基于无证书标识认证的云KEY密钥分割与存储技术

Key Segmentation and Storage Technology of Cloud KEY Based on Certificateless Identity Authentication

武亮亮，王首媛，孙宁宁，陶俊明（中讯邮电咨询设计院有限公司，北京 100048）
Wu Liangliang，Wang Shouyuan，Sun Ningning，Tao Junming（China Information Technology Designing & Consulting Institute Co.，Ltd.，Beijing 100048，China）

摘　要：
针对接入设备数量繁多，传统密钥生成与存储不足的问题，以UID安全盾软件为载体，提出了一整套基于CLA无证书标识认证的创新型国密算法来进行密钥的分割与存储，为移动终端平台的用户提供高安全、高效率、高可靠性的移动办公安全体验，实现了智能移动终端身份认证和电子签名，解决了密钥托管的问题，兼顾了易用性和安全可信性，并联合网络云卡中心实现去介质的强安全密码能力。

关键词：
5G；密钥分割；国密算法；CLA
doi：10.12045/j.issn.1007-3043.2023.04.002
文章编号：1007-3043（2023）04-0005-05
中图分类号：TN915.08
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
Aiming at the problem of a large number of access devices and insufficient traditional key generation and storage，a set of innovative national secret algorithm based on CLA certificateless identification authentication is proposed using UID security shield software as the carrier to segment and store keys，which provides users of mobile terminal platform with a safe，efficient and reliable mobile office security experience，and achieves intelligent mobile terminal identity authentication and electronic signature，so the problem of KEY escrow is solved，and the ease of use and security credibility are taken into account. and the network cloud card center is combined to achieve strong security encryption capability of de-media.

Keywords：
5G；Key segmentation；National secret algorithm；CLA

引用格式：武亮亮，王首媛，孙宁宁，等. 基于无证书标识认证的云KEY密钥分割与存储技术[J]. 邮电设计技术，2023（4）：5-9.

1 概述

随着5G的发展，移动互联网中有大量的终端设备接入。信息通信渠道、数据存储与处理呈现爆炸式增长[1]。一方面，互联网的高速发展带来了巨大的经济效益，另一方面，由于数据的增长，数据存储安全以及终端身份认证的安全显得尤为重要，国家出台了多项网络安全、信息安全的法律法规。因此，基于国际密码算法的密钥生成与托管技术面临着巨大的威胁[2]。传统解决移动终端身份认证、鉴权以及数据保护的方法是采用公钥密码技术，来实现数字签名和公钥加密，而该方法的核心在于保证私钥的安全。为了保障私钥的存储和使用安全，其一般都保存在密码设备内，相应的密码运算也由专门密码设备完成。但随着移动网络的发展，私钥不得不保存在移动设备中，如手机、电脑等终端上，这就给私钥的存储、使用和运算带来了巨大的隐患[3]。

本文在CLA无证书标识认证技术的基础上[4-7]，采用国密算法提出了一种新型的云KEY密钥分割与存储技术。与传统基于CA证书分割技术相比，该技术基于密钥分割技术，占用终端硬件资源小，为终端设备的认证和接入提供了高安全解决方案，且所采用的

收稿日期：2023-02-10

算法均基于国密SM2、SM3和SM4算法，符合国家安全认证要求，可以被广泛应用在智慧工厂、车联网等物联网场景。

2 云KEY

2.1 云KEY系统简介

云KEY系统是一种基于密钥分割和联合计算的密码系统，模拟智能IC卡和USBKEY的功能。通过云KEY终端（客户端）和云KEY服务器共同组成一种个人密码设备，用于私钥的分散存储和两方联合计算。云KEY客户端SDK提供调用接口，与上层应用集成，应用系统通过对接口的调用使用云KEY完成用户密钥生成、用户密钥保存和相应的密码运算，满足身份鉴别、数字签名和数据加解密等安全应用需求。云KEY客户端与云KEY服务器之间的数据交互由SDK内部解决，对上层应用系统透明。

该系统是一种新型密钥存储和密码运算的虚拟密码设备。综合采用了国产密码算法、强制访问控制和安全隔离等系列新技术，配合密钥分割存储与两方联合计算技术，实现对用户密钥的管理和使用。

2.2 云KEY系统结构

云KEY系统由云KEY客户端和云KEY中心组成（见图1）。云KEY客户端为智能手机、移动终端或者PC机，用于保存用户密钥分量。云KEY中心由云KEY服务器为用户提供密钥分量托管，由密码设备提供用户密钥分量的保存并执行密码运算。使用时，由云KEY客户端和云KEY中心联合完成数字签名、私钥解密等运算。云KEY中心服务器对应用系统是透明的，云KEY客户端完成与应用系统的交互。

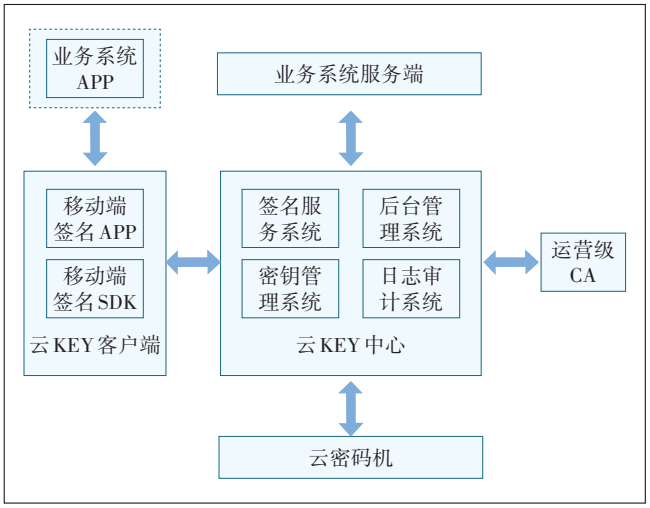

图1 云KEY系统架构图

云KEY系统架构包括两大部分，分别是终端侧的云KEY客户端以及服务端的云KEY中心，终端以嵌入式SDK和独立APP 2种形态实现签名加密安全功能；服务端与业务系统集成，提供密钥管理、签名服务等能力。其中，用户的私钥被分割为2个分量，一个私钥分量由云KEY中心使用，另一个私钥分量由用户端使用。用户使用私钥时，由云KEY服务器和云KEY用户端联合计算产生签名或对数据进行私钥解密。

云KEY中心将密码机部署在网上，通过用户PIN码（认证口令）、用户硬件特征码（DID）和云KEY中心密码设备主密钥对用户的私钥分量加密后保存，签名和加解密运算在密码设备中完成。用户只有使用PIN码和DID对密钥解密后，才能使用自己的密钥。多种技术的综合使用，实现了云KEY密钥的安全隔离和强制访问控制，可充分保证用户私钥分量的安全存储和使用。

2.3 云KEY与CLA密钥管理系统及应用系统关系

云KEY与CLA密钥管理系统以及云KEY与应用系统之间的关系如图2所示。

a）用户私钥存储以及与私钥有关的运算由云KEY客户端和云KEY服务器联合完成。云KEY服务器对上层应用APP是透明的，与云KEY服务器的交互由SDK内部完成。应用APP对云KEY的调用由客户端接口完成。

b）用户管理系统是由建设单位建立的应用系统，用于管理本单位所有的用户，包括用户的注册、用户密钥的申请、用户密钥的挂失和注销以及用户信息的更新等。在用户管理系统上要配置签名认证服务器，在用户通过用户管理系统申请密钥时，需要对用户相关信息进行数字签名。应用对签名认证服务器的调用通过“签名认证服务器接口完成。用户终端在用户管理系统上注册时，用户管理系统需要对用户提交的资料进行合法性和有效性审查。用户管理系统与客户端的通信由开发单位定义。

c）CLA密钥管理系统，用于为用户生成密钥和颁发公钥标识，发布用户的密钥状态。用户管理系统与CLA密钥管理系统之间的通信采用Http协议。

d）应用系统是指建设单位建立的应用服务系统，应用系统配备签名认证服务器，用于认证客户身份和签名验签。应用系统与云KEY客户端之间的通信协议和过程由开发单位定义。应用系统对签名认证服

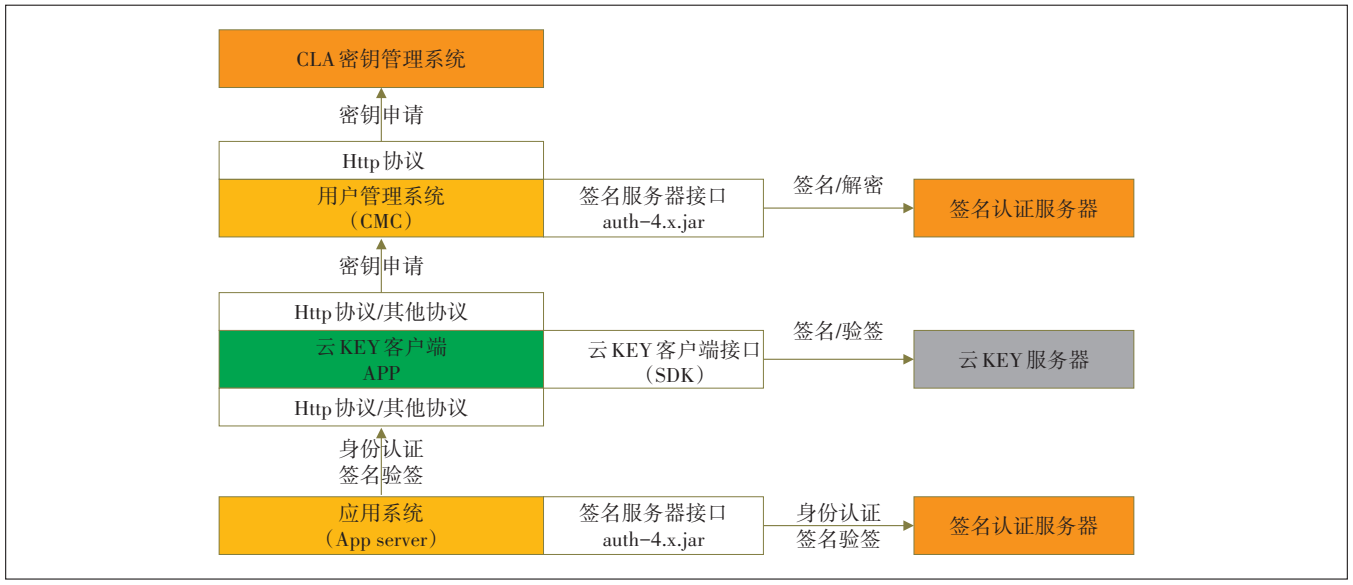

图2　云KEY、CLA与密钥管理系统逻辑关系图

务器的调用通过签名认证服务器接口完成。

3 云KEY密钥保护及存储机制

用户密钥对生成时，由云KEY中心密码设备、用户端安全组件或APP与CLA密钥管理系统联合完成用户2个私钥分量的生成。在云KEY中心，为保证用户私钥分量的安全，利用用户端设备硬件特征码（DID）、用户口令（PIN）、密码机设备主密钥（MK）对用户私钥分量进行多重加密后保存。在用户端，私钥分量生成后使用设备硬件特征码（DID）、用户口令（PIN）等信息加密保存。

用户端设备硬件特征码可用于绑定用户密钥和手机设备，如果有条件，可使用TEE可信计算或指纹等生物特征进行保护。

用户私钥的分割存储与保护方式如图3所示。

4 基于CLA的云KEY密钥分割与协同计算

4.1 用户签名密钥生成算法

a）用户端随机生成$k_1 \in [1, n-1]$，计算$P_1=k_1G$，将P_1发送到云KEY中心。

b）云KEY中心随机生成$k_2, k_3 \in [1, n-1]$，计算$P_2=k_2P_1+k_3G$，返回P_2到用户端。

c）用户端发送ID和P_2到CLA，请求为用户生成签名密钥。

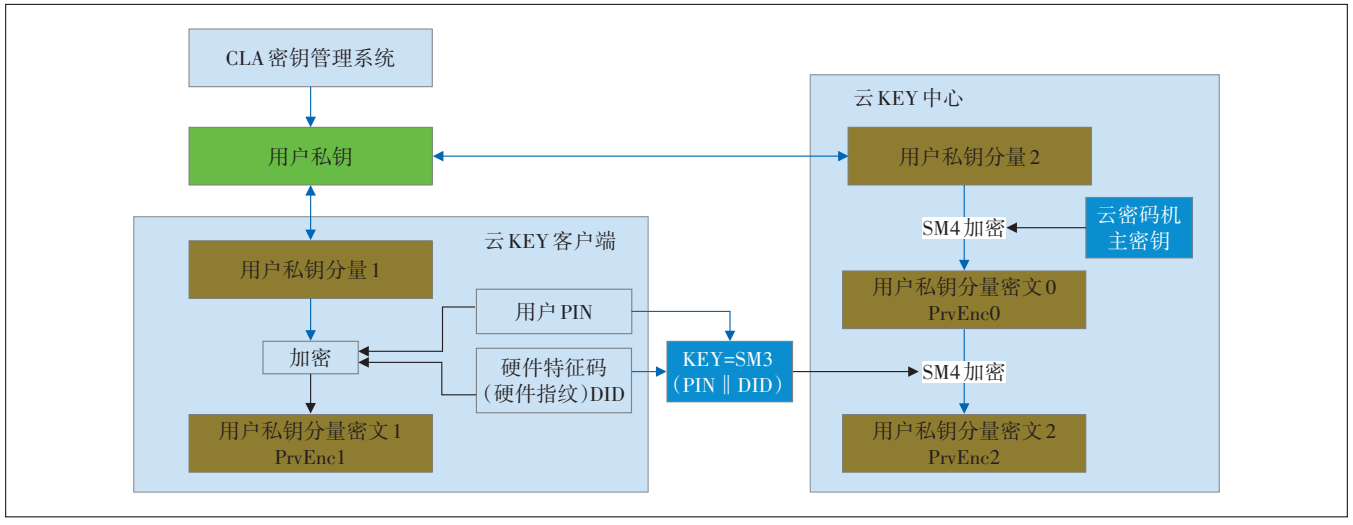

图3　用户私钥的分割存储与保护方式

d）CLA按无证书用户密钥生成算法为用户生成部分签名密钥。随机生成$k_0\in[1,n-1]$，有效期为T，计算：

$$P=P_2+k_0G$$
$$s_0=k_0+h(\mathrm{ID}\|P\|T)s_M(\mathrm{mod}\ n)$$
$$Q=P+h(\mathrm{ID}\|P\|T)P_{pub}$$
$$\mathrm{PID}=\mathrm{ID}\|P\|T\|Q[4]$$

用P_2对s_0做公钥加密生成密钥包EVK_1，EVK_1中的公钥为Q（其中s_M为KGS私钥，P_{pub}为KGS公钥，$Q[4]$为Q的前4个字节）。

e）CLA发送EVK_1、P、Q、PID和系统公钥标识SysPID到用户端，并将PID作为用户的公钥标识（签名公钥标识可以不发布）。

f）用户端从EVK_1中取出随机值(x,y)构成椭圆曲线点R，计算$R_1=k_1R$。发送EVK_1、R_1、P、Q到云KEY中心。

g）云KEY中心从EVK_1中取出随机值(x,y)构成椭圆曲线点R，计算$R_0=k_2R_1+k_3R$，用R_0对EVK_1解密获取s_0。再验证$Q=P+h(\mathrm{ID}\|P\|T)P_{pub}$和$s_0G+P_2=Q$是否成立。若成立，随机生成一个$d_2\in[1,n-1]$，计算：

$$s_2=d_2k_2(\mathrm{mod}\ n)$$
$$s_3=d_2(k_3+s_0+1)(\mathrm{mod}\ n)$$
$$Q_2=(d_2)^{-1}G$$

返回s_2、s_3、Q_2到用户端。云KEY中心将d_2作为用户的私钥分量2加密保存。

h）用户端计算：

$$d_1=(k_1s_2+s_3)^{-1}$$
$$Q_1=(d_1)^{-1}Q_2=(d_1d_2)^{-1}\mathrm{G}$$

检验$Q=P+h(\mathrm{ID}\|P\|T)P_{pub}$和$Q_1=Q+G$是否成立，若成立，则将$d_1$作为用户的私钥分量1加密保存，$Q$作为用户的实际签名公钥，并保存$Q$、PID和SysPID。

生成的用户签名密钥信息为：

部分公钥为$P=kG$，其中$k=k_1k_2+k_3+k_0(\mathrm{mod}\ n)$

私钥为$d=k+h(\mathrm{ID}\|P\|T)s_M(\mathrm{mod}\ n)$

公钥为$Q=dG=P+h(\mathrm{ID}\|P\|T)P_{pub}$

私钥分量1为d_1

私钥分量2为d_2

满足$(d_1d_2)^{-1}=d+1(\mathrm{mod}\ n)$

$Q_1=(d_1d_2)^{-1}G=Q+G=(d+1)G$

用户端和云KEY中心互相不知道对方的私钥分量，也不知道完整的私钥d。私钥分量d_1、d_2和完整私钥d对CLA也是未知的。

4.2 两方协同数字签名算法

用户端和云KEY中心的共同私钥为d，公钥为$Q=dG$，$Q_1=(d_1d_2)^{-1}G=Q+G$，由两方协同完成对消息M的SM2签名。记摘要值$e=h(Z\|M)$。

a）用户端随机选取$k_1\in[1,n-1]$，计算$s_1=d_1k_1$，$P_1=s_1Q_1$（或$P_1=d_1Q_1$）发送P_1到云KEY中心。

b）云KEY中心随机选取$k_2\in[1,n-1]$，计算：

$$P_2=P_1+k_2G=(x_1,y_1)$$
$$r=(e+x_1)(\mathrm{mod}\ n)$$
$$s_2=d_2(k_2+r)(\mathrm{mod}\ n)$$

发送(r,s_2)到用户端。

c）用户端验证云KEY中心的部分签名(r,s_2)：

$$P_1+s_2Q_2-rG=(x_1,y_1)$$

其中，$Q_2=d_1$，$Q_1=(d_2)^{-1}G$，验证$r=(e+x_1)(\mathrm{mod}\ n)$是否成立。若成立，计算：

$s=d_1(k_1+s_2)-r(\mathrm{mod}\ n)$，当$P_1=s_1Q_1$时，或$s=k_1+d_1s_2-r(\mathrm{mod}\ n)$，当$P_1=k_1Q_1$时输出签名$(r,s)$。

4.3 两方协同私钥解密算法

设$C=C_1\|C_2\|C_3$是使用用户公钥Q对消息M做SM2公钥加密后的密文。对C的解密过程如下。

a）客户端从C中取椭圆曲线上的点C_1，发送C_1到云KEY中心。

b）云KEY中心计算：$R_2=d_2C_1$，发送R_2到客户端。

c）客户端计算：$d_1R_2=(x_2,y_2)$。

d）以下步骤同SM2解密算法B4—B7。

对签名的验证和用公钥对数据加密同SM2算法。

4.4 用户加密密钥生成算法

步骤a）~c）与用户签名密钥生成步骤相同，并借用在那里生成的所有参数。

d）CLA按无证书用户密钥生成算法为用户生成加密密钥。随机生成$k'\in[1,n-1]$，有效期为T，计算：

$$P'=k'G$$
$$d'=k'+h(\mathrm{ID}\|P'\|T)s_M(\mathrm{mod}\ n)$$
$$Q'=P'+h(\mathrm{ID}\|P'\|T)P_{pub}$$
$$\mathrm{PID}'=\mathrm{ID}\|P'\|T\|Q[4]$$

再将d'随机分拆成2个分量的积：$d'=b_1b_2(\mathrm{mod}\ n)$，用$P_2$分别对$b_1$和$b_2$做公钥加密生成2个密钥包$EVK_2$和$EVK_3$，$EVK_2$和$EVK_3$中的公钥为$Q$。

e）CLA发送EVK_2、EVK_3、P'、Q'、PID′和系统公钥标识SysPID到用户端，并将d'加密保存到数据库，发布用户的加密公钥标识PID。

f）用户端从EVK_3中取出随机值(x,y)构成椭圆曲

线点R，计算$R_1=k_1R$。发送R_1、EVK_2、EVK_3到云KEY中心。

g）云KEY中心从EVK_3中取出随机值(x,y)构成椭圆曲线点R，计算$R_0=k_2R_1+k_3R$，用R_0对EVK_3解密恢复b_2。云KEY中心随机生成$d'_2\in[1,n-1]$，计算：

$$s'_2=(d'_2)^{-1}b_2(\mathrm{mod}\ n)$$

$$Q'_2=d'_2G$$

云KEY中心将d'_2作为用户的加密私钥分量2加密保存。再从EVK_2中取出随机值(x,y)构成椭圆曲线点R'，计算$R'_2=k_2R'$，$R'_3=k_3R'$，发送s'_2、Q'_2、R'_2、R'_3到用户端。

h）用户端用计算$R'_0=k_1R'_2+R'_3$，用R'_0对EVK_2作完全解密获取b_1，再计算：

$$d'_1=s'_2b_1(\mathrm{mod}\ n)$$

检验$Q'=P'+h(ID\|P'\|T)P_{pub}$和$d'_1Q'_2=Q'$是否成立，若成立，则将$d'_1$作为用户的加密私钥分量1，$Q'$作为用户的实际加密公钥，并保存$Q'$、PID′和SysPID。

4.5 应用使用流程

UID安全盾提供接口和应用系统对接，其整体应用框架和流程如图4所示。

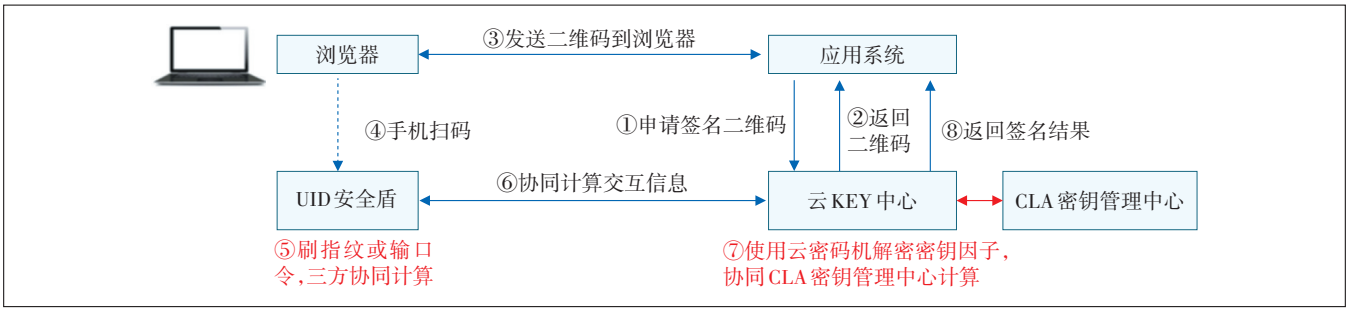

图4 UID安全盾整体应用框架和流程

UID安全盾中心使用Http restful接口与应用系统对接，主要传送申请签名二维码、推送签名结果等信息。调用流程如下。

a）应用系统调用“申请签名二维码”。

b）UID安全盾中心返回二维码URL。

c）应用系统发送二维码URL到浏览器。

d）用户使用手机UID安全盾APP扫描二维码。

e）用户在手机上输入口令或指纹，启动三方协同计算。

f）手机端和安全盾中心交互进行协同计算。

g）安全盾中心配合云密码机和CLA密钥管理中心以及手机端完成协同计算。

h）推送签名结果到应用系统。

5 结束语

本文基于CLA无证书标识认证技术，采用国密算法提出了一种新型的云KEY密钥分割与存储技术。在此技术上，通过密钥分割和联合计算设计出了一套云KEY系统。该系统通过接口的调用使用云KEY完成用户密钥生成、用户密钥保存和相应的密码运算，满足身份鉴别、数字签名和数据加解密等安全应用需求。同时，将用户私钥分割为2个部分，且分别保存在不通的密钥托管系统中，在需要使用私钥进行签名和解密时，由云KEY中心和云KEY客户端联合完成签名计算。

参考文献：

[1] 杨婷，张光华，刘玲，等．物联网认证协议综述[J]．密码学报，2020,7(1):87-101.

[2] 杨明，樊海剑，杨晓珍．5G移动通信发展趋势与若干关键技术研究[J]．中国新通信，2021,23(7):1-2.

[3] 武传坤，王九如，崔沂峰．物联网的OT安全技术探讨[J]．密码学报，2020,7(1):134-144.

[4] 张玉明．5G无线通信关键技术及其发展现状思路构建[J]．中国新通信，2021,23(6):34-35.

[5] 毕兴，唐朝京．基于模型检测的TLS协议实现库安全性分析[J]．系统工程与电子技术，2021,43(3):8

[6] 熊荣华．一种无双线性对运算的无证书公钥密码体制的实现方法:CN104539423.3[P]．2015-04-22.

[7] 张晓辉，王首媛，慕江林．基于CLA和TLS结合实现的物联网通信安全研究[J]．邮电设计技术，2021,545(7):24-26.

作者简介：

武亮亮，工程师，硕士，主要从事5G网络安全、密码算法以及移动增值业务相关咨询设计工作；王首媛，工程师，硕士，主要从事物联网云密码产品软硬研发、网络安全等业务相关咨询设计工作；孙宁宁，高级工程师，硕士，主要从事物联网标识认证算法、车联网以及蜂窝定位等垂直行业解决方案工作；陶俊明，助理工程师，硕士，主要从事5G终端安全、组网以及移动增值业务相关咨询设计工作。