVT)等概念,由TCVP为无线通信节点(WN)生成短时有效的CVT,WN通过交换CVT来完成证书的有效性检查和公钥交换。基于此,提出了一种通用无线认证协议(GWAP)。在GWAP框架下,采用ECC算法设计了一种具体的无线安全认证协议,并进行了效率分析。结果表明,该协议在确保安全的前提下降低了通信开销。

关键词 无线认证协议,公钥密码,PKI,身份认证,ECC
中图法分类号 TP393 **文献标识码** A

Research on General Wireless Authentication Protocol Based on PKI

CHEN Shuang-shuang CHEN Ze-mao WANG Hao
(Department of Electronic Engineering, Naval University of Engineering, Wuhan 430033, China)

Abstract The WTLS protocol based on PKI requires complicated processing of certificate, which causes the communicating and computing overload is too much. Moreover, it doesn't verify the server certificate. In order to solve these issues, trust certificate verification proxy (TCVP) and certificate validity ticket (CVT) were introduced. CVT generated by TCVP for wireless communication nodes (WN) has a short life time and WN exchanges and uses it to verify certificate and share public keys in its life time. On this basis, a general wireless authentication protocol (GWAP) was proposed. Under the guidance of GWAP, a specific wireless security authentication protocol was designed by adopting Elliptic Curve Cryptography (ECC). Result of performance analysis shows that new protocol improves the efficiency of wireless communication without security losses.

Keywords Wireless authentication protocol, Public key cryptography, Public key infrastructure, Identity authentication, Elliptic curve cryptography

无线传输层安全(Wireless Transport Layers Security, WTLS)对维护无线通信安全起着重要作用[1]。WTLS是基于PKI构建的安全协议,其开展认证服务时涉及证书的路径构造、解析、传递、状态查询等复杂操作,且经优化的证书大小约为1k字节,因而需要耗费较大的计算和通信开销。在安全性方面,WTLS协议存在缺乏对服务器证书的有效性检查、易泄露用户身份信息等不足。

相继提出一些以提高效率和安全性为目的的改进方案。文献[2,3]分别采用ECC算法提高了协议的安全性,并降低了计算开销,但由于其需要在无线信道上传递证书,因而通信开销较大。文献[4]采用以传递用户证书URL代替传递证书实体的方法,服务器通过证书URL在线获取相应的证书,从而减少了一次证书传递,但该方案仍需传递服务器的证书,且没有检查服务器证书的有效性。文献[5]采用预存服务器证书的方法来降低通信开销,但该方法有一定的局限性。文献[6]设计了一种大小为280字节的微型证书来降低开销,但证书链路上一般不止一个证书,所以其通信开销仍然较大,且需要系统更换证书,降低了兼容性。

随着无线网络用户的增多,无线带宽将成为其效率的瓶颈。因此,在确保安全的前提下,如何降低无线认证协议的通信开销,是一个值得研究的问题。

1 通用无线认证协议

为实现证书有效性检查,引入了可信证书验证代理(Trust Certificate Verification Proxy, TCVP),它作为第三方可信服务器为无线通信节点(Wireless communication Node, WN)生成一个短时有效的证书有效性凭据(Certificate Validation Ticket, CVT)。在开展认证操作时,*WN* 通过出示CVT,即可证明其证书的有效性。

本文协议包括主协议:通用无线认证协议(General Wireless Authentication Protocol, GWAP)和附加协议,即凭据申请协议(Ticket Application Protocol, TAP)。TAP为GWAP提供服务,用户先通过TAP申请CVT,在GWAP认证过程中通过出示CVT证明自己证书的有效性,进而完成其它安全操作。

到稿日期:2011-08-18 返修日期:2011-11-05 本文受中国博士后特别基金资助项目(201003757)资助。
谌双双(1986-),男,硕士生,主要研究方向为网络安全,E-mail:doubleshuangjy@163.com;陈泽茂(1975-),男,博士,副教授,主要研究方向为信息与网络安全。

1.1 假设与约定

给出如下约定，符号表如表 1 所列。

表 1 符号表

符号	含义
CID_E	实体 E 的证书标识
ID_E	实体 E 的身份标识
SK_E	实体 E 的私钥
PK_E	实体 E 的公钥
CVT_E	实体 E 的证书有效性凭据
$Sig_E(m)$	使用实体 E 的私钥对 m 进行签名
$\{m\}_k$	使用对称密钥 k 对 m 进行加密
R_E	实体 E 生成的随机数
DH_E	实体 E 的 D-H 密钥交换参数
M_E	实体 E 选择的协议模式信息
$\|m\|$	数据 m 的长度
H()	单向哈希函数
KH()	带密钥的单向哈希函数
A? =B	判断 A 是否与 B 相等
||	级联符

本协议基于如下假设：

假设 1　TCVP 为引入的可信服务器，它可根据证书标识检索到相应证书，并能在线检查该证书的有效性，且 TCVP 的公钥及公开参数为所有无线通信节点预存。

假设 2　在 PKI 证书状态查询系统中，若在 T_1 时刻证书的状态为有效，则在一个较短时间窗 Δt 内，该证书被撤销的概率可忽略不计，即 T_1 时刻的状态可有效反映 $T_1 \sim T_1+\Delta t$ 时间内的状态。

上述假设都是合理的、可实现的。其中，假设 2 是使用证书有效性凭据的基础。

1.2 TAP

TVCP 为新引入的可信服务器，负责在线验证用户证书的有效性，并生成证书有效性凭据。假定 TCVP 的公钥为 PK_T，TAP 工作流程如下：

1)WN 选择随机数 R_{WN}，向 TVCP 发送消息 1：

$WN \rightarrow TCVP: CID_{WN}, R_{WN}, Sig_{WN}(H(m))$

此处，$m=\{CID_{WN}||R_{WN}\}$。

2)TCVP 根据 CID_{WN} 通过 PKI/CA 现有机制在线验证 WN 证书的有效性。若证书有效，则验证签名 $Sig_{WN}(H(m))$，以上检查通过则计算：

$CVT_{WN}=Sig_{TCVP}(ID_{WN}||PK_{WN}||T_{WN})$

向 WN 响应消息 2：

$TCVP \rightarrow WN: CVT_{WN}, R_{WN}$

最后，WN 用 PK_T 验证 CVT_{WN} 的正确性并保存，以备后用。在有效期 T_{WN} 内，WN 可通过出示 CVT_{WN} 来证明其证书的有效性。

1.3 GWAP

无线通信节点包括移动通信设备(无线用户)和固定通信设备(服务器)。后者一般连接于高速有线网络。在检查证书有效性时，两者都可通过证书有效性凭据来验证对方证书的有效性，而后者还可采用 PKI 现有证书验证机制。因而根据通信节点的不同，GWAP 有以下 3 种模式：

(1)GWAP-1

本模式下，通信的发起方 WN_1 和接收方 WN_2 分别为移动通信设备、固定通信设备。此时通信流程如下：

1)WN_1 选择参数 DH_1，发送消息 1：

$WN_1 \rightarrow WN_2: M_1, DH_1$

M_1 为待选的模式信息。

2) WN_2 根据 M_1 选择模式 M_2，并进行如下处理：按照 TAP 申请 CVT_{WN2}，然后选择参数 DH_2。使用 DH_1 和 DH_2 计算会话密钥 k，然后计算签名 $Sig_{WN2}(H(m_1))$，最后响应消息 2：

$WN_2 \rightarrow WN_1: M_2, \{CVT_{WN2}\}_k, DH_2, Sig_{WN2}(H(m_1))$

此处，$m_1=\{$消息 1$||M_2||\{CVT_{WN2}\}_k||DH_2\}$。

3)WN_1 根据模式 M_2 进行如下处理：计算 k，用 k 解密得到 CVT_{WN2}，并据此检查 WN_2 证书的有效性，最后提取 WN_2 的公钥 PK_{WN2}，并验证签名 $Sig_{WN2}(H(m_1))$。以上检查通过，则发送消息 3：

$WN_1 \rightarrow WN_2: \{CID_{WN1}\}_k, Sig_{WN1}(H(m_2))$

此处，$m_2=\{$消息 1$||$消息 2$||\{CID_{WN1}\}_k\}$。

最后，WN_2 进行如下处理：用 k 解密得到 WN_1 的证书标识 CID_{WN1}，根据该标识在线检索 WN_1 的证书，再按照传统方式验证 WN_1 证书的有效性，最后验证 WN_1 的签名 $Sig_{WN1}(H(m_2))$。

此时，认证协议结束，双方完成了彼此的身份认证，并通过 D-H 交换协商了密钥 k。

(2)GWAP-2

本模式下，通信的发起方 WN_1 和接收方 WN_2 分别为固定通信设备、移动通信设备。此时通信流程如下：

1) WN_1 执行 TAP 协议申请 CVT_{WN2}，然后选择参数 DH_1，发送消息 1：

$WN_1 \rightarrow WN_2: M_1, DH_1$

2) WN_2 根据 M_1 选择模式 M_2，再进行如下处理：选择参数 DH_2，根据 DH_1 和 DH_2 计算会话密钥 k，响应消息 2：

$WN_2 \rightarrow WN_1: M_2, \{CID_{WN2}\}_k, DH_2, Sig_{WN2}(H(m_1))$

此处，$m_1=\{$消息 1$||M_2||\{CID_{WN2}\}_k||DH_2\}$。

3)WN_1 根据模式 M_2 进行如下处理：计算 k，用 k 解密得到 CID_{WN2}，根据 CID_{WN2} 在线检索 WN_2 的证书，再按照传统方式检查该证书的有效性，最后使用 WN_2 的公钥验证签名 $Sig_{WN2}(H(m_1))$。以上检查通过，则发送消息 3：

$WN_1 \rightarrow WN_2: \{CVT_{WN1}\}_k, Sig_{WN1}(H(m_2))$

此处，$m_2=\{$消息 1$||$消息 2$||\{CVT_{WN1}\}_k\}$。

最后，WN_2 进行如下处理：用 k 解密得到 CVT_{WN1}，根据 CVT_{WN1} 检查 WN_1 证书的有效性，最后提取 WN_1 的公钥 PK_{WN1}，并验证签名 $Sig_{WN1}(H(m_2))$。

此时，认证协议结束，双方完成了彼此的身份认证，并通过 D-H 交换协商了密钥 k。

(3)GWAP-3

本模式下，通信的发起方 WN_1 和接收方 WN_2 可为任意通信节点。此时通信流程如下：

1) WN_1 执行 TAP 协议申请 CVT_{WN1}，然后选择参数 DH_1，发送消息 1：

$WN_1 \rightarrow WN_2: M_1, DH_1$

2)WN_2 根据 M_1 选择模式 M_2，再进行如下处理：执行 TAP 协议申请 CVT_{WN2}，然后选择参数 DH_1，用 DH_1 和 DH_2 计算会话密钥 k，响应消息 2：

$WN_2 \rightarrow WN_1: M_2, \{CVT_{WN2}\}_k, DH_2, Sig_{WN2}(H(m_1))$

此处，$m_1 = \{$消息 1$||M_2||\{CVT_{WN2}\}_k||DH_2\}$。

3)WN_1 根据模式 M_2 进行如下处理：计算 k，用 k 解密得到 CVT_{WN2}，并据此验证 WN_2 证书的有效性，最后提取 WN_2 的公钥 PK_{WN2} 并验证签名 $Sig_{WN2}(H(m_1))$。以上检查通过，则发送消息 3：

$WN_1 \rightarrow WN_2: \{CVT_{WN1}\}_k, Sig_{WN1}(H(m_2))$

此处，$m_2 = \{$消息 1$||$消息 2$||\{CVT_{WN1}\}_k\}$。

最后，WN_2 进行如下处理：用 k 解密得到 CVT_{WN1}，并据此检查 WN_1 证书的有效性，最后提取 WN_1 的公钥 PK_{WN1} 并验证签名 $Sig_{WN1}(H(m_2))$。

此时，认证协议结束，双方完成了彼此的身份认证，并通过 D-H 交换协商了密钥 k。

在 GWAP 的 3 种模式中，协议的第一条消息格式相同并包含待选择的模式信息 M_1，因此接收方可根据需要进行协议模式选择。上述协议提供了一种适用于无线通信的公钥密码通用认证协议框架，因而不局限于具体的密码算法。在该框架下，可根据需要使用 RSA、ECC 等公钥密码算法来设计具体的安全协议。

2 基于 ECC 的无线认证协议

根据上述通用认证协议框架，下面使用 ECC 算法设计具体的无线认证协议。

2.1 TAP-ECC

假定 TCVP 的 ECC 公私钥对为 (P_T, x_T)，WN 的公私钥对为 (P_{WN}, x_{WN})。系统初始化：TCVP 随机生成 R_T，计算 $k_T = R_T P$，秘密保存 R_T，公开 (P_T, k_T)。协议流程如下：

1)WN 选择随机数 R_{WN}，向 TVCP 发送消息 1：

$WN \rightarrow TCVP: CID_{WN}, R_{WN}, s_1$

此处，$k_P = R_{WN} P$，$r_1 = KH_{kP}(H(m_1))$，$m_1 = CID_{WN}||R_{WN}$，$s_1 = R_{WN}/(r_1 + x_{WN}) \bmod q$。

2)TCVP 根据 CID_{WN} 在线检索 WN 的证书并验证其有效性。若证书有效，则验证签名 s_1：计算 $k_P = R_{WN} P$ 和 $r_1 = KH_{kP}(H(m_1))$，并判断 $k_P ? = (P_{WN} + r_1 P) \cdot s_1$。若以上成立，则计算 $r_2 = KH_{kT}(H(m_2))$，$m_2 = ID_{WN}||P_{WN}||T_{WN}$，$s_2 = R_T/(r_2 + x_T) \bmod q$，最后为 WN 生成证书有效性凭据：$CVT_{WN} = m_2||s_2$，向 WN 响应消息 2：

$TCVP \rightarrow WN: CVT_{WN}, R_{WN}$

最后，WN 验证 CVT_{WN} 的正确性：提取 m_2 并核实信息，计算 $r_2 = KH_{kT}(H(m_2))$，判断 $k_T ? = (P_T + r_2 P) \cdot s_2$。若 CVT_{WN} 正确，则保存，以备后用。其他用户可采用相同的方法验证 CVT_{WN}。因此在有效期 T_{WN} 内，WN 可通过出示 CVT_{WN} 来证明其证书的有效性。

2.2 GWAP-1-ECC

假定 WN_1 和 WN_2 的公私钥对分别为 (P_{WN1}, x_{WN1})，(P_{WN2}, x_{WN2})。协议流程如下：

1)WN_1 生成随机数 R_{WN1}，计算 $R_{WN1} P$，并秘密保存 R_{WN1}，发送消息 1：

$WN_1 \rightarrow WN_2: M_1, R_{WN1} P$

2)WN_2 根据 M_1 选择模式 M_2，并进行如下处理：执行 TAP-ECC 向 TCVP 申请 CVT_{WN2}，再生成随机数 R_{WN2}，计算 $R_{WN2} P$、$k_P = R_{WN1} R_{WN2} P$ 和 $k = H(R_{WN1} R_{WN2} P)$，并秘密保存 R_{WN2}，响应消息 2：

$WN_2 \rightarrow WN_1: M_2, \{CVT_{WN2}\}_k, R_{WN2} P, s_1$

此处，$r_1 = KH_{kp}(H(m_1))$，$s_1 = R_{WN2}/(r_1 + x_{WN2}) \bmod q$，$m_1 = \{$消息 1$||M_2||\{CVT_{WN2}\}_k||R_{WN2} P\}$。

3)WN_1 根据模式 M_2 进行如下处理：计算 $k_P = R_{WN1} R_{WN2} P$ 和 $k = H(R_{WN1} R_{WN2} P)$，用 k 解密得到 CVT_{WN2}，并据此验证 WN_2 证书的有效性，最后提取 WN_2 的公钥 P_{WN2} 验证签名 s_1：计算 $r_1 = KH_{kp}(H(m_1))$，判断 $k_P ? = (P_{WN2} + rP) \cdot s_1 R_{WN1}$。以上检查通过，则发送如下消息：

$WN_1 \rightarrow WN_2: \{CID_{WN1}\}_k, s_2$

此处，$r_2 = KH_{kp}(H(m_2))$，$s_2 = R_1/(r_2 + x_1) \bmod q$，$m_2 = \{$消息 1$||$消息 2$||\{CID_{WN1}\}_k\}$。

最后，WN_2 进行如下处理：用 k 解密得到 CID_{WN1}，根据 CID_{WN1} 在线检索 WN_1 的证书，再按照传统方式验证 WN_1 证书的有效性，最后验证 WN_1 的签名 s_2：计算 $r_2 = KH_{kp}(H(m_2))$，判断 $k_P ? = (P_{WN1} + r_2 P) \cdot s_2 R_{WN2}$。此时，认证协议结束，双方完成了彼此的身份认证，并协商了安全的会话密钥 k。

在 GWAP 框架下，也可对 GWAP-2-ECC 和 GWAP-3-ECC 进行具体设计，这里不再赘述。

3 协议安全性分析

TAP 和 GWAP 组成了一个通用认证协议框架，规定了各个阶段的安全操作。下面分析其安全性。

3.1 TAP

消息 1 中包含 $Sig_{WN}(H(m))$ 和随机值 R_{WN}。$Sig_{WN}(H(m))$ 用于验证申请者的身份，R_{WN} 用来抵抗重放攻击。证书有效性凭据 CVT_{WN} 中包含 TCVP 的签名，任何第三方可验证该签名，以防止攻击者伪造。由于 TAP-ECC 是在 TAP 框架下设计的，其安全操作步骤与 TAP 相同，因此满足与 TAP 相同的安全性。

3.2 GWAP

GWAP-1 中，WN_1 和 WN_2 分别使用 CVT_{WN2} 和在线方式检查对方证书的有效性并对消息计算了签名 $Sig_{WN1}(H(m_2))$ 和 $Sig_{WN2}(H(m_1))$。根据假设 2，在 T_{WN} 内 CVT_{WN2} 可有效地反映证书的当前状态，并且 WN_1 信任由 CVT_{WN2} 得到的证书状态。$Sig_{WN1}(H(m_2))$ 和 $Sig_{WN2}(H(m_1))$ 可用来认证双方身份，同时确保非否认性和消息完整性。通信双方通过交换 DH 参数协商了密钥，该密钥具有前向安全性，且 DH 参数为随机选择的，可抵抗重放攻击。协议中，可能泄露双方身份信息的数据 CVT_{WN2} 和 CID_{WN1} 经加密保护，可确保身份的机密性。在 GWAP-1 框架下，严格按照安全操作步骤设计的协议满足与其相同的安全性，即 GWAP-1-ECC 与 GWAP 的安全性相同。

可以得出，GWAP-2 和 GWAP-3 满足与 GWAP-1 相同的安全性。

4 协议效率分析

基于不同的公钥密码算法，TAP 和 GWAP 的计算开销和通信开销会有所不同。下面对使用 ECC 算法设计的认证协议的效率进行定量分析。由于证书有效性凭据在有效期内可重复使用，因而凭据申请协议不是每次开展认证操作时都需执行，根据是否需要执行 TAP 等不同情况，计算新协议的开销时有多种结果。

4.1 计算开销

由于哈希运算、加法运算、模分运算和对称加解密运算等与点积运算和非对称加解密运算相比，其计算量很小，在此不予考虑。为定量分析协议的计算量而引入单位 MMs，并用 CP 表示一次证书解析、验证等操作的计算量。其中，1MMs 相当于 1024 位模乘运 abModn 的计算量，也即点积运算的计算量约为 29MMs[7]。

(1)TAP-ECC

1)WN_1 计算 $R_{WN}P$ 需 1 次点积运算。

2)TCVP 计算 $R_{WN}P$ 和验证签名 s 共需 3 次点积运算。

3)WN_1 验证 CVT_{WN} 需两次点积运算。

因此，TAP-ECC 需要 6 次点积运算，共耗费 174MMs。

(2)GWAP-1-ECC

1)WN_1 计算 $R_{WN1}P$ 需 1 次点积运算。

2)WN_2 计算 $R_{WN2}P$ 和 $R_{WN1}P_{WN2}P$ 需 2 次点积运算及执行 1 次 TAP-ECC 的计算量。

3)WN_1 计算 $R_{WN1}R_{WN2}P$、验证 CVT_{WN2} 和验证签名 s_1 共需 5 次点积运算。

4)WN_2 需要 1 次证书操作，验证签名时需 2 次点积运算。

因此，GWAP-1-ECC 需要 10 次点积运算、1 次证书操作和执行 1 次 TAP-ECC，总计算量为 464 MMs +CP。若在认证过程中，WN_2 已有一个有效的证书有效性凭据，则不需要进行临时申请操作，此时计算量可降为 290MMs+CP。按此方法计算，各协议的计算开销如表 2 所列。

表 2 协议性能分析

协议	计算量(MMs)	通信量(字节)	消息数
文献[2]	232+2*CP	2213	10
文献[3]	290+2*CP	2244	10
文献[5]	261+CP	1168	10
GWAP-1-ECC	290/464+CP	134/246	3/5
GWAP-2-ECC	290/464+CP	134/246	3/5
GWAP-3-ECC	348/522/696	162/274/386	3/5/7

在实际应用中，证书的解析、验证等操作比较复杂，因此避免对证书的操作可减少协议的计算量。在 GWAP-1-ECC 和 GWAP-2-ECC 中，固定通信设备一般通过高速网络连接于 TCVP，因而可采用按期申请 CVT 的策略，使固定通信设备始终保有一个有效的 CVT，在此情况下，两个协议的计算量都为 290MMs+CP。GWAP-3-ECC 无需证书操作，该协议可分为通信双方都需要、仅一方需要或都不需要申请证书有效性凭据等 3 种情况，此时计算量分别为 348MMs、522MMs 和 696MMs。

4.2 通信开销

针对无线信道中耗费的通信量及传递的消息条数分析协议的通信开销。在实际应用中，参数的典型长度为(字节) $|R_E|=16$，$|M_E|=1$，$|T_E|=8$，$|P_E|=|R_EP|=20$，$|CID_E|=|ID_E|=12$，$|CVT_E|=40$，$|s_E|=20$。假定证书路径上仅包含发送者的证书，且 WTLS 证书大小按 1kB 估算，与文献[2,3,5]中 WTLS 认证协议相比，其通信量和消息数如表 2 所列。在临时申请 CVT 的情况下，GWAP-1-ECC 的通信量需要加上一次执行 TAP-ECC 的通信量，共为 246 字节，消息数为 5。若 WN_2 当前拥有一个有效的 CVT，则不需要临时申请 CVT，此时通信量可降为 134 字节，消息数为 3。同理，可计算 GWAP-2-ECC 和 GWAP-3-ECC 的通信量和消息数。

由表 2 可知，新协议的通信量和消息条数都有明显减少，且表 2 中不包括文献[2,3,5]中的查询证书状态等其它通信开销。在最坏情况下，即各通信终端都没有可用的证书有效性凭据而需要临时申请时，新协议在 3 种模式下的无线通信总量分别为 246 字节、246 字节和 386 字节。

结束语 在安全协议中，通信双方传递证书的目的是交换合法的公钥。但在无线信道中，传递证书并不明智。新协议通过引入证书有效性凭据来完成证书的有效性检查及公钥的传递，在确保安全的前提下降低了通信开销，且计算开销没有增加，有效提高了协议的执行效率。

证书有效性凭据的有效期长短决定了其申请策略。若有效期较长，则不能有效反映证书的当前状态；若太短，则用户需要频繁地执行申请操作。确定合适的有效期才能进一步提高协议的执行效率。因此，如何根据需要选择合适的有效期及凭据申请策略，是下一步需解决的问题。

参 考 文 献

[1] WAP Forum. Wireless Application Protocol Wireless Transport Layer Security Specification Version 06-Apr-2001[EB/OL]. http://www.wapforum.org,2011-03

[2] Kwak D, Ha J C, Lee H. A WTLS Handshake Protocol with User Anonymity and Forward Secrecy[C]// Proceedings of Mobile Communications: the 7th CDMA International Conference. LNCS 2524. Berlin: Springer-Verlag, 2002: 219-230

[3] 邹学强，冯登国. WTLS 握手协议的安全性分析及改进[J]. 中国科学院研究生院学报，2004，21(4)：495-500

[4] Lee Y, Lee J, Song J S. Design and implementation of wireless PKI technology suitable for mobile phone in mobile-commerce [J]. ScienceDirect: Computer Communications, 2006, 30: 893-903

[5] 向文，陶良升，王同洋. 一种高效的 WTLS 握手协议 [J]. 计算机应用，2008，28(11)：2798-2800

[6] 王治国，肖德贵. 基于无线 PKI 的微型证书的分析与实现[J]. 科学技术与工程，2006，6(3)：278-282

[7] Jurisic A, Memezes A J. ECC whitepapers: Elliptic curves and cryptography[EB/OL]. http://www.Certicom.com/research/weccrypt.html, 2011-04