ICS 35.040
L80
备案号：

中华人民共和国密码行业标准化指导性技术文件

GM/Z 0001—2013

密码术语

Cryptology Terminology

2013-××-××发布

国家密码管理局 发布

目　次

前言

本指导性技术文件依据 GB/T 1.1-2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本指导性技术文件仅供参考。有关对本指导性技术文件的建议和意见，向国家密码行政主管部门反映。

本指导性技术文件由国家密码管理局提出并归口。

本指导性技术文件起草单位：北京海泰方圆科技有限公司、上海格尔软件股份有限公司、北京数字认证股份有限公司、北京握奇智能科技有限公司、山东得安信息技术有限公司、成都卫士通信息产业股份有限公司、无锡江南信息安全工程技术中心、。

本指导性技术文件起草人：刘平、柳增寿、谭武征、李述胜、胡俊义、孔凡玉、李元正、徐强。

密码术语

1 范围

本指导性技术文件给出了商用密码工程领域的基础术语及其定义。

本指导性技术文件适用于为密码有关标准、指导性技术文件的编制提供指导，也可用于指导密码技术和产品的论证、设计、生产、使用、检测和评估等。

2 术语

2.1

安全模块 security module

含有密码算法、安全功能，可实现密钥管理机制的相对独立的软件、硬件、固件或其组合。

2.2

安全凭证 security credential

用户通过身份鉴别后，由鉴别者为用户出具的一种可信任的电子凭据。

2.3

安全芯片 security chip

含有密码算法、安全功能，可实现密钥管理机制的集成电路芯片。

2.4

差分密码分析 differential cryptanalysis

一种选择明文攻击，通过分析特定明文差分对相应的密文差分的影响，以获得可能性最大的密钥。

2.5

差分能量分析 differential power analysis（DPA）

一种密码分析方法，使用统计方法和纠错技术等对密码设备功耗的变化进行分析，以提取密钥的有关信息。

2.6

重放攻击 replay attack

一种主动攻击方法，攻击者通过记录通信会话，并在以后某个时刻重放整个会话或者会话的一部分。

2.7

初始化向量/值 initialization vector/initialization value（IV）

在密码变换中，为增加安全性或使密码设备同步而引入的用于数据变换的起始数据。

2.8

带密钥的杂凑算法 keyed-hash message authentication code（HMAC）

一种密码杂凑算法，密钥作为其输入参数参与运算。

2.9

单点登录 single sign on (SSO)

用户一次性进行身份鉴别之后就能够访问多个授权应用的登录机制。

2.10

电码本工作模式 electronic codebook operation mode (ECB)

分组密码算法的一种工作模式，其特征是将明文分组直接作为算法的输入，对应的输出作为密文分组。

2.11

电子签章 digitally seal

使用电子印章签署电子文件的过程。

2.12

电子印章 digital stamp

一种由制作者签名的包括持有者信息和图形化内容的数据，可用于签署电子文件。

2.13

电子证据 electronic evidence

电子证据是被存储在电子设备上或被电子设备所传送的可作为证据的信息和数据。

2.14

Diffie-Hellman 协议 Diffie-Hellman protocol

又称 DH 算法，一种基于离散对数问题的、用于密钥协商的密码协议。

2.15

动态口令 one-time-password (OTP), dynamic password

基于时间、事件等方式动态生成的一次性口令。

2.16

动态口令令牌 one-time-password token

生成并显示动态口令的载体。

2.17

动态认证系统 one-time-password system

对动态口令进行认证，对动态口令令牌进行管理的系统。

2.18

端到端加密 end-to-end encipherment/encryption

数据在源端进行加密，在目的端解密。

2.19

对称密码算法 symmetric cryptographic algorithm

加密和解密使用相同密钥的密码算法。

2.20

对称密钥 secret key

用于对称密码算法的密钥。

2.21

对称密钥管理系统 symmetric key management system

以对称密钥为管理对象的密钥管理系统。

2.22

访问控制 access control

按照特定策略，允许或拒绝用户对资源访问的一种机制。

2.23

非对称密码算法/公钥密码算法 asymmetric cryptographic algorithm/public key cryptographic algorithm

加密和解密使用不同密钥的密码算法。其中一个密钥（公钥）可以公开，另一个密钥（私钥）必须保密，且由公钥求解私钥是计算不可行的。

2.24

非对称密钥对 asymmetric key pair

非对称密码算法中相关联的公钥和私钥。

2.25

分组密码算法 block cipher algorithm

将输入数据划分成固定长度的分组进行加解密的一类对称密码算法。

2.26

分组密码算法工作模式 block cipher operation mode

分组密码算法的使用方式，主要包括电码本工作模式（ECB）、密码分组链接工作模式（CBC）、密码反馈工作模式（CFB）、输出反馈工作模式（OFB）、计数器工作模式（CTR）等。

2.27

服务器密码机 cryptographic server

又称主机加密服务器，能独立或并行为多个应用实体提供密码服务和密钥管理的设备。

2.28

公钥 public key

非对称密码算法中可以公开的密钥。

2.29

公钥基础设施 public key infrastructure（PKI）

基于公钥密码技术实施的具有普适性的基础设施，可用于提供机密性、完整性、真实性及抗抵赖性等安全服务。

2.30

后向保密性 backward secrecy

保证通过当前或者后续数据不能推算出以前的数据值。

2.31

数据加密密钥 data encipherment/encryption key

用于数据加解密的密钥。

2.32

会话密钥 session key

在一次会话中使用的数据加密密钥。

2.33

IKE 协议 Internet key exchange protocol

由 IETF 制定的密钥协商协议，定义了通信双方进行身份鉴别、协商加密算法以及生成共享会话密钥的一种方法。

2.34

IPSec 协议 Internet Protocol Security

由 IETF 制定的端到端的确保基于 IP 通信数据安全性的一种网络层协议，可以提供数据完整性保护、数据源鉴别、载荷机密性和抗重放攻击等安全服务。

2.35

ISAKMP 协议 Internet Security Association and Key Management Protocol

IPsec 协议中使用的一种安全关联和密钥管理协议，用于在两个主机间通信时鉴别通信身份和协商安全参数。

2.36

机密性 confidentiality

保证信息不被泄露给非授权的个人、进程等实体的性质。

2.37

计数器工作模式 counter operation mode(CTR)

用分组密码算法构造序列密码的一种工作模式。其特征是，使用计数器的值作为算法的输入序列进行分组运算，将运算输出的若干比特与明文逐比特异或得到密文，然后对计数器作增量或者减量运算作为算法下一时刻的输入序列。

2.38

假冒攻击 masquerade attack

攻击者假冒用户，欺骗验证者的攻击方法。

2.39

假冒验证者攻击 verifier impersonation attack

攻击者假冒验证者，欺骗被验证者的攻击方法。

2.40

加密 encipherment/encryption

对数据进行密码变换以产生密文的过程。

2.41

加密公钥 public key for encryption

非对称密码算法中用于实现数据机密性的公钥。

2.42

加密私钥 private key for decryption

非对称密码算法中用于实现数据机密性的私钥。

2.43

加密证书 encipherment certificate/exchange certificate

用于证明加密公钥的数字证书。

2.44

解密 decipherment/decryption

加密过程对应的逆过程。

2.45

近代密码学 current cryptology

特指 20 世纪 40 年代末，在香农保密系统的通信理论影响下，以电子密码理论和技术为标志的密码学。

2.46

抗抵赖性 non-repudiation

也称不可否认性，证明一个已经发生的操作行为无法否认的性质。

2.47

离线攻击 off-line attack

一种利用已经获取的数据进行分析的密码攻击方法。

2.48

链路逐段加密 link-by-link encipherment/encryption

数据在节点之间链路层加密传输，从一个节点发出的加密数据，在下一个节点解密。

2.49

密码 cipher

按约定规则，为隐藏消息原形而生成的一组具有随机特性的特定符号。

2.50

密码学 cryptology

研究密码与密码活动本质和规律，指导密码实践科学，主要探索密码编制、密码破译以及密码管理的一般规律。

2.51

密码机 cryptographic machine

能够独立运行的，实现密码运算、密钥管理等功能，提供密码服务的设备。

2.52

密码理论 cryptographic theory

研究密码编制、密码破译、密码管理和密码应用的理论。

2.53

密码模块 cryptographic module

实现密码运算功能的、相对独立的软件、硬件、固件或其组合。

2.54

密码算法 cryptographic algorithm

描述密码处理过程的运算规则。

2.55

密码算法芯片 cryptographic algorithm chip

实现密码运算功能的集成电路芯片。

2.56

密码系统 cryptosystem

采用密码算法、密码协议、密码设备及相关技术，实现密码功能（如：加密传输、加密存储、鉴别认证、密钥管理等）的系统。

2.57

密码协议 cryptographic protocol

两个或两个以上参与者使用密码算法，按照约定的规则，为达到某种特定目的而采取的一系列步骤。

2.58

密码杂凑算法 hash algorithm

又称杂凑算法、密码散列算法或哈希算法。该算法将一个任意长的比特串映射到一个固定长的比特串，且满足下列三个特性：

（1）为一个给定的输出找出能映射到该输出的一个输入是计算上困难的；

（2）为一个给定的输入找出能映射到同一个输出的另一个输入是计算上困难的。

（3）要发现不同的输入映射到同一输出是计算上困难的。

2.59

秘密共享 secret sharing

也称秘密分享，将秘密分解成多个子秘密，使用超过阈值数目的子秘密才能恢复该秘密的机制。

2.60

密文 ciphertext

加密后的数据。

2.61

密文反馈工作模式 cipher feedback operation mode（CFB）

用分组密码算法构造序列密码的一种工作模式。其特征是，使用分组算法当前输出的若干比特，与明文逐比特异或得到密文，该密文同时更新算法下一时刻的输入序列。

2.62

密文分组链接工作模式 cipher block chaining operation mode(CBC)

分组密码算法的一种工作模式，其特征是将当前的明文分组与前一密文分组进行异或运算后再进行加密得到当前的密文分组。

2.63

密钥 key

控制密码算法运算的关键信息或参数。

2.64

密钥备份 key backup

从密码设备中将密钥安全复制到存储载体的过程，备份的密钥用于密钥恢复。

2.65

密钥编排 key schedule

分组密码算法中由工作密钥扩展生成轮密钥的实现方法。

2.66

密钥产生 key generation

按特定规则产生密钥的过程。

2.67

密钥撤销 key revocation

使密钥失效的过程。

2.68

密钥传送 key transportation

实体间传送受保护的密钥的过程。

2.69

密钥存储 key storage

将密钥保存在指定受控空间的过程。

2.70

密钥分发 key distribution

按照安全协议将密钥分配给对应实体的过程。

2.71

密钥分量 key division

使用秘密共享技术将密钥分割为多个部分，每个部分称为密钥分量。

2.72

密钥更新 key update

用一个新密钥来代替旧密钥的过程。

2.73

密钥管理 key management

根据安全策略，对密钥的产生、分发、存储、更新、归档、撤销、备份、恢复和销毁等密钥全生命周期的管理。

2.74

密钥管理系统 key management system

实现密钥管理功能的系统。

2.75

密钥管理中心 key management center（KMC）

负责密钥管理的机构。

2.76

密钥归档 key archive

将已分发且不再使用的密钥分类记录并安全保存的管理过程。

2.77

密钥恢复 key recovery

将归档或备份的密钥恢复到可用状态的过程。

2.78

密钥加密密钥 key encryption key （KEK）

用于对密钥进行加密或解密的密钥。

2.79

密钥空间 key space

所有可能的密钥组成的集合。

2.80

密钥确认 key confirmation

一个实体确信另一个已识别的实体拥有正确的密钥。

2.81

密钥生存期 key lifetime

密钥从产生开始到最终被销毁的整个生命周期。

2.82

密钥销毁 key destruction

将密钥通过物理或逻辑的方式消除，使其无法再恢复。

2.83

密钥协商/密钥交换 key agreement/key exchange

两个或多个实体通过相互传送一些消息来共同建立一个共享的秘密密钥的协议，且各个实体无法预先确定这个秘密密钥的值。

2.84

密钥周期 key cycle

同密钥生存期。

2.85

明文 plaintext

未加密的数据或解密还原后的数据。

2.86

PCI 密码卡 PCI cryptographic module

以 PCI/PCI-E 总线接口与相关设备相连接的、能够独立提供密码服务和密钥管理功能的板卡设备。

2.87

签名策略 signature policy

创建和验证数字签名的一套规则。

2.88

签名公钥 public key for signature

非对称密码算法中用于验证签名有效性的公钥。

2.89

签名私钥 private key for signature

非对称密码算法中用于计算签名的私钥。

2.90

签名证书 signature certificate

用于证明签名公钥的数字证书。

2.91

前向保密性 forward secrecy

保证通过当前或者以前的数据不能推算出后续的数据值。

2.92

穷举攻击 exhaustive attack

通过尝试口令或密钥所有的可能值以获得真实口令或密钥的攻击方法。

2.93

RSA 算法 Rivest-Shamir-Adleman algorithm（RSA）

一种基于大整数因子分解问题的公钥密码算法。

2.94

SHA-1 算法 secure hash algorithm(SHA)

一种密码杂凑算法，其输出为 160 比特。

2.95

SHA-256

一种密码杂凑算法，其输出为 256 比特。

2.96

SHA-3

一种密码杂凑算法，其输出为 160 比特。

2.97

设备密钥对 device key pair

用于表明设备身份、对设备进行管理的非对称密钥对。

2.98

身份鉴别/实体鉴别 authentication/entity authentication

确认一个实体所声称身份的过程。

2.99

生日攻击 birthday attack

一种主要针对密码杂凑算法的攻击方法，试图找出两个具有相同杂凑值的消息（即找到一个碰撞）。

2.100

时间戳 time stamp(TS)

对时间和其它待签名数据进行签名得到的数据，用于表明数据的时间属性。

2.101

时间戳机构 time stamp authority(TSA)

用来产生和管理时间戳的可信服务机构。

2.102

时间戳系统 time stamp authority system

用来产生和管理时间戳的管理系统。

2.103

时间戳协议 time stamp protocol（TSP）

描述时间戳的格式及相关消息格式的协议。

2.104

授权 privilege authorization

在属性管理系统中，将主体与角色绑定的过程。

2.105

授权管理基础设施 privilege management infrastructure (PMI)

提供属性服务，访问控制和权限管理，实现用户身份到应用授权的映射，与实际应用处理模式相对应的、与具体应用系统无关的访问控制功能。

2.106

授权信息 privilege information

在属性管理系统中，用于标识主体与角色间分配关系的信息。

2.107

授权证书 privilege certificate

在属性管理系统中，证明主体与角色关系的属性证书。

2.108

输出反馈工作模式 output feedback operation mode（OFB）

用分组密码算法构造序列密码的一种工作模式，其特征是，将算法当前时刻输出的若干比特与明文逐比特异或得到密文，同时算法当前时刻的输出作为算法下一时刻的输入。

2.109

数据完整性 data integrity

数据没有遭受以非授权方式所作的篡改或破坏的性质。

2.110

属性管理机构 attribute authority（AA）

对属性证书进行全生命周期管理的可信服务机构。

2.111

属性管理系统 attribute authority system

用来产生、签发、发布、更新和撤销属性证书的管理系统。

2.112

属性证书 attribute certificate

将用户身份与属性信息绑定，用于证明用户属性的一种数据结构，由属性管理机构签发。

2.113

数字签名 digital signature

签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

2.114

数字信封 digital envelope

一种数据结构，包含用对称密钥加密的密文和用公钥加密的该对称密钥。

2.115

数字证书 digital certificate

也称公钥证书，由证书认证机构（CA）签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。

2.116

私钥 private key

非对称密码算法中只能由拥有者使用的不公开密钥。

2.117

SM1 算法 SM1 algorithm

一种分组密码算法，分组长度为 128 比特，密钥长度为 128 比特。

2.118

SM2 算法 SM2 algorithm

一种椭圆曲线公钥密码算法，其密钥长度为 256 比特。

2.119

SM3 算法 SM3 algorithm

一种密码杂凑算法，其输出为 256 比特。

2.120

SM4 算法 SM4 algorithm

一种分组密码算法，分组长度为 128 比特，密钥长度为 128 比特。

2.121

SM7 算法 SM7 algorithm

一种分组密码算法，分组长度为 128 比特，密钥长度为 128 比特。

2.122

SM9 密码算法

一种基于身份标识的非对称密码算法。

2.123

SSL 协议 secure socket layer protocol

一种传输层安全协议，用于构建客户端和服务端之间的安全通道。

2.124

算法标识 algorithm identifier

用于对密码算法进行唯一标识的符号。

2.125

随机数 random number

一种数据序列，其产生不可预测，其序列没有周期性。

2.126

随机数发生器 random number generator

产生随机二元序列的器件或程序。

2.127

椭圆曲线 DH 密钥协商协议 elliptic curve Diffie-Hellman key agreement (ECDH)

又称椭圆曲线 DH 密钥协商算法，是一种基于椭圆曲线离散对数问题的 Diffie-Hellman 密钥协商协议。

2.128

椭圆曲线密码算法 elliptic curve cryptography algorithm（ECC）

基于有限域上椭圆曲线离散对数问题的非对称密码算法。

2.129

VPN 密码机 VPN cryptographic machine

实现 VPN 功能的专用密码设备，也称 VPN 安全网关。

2.130

唯密文攻击 ciphertext-only attack

一种密码分析者只拥有密文进行密码攻击的方法。

2.131

现代密码学 modern cryptology

特指 20 世纪 70 年代以来，伴随微电子技术、通信技术及计算机技术的发展而建立的以公钥密码为标志，以实现保密为准则、以计算复杂性理论为基础的密码学。

2.132

线性密码分析 linear cryptanalysis

一种分析明文、密文和密钥之间的若干比特的线性关系进行密码攻击的方法。

2.133

消息鉴别码 message authentication code（MAC）

又称消息认证码，是消息鉴别算法的输出。

2.134

消息鉴别算法 MAC algorithm

使用密码算法计算消息鉴别码的计算方法，可用于数据完整性的鉴别。

2.135

消息摘要 message digest

消息经过密码杂凑运算得到的结果。

2.136

序列密码算法 stream cipher algorithm

将明文逐比特/字符运算的一种对称密码算法。

2.137

虚拟专用网 virtual private network（VPN）

使用密码技术在通信网络中构建安全通道的技术。

2.138

选择密文攻击 chosen-ciphertext attack

一种选择特定密文和对应明文进行分析的密码攻击方法。

2.139

选择明文攻击 chosen-plaintext attack

一种选择特定明文和对应密文进行分析的密码攻击方法。

2.140

已知明文攻击 known-plaintext attack

一种利用大量互相对应的明文和密文进行分析的密码攻击方法。

2.141

杂凑值 hash value

密码杂凑运算的结果。

2.142

在线攻击 on-line attack

一种在协议进行过程中对交互数据进行窃听、篡改、替换、插入等的攻击方法。

2.143

证书标识符 certificate identifier

数字证书中用于标识其唯一性的一段数据。

2.144

证书撤销列表 certificate revocation list （CRL）

由证书认证机构（CA）签发并发布的被撤销证书的列表。

2.145

证书认证机构 certification authority（CA）

对数字证书进行全生命周期管理的实体。也称为电子认证服务机构。

2.146

证书认证系统 certificate authentication system

对数字证书的签发、发布、更新、撤销等数字证书全生命周期进行管理的系统。

2.147

证书验证 certificate validation

按照验证策略确认证书有效性和真实性的过程。

2.148

证书注册机构 registration authority （RA）

受理数字证书的申请、更新、恢复和注销等业务的实体。

2.149

智能 IC 卡 smart card

实现密码运算和密钥管理的含 CPU（中央处理器）的集成电路卡。

2.150

智能密码钥匙 cryptographic smart token

实现密码运算、密钥管理功能，提供密码服务的终端密码设备，一般使用 USB 接口形态。

2.151

中间人攻击 man-in-the-middle attack

一种拦截并有选择地修改通信数据以冒充通信中实体的攻击方法。

2.152

主密钥 master key

处于对称密码系统层次化密钥结构中的顶层，用于下层密钥的产生或保护。

2.153

字典攻击 dictionary attack

一种由可能的密钥或口令组成字典，遍历字典中的所有条目以猜测密钥或口令的攻击方法。

2.154

祖冲之序列密码算法 ZUC stream cipher algorithm

一种序列密码算法。

3 中文索引

假冒验证者攻击	erifier impersonation attack	2.39	4
加密	encipherment/encryption	2.40	4
加密公钥	public key for encryption	2.41	4
加密私钥	private key for decryption	2.42	4
加密证书	encipherment certificate/exchange certificate	2.43	5
解密	decipherment/decryption	2.44	5
近代密码学	current cryptology	2.45	5
抗抵赖性	non-repudiation	2.46	5
离线攻击	off-line attack	2.47	5
链路逐段加密	link-by-link encipherment/encryption	2.48	5
密码	cipher	2.49	5
密码学	cryptology	2.50	5
密码机	cryptographic machine	2.51	5
密码理论	cryptographic theory	2.52	5
密码模块	cryptographic module	2.53	5
密码算法	cryptographic algorithm	2.54	5
密码算法芯片	cryptographic algorithm chip	2.55	6
密码系统	cryptosystem	2.56	6
密码协议	cryptographic protocol	2.57	6
密码杂凑算法	hash algorithm	2.58	6
秘密共享	secret sharing	2.59	6
密文	ciphertext	2.60	6
密文反馈工作模式	cipher feedbackoperation mode（CFB）	2.61	6
密文分组链接工作模式	cipher block chaining operation mode（CBC）	2.62	6
密钥	key	2.63	6
密钥备份	key backup	2.64	6
密钥编排	key schedule	2.65	7
密钥产生	key generation	2.66	7
密钥撤销	key revocation	2.67	7
密钥传送	key transportation	2.68	7
密钥存储	key storage	2.69	7
密钥分发	key distribution	2.70	7
密钥分量	key division	2.71	7
密钥更新	key update	2.72	7
密钥管理	key management	2.73	7
密钥管理系统	key management system	2.74	7
密钥管理中心	key management center（KMC）	2.75	7
密钥归档	key archive	2.76	7
密钥恢复	key recovery	2.77	8
密钥加密密钥	key encryption key （KEK）	2.78	8
密钥空间	key space	2.79	8
密钥确认	key confirmation	2.80	8
密钥生存期	key lifetime	2.81	8

密钥销毁	key destruction	2.82	8
密钥协商/密钥交换	key agreement/key exchange	2.83	8
密钥周期	key cycle	2.84	8
明文	plaintext	2.85	8
PCI 密码卡	PCI cryptographic module	2.86	8
签名策略	signature policy	2.87	8
签名公钥	public key for signature	2.88	8
签名私钥	private key for signature	2.89	9
签名证书	signature certificate	2.90	9
前向保密性	forward secrecy	2.91	9
穷举攻击	exhaustive attack	2.92	9
RSA 算法	Rivest-Shamir-Adleman algorithm（RSA）	2.93	9
SHA-1 算法	secure hash algorithm-1(SHA-1)	2.94	9
SHA-256 算法	secure hash algorithm-256(SHA-256)	2.95	9
SHA-3 算法	secure hash algorithm-3(SHA-3)	2.96	9
设备密钥对	device key pair	2.97	9
身份鉴别/实体鉴别	authentication/entity authentication	2.98	9
生日攻击	birthday attack	2.99	9
时间戳	time stamp(TS)	2.100	9
时间戳机构	time stamp authority(TSA)	2.101	10
时间戳系统	time stamp authority system	2.102	10
时间戳协议	time stamp protocol（TSP）	2.103	10
授权	privilege authorization	2.104	10
授权管理基础设施	privilege management infrastructure (PMI)	2.105	10
授权信息	privilege information	2.106	10
授权证书	privilege certificate	2.107	10
输出反馈工作模式	output feedback operation mode（OFB）	2.108	10
数据完整性	data integrity	2.109	10
属性管理机构	attribute authority（AA）	2.110	10
属性管理系统	attribute authority system	2.111	10
属性证书	attribute certificate	2.112	10
数字签名	digital signature	2.113	11
数字信封	digital envelope	2.114	11
数字证书	digital certificate	2.115	11
私钥	private key	2.116	11
SM1 算法	SM1 algorithm	2.117	11
SM2 算法	SM2 algorithm	2.118	11
SM3 算法	SM3 algorithm	2.119	11
SM4 算法	SM4 algorithm	2.120	11
SM7 算法	SM7 algorithm	2.121	11
SM9 密码算法	SM9 algorithm	2.122	11
SSL 协议	secure socket layer protocol	2.123	11
算法标识	algorithm identifier	2.124	11

随机数	random number	2.125	12
随机数发生器	random number generator	2.126	12
椭圆曲线 DH 密钥协商协议	elliptic curve Diffie-Hellman key agreement(ECDH)	2.127	12
椭圆曲线密码算法	elliptic curve cryptographyalgorithm（ECC）	2.128	12
VPN 密码机	VPN cryptographic machine	2.129	12
唯密文攻击	ciphertext-only attack	2.130	12
现代密码学	modern cryptology	2.131	12
线性密码分析	linear cryptanalysis	2.132	12
消息鉴别码	message authentication code（MAC）	2.133	12
消息鉴别算法	MAC algorithm	2.134	12
消息摘要	message digest	2.135	12
序列密码算法	stream cipher algorithm	2.136	12
虚拟专用网	virtual private network（VPN）	2.137	13
选择密文攻击	chosen-ciphertext attack	2.138	13
选择明文攻击	chosen-plaintext attack	2.139	13
已知明文攻击	known-plaintext attack	2.140	13
杂凑值	hash value	2.141	13
在线攻击	on-line attack	2.142	13
证书标识符	certificate identifier	2.143	13
证书撤销列表	certificate revocation list （CRL）	2.144	13
证书认证机构	certification authority（CA）	2.145	13
证书认证系统	certificate authentication system	2.146	13
证书验证	certificate validation	2.147	13
证书注册机构	registration authority （RA）	2.148	13
智能 IC 卡	smart card	2.149	14
智能密码钥匙	cryptographic smart token	2.150	14
中间人攻击	man-in-the-middle attack	2.151	14
主密钥	master key	2.152	14
字典攻击	dictionary attack	2.153	14
祖冲之序列密码算法	ZUC stream cipher algorithm	2.154	14

4 英文索引

decipherment/decryption	解密	2.44	5
device key pair	设备密钥对	2.97	9
dictionary attack	字典攻击	2.153	14
differential cryptanalysis	差分密码分析	2.4	1
differential power analysis（DPA）	差分能量分析	2.5	1
Diffie-Hellman protocol	Diffie-Hellman 协议	2.14	2
digital certificate	数字证书	2.115	11
digital envelope	数字信封	2.114	11
digital signature	数字签名	2.113	11
digital stamp	电子印章	2.12	2
digitally seal	电子签章	2.11	2
electronic codebook operation mode（ECB）	电码本工作模式	2.10	2
electronic evidence	电子证据	2.13	2
elliptic curve cryptographyalgorithm（ECC）	椭圆曲线密码算法	2.128	12
elliptic curve Diffie-Hellman key agreement(ECDH)	椭圆曲线 DH 密钥协商协议	2.127	12
encipherment certificate/exchange certificate	加密证书	2.43	5
encipherment/encryption	加密	2.40	4
end-to-end encipherment/encryption	端到端加密	2.18	2
erifier impersonation attack	假冒验证者攻击	2.39	4
exhaustive attack	穷举攻击	2.92	9
forward secrecy	前向保密性	2.91	9
hash algorithm	密码杂凑算法	2.58	6
hash value	杂凑值	2.141	13
initialization vector/initialization value（IV）	初始化向量/值	2.7	1
Internet key exchange protocol	IKE 协议	2.33	4
Internet Protocol Security	IPSec 协议	2.34	4
Internet Security Association and Key Management Protocol	ISAKMP 协议	2.35	4
key	密钥	2.63	6
key agreement/key exchange	密钥协商/密钥交换	2.83	8
key archive	密钥归档	2.76	7
key backup	密钥备份	2.64	6
key confirmation	密钥确认	2.80	8
key cycle	密钥周期	2.84	8
key destruction	密钥销毁	2.82	8
key distribution	密钥分发	2.70	7
key division	密钥分量	2.71	7
key encryption key （KEK）	密钥加密密钥	2.78	8
key generation	密钥产生	2.66	7
key lifetime	密钥生存期	2.81	8
key management	密钥管理	2.73	7
key management center（KMC）	密钥管理中心	2.75	7
key management system	密钥管理系统	2.74	7

key recovery	密钥恢复	2.77	8
key revocation	密钥撤销	2.67	7
key schedule	密钥编排	2.65	7
key space	密钥空间	2.79	8
key storage	密钥存储	2.69	7
key transportation	密钥传送	2.68	7
key update	密钥更新	2.72	7
keyed-hash message authentication code（HMAC）	带密钥的杂凑算法	2.8	1
known-plaintext attack	已知明文攻击	2.140	13
linear cryptanalysis	线性密码分析	2.132	12
link-by-link encipherment/encryption	链路逐段加密	2.48	5
MAC algorithm	消息鉴别算法	2.134	12
man-in-the-middle attack	中间人攻击	2.151	14
masquerade attack	假冒攻击	2.38	4
master key	主密钥	2.152	14
message authentication code（MAC）	消息鉴别码	2.133	12
message digest	消息摘要	2.135	12
modern cryptology	现代密码学	2.131	12
non-repudiation	抗抵赖性	2.46	5
off-line attack	离线攻击	2.47	5
one-time-password	动态口令	2.15	2
one-time-password system	动态认证系统	2.17	2
one-time-password token	动态口令令牌	2.16	2
on-line attack	在线攻击	2.142	13
output feedback operation mode（OFB）	输出反馈工作模式	2.108	10
PCI cryptographic module	PCI 密码卡	2.86	8
plaintext	明文	2.85	8
private key	私钥	2.116	11
private key for decryption	加密私钥	2.42	4
private key for signature	签名私钥	2.89	9
privilege authorization	授权	2.104	10
privilege certificate	授权证书	2.107	10
privilege information	授权信息	2.106	10
privilege management infrastructure (PMI)	授权管理基础设施	2.105	10
public key	公钥	2.28	3
public key for encryption	加密公钥	2.41	4
public key for signature	签名公钥	2.88	8
public key infrastructure（PKI）	公钥基础设施	2.29	3
random number	随机数	2.125	12
random number generator	随机数发生器	2.126	12
registration authority （RA）	证书注册机构	2.148	13
replay attack	重放攻击	2.6	1
Rivest-Shamir-Adleman algorithm（RSA）	RSA 算法	2.93	9

secret sharing	秘密共享	2.59	6
secure hash algorithm-1(SHA-1)	SHA-1 算法	2.94	9
secure hash algorithm-256(SHA-256)	SHA-256 算法	2.95	9
secure hash algorithm-3(SHA-3)	SHA-3 算法	2.96	9
secure socket layer protocol	SSL 协议	2.123	11
security chip	安全芯片	2.3	1
security credential	安全凭证	2.2	1
security module	安全模块	2.1	1
session key	会话密钥	2.32	4
signature certificate	签名证书	2.90	9
signature policy	签名策略	2.87	8
single sign on（SSO）	单点登录	2.9	2
SM1 algorithm	SM1 算法	2.117	11
SM2 algorithm	SM2 算法	2.118	11
SM3 algorithm	SM3 算法	2.119	11
SM4 algorithm	SM4 算法	2.120	11
SM7 algorithm	SM7 算法	2.121	11
SM9 algorithm	SM9 密码算法	2.122	11
smart card	智能 IC 卡	2.149	14
stream cipher algorithm	序列密码算法	2.136	12
symmetric cryptographic algorithm	对称密码算法	2.19	2
symmetric key	对称密钥	2.20	2
symmetric key management system	对称密钥管理系统	2.21	3
time stamp authority system	时间戳系统	2.102	10
time stamp authority(TSA)	时间戳机构	2.101	10
time stamp protocol（TSP）	时间戳协议	2.103	10
time stamp(TS)	时间戳	2.100	9
virtual private network（VPN）	虚拟专用网	2.137	13
VPN cryptographic machine	VPN 密码机	2.129	12
ZUC stream cipher algorithm	祖冲之序列密码算法	2.154	14

参考文献

[1] 密码术语/中国密码学会组编.—北京：电子工业出版社，2009.6
[2] GB/T 5271.8-2001 信息技术 词汇 第 8 部分：安全
[3] ISO JTC 1/SC 27 Standing Document 6 (SD6): Glossary of IT Security Terminology