doi:10.11959/j.issn.1000-436x.2016267

# 基于标识密钥技术的证书集成管理平台

刘牧洲，仇剑书，张云勇，严斌峰，张思遥，汤雅妃
（中国联合网络通信有限公司研究院，北京 100032）

**摘 要**：非对称密钥密码体制（公钥密码体制）在当今信息安全领域中扮演着重要的角色。与传统的公钥密码体制相比，基于标识的公钥密码体制简化了证书的管理，减少系统通信量和存储开销。在分析了已有加密安全方案以及对比不同安全方案的优点及缺点后，介绍一种使用国密算法、基于标识密钥技术的证书集成管理平台及其所独具的优势。通过对此平台技术原理和功能作用的剖析，揭示其作为高效信息安全产品具有很好的应用前景。

**关键词**：标识密钥；国密算法；信息安全
**中图分类号**：TN918.4 **文献标识码**：A

# Certificate integration management platform based on identity key

LIU Mu-zhou, QIU Jian-shu, ZHANG Yun-yong, YAN Bin-feng, ZHANG Si-yao, TANG Ya-fei
(China Unicom Research Institute , Beijing 100032, China)

**Abstract:** Asymmetric key cryptosystem plays an significant role in the field of information security. Compared with traditional public key cryptosystem, the public key crypto system based on identity simplifies certificate management and reduces system communication and storage cost. A management platform and its unique merits were introduced after analyzing the current security schemes and comparing their various advantages and defects. According to the analysis of technical principles and functions, this product has a promising future.

**Key words:** identity key, national secret algorithm, information security

## 1 引言

进入 21 世纪以来，网络信息安全问题已成为各国安全领域聚焦的重点[1]。保密性、完整性与可用性并称为信息安全的三大要素[2]。公钥密码体制是现在信息安全领域中的重要代表。但在传统的公钥密码体制当中，标识和公钥需由证书权威 CA 颁发的公钥证书来承载。为简化证书管理，基于标识的公钥密码体制这一概念随之被提出。在基于标识的公钥密码体系中，公钥从用户的唯一可标识信息中获取，无需证书就可进行公钥的认证[3]。本文所提到的便是一种基于标识公钥密码技术的新产品——标识密钥集成平台(IKI)。此平台借助 SM2 数字证书体系(国密规范)来实现其安全性，其算法包括 SM2 椭圆曲线公钥密码算法、SM3 杂凑算法以及 SM4 对称算法。在对国密算法和安全方案进行描述分析的同时，本文着重对 IKI 标识密钥平台做详细介绍。

## 2 国密算法简述

1) SM2 椭圆曲线公钥密码算法。此算法属于 ECC 椭圆曲线密码机制，而椭圆曲线密码体制是一种基于代数曲线的公钥密码体制，可方便用于计算资源有限的应用场合[4]。SM2 算法在签名和密钥交换等方面不同于国际算法，是更安全的机制。国际算法 RSA 作为一种公钥加密算法，其安全性主要依赖大数分解的困难性[5]。

国密算法 SM2 与国际算法 RSA 对比如下。在计算复杂度上，前者是完全指数级，RSA 则是亚指数级；SM2 在相同安全性能下所需的公钥比特数要少

**收稿日期**：2016-08-28

于 RSA 所需要的（160 bit 的 SM2 对应 1 024 bit 的 RSA）；在密钥生成速度方面，SM2 也要远快于 RSA；SM2 的机密加密速度相比于 RSA 要更快速一些。

2) SM3 密码杂凑算法。杂凑算法可将任意长度的消息压缩成固定长度的摘要。它可赋予每条消息唯一的“数字指纹”，稍微修改信息内容便会引起“数字指纹”的变化[6]。因此，杂凑算法适用于商用密码应用中的数字签名和验证，消息认证码的生成、验证以及随机数的生成，从而满足多重密码应用的安全需求。杂凑算法 SM3 的安全性能较高。

3) SM4 对称算法。该算法为分组算法，适用于无线局域网产品。算法的分组长度与密钥长度皆为 128 bit，加密与解密密钥相同[7]。加、解密算法结构相似，只在轮密钥的使用顺序上相反，解密轮密钥为加密轮密钥的逆序。国际算法 DES 作为迭代型对称密钥算法，安全性依赖于其密钥的安全与否，算法本身则是公开的[8]。

国密算法 SM4 与国际算法 DES 对比如下。前者在计算轮数、分组长度、密钥长度和有效密钥长度上的比特数皆多于 DES；在实现性能的比对上，SM4 在软、硬件的实现上都很快速，而 DES 则在软件上实现较慢；SM4 在安全性方面也要优于 DES，后者安全性较低。

## 3 安全方案分析

### 3.1 对称密钥密码体制

对称密钥密码体制是一种传统的密码体制，也可称为单密钥密码体制或秘密密钥密码体制[9]。在对称加密系统中，采用的是相同的密钥来进行加密和解密[10]。虽然加密与解密的密钥及流程是完全相同的，但是在加密与解密时密钥序列的施加顺序刚好相反[11]。唯一密钥被通信双方共同使用，需双方相互信任，才可实现数据的机密性与完整性。对称加密系统只适用于网络用户量较小的情况，针对网络用户量较大的情况，密钥的分配和保存将成为不可忽视的问题。

优点：加密的算法比较简单，计算开销较小；加密与解密的速度快。

缺点：仅可用于对数据进行加密与解密处理，提供数据机密性，不可进行数字签名；密钥安全交换方法复杂。

### 3.2 非对称密钥密码体制

非对称密钥密码体制也称公钥加密技术，采用完全不同却又相互匹配的一对密钥[12]。在公钥加密系统中，加密与解密过程是相对独立的，加密与解密的密钥共有 2 把，分为公钥和私钥，公钥与私钥不能通过计算得出彼此。此外，公钥密码体系中，易于建立相距遥远的终端用户间的密钥信道，从而可以克服传统对称技术的缺点[13]。密钥的管理也较为简单且安全性高，可用于开放式环境，因此，成为数字签名和验证的核心支撑技术[14]。另外，私钥是持有者秘密保存的，只有持有者才可使用此私钥对密文进行解密。

优点：不存在密钥分配和交换问题；可用于数据加密，亦可用于数字签名；

缺点：算法复杂，加密数据速率较低。

### 3.3 基于身份标识的密码体制

基于身份标识的密码体制（IBC，identity-based cryptograph）是一种非对称公钥密码体制，用户拥有一对相关联的公钥与私钥。由于无需任何关于公钥的管理与认证，所以，IBC 并不是一种密钥管理技术[15]。IBC 的特点是标识密码系统中不再需要证书，使用用户自定义的标识作为公钥，通过数学方式生成与之对应的用户私钥。公钥是代表用户身份的任意字符串（如手机号码、电子邮箱地址和姓名等）[16]。在 IBC 体制当中，用户身份与公钥自然捆绑，私钥则在私钥生成中心产生[17]。

优点：标识即是公钥；密码系统管理简单。

缺点：私钥分发复杂；密钥托管，不可强签名。

### 3.4 公钥基础设施

公钥基础设施（PKI, public key infrastructure）是利用公钥密码理论和技术建立起来的，提供安全服务的普适性安全设施[18]。它是由公开密钥密码技术、数字证书、证书发放机构和关于公开密钥的安全策略等部分共同组成的。其中，安全认证系统是公钥基础设施 PKI 不可或缺的核心部分，它负责生成、分发和注销数字证书[19]。在 PKI 系统中，独立且值得信赖的认证中心 CA（通常由第三方充当）可以帮助公开密钥系统确认公钥拥有人的真实身份，从而确保用户身份以及其持有的密钥正确匹配。数字证书便是认证机构发放的身份证明，它包含了有关用户身份的部分信息和用户持有的公钥。认证中心可利用自身私钥为数字证书进行数字签名。用户可凭借到认证中心申请证书来开放自身持

有的公钥。待认证中心检核过该申请人的真实身份后，便可对其发放含有此用户公钥的数字签名。而其他用户则可通过信任认证机构以及验证证书真实性后，确认该用户的公钥。由于 PKI 可以解决网络中的访问授权与身份认证等问题，其可以广泛适用于诸如电子商务和电子政务等方面[20]。

优点：管理体制完善；强签名；提供证书撤销机制。

缺点：需要解密密钥数据库；证书规模化管理复杂。

### 3.5　标识密钥集成平台

进行全生命周期、全过程管理标识密钥的安全系统。IKI 使用数字签名验签及加密、解密双密钥机制，但也可适用于单密钥机制，并且可以建设标识管理中心和密钥生产中心。在逻辑上共有 4 个区域的划分：核心区、管理区、服务区和公共区；其中，以密钥生产中心为核心区，标识管理中心为管理区，标识注册管理中心与凭信认证中心为服务区，Web 前端服务则作为公共区。

优势：符合电子签名法的标识密码管理体系、签名私钥无托管；标识与密钥一一对应；系统运行效率高；标识证明公钥和私钥、无需第三方认证；无需解密私钥库；划域认证；标识和密钥数量庞大；去中心化、P2P 自认证模式；密钥安全分发；提供更新、撤销机制；成本低廉。

## 4　IKI 概述

IKI 作为安全系统可对标识密钥进行全生命周期和全过程的管理。IKI 采用数字签名验签和加、解密双密钥机制，同时也兼容单密钥机制，并建立标识管理中心与密钥生产中心。在部署逻辑上，IKI 可划分成 4 个部分，分别为由密钥生产中心构成的核心区、标识管理中心构成的管理区、标识注册管理中心与凭信认证中心构成的服务区以及 Web 前端服务构成的公共区。IKI 拥有四大功能模块：密钥管理中心（KGC）、标识管理中心（IMC）、注册认证（RA）中心以及凭信认证中心（TPA），其相互之间的关系如图 1 所示。此外，IKI 平台的安全是建立在国密规范上的。

## 5　IKI 技术原理

### 5.1　标识凭信生产实现原理

标识凭信生产原理如图 2 所示用户向注册认证

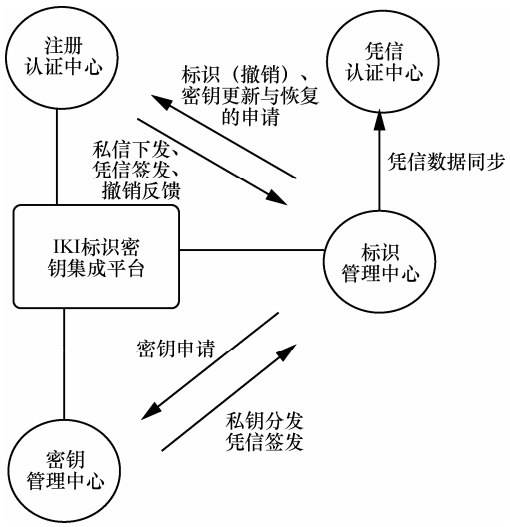


图 1　平台四区关系

中心（RA）提供身份信息、标识 ID 以及生效日期和失效日期等进行审核。同时，用户使用 UKey（智能密钥匙）来随机产生秘密值 *xID*、秘密值公钥 *PKx*，通过根公钥 *RPK* 加密 *PKx*、*ID*、生效日期和失效日期。所加密的信息则将发送至 RA 以及标识管理中心（IMC），再由 IMC 借助通用加密/加密机，以根私钥 *RSK* 解密出秘密值公钥 *PKx*，将此秘密值公钥 *PKx* 发送到密钥生产中心（KGC）来产生加密公钥 *PKE* 与验签公钥 *PKS*，从而生成标识凭信（*PKE*、*PKS*、生效日期、失效日期和签发机关）。*KGC* 将凭信发给通用加密/加密机，由标识私钥 $SK_{ID}$ 对凭信进行签名，随后下发至 KGC 处。于是，计算解密私钥 *SKE*，并使秘密值公钥 *PKx* 对私钥 *SKE* 加密以输出 *PKx*[*SKE*]（方括号中为被加密的内容，下同）。KGC 向通用加密/加密机发送根公钥和根私钥后，后者离线下发回根公钥和公钥矩阵 ***pkm***。秘密值公钥 *PKx* 对公钥矩阵 ***pkm*** 加密输出 *PKx*[***pkm***] 随后连同凭信以及 *PKx*[*SKE*]分别下发至 RA 和 IMC。IMC 再将凭信下发给 TPA，由后者来公布凭信。用户使用 UKey 来解密凭信、秘密值 *xID* 和由 *PKx* 所加密的内容（*SKE* 与公钥矩阵 ***pkm***），再通过 ID 和公钥矩阵 ***pkm*** 计算得到标识公钥 $PK_{ID}$ 来验证凭信签名。秘密值 *xID* 和部分私钥 *SKE* 组成签名私钥（*SKS*），随后删除秘密值 *xID*，并保存 *SKS*、*SKE*、公钥矩阵 ***pkm*** 与凭信。最后，删除 RA 与 IMC 的加密内容 SKE 和公钥矩阵 ***pkm***。

### 5.2　标识凭信申请流程

用户 A 提交标识申请到 RA，RA 对其签名并

发送给 IMC，IMC 将请求内容签名后发送至 KGC 进行密钥申请，KGC 验证通过 IMC 签名后，进行生产。随后，KGC 将标识凭信签发私钥下发至 IMC 处，IMC 将其发送给 RA，并同步发送标识凭信至 TPA 处。用户可从 RA 处下载标识凭信和私钥，使用用户 A 的私钥签名来生成签名私钥。用户 B 则可使用 A 的标识验证凭信分别获取 A 的凭信以及自 TPA 处下载 A 的凭信。最后，用户 B 可使用 A 的公钥验签。

### 5.3　标识验证凭信流程

用户 A 将 *ID* 提交到 KGC 用于计算标识私钥 $SK_{ID}$，再以 $SK_{ID}$ 签名来制作凭信。用户 B 则使用用户 A 的标识验证凭信来获取用户 A 的凭信和 *ID*，来用于计算标识公钥 $PK_{ID}$，用此 $PK_{ID}$ 验证标识凭信。

## 6　IKI 系统组成

IKI 标识密钥集成平台由四大子系统共同构成，它们分别是 KGC 密钥生产子系统、IMC 标识管理子系统、RA 注册认证子系统以及 TPA 凭信认证子系统。

### 6.1　KGC 密钥生产子系统

KGC 密钥生产子系统用于密钥的生产、凭信的签发、司法恢复（解密私钥）和操作员权限的分配管理。KGC 密钥生产子系统主要的三大模块包括权限控制管理模块、密钥生产模块和司法恢复模块。此子系统与 IMC 标识管理子系统之间完成密钥申请、私钥分发和凭信签发。由 IMC 标识管理子系统完成申请的提交。然后，KGC 密钥生产子系统进行分发和签发。

### 6.2　IMC 标识管理子系统

IMC 标识管理子系统包含权限控制管理模块、标识管理模块、凭信管理模块、司法恢复申请模块和 IMC 数据库。此子系统与 RA 注册认证子系统共同完成标识（撤销）申请、密钥更新申请、密钥恢

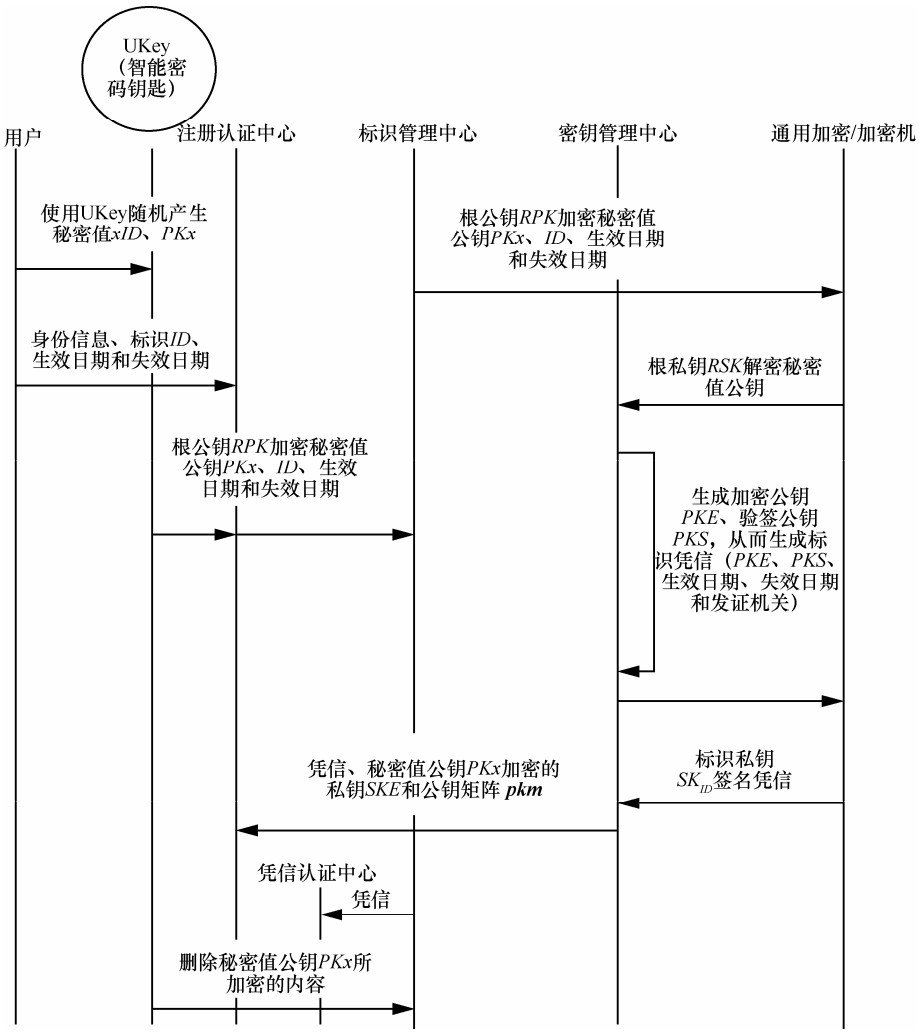


图 2　标识凭信生产原理流程

复申请、私信下发、凭信签发和撤销反馈。3 个申请项由 RA 注册认证子系统提交到 IMC 标识管理子系统，其余下发、签发和反馈则由 IMC 标识管理子系统下发至 RA 处。IMC 标识管理子系统可以将凭信数据同步到 TPA 凭信认证子系统。此外，此子系统可向 KGC 密钥生产子系统处提交密钥申请，后者下发回私钥分发和凭信签发结果。通过使用 IMC 标识管理子系统可以进行标识申请的审核、标识的撤销操作、密钥更新/恢复申请审核、凭信数据同步、凭信归档以及操作员权限分配管理。

### 6.3　RA 注册认证子系统

RA 注册认证子系统包含了供用户使用的 RA 用户服务模块、RA 管理员使用的权限控制管理模块和 RA 的数据库。使用 RA 注册认证子系统可以提交标识（撤销）申请和密钥更新、恢复申请到 IMC 标识管理子系统，再由后者反馈回私钥下发、凭信签发和撤销反馈结果。RA 注册认证子系统包括的功能有账号注册管理、身份认证审核、标识（撤销）申请、密钥更新/恢复申请和操作员权限分配管理。

### 6.4　TPA 凭信认证子系统

TPA 凭信认证子系统则是完全供用户使用的子系统，其系统包括 IRL 服务模块、OISP 服务模块和 TPA 内存数据库。用户可使用 TPA 凭信认证子系统进行 IRL 的存储、更新以及标识状态查询。此外，该子系统亦可同 IMC 标识管理子系统进行凭信数据同步。

## 7　IKI 平台核心功能

1) 密钥申请。插入新的空白 UKey，提交申请给 RA 标识服务模块，由 RA 签名所请求的内容，发送给 IMC。经过 IMC 验证 RA 的签名。在 IMC 签名后，申请被 IMC 发送至 KGC 处。此时，KGC 将会进行 2 步操作：① 验证通过 IMC 签名，进行密钥生产；② 将密钥和凭信签名下发回 IMC 处；在经过 IMC 对 KGC 签名的验证后，凭信由 IMC 下发给 TPA，显示凭信为有效状态。

2) 密钥撤销。撤销申请通过使用待撤销的 UKey 进行授权撤销操作，签名发送请求给 RA 撤销服务模块，RA 签名撤销内容后，传送至 IMC 处，由 IMC 执行撤销操作，且下发给 TPA，显示凭信为无效状态。

3) 密钥更新。使用原 UKey 授权更新操作，原 UKey 对本次操作内容进行签名，插入新的 UKey 进行密钥申请操作。

4) 密钥下载。申请标识时所对应的 UKey 将标识下载请求发送到 RA 服务中心，签名后将下载请求提交到 IMC 处，由后者验证 RA 的请求并对标识的凭信和密钥签名。随后，下发签名内容回 RA 处，RA 验证 IMC 签名，下发凭信与密钥到 UKey。

5) 密钥恢复。在 UKey 损坏或丢失的情况下，用户凭有效证件前往 RA 服务中心，由 RA 操作员授权后代理执行密钥恢复申请操作，并对操作内容签名，插入新的 UKey 执行恢复操作，过程同密钥申请。

6) 密钥挂起。待挂起的 UKey 授权撤销操作，签名后的挂起申请发送至 RA 挂起服务模块，由后者签名后的挂起请求被提交到 IMC 处。IMC 执行挂起操作，并下发所挂起的表示信息到 TPA 处，显示凭信为无效状态。

已挂起的 UKey 授权启用操作将启用请求发送给 RA 启用服务模块，在 RA 处完成对请求内容的签名。随后，将内容提交到 IMC，由 IMC 将标识信息改为启用状态，并下发给 TPA,显示出凭信为有效状态。

7) 密钥冻结。RA 管理员使用 UKey 授权解冻操作，授权签名并把冻结申请发送给 RA 冻结服务模块。RA 对冻结请求内容签名后发送至 IMC 处，后者执行标识冻结后，下发冻结标识信息给 TPA,显示凭信为无效状态。

RA 管理员使用 UKey 授权解冻操作，签名后发送冻结申请给 RA 解冻服务模块，在将解冻请求内容签名后，提交到 IMC 处，由 IMC 执行标识解冻后，下发解冻标识信息给 TPA，显示凭信为有效状态。

8) 司法恢复。由 IMC 授权签名，并把司法恢复申请发送给 KGC， KGC 验证签名通过之后，生产出此标识的加密、解密密钥对，并于 IMC 处进行下载，以供司法取证。

## 8　应用实例

如图 3 所示，IKI 标识密钥基础设施可以作用于物联网中，为物联网中的应用层（如智能家居、智能医疗和环境监测）解决权限访问控制与数据存储安全等问题，为网络层（有线网络与无线网络）的可靠安全通信增加保障，并给感知层（如传感器、智能摄像头和可穿戴设备等）提供海量标识编码的同时，进行设备接入的认证。

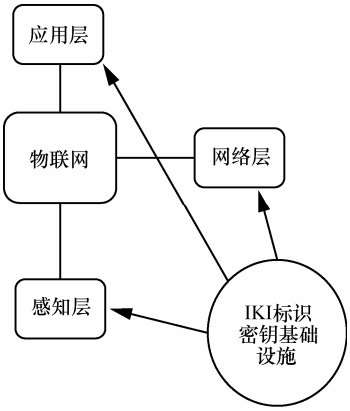


图 3　IKI 标识密钥基础设施应用于物联网

## 9　结束语

IKI 作为使用基于标识的公钥密码体制、采用国密算法的安全产品。它可以被应用在众多的场景中：移动互联网、物联网、云安全、Web 安全、金融证券、电力传输和军工安全。鉴于 IKI 平台可以满足对信息安全的完整性、可用性、真实性、可控性和保密性等需求，其未来在具体应用中的表现将值得期待。

## 参考文献：

[1] 王世伟.论信息安全、网络安全、网络空间安全[J].中国图书馆学报，2015.
WANG S W. On information security, network security and cyberspace security[J]. Journal of Library Science in China, 2015.

[2] 曾凡平.网络信息安全[M]. 北京: 机械工业出版社, 2015.
ZENG F P. Network information security[M]. Beijing:China Machine Press,2015.

[3] 张志.基于标识的密码体制研究[D]. 华中科技大学, 2009.
ZHANG Z. Research on identity-based cryptography[D]. Huazhong University of Science and Technology,2009.

[4] 许德武, 陈伟.基于椭圆曲线的数字签名和加密算法[J].计算机工程, 2011, 37(4): 168.
XU W D,CHEN W. Digital signature and encrypt algorithm based on elliptic curve[J]. Computer Engineering, 2011, 37(4): 168.

[5] 王茜, 倪建伟.一种基于 RSA 的加密算法[J].重庆大学学报（自然科学版), 2005(1): 68-72.
WANG Q, NI J W. Encryption algorithm based on RSA[J]. Journal of Chongqing University(Natural Science Edition),2005(1): 68-72.

[6] 王小云, 于洪波.密码杂凑算法综述[J]. 信息安全研究, 2015,1(1): 19-30.
WANG X Y, YU H B. Survey of hash functions[J]. Journal of Information Security Research, 2015,1(1): 19-30.

[7] 伍娟. 基于国密 SM4 和 SM2 的混合密码算法研究与实现[J]. 软件导刊, 2013(8):127-130.
WU J. Research and implementation of hybrid cipher algorithm based on SM4 and SM2[J]. Software Guide, 2013(8): 127-130.

[8] 解双建, 原亮, 谢方方. DES 算法原理及其 EPGA 实现[J].计算机技术与发展, 2011(7): 158-160.
XIE S J, YUAN L, XIE F F. The principle of DES algorithm and realization on EPGA[J]. Computer Technology and Development, 2011(7): 158-160.

[9] 包伟. 对称密码体制与非对称密码体制比较与分析[J]. 硅谷, 2014(10): 138-139.
BAO W. Comparison and analysis of symmetric and asymmetric cryptosystem[J]. Silicon Valley, 2014(10): 138-139.

[10] 毕方明, 苏成, 张虹.网络通讯中基于对称密码体制的密钥管理[J]. 计算机工程与设计, 2006, 27(10): 1479-1751.
BI F M, SU C, ZHANG H. Key management of symmetrical cipher system on network communication[J]. Computer Engineering and Design, 2006, 27(10): 1479-1751.

[11] 曾宪文, 高桂革. 对称密码加密系统与公钥密码加密系统[J]. 上海电机学院学报, 2005, 8(2): 49-52.
ZENG X W, GAO G G. Analysis of the differentials between private and public key cryptography[J].Shanghai College of Electricity & Machinery Technology, 2005, 8(2): 49-52.

[12] 任华新. 数据加密算法的综述[J]. 电子世界, 2016(18):95.
REN H X. Survey of data encryption algorithms[J]. Electronics World, 2016(18):95.

[13] 卓先德, 赵菲, 曾德明. 非对称加密技术研究[J]. 四川理工学院学报(自然科学版), 2010,23(5):562-564.
ZHUO X D, ZHAO F, ZENG D M. Research or asymmetric encryption technology[J]. Journal of Sichuan University of Science & Engineering(Natural Science Edition), 2010,23(5):562-564.

[14] 李霞, 王建民, 李善治.密码体制及其应用研究[J].网络安全技术与应用, 2008(8):47, 91-92.
LI X, WANG J M, LI S Z. Research on cryptography and application[J]. Network Security Technology & Application, 2008(8): 47, 91-92.

[15] 周加法, 马涛, 李益发. PKI、CPK、IBC 性能浅析[J]. 信息工程大学学报, 2005, 6(3):26-31.
ZHOU J F, MA T, LI Y F. Comparison and analysis of PKI, CPK and IBC[J]. Journal of Information Engineering University, 2005, 6(3): 26-31.

[16] 黄仁季, 吴晓平, 李洪成.基于身份标识加密的身份认证方案[J].网络与信息安全学报, 2016,2(6): 32-37.
HUANG R J, WU X P, LI H C. Identity authentication scheme based on identity-based encryption[J]. Chinese Journal of Network and Information Security, 2016, 2(6): 32-37.

[17] 陈华. 基于身份的公钥密码系统的研究[D]. 武汉大学, 2012.
CHEN H. Research on public key cryptography based on identity[D]. Wuhan University, 2012.

[18] 张仕斌, 何大可, 代群. PKI 安全认证体系的研究[J]. 计算机应用研究, 2005,22(7): 127-130.
ZHANG S B, HE D K, DAI Q. Research of PKI secure certification architecture[J]. Application Research of Computers, 2005,22(7): 127-130.

[19] 刘小勇, 李卫平. 公钥基础设施（PKI）技术及应用研究[J].中国西部科技, 2009, 8(16): 12-14.
LIU X Y, LI W P. Research on public key infrastructure (PKI) technology and its application[J]. Science and Technology of West China, 2009, 8(16): 12-14.

[20] 孙美青, 王如龙. PKI 技术及其在企业中的应用[J].计算机系统应用, 2009, 18(7): 141-145.
SUN M Q, WANG R L. PKI Technology and its application in enterprises[J]. Computer Systems & Applications, 2009, 18(7): 141-145.