《商用密码应用与安全性评估》

密码基础知识

目录

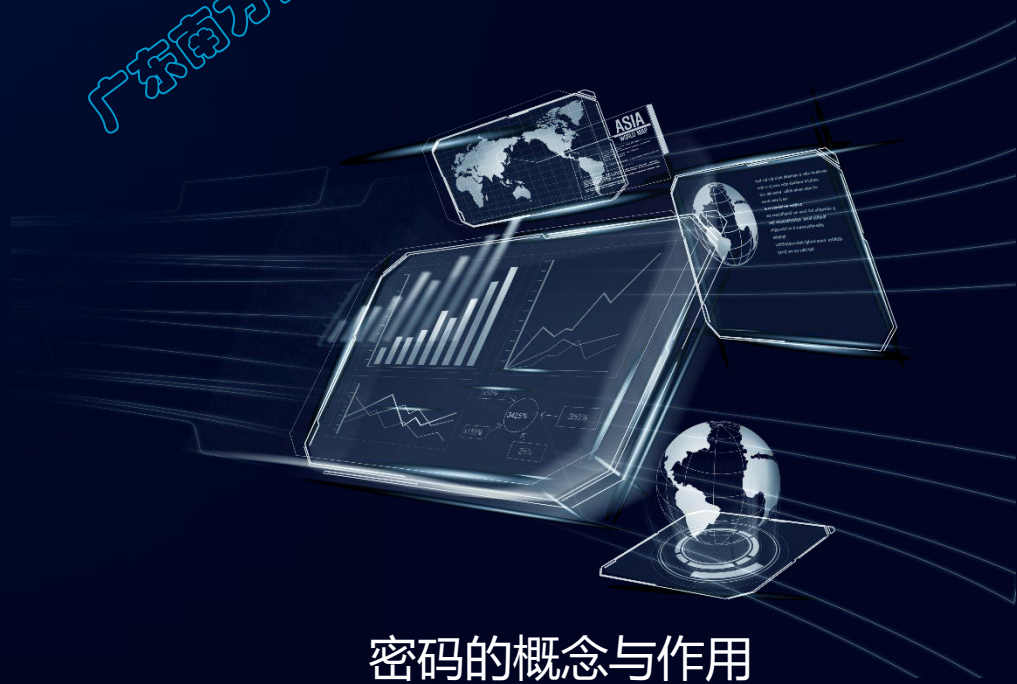
一、密码应用概述

一、密码应用概述

密码是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。

密码
Cipher

口令
Password



密码的概念与作用

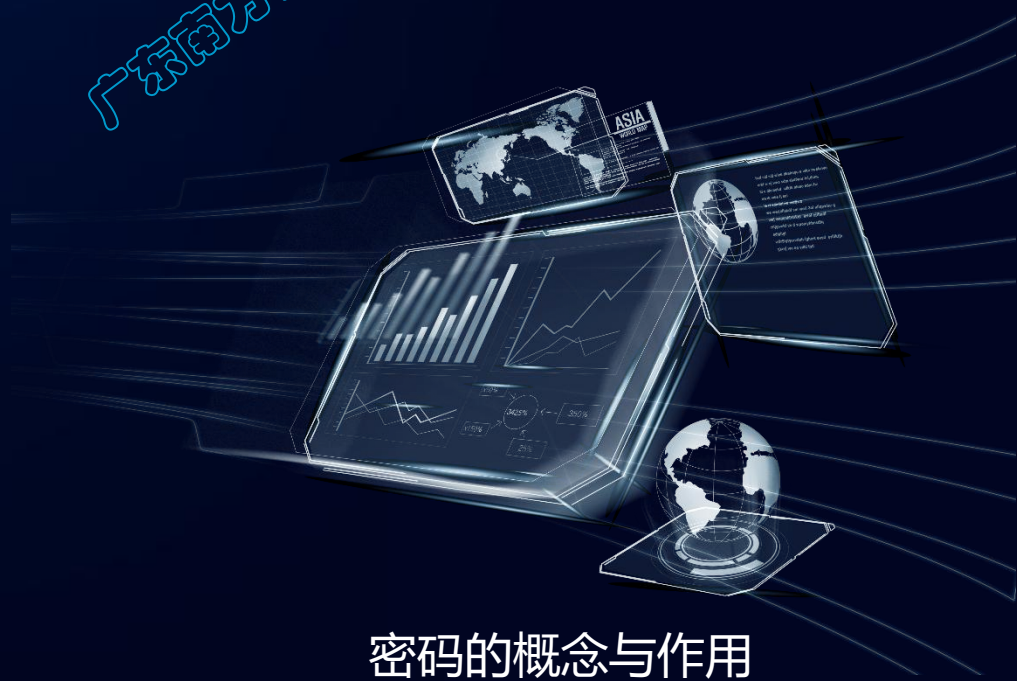
一、密码应用概述

密码是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。

特定变换：明 ⟷ 密

加密保护：你好 → @#￥T

安全认证：完整、真实、不可否认



密码的概念与作用

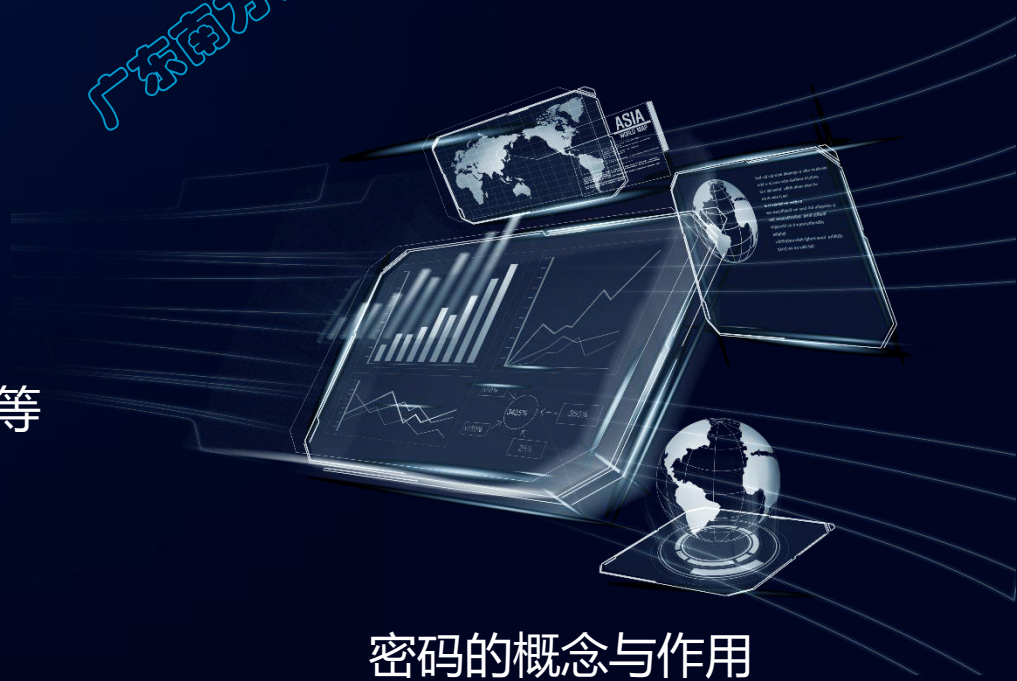
一、密码应用概述

密码是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。

技术：　典型的技术包括密码算法、密钥管理、密码协议

产品：　设备和系统

服务：　基于技术和产品，为他人提供集成、运营、监理等密码支持和保障活动



密码的概念与作用

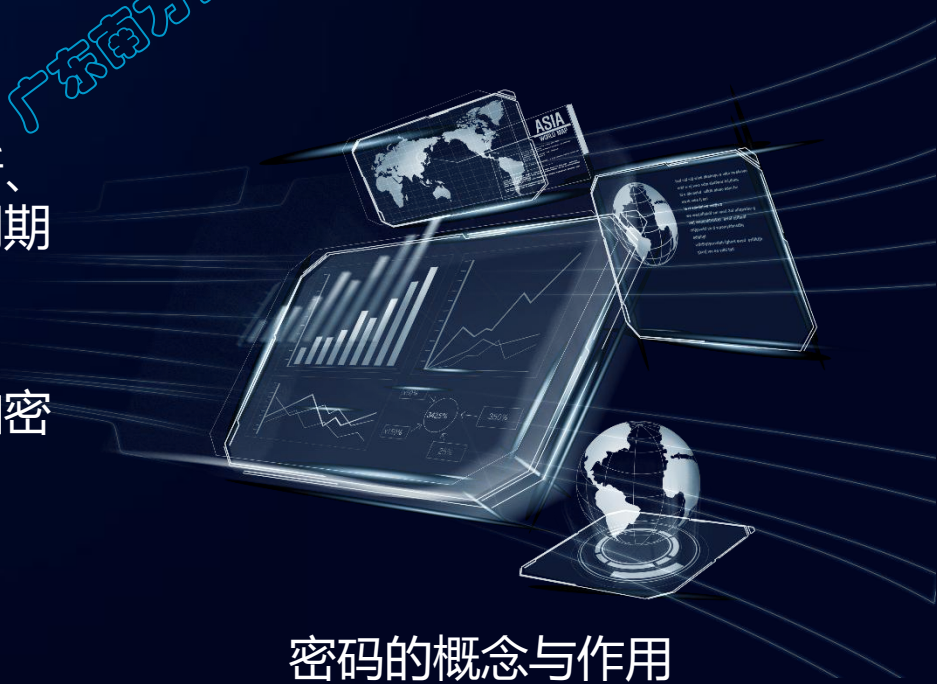
一、密码应用概述

典型的密码技术

密码算法：　实现密码对信息进行“明”“密”变换、产生“标签”的一种特定规则。

密钥管理：　根据安全策略，对密钥产生、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。

密码协议：　两个或两个以上参与者使用密码算法，为达到加密保护或安全认证目的而约定的交互规则。



密码的概念与作用

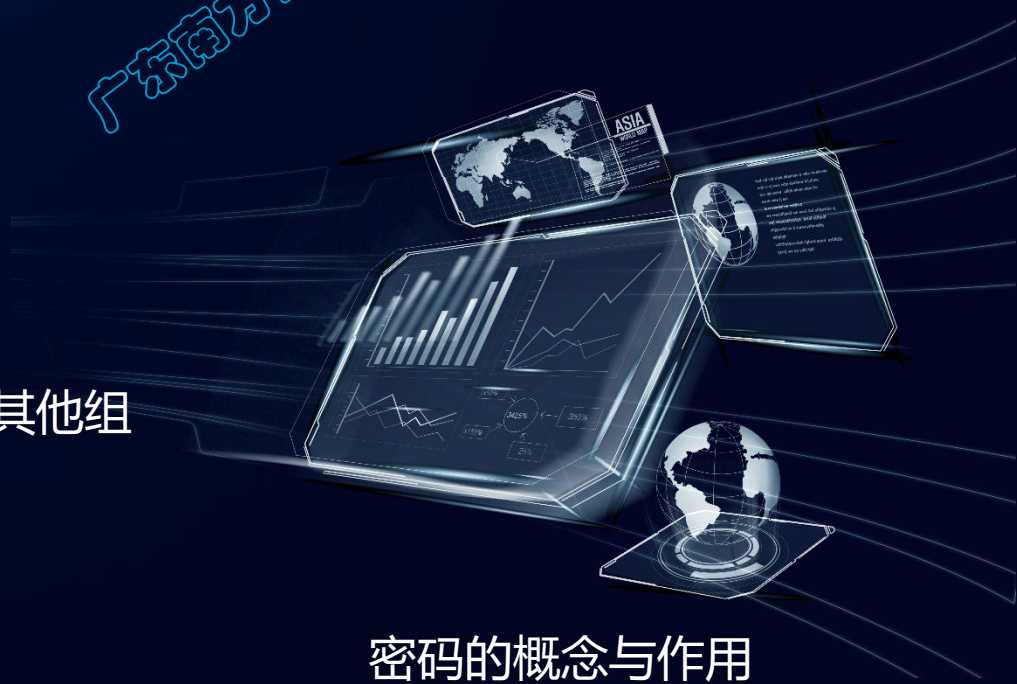
一、密码应用概述

密码的重要作用

“基因” 是网络安全的核心技术和基础支撑

“信使” 是构建网络信任体系的基石

“卫士” 无处不在，时刻守卫着国家、公民、法人和其他组织的安全



密码的概念与作用

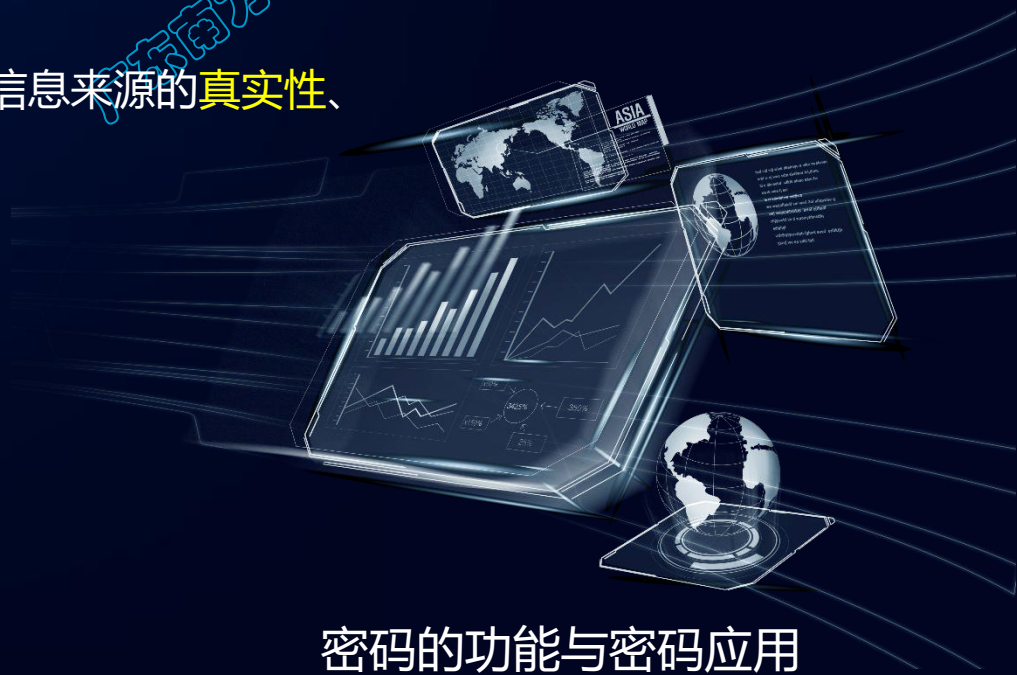
一、密码应用概述

密码的功能

信息安全，最为通用的的定义是“CIA “，即保密性（Confidentiality）、完整性(Integrity)、可用性(Availability).
近年来，真实性(Authenticity)、不可否认性（Non-repudiation）的作用也日益凸显。

所以密码的功能归纳为四项，即信息的保密性、数据的完整性、信息来源的真实性、行为的不可否认性。

保密性——加密、解密技术
完整性——杂凑算法
真实性——安全认证技术
不可否认性——数字签名算法



密码的功能与密码应用

密码应用技术框架

信息系统

密码应用层

安全电子邮件系统 | 电子印章系统 | 安全公文传输 | 桌面安全防护 | 权限管理系统 | 可信时间戳系统 | 其它

通用密码应用

密码服务层（提供密码应用接口）

对称密码服务 | 公钥密码服务 | 其它密码服务

密码应用程序接口

密码支撑层（提供密码资源调用）

安全芯片类 | 密码模块类 | 密码整机类 | 其它

密码功能产品及其集成关系

密码资源层（提供基础密码资源）

算法软件 | 算法IP核 | 算法芯片 | 其它

序列算法 | 分组算法 | 公钥算法 | 杂凑算法 | 随机数生成算法 | 其它

基础密码算法

密码管理基础设施

运维管理

信息管理

设备管理

密钥管理

一、密码应用概述

存在的问题

密码技术被弃用

密码技术被乱用

密码技术被误用

密码应用中的安全性问题

二、密码应用安全性评估的基本原理

二、密码应用安全性评估的基本原理

商用密码应用安全性评估概念

商用密码应用安全性评估（简称“密评）是指在采用商用密码技术、产品和服务集成建设的网络与信息系统中，对其密码应用的合规性、正确性、有效性等进行评估。

信息安全管理过程

国际上重要的信息安全管理标准中，以英国标准协会（BSI）制定的BS7799影响力最为广泛，并于2000年成为国际标准ISO/IEC17799，2005年改版后成为ISO/IEC27001

我国的信息安全管理标准GB/T 22080-2016《信息技术 安全技术 信息安全管理体系要求》就是等同采用的标准ISO/IEC27001:2013

信息安全管理过程

PDCA管理循环

计划
(Plan)

建立信息安全管理体系环境

改进信息安全管理体系

改进
(Act)

实施
(Do)

实施并运行信息安全管理体系

监视并评审信息安全管理体系

检查
(Check)

二、密码应用安全性评估的基本原理

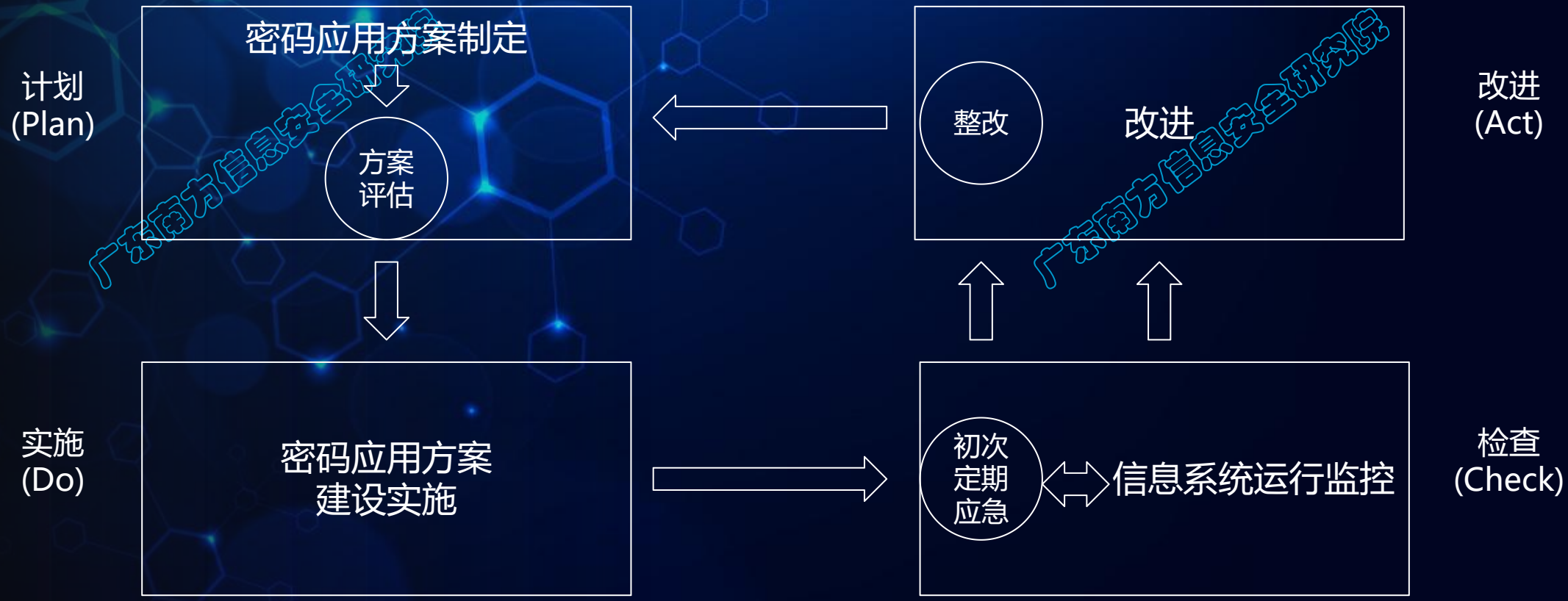
信息安全风险评估概念

信息系统的安全风险，是由来自于自然、环境或人为的威胁，利用系统存在的脆弱性，给系统造成的负面影响的潜在可能
信息安全风险评估是确定和认识信息系统安全风险，并对风险进行分析，根据选定的标准对风险进行评价，从而为进一步处置风险提供科学依据的过程

评估的基本要素

资产，被保护的对象
威胁，造成负面影响的潜在可能
脆弱性，漏洞
风险，威胁发生时带来的损失
安全措施，保护资产、抵御威胁、减少脆弱性、降低风险的影响，以及打击信息犯罪的各种实践、规程和机制

密码应用安全性评估在密码应用管理中的定位

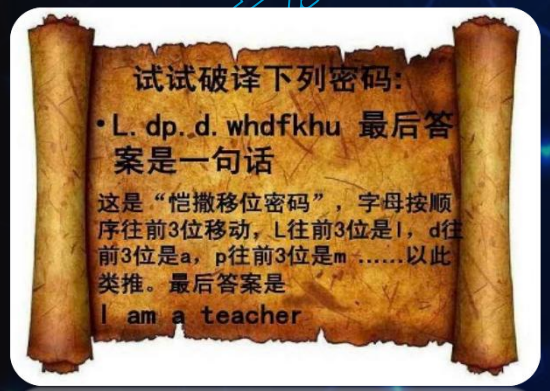


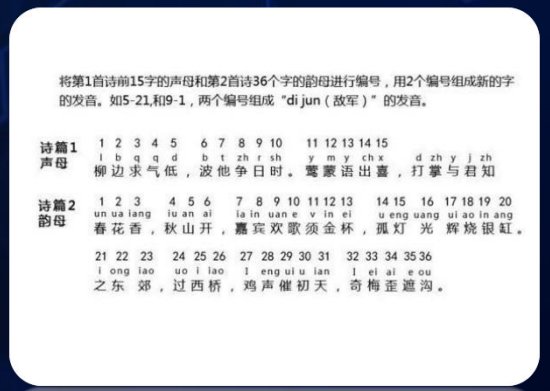
三、密码技术发展

三、密码技术发展

古典密码

这个时期密码还算不上一门学科，靠人的头脑和直觉来设计和分析
主要有两种体制，代换密码和置换密码



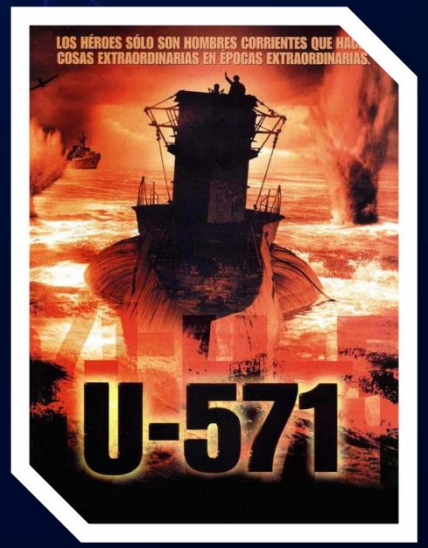


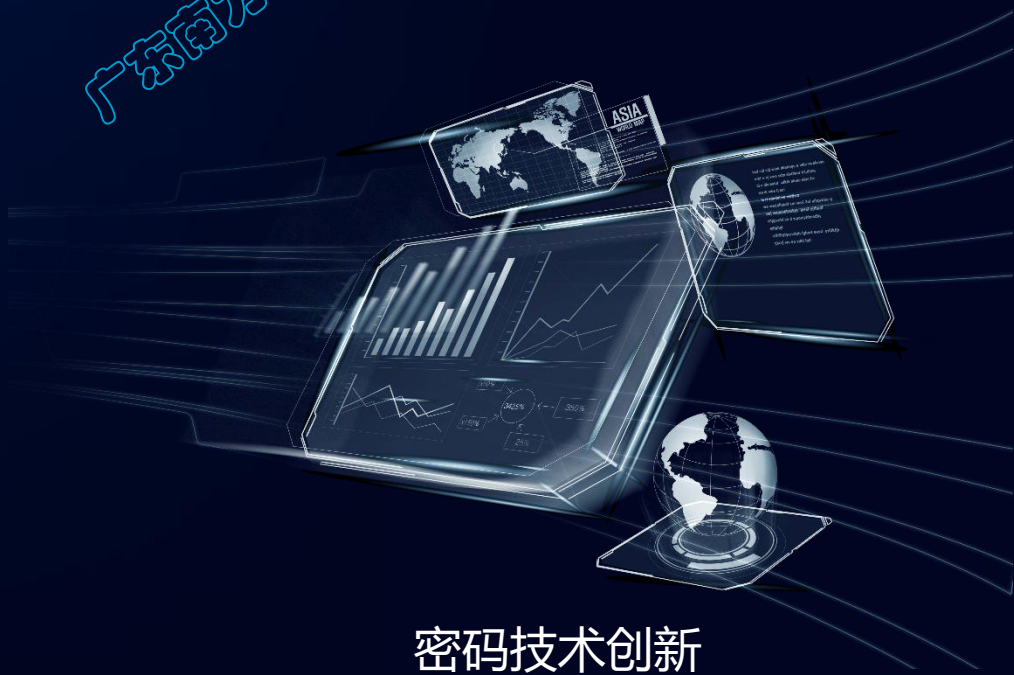
密码技术创新

三、密码技术发展

机械密码

密码研究者设计出一些机械和电动设备，自动实现加密和解密计算，典型代表就是二战时德国使用的恩尼格玛密码机，它的设计提供了1亿亿种不同的密码变换组合





密码技术创新

三、密码技术发展

现代密码

“信息论之父”香农关于保密通信理论的发表和美国数据加密标准DES的公布以及公钥密码思想的提出，标志着现代密码时期的开启

香农，提出“一次一密”的理想密码模型
DES算法，分组密码算法
AES算法，分组密码算法，能够抵抗差分分析、线性分析、代数攻击等
RSA算法，公钥密码算法，加密密钥公开，解密密钥保密，基于数学难题
MD5算法，密码杂凑算法
SHA，密码杂凑算法

密码技术创新

三、密码技术发展

抗量子攻击

量子计算出现后，给RSA等公钥密码算法带来了致命影响
目前可以对抗量子攻击的公钥密码体制
基于格的密码
基于多变量的密码
基于编码的密码
基于杂凑函数的密码

量子密钥分发

量子密钥分发，量子通信提供了一种新的方法来实现密钥共享，其安全性依赖于物理原理而不是传统的数学和计算复杂性理论，能够从理论上确保通信的绝对安全
目前，量子密钥分发需要通过“量子信道+经典信道“来完成，量子信道传递量子信息，经典信道传递密钥分发设备之间交互的数据和信令

密码技术发展趋势

四、密码算法

密码算法

对称密码

公钥密码

杂凑算法

ZUC

SNOW、RC4...

SM4

DES、TDEA、AES...

SM2

SM9

RSA.....

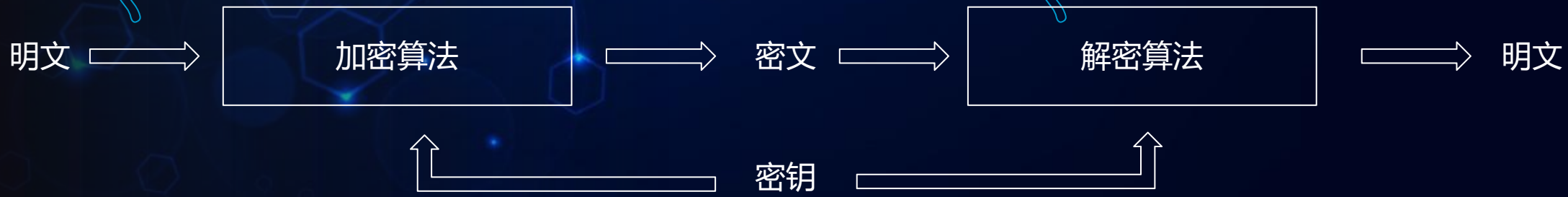
SM3

MD5、SHA.....

四、密码算法

对称密码算法概念

加密过程与解密过程使用相同的或容易相互推导得出的密钥，即加密和解密两方的密钥是“对称”的。



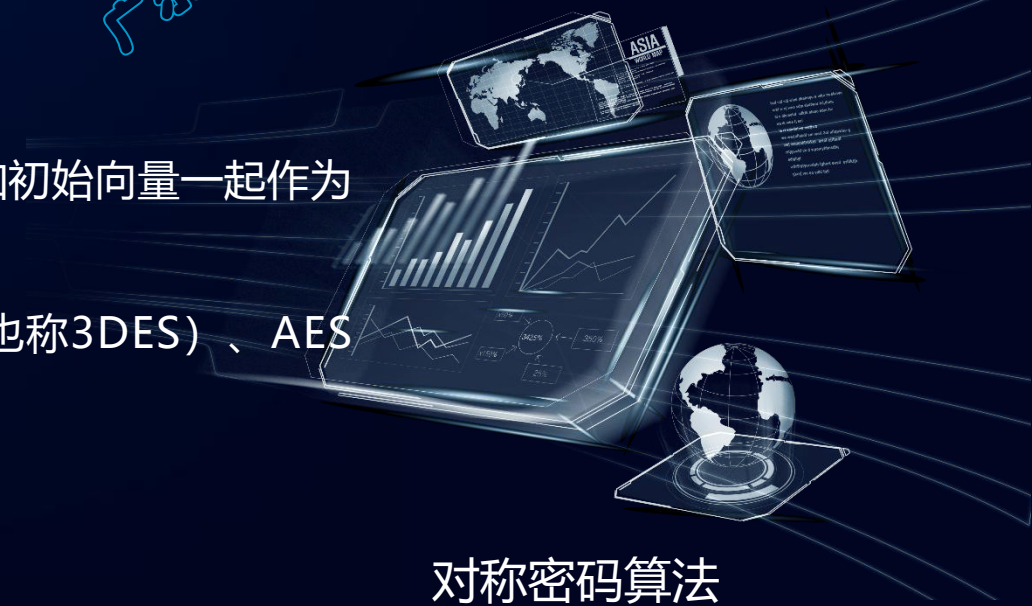
四、密码算法

对称密码算法分类

对称密码主要有两种形式，序列密码、分组密码

序列密码（也称流密码，steam cipher），
将密钥和初始向量作为输入，通过密钥流生成算法输出密钥流（也称扩展密钥序列），然后将明文序列和密钥进行异或，得到密文序列
我国，ZUC（祖冲之算法）
外国，SNOW、RC4

分组密码（也称块密码，block cipher）
首先对明文消息根据分组大小进行分组，再将明文分组、密钥和初始向量一起作为输入，通过分组加密算法直接输出密文分组
我国，SM4
外国，DES（数据加密标准）、TDEA（三重数据加密算法，也称3DES）、AES（高级加密标准）

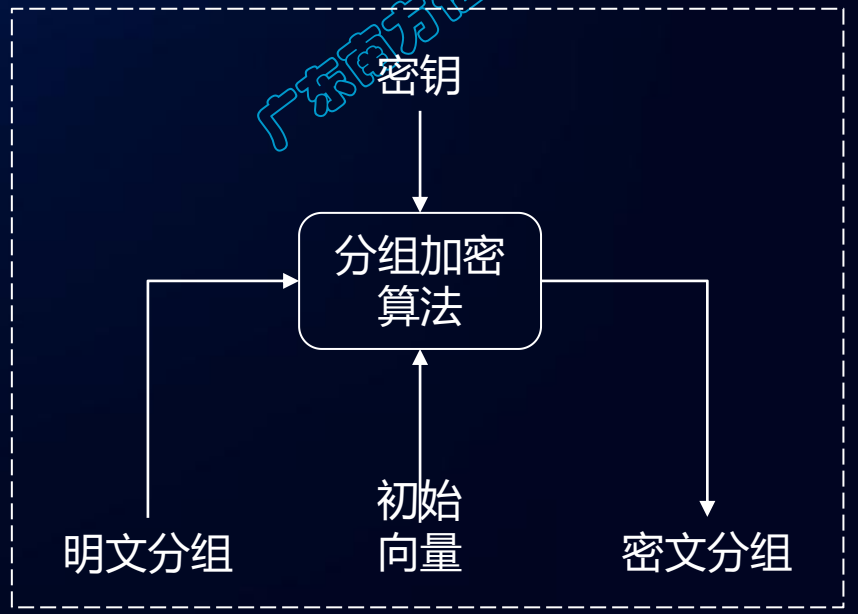


对称密码算法

四、密码算法

特点区别

序列密码的特点在于密钥流可以在明文序列到来之前生成。加密操作仅仅是一次异或，因此执行速度通常很快，占用计算资源少，常用于功耗或者计算能力受限的系统，如嵌入式系统、移动终端等，还有实时性要求高的场景，如语音、视频通信



对称密码算法

四、密码算法

分组密码

主要有七种工作模式

电码本（ECB）
密文分组链接（CBC）
密文反馈（CFB）
输出反馈（OFB）
计数器（CTR）
分组链接（BC）
带非线性函数的输出反馈（OFBNLF）

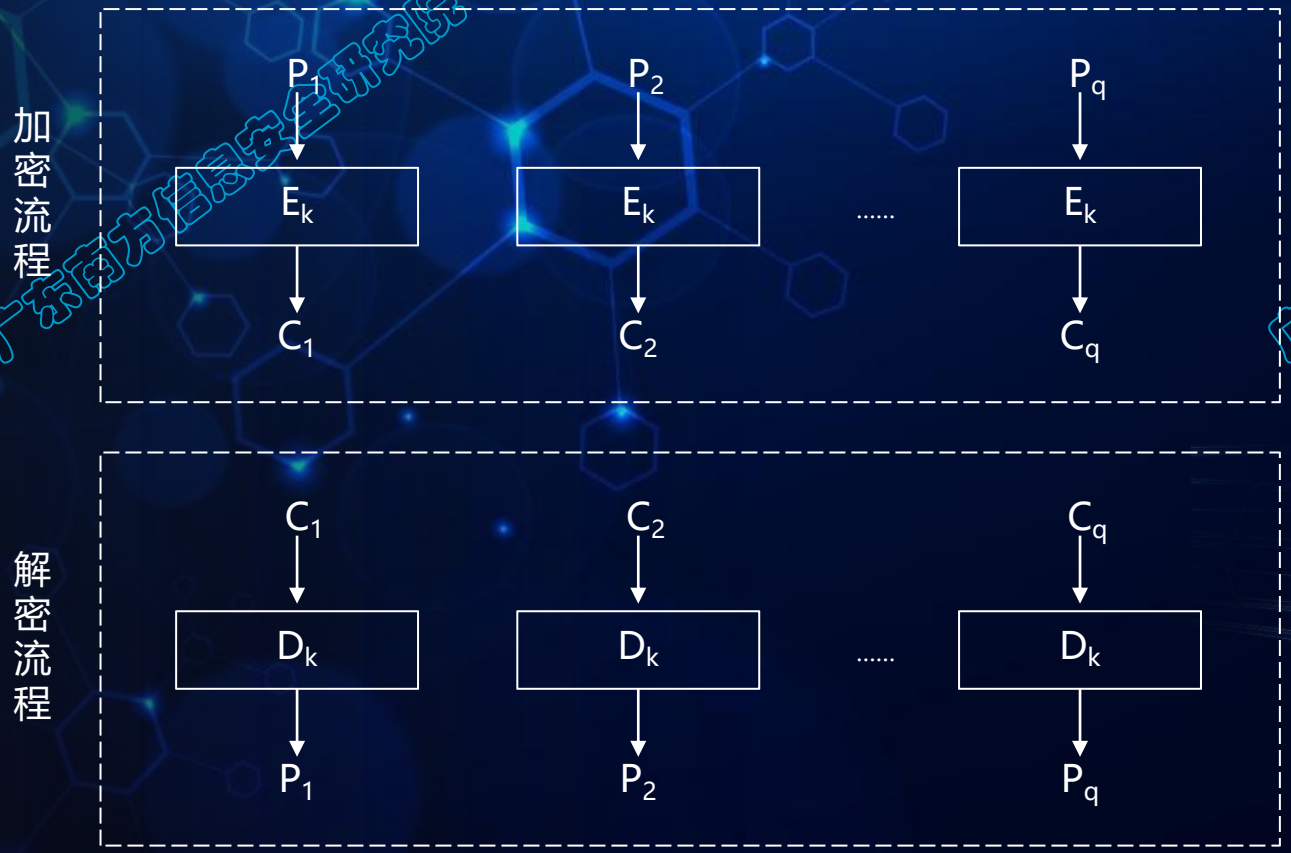
表 3　7 种加密模式的特点对比

模式特点	BC	OFBNLF	ECB	CBC	OFB	CFB	CTR
运行效率	1	2	1	1	1	⩾1	1
差错扩散	✓	✓	×	✓	×	✓	×
自同步	×	×	×	×	×	✓	×
并行计算	×	✓	✓	×	×	×	✓
预处理	×	✓	×	×	✓	×	✓
不含逆	×	×	×	×	✓	✓	✓

对称密码算法

四、密码算法

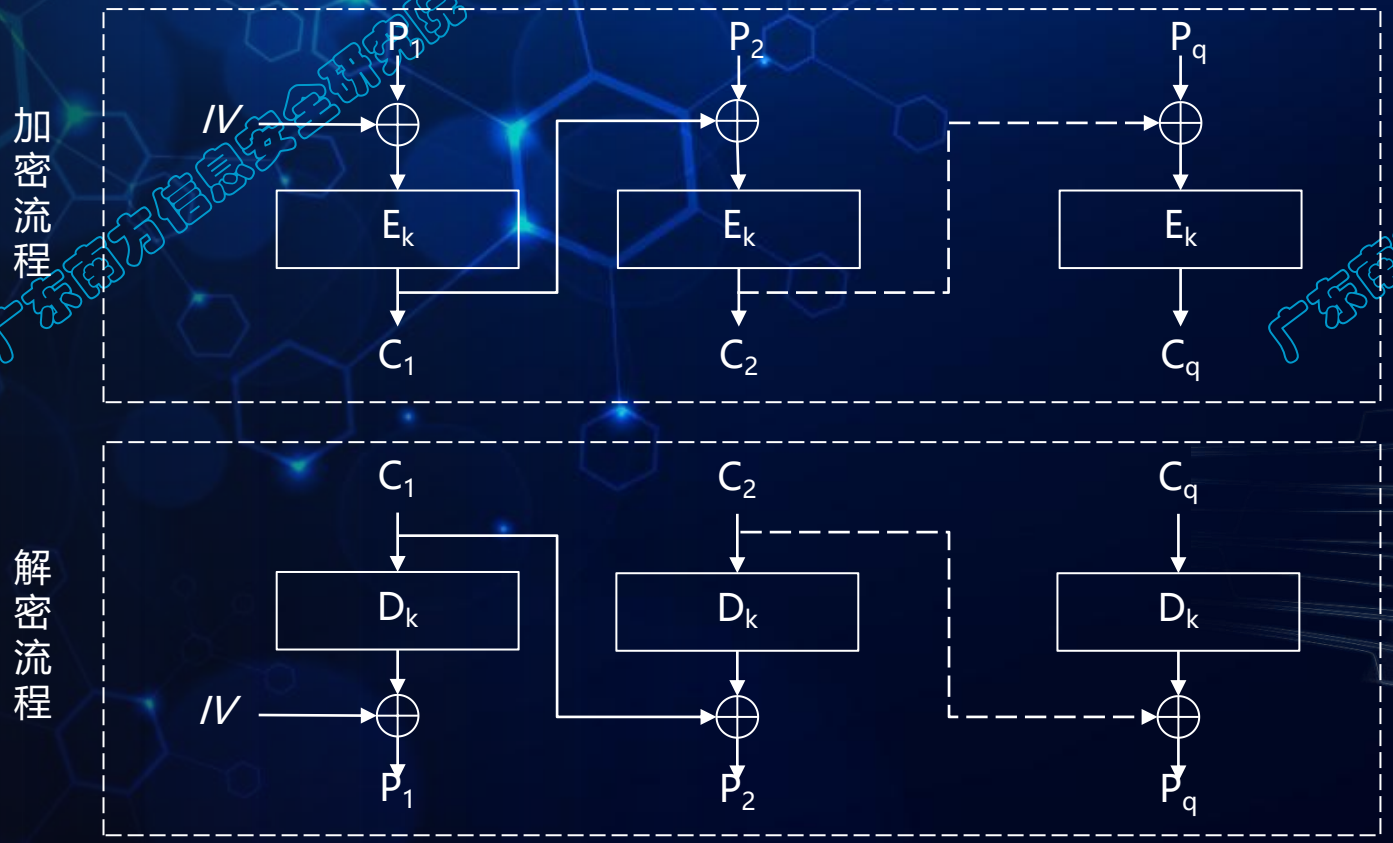
ECB模式



对称密码算法

四、密码算法

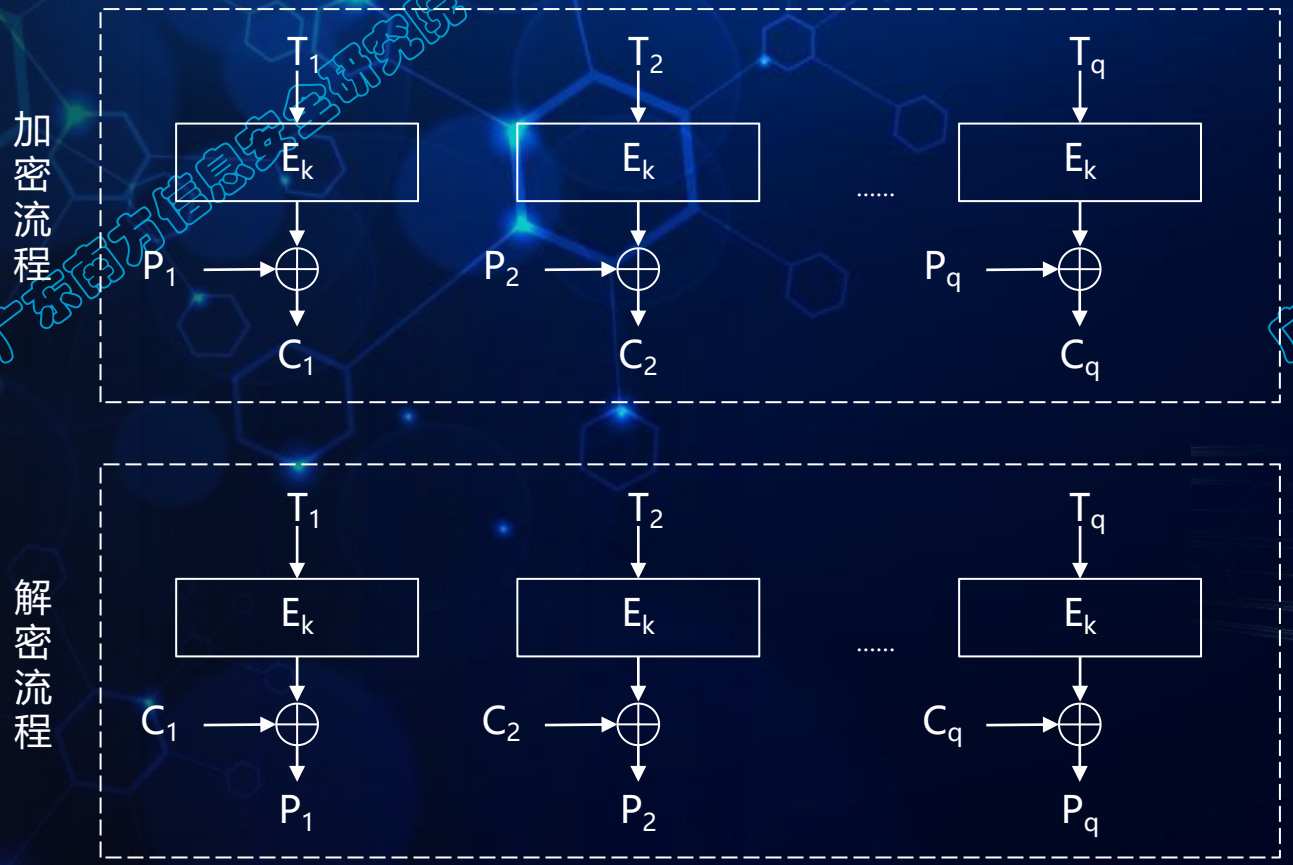
CBC模式



对称密码算法

四、密码算法

CTR模式



对称密码算法

四、密码算法

ZUC序列密码算法

以中国古代数学家祖冲之的拼音首字母命名，2011年，与美国的AES、欧洲的SNOW共同成为了4G移动通信密码算法国际标准

由线性反馈移位寄存器（LFSR）、比特重组（BR）、非线性函数（F）三个基本部分组成，逻辑上分为上、中、下三层，上层是16级LFSR，中间层是BR，下层是非线性函数F

上层：LFSR以一个有限域GF（2^{31}-1）上的16次本原多项式为连接多项式，输出具有良好的随机统计特性

中间层：BR从LFSR的状态中取出128比特，拼成4个字（X_0、X_1、X_2、X_3），供下层的非线性函数F和输出密钥序列使用

下层：非线性函数F从中层的BR接收3个字（X_0、X_1、X_2）作为输入，经过内部的异或、循环移位和模2^{32}加法运算，以及两个非线性S盒变换，最后输出一个32比特W

最后，非线性函数F输出的W与BR输出的X_3异或，形成输出密钥字序列Z

四、密码算法

ZUC序列密码算法

算法使用
在生成密钥流时，ZUC算法采用128比特的初始密钥和128比特的IV作为输入参数，共同决定LFSR里寄存器的初始状态。
随着电路时钟的变化，LFSR的状态被比特重组之后输入非线性函数F，每一拍时钟输出一个32比特的密钥流Z。随后，密钥流与明文按位异或生成密文

ZUC的算法包括机密性算法和完整性算法两种

基于ZUC的机密性算法128-EEA3，主要用于4G移动通信中移动用户设备和无线网络控制设备之间的无线链路上通信信令和数据的加密和解密

基于ZUC的完整性算法128-EIA3，主要用于通信信令和数据完整性校验，并对令源进行鉴别

对称密码算法

四、密码算法

SM4分组密码算法

它是迭代分组密码算法，加密算法和密钥扩展算法都采用32轮非线性迭代结构（Feistel结构），加密和解密的算法结构完全一致，解密过程只需要把加密过程中产生的轮密钥逆序排列就能从密文分组中恢复出明文分组

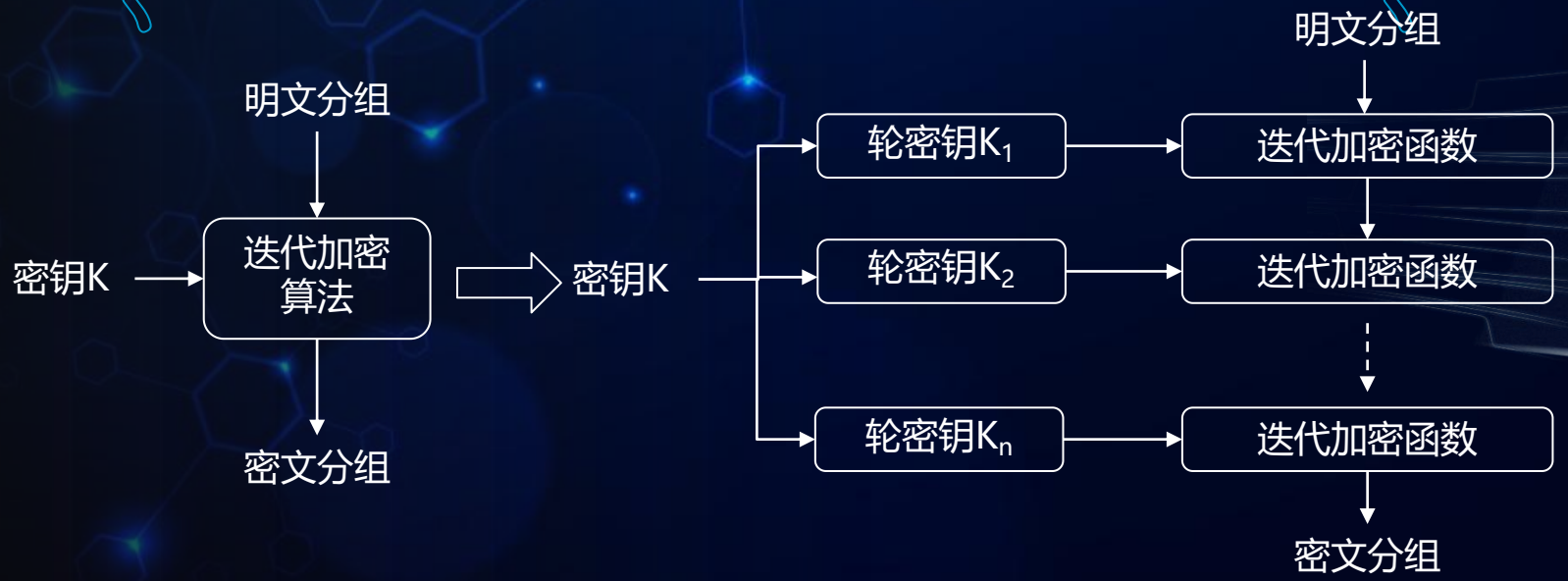
明文分组经过迭代加密函数变换后的输出又成为下一轮迭代加密函数的输入，如此迭代32轮，最终得到密文分组，每一轮迭代函数是相同的，不同的是输入的轮密钥

对称密码算法

四、密码算法

SM4分组密码算法优势

在设计上实现了资源重用，密钥扩展过程和加密过程类似
加密过程与解密过程相同，只是轮密钥使用顺序正好相反，它不仅适用于软件编程实现，更适合硬件芯片实现
轮变换使用的模块包括异或运算、8比特输入8比特输出的S盒，还有一个32比特输入的线性转换，非常适合32位处理器的实现



对称密码算法

四、密码算法

公钥密码算法概念

公钥密码算法又称非对称密码算法，既可用于加密和解密，也可用于数字签名，打破了对称密码算法加密和解密必须使用相同密钥的限制，很好的解决了对称密码算法中存在的密钥管理难题

加密的密钥可以公开，称为公钥，解密的密钥需要保密，称为私钥。公钥和私钥是密切关联的，从私钥可推导出公钥，但从公钥推导出私钥在计算上不可行的

一般建立在公认的计算困难问题之上。这样的公钥密码具有可证明安全性，即如果所依赖的问题是困难的，那么所设计的算法就可证明是安全的
比如：
RSA，大整数因子分解困难性
ElGamal，有限域上的离散对数问题
SM2，椭圆曲线上的离散对数问题
后量子密码（如基于格的密码）

公钥密码算法

四、密码算法

公钥密码算法种类

公钥密码算法
由于公钥密码运算操作计算复杂度较高，加密速度一般比对称加密算法的加密速度慢很多，因此主要用于短数据的加密，如建立共享密钥
在执行公钥加密前，需要先查找接收者的公钥，然后用该公钥加密要保护的消息。
当接收方收到消息后，用自己的私钥解密出原消息

数字签名算法
主要用于确认数据的完整性、签名者身份的真实性和签名不可否认性等
与公钥密码算法使用公钥、私钥的顺序不同，数字签名使用私钥对消息进行签名，使用公钥对签名进行验证
需要注意，为提升效率和安全性，数字签名算法中一般都需要先使用密码杂凑算法对原始消息进行杂凑运算，再对得到的消息摘要进行数字签名

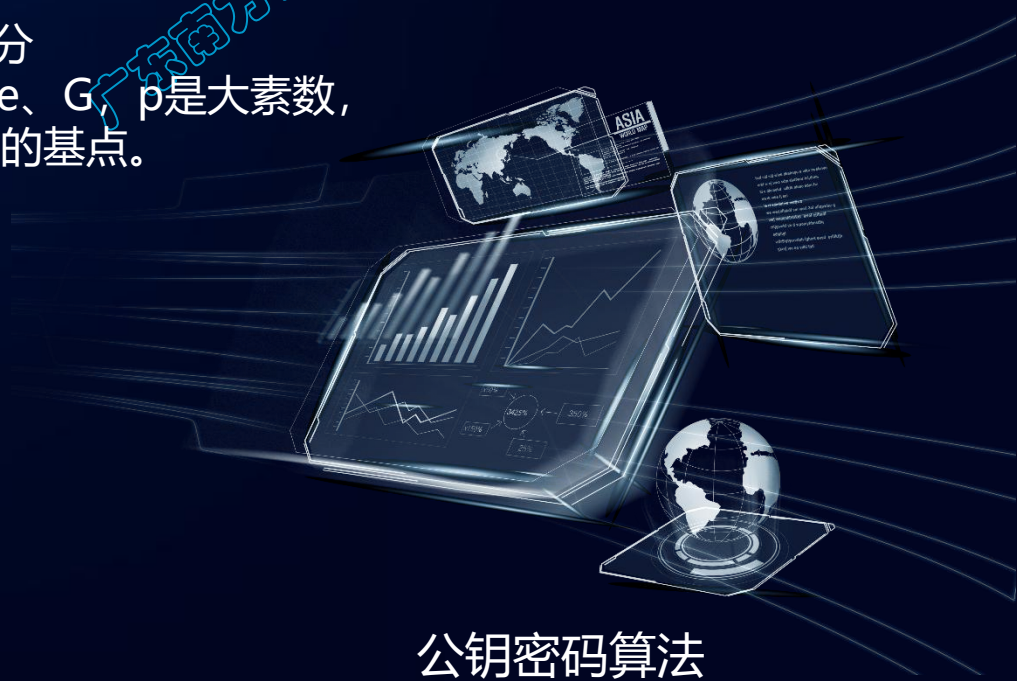
公钥密码算法

四、密码算法

SM2椭圆曲线公钥密码算法

由于基于椭圆曲线上的离散对数问题的困难性要高于一般乘法群上的离散对数问题的困难性，且椭圆曲线所基于的域的运算位数要远小于传统离散对数的运算位数，因此椭圆曲线密码体制比原有的密码体制（如RSA）更具优越性

SM2主要包括数字签名算法、密钥交换协议和公钥加密算法三部分
使用该算法之前，各通信方先设定相同的公开参数，包括p、n、e、G，p是大素数，E是定义在有限域GF（p）上的椭圆曲线，G=（x_G,y_G）是E上n阶的基点。



公钥密码算法

四、密码算法

SM2椭圆曲线公钥密码算法

SM2数字签名算法

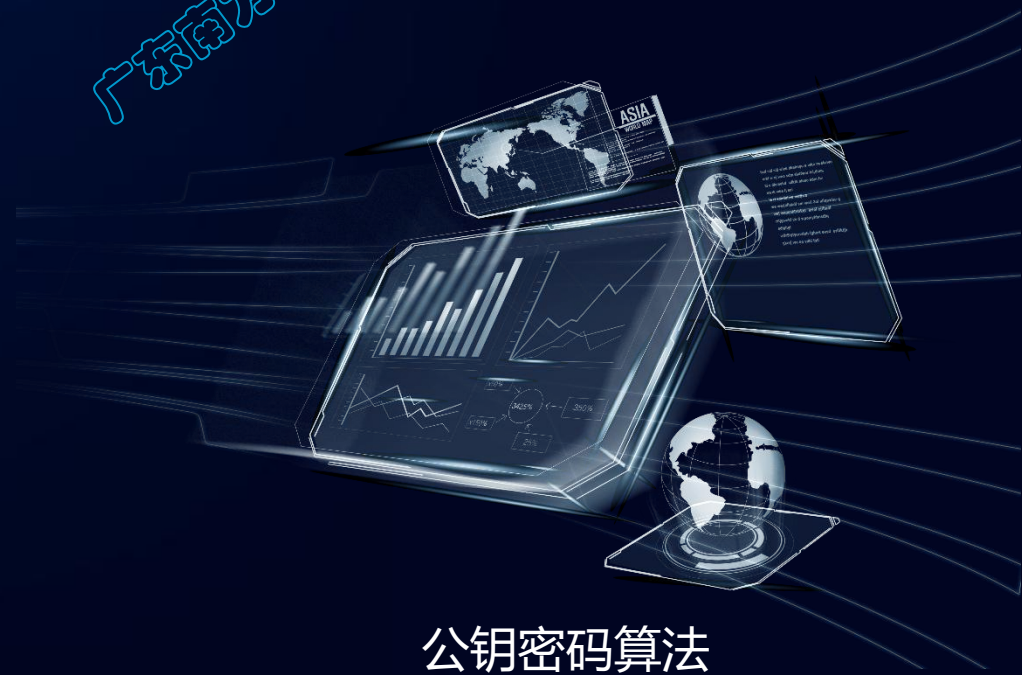
在执行签名过程之前，要用密码杂凑函数对用户的可辨别标识、部分椭圆曲线系统参数和用户的公钥杂凑值以及待签名消息进行压缩

在验证过程之前，要用密码杂凑函数对用户的可辨别标识、部分椭圆曲线系统参数和用户的公钥杂凑值以及待验证消息进行压缩

密码生成

随机产生一个秘密变量d，d∈[1,n-2]

计算P=dG，并将P作为公钥，d作为私钥保存



公钥密码算法

四、密码算法

SM2椭圆曲线公钥密码算法

签名生成
签名者选取随机数k，k∈[1,n-1]，计算$kG(x_1,y_1)$
计算$r=(H(M)+x_1)\bmod n$，其中$M=Z_A \| m$，Z_A是用户的可辨别标识、部分椭圆曲线系统参数和用户的公钥杂凑值，m是待签名消息；H为国家密码管理局标准的杂凑函数，如SM3；若r=0或r+k=n，则重新选取随机数k
计算$s=(1+d)^{-1}(k-rd)\bmod n$，若s=0，则重新选取随机数k，否则，将（r,s）作为签名结果

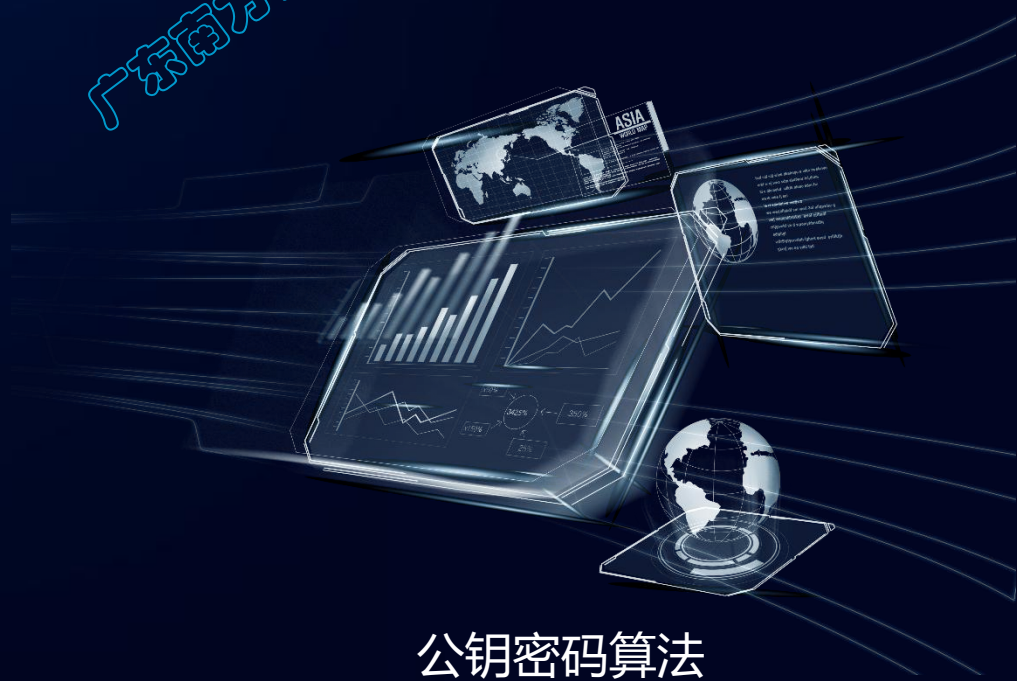
签名验证
验证者接收到M和（r,s）后，先检查r,s，先检查r,s∈[1,n-1]，且r+s≠n；然后计算（x1,y1）=sG+(r+s)P
计算$r'=(H(M)+x_1')\bmod n$；判断r’与r是否相等，相等则验证通过，否则失败

公钥密码算法

四、密码算法

SM2椭圆曲线公钥密码算法

SM2密钥交换协议
又称密钥协商，是两个用户A和B通过交互的信息传递，用各自的私钥和对方的公钥来商定一个只有他们知道的秘密密钥。这个共享的秘密密钥通常用在对称密码算法中，即“会话密钥 “



公钥密码算法

四、密码算法

SM2椭圆曲线公钥密码算法

A：选择一个随机数r_A，计算其的G函数值R_A，发送给B

B：选择随机数r_B，计算其的G函数值R_B，发送给A
代入r_B、d_B（私钥），计算x_B
验证收到的R_A为椭圆曲线E上的点，验证通过则计算x_A
代入P_A、R_A、x_A，计算V点是否曲线上的无穷远点，如果不是，得到$x_V y_V$
计算$K_B=KDF(x_V \| y_V \| Z_A \| Z_B, klen)$, klen为随机数比特长度

A：代入r_A、d_A（私钥），计算x_A
验证收到的R_B为椭圆曲线E上的点，验证通过则计算x_B
代入P_B、R_B、x_B，计算U点是否曲线上的无穷远点，如果不是，得到$x_U y_U$
计算$K_A=KDF(x_U \| y_U \| Z_U \| Z_U, klen)$, klen为随机数比特长度

通过以上协商，协商出共享密钥$K_A=K_B$

公钥密码算法

四、密码算法

SM2椭圆曲线公钥密码算法

SM2公钥密码算法

加密算法

选择随机数l，计算密文C_1

代入公钥，计算密钥序列e=KDF()

通过明文M和e计算C_2

通过杂凑函数H和明文M计算C_3

输出密文$C=C_1 \| C_3 \| C_2$

解密算法

验证C_1是否在椭圆曲线上

代入私钥，计算密钥序列e=KDF()

通过密文C_2和e计算明文M

通过杂凑函数H计算C_3'，并验证$C_3'=C_3$是否成立，不成立报错退出

输出明文M

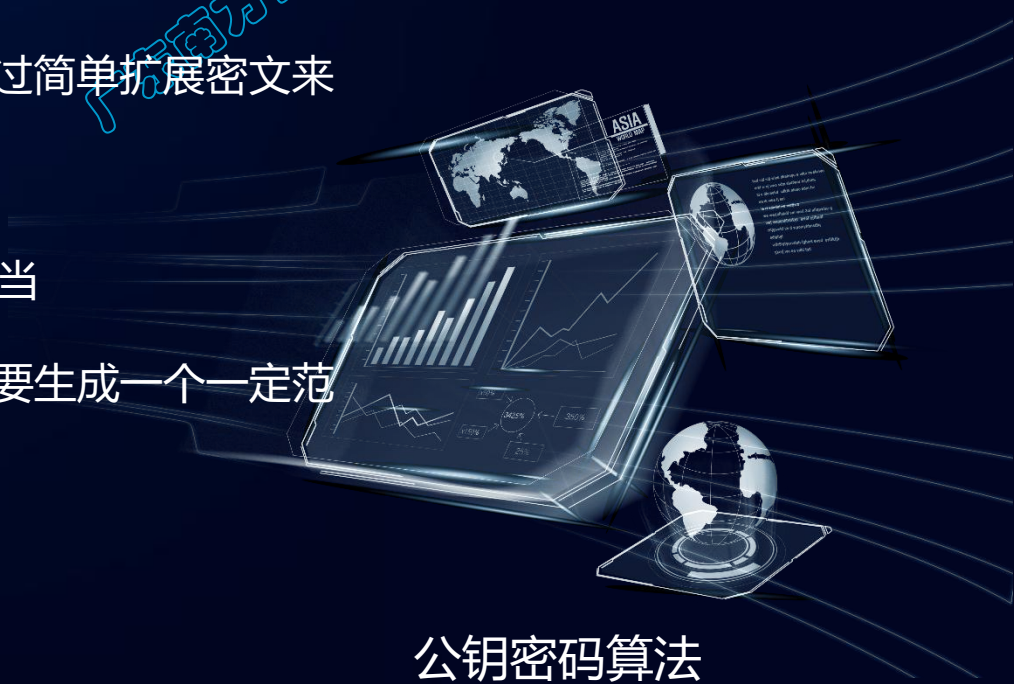
公钥密码算法

四、密码算法

SM2椭圆曲线公钥密码算法

安全性和效率
算法具备单向性，即未授权第三方在未得到私钥的情况下，从密文计算出明文在计算上是不可行的
算法产生的明文和密文具备不可区分性，即恶意第三方对于给定的密文无法区分其是由给定的两个明文中的哪一个加密而来
密文具备不可延展性，即第三方无法在不解密密文的前提下，通过简单扩展密文来构造出新的合法密文

与RSA算法相比
安全性高，256比特的SM2强度超过RSA-2048，与RSA-3072相当
密钥短，256比2048
私钥产生简单，RSA需要用到两个随机生产的大素数，SM2只需要生成一个一定范围内的256比特随机数



公钥密码算法

四、密码算法

SM9标识密码算法

标识密码算法（IBC）使用的是公钥密码体制，加密与解密使用两套不同的密钥，每个人的公钥就是他的身份标识，如E-mail地址，因此IBC的密钥管理相对简单

用户的私钥由密钥生成中心根据主密钥和用户标识计算得出，用户的公钥由用户标识唯一确定，用户不需要第三方保证其公钥来源的真实性

SM9采用的基本技术
涉及有限域和椭圆曲线、双线性对及安全曲线、椭圆曲线上的双线性对的运算
应用和管理不需要数字证书、证书库或密钥库

公钥密码算法

四、密码算法

SM9标识密码算法

SM9数字签名算法

用椭圆曲线对实现的、基于标识的数字签名算法，包括数字签名生成算法和验证算法

签名者持有一个标识和相应的私钥，该私钥由密钥生成中心通过主私钥和签名者的标识结产生

签名者用自身私钥对数据产生数字签名

验证者用签名者的标识生成其公钥，验证签名的可靠性，即验证发送数据的完整性、来源的真实性和数据发送者的身份

SM9密钥交换协议

与SM2类似，不同只是双方有标识。双方各自持有一个标识和相应的私钥，通过交互信息，商定一个只有他们知道的秘密密钥

SM9密码密钥封装机制和加密算法

封装者利用解封装用户的标识产生并加密一个秘密密钥给对方，解封装用户则用相应的私钥解封装该秘密密钥，也唯有拥有此标识的用户才能解封装

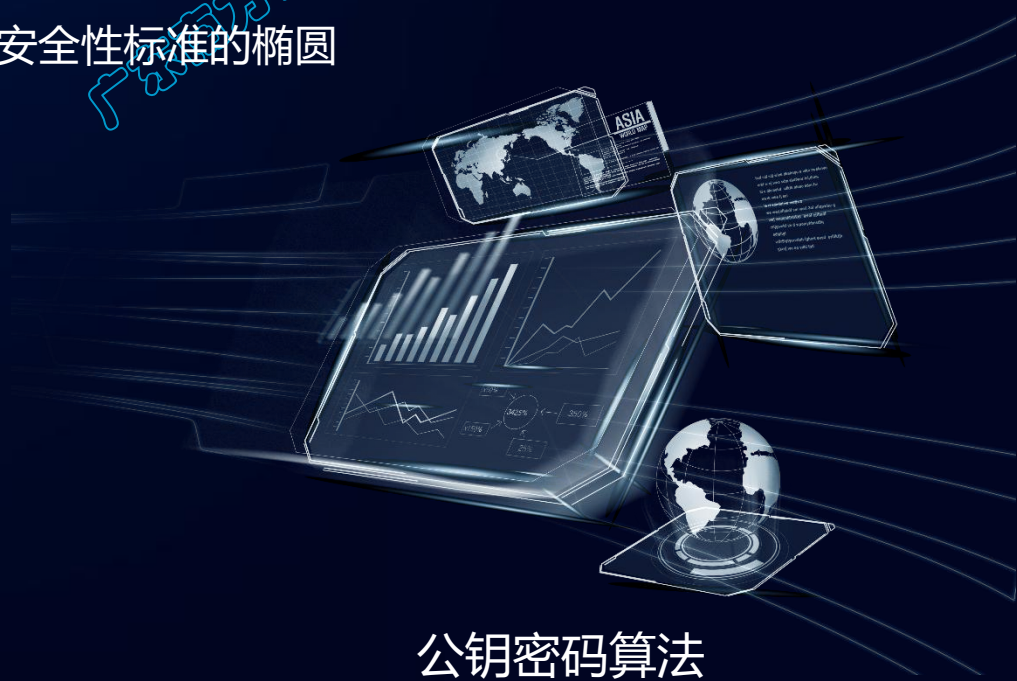
公钥密码算法

四、密码算法

SM9标识密码算法

安全性和效率
目前，没有发现明显影响双性线对密码系统应用的安全性风险，安全性远远高于同类算法

其安全性和嵌入次数有关，目前SM9采取了嵌入次数适中且达到安全性标准的椭圆曲线



公钥密码算法

四、密码算法

RSA公钥密码算法

基于大整数因子分解难题设计，原理清晰、结构简单，是第一个投入使用，也是迄今为止用就最广泛的公钥密码算法
公钥相当于两个素数的乘积，私钥相当于两个独立的素数

算法安全性和效率
密钥长度为1024比特及以下的RSA已经不推荐使用，至少需要2048比特
因为长度比SM2长，执行效率要慢很多

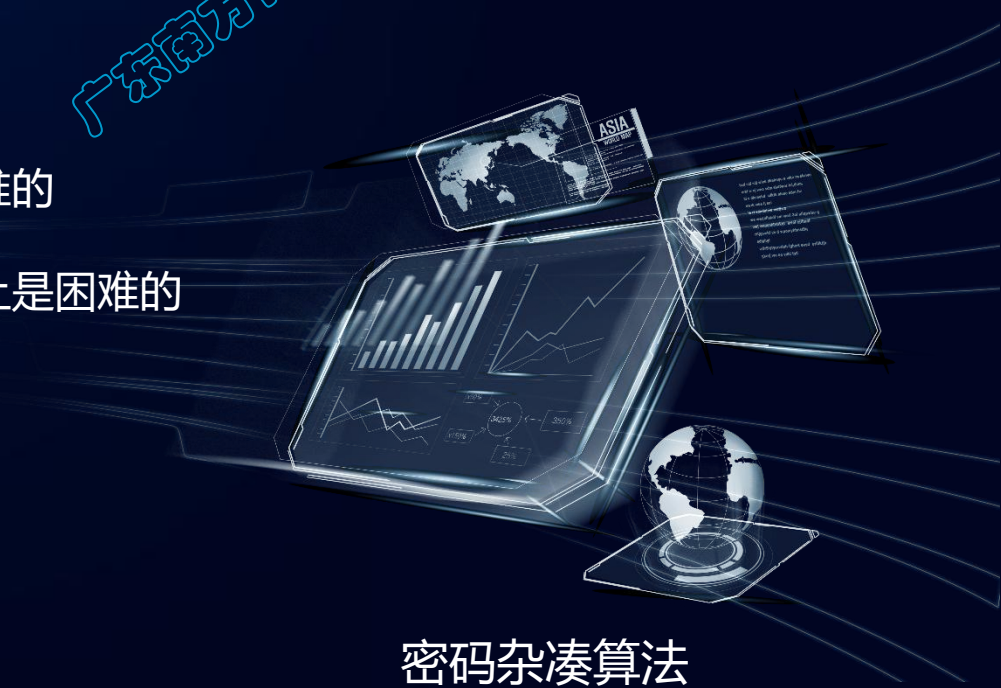
公钥密码算法

四、密码算法

密码杂凑算法概念

也称作“散列算法“或”哈希算法“，目前统称为密码杂凑算法，简称”杂凑算法“或”杂凑函数“

对任意长度的消息进行压缩，输出定长的消息摘要或杂凑值
h=H(M),M是输入消息，h是经杂凑算法H处理后的杂凑值
一般具有的性质
抗原像攻击（单向性）
为一个给定的输出找出能映射到该输出的一个输入在计算上是困难的
抗第二原像攻击（弱抗碰撞性）
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在计算上是困难的
强抗碰撞性
要发现不同的输入映射到同一输出在计算上是困难的



密码杂凑算法

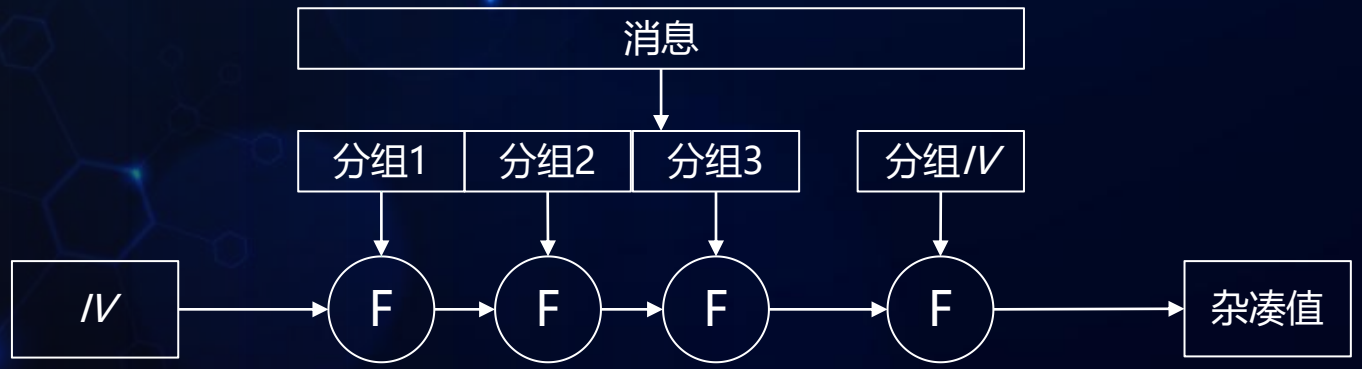
四、密码算法

密码杂凑算法结构

M-D结构，MD5、SHA-1、SHA-2和我国的SM3
海绵结构，SHA-3

M-D结构，先对经过填充后的消息进行均匀的分组，而后消息分组顺序进入压缩函数F。F先由初始向量进行初始化，结合上一组消息的结果和本级消息产生一个中间值，最后一个F即是最终的杂凑值
可以看出，一个很长的消息也很容易被压缩到一个固定的比特长度

其安全性取决于压缩函数的安全性



密码杂凑算法

四、密码算法

密码杂凑算法应用

直接应用就是产生消息摘要，进一步可以检验数据的完整性，被广泛应用于各种不同的安全应用和网络协议中。

在传输信道不能保证安全的情况下，攻击者可以将消息和杂凑值一同篡改，即在修改或替换消息后重新计算一个杂凑值，因此，用于保护完整性时，杂凑算法常常和密钥一同使用，生成的杂凑值称为MAC，这样的算法称为带密钥的杂凑算法HMAC

密码杂凑算法

四、密码算法

SM3密码杂凑算法

SM3采用M-D结构，输入消息经过填充、扩展、迭代压缩后，生成长度为256比特的杂凑值

填充分组

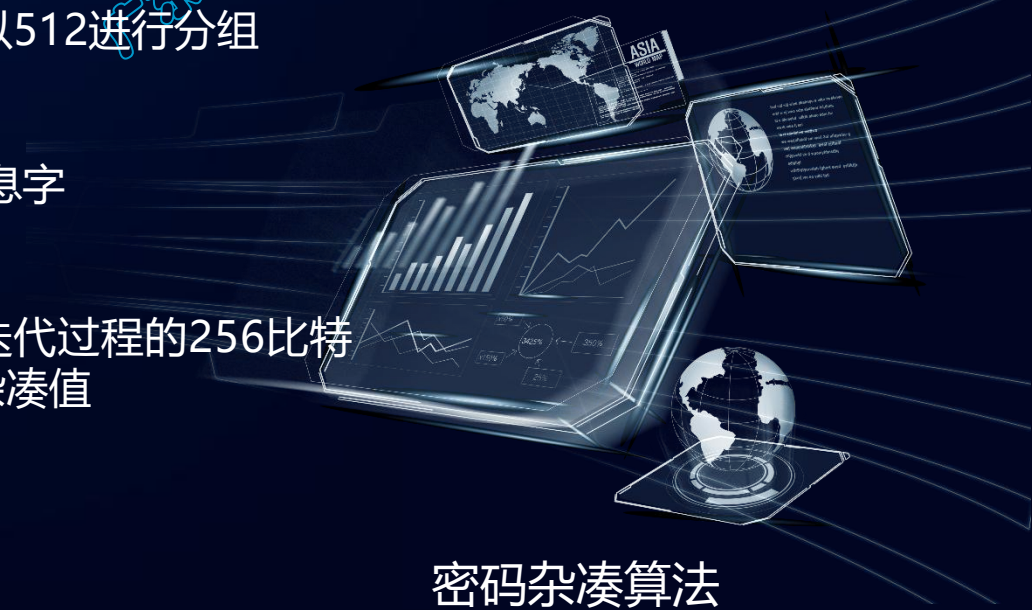
在消息尾部按一定规则填补至512比特的整数倍，再按512比特长度分为若干组
即在长度为L的消息末尾先填充比特“1“，然后填充k个“0”,再填充64比特的L长度的二进制表示，使L末尾不够512的部分+1+k+64=512，再以512进行分组

消息扩展

每个512比特的输入消息分组，先进行消息扩展，生成132个消息字

迭代过程

第一次迭代过程的输入由一个512比特的输入消息分组和上次迭代过程的256比特输出组成，输出256比特，经过n次迭代后，最终得到256比特杂凑值
单次迭代过程包含64轮迭代的压缩



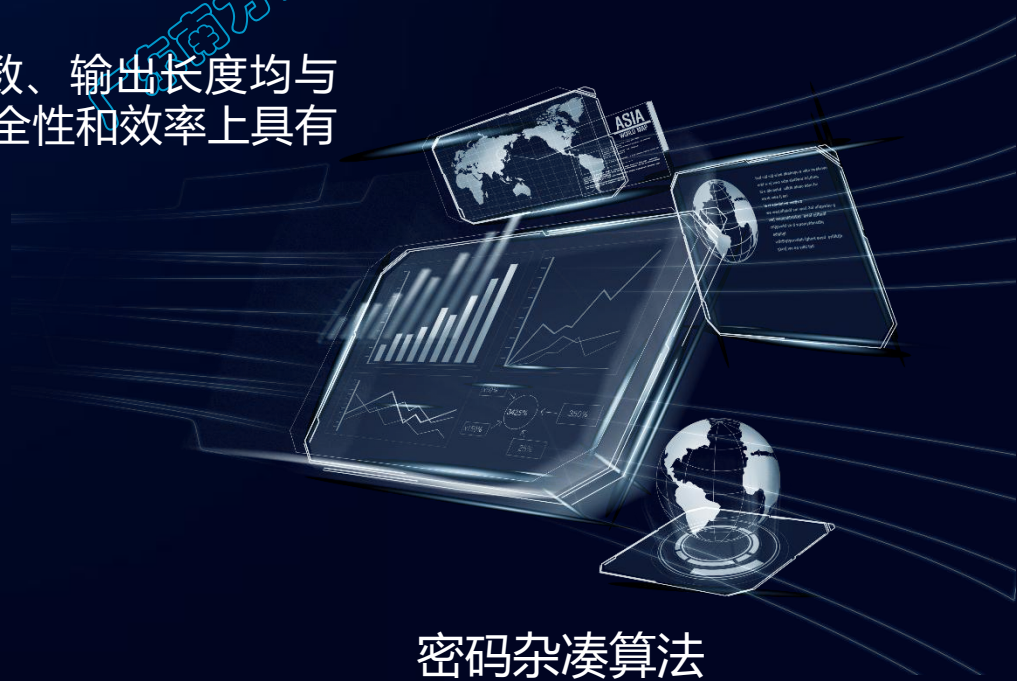
密码杂凑算法

四、密码算法

SM3密码杂凑算法

安全性和效率
在M-D结构的基础上，新增了16步全异或操作、消息双字介入、加速雪崩效应的P转换等多种设计技术，能够有效避免高概率的局部碰撞，有效抵抗强碰撞性的差分分析、弱碰撞性的线性分析和比特追踪等密码分析方法

SM3算法在结构上和SHA-256相似，消息分组大小、迭代轮数、输出长度均与SHA-256相同，SM3又增加了多种新的设计技术，因此在在安全性和效率上具有优势



密码杂凑算法

四、密码算法

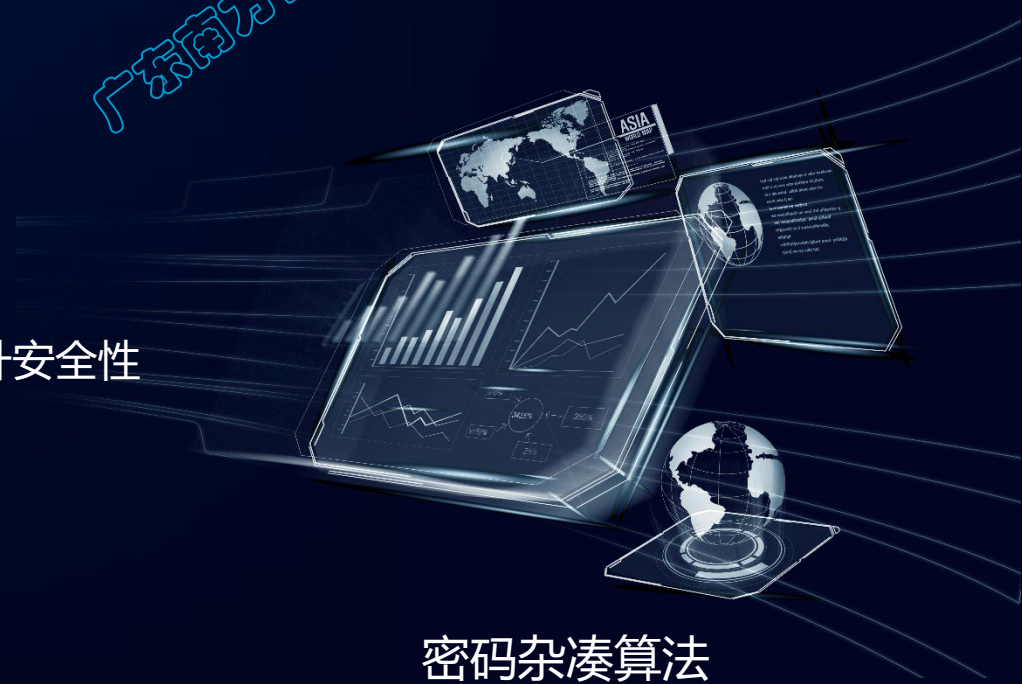
国外密码杂凑算法

MD5
麻省理工学院提出，可用于数字签名、完整性保护、安全认证、口令保护等
128比特消息摘要
一部智能手机仅用30秒就能找到MD5算法的碰撞，表明该算法已不适合实际应用

SHA-1
NAS、NIST提出，设计算法基于MD4，与MD5有相似之处
160比特消息摘要
目前也因碰撞实例，退出历史舞台

SHA-2
NAS、NIST提出，基于M-D结构，但增加了很多重大变化，提升安全性
支持224、256、384、512比特四种长度输出
目前未发现有效的攻击

SHA-3
采用了新的结构——海绵结构



密码杂凑算法

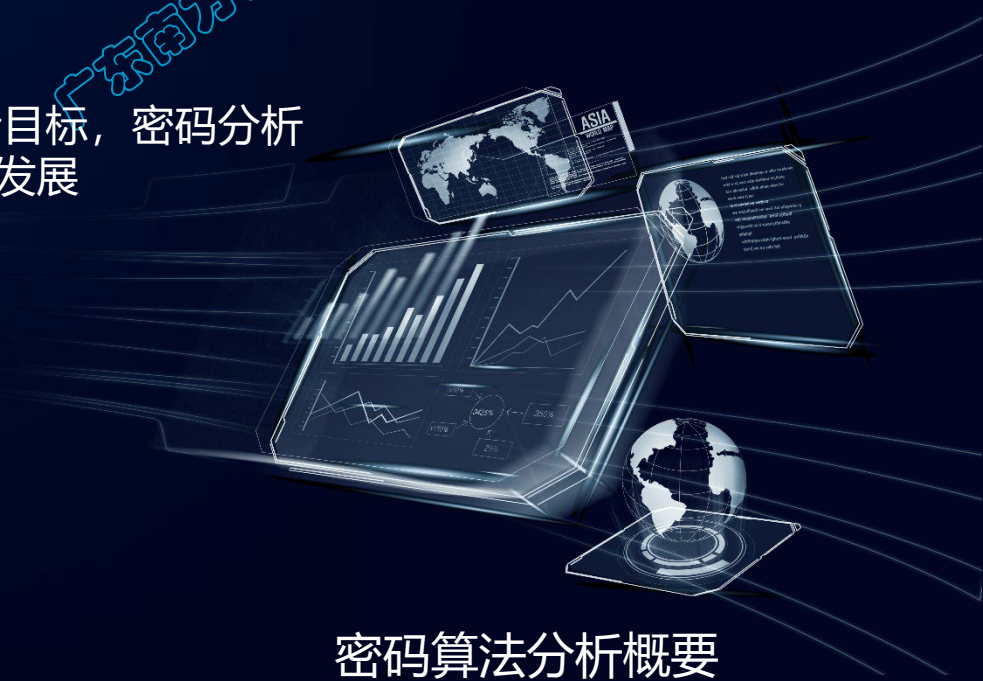
四、密码算法

密码算法分析

密码算法的安全性应该基于密钥的保密，即密钥不被攻击者所知，而不是所有算法的隐蔽性

密码算法分析的目的是通过各种攻击方式，找到密码算法的弱点或者不完美的地方

密码分析和密码编码是对立统一，互不可缺的两个方面
密码编码为密码分析提供对象，并且以抵抗现有的分析方法为设计目标，密码分析为密码编码提供表示安全强度的具体数据，同时促进密码编码不断发展



密码算法分析概要

四、密码算法

密码算法分析的方式

唯密文攻击。攻击者只能获得密文的信息，这是在公开的网络中能获得的最现实的能力

已知明文攻击。攻击者拥有某些密文以及相应的明文。对于许多弱密码系统来说，知道一些明密文对，就足以找到密钥了

选择明文攻击。攻击者有接触加密机器的机会，不能打开机器找到密钥，但可以加密大量经过精心挑选的明文，然后利用所得的密文推断密钥的信息或试图对其他密文进行解密

选择密文攻击。攻击者有接触解密机器的机会，对选择的密文进行解密操作，然后试着用所得结果推断密钥或试图对其他密文解密

密码算法分析概要

四、密码算法

针对性分析

对称密码的分析

差分类攻击和线性类攻击成为分析对称密码最有效的方法

公钥密码的分析

公钥密码的设计一般依赖于困难的数学问题，这些问题被证明或公认是实际难解的，它们可以提供正确设计的公钥密码系统理论上的安全。因此，对公钥密码的分析多集中于对底层困难问题的分析，以及上层方案实际安全性的分析

杂凑函数的分析

很多与分组密码的分析相通，主要包括差分攻击、模差分攻击、中间相遇攻击

侧信道分析

上述基于数据理论的分析，假定了封闭可信的环境，因此还有针对密码的实现方式和应用方式提出的侧信道攻击

如能量消耗、电磁辐射、运行时间等，这些无须实施入侵或破解密码算法就能分析获得密钥数据的方法，对密码算法的实际安全构成了巨大威胁

密码算法分析概要

五、密钥管理

五、密钥管理

密钥生命周期概念

是指密钥从生成到销毁的时间跨度

不同的密钥有不同的生命周期
一般而言，使用频率越高的密钥要求其生命周期尽量短

生成 → 存储 → 导入 导出 → 分发 → 使用 → 备份 恢复 → 归档 → 销毁

密钥生命周期管理管理

五、密钥管理

密钥生成

密钥生命周期的起点，所有密钥都应当直接或间接地根据随机数生成，包括利用随机数直接生成、通过密钥派生函数（KDF）间接生成
KDF一般基于对称密码算法或密码杂凑算法来构造

KDF生成密钥主要有两种情形，
在密钥协商过程中从共享秘密派生密钥，主要示例包括SM2/SM9的密钥协商和公钥加密算法中使用的基于SM3的KDF
从主密钥派生密钥，也称为密钥分散，比如大规模分发智能IC卡，发卡只保存主密钥，根据实体唯一标识和其它相关信息，从主密钥中派生出每一个实体单独的密钥

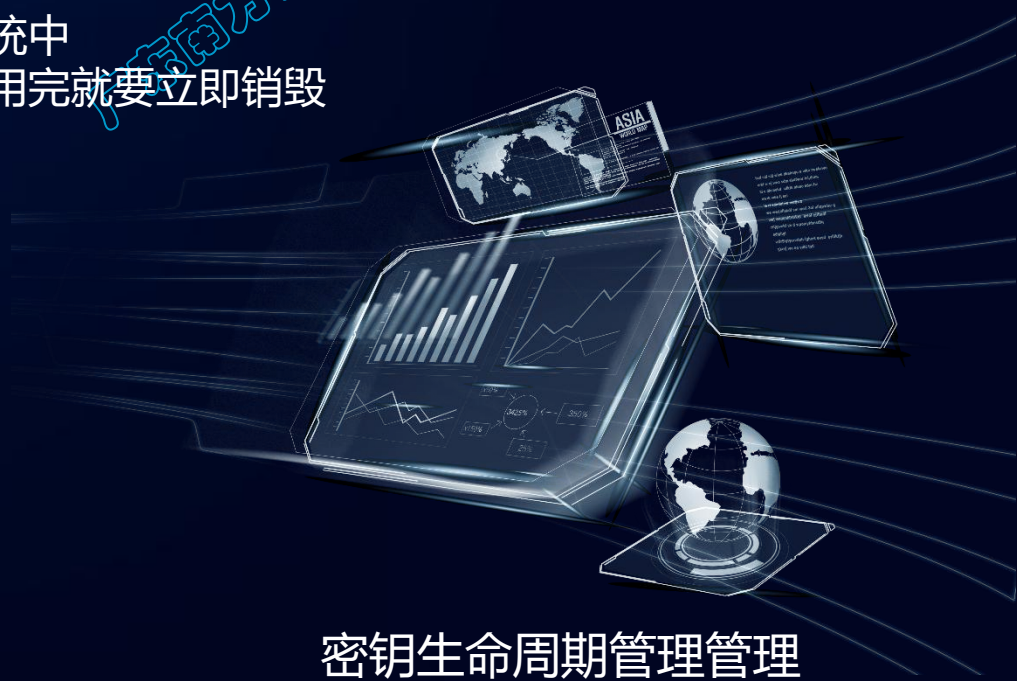
密钥生命周期管理管理

五、密钥管理

密钥存储

将密钥存储在核准的密码产品中
一般采取分层方式，下层密钥利用上层的密钥加密密钥保护，顶层的密钥加密密钥，
采取安全措施在密码产品中明文存储

在对密钥进行保密性和完整性保护后，存储在通用存储设备或系统中
并非所有密钥都需要存储，一些临时密钥或一次一密的密钥在使用完就要立即销毁



密钥生命周期管理管理

五、密钥管理

密钥导入和导出

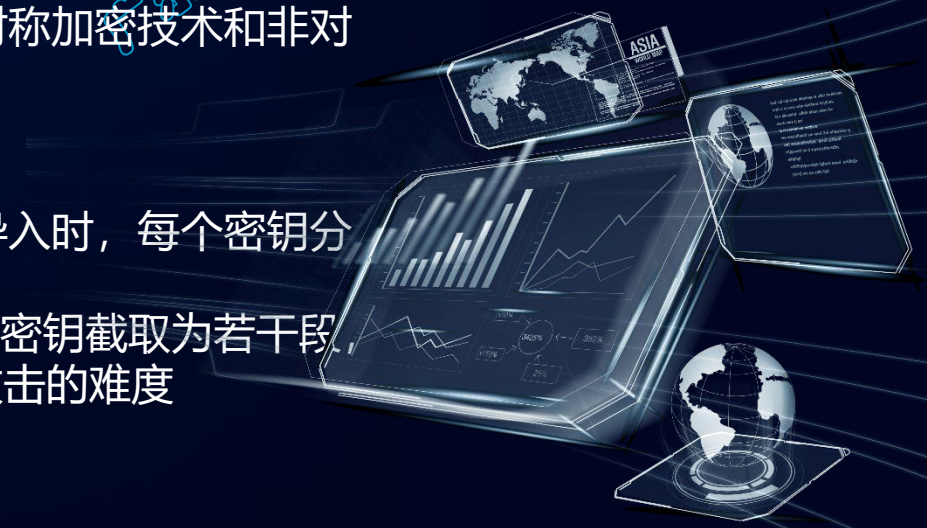
主要指密钥在密码产品中的进出
可以在同一个密码产品中进行密钥的导入和导出，用于密钥的外部存储、备份和归档
也可以将密钥从一个密码产品导出后再导入另一个密码产品，用于密钥的分发

加密传输

利用加密算法进行密钥的导入和导出是最简单和高效的方法，对称加密技术和非对称加密技术都可以完成密钥的导入和导出

知识拆分

指将密钥拆分成几个独立的密钥分量，导出到密码产品外部；导入时，每个密钥分量单独导入，最终在密码产品内部进行合成
需要注意，知识拆分不应当降低密钥的安全性，即不是简单的将密钥截取为若干段，比如将128比特的SM4拆分成两个64比特，这会极大降低穷举攻击的难度



密钥生命周期管理管理

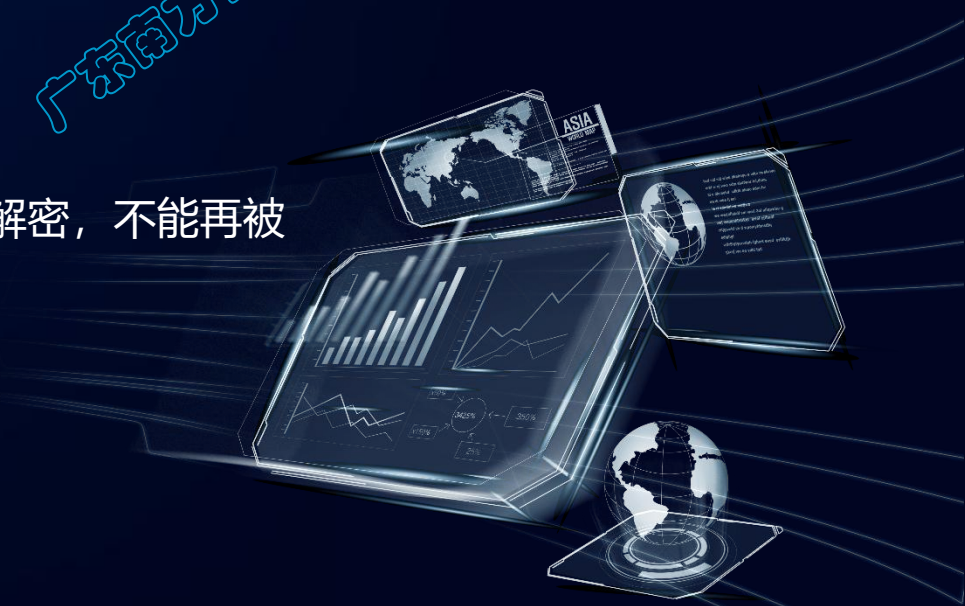
五、密钥管理

密钥分发

主要用于不同密码产品间的密钥共享
人工分发，指通过人工将密钥从一个密码产品分发到其他产品中，实现密钥共享
自动分发，借助对称密钥和公钥加密密钥等密码技术自动完成分发

密钥使用

密钥一般只能在核准的密码产品内部使用。用于核准的密码算法的解密，不能再被非核准的密码算法使用，否则可能导致密钥泄露
将一个密钥用于不同的用途，可能会降低密钥的安全性
不同用途的密钥对密钥的要求互不相同
限制密钥的用途可以降低密钥泄露时可能造成的损害



密钥生命周期管理管理

五、密钥管理

密钥的备份和恢复

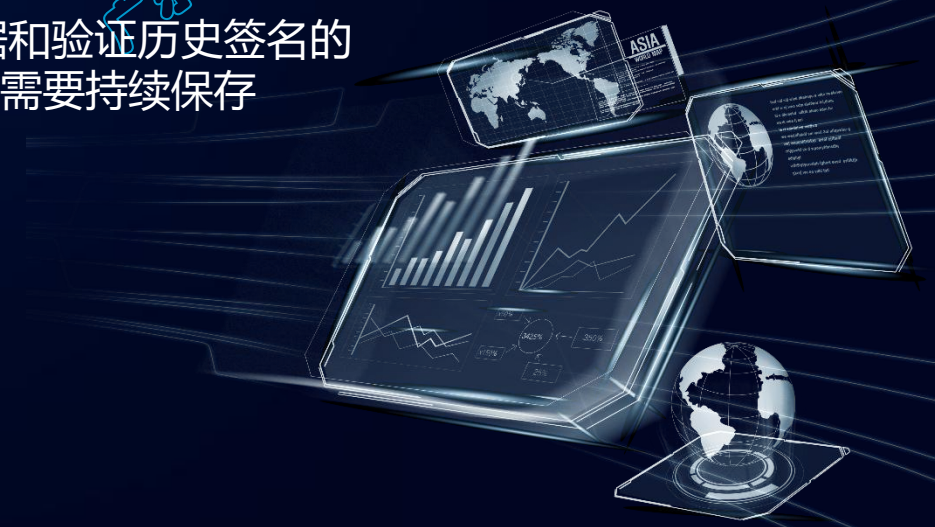
备份的主要目的是保护密钥的可用性，以防密钥的意外损坏
备份的密钥处于不激活状态，只有完成恢复后才可以激活

密钥归档

密钥在其生命周期结束时，应当进行销毁。但出于解密历史数据和验证历史签名的需要，有些密钥在生命周期外（密钥备份是在生命周期内）可能需要持续保存

密钥销毁

密钥生命周期的终点。分为正常销毁和应急销毁



密钥生命周期管理管理

五、密钥管理

典型应用

门禁系统

后台管理系统先通过密钥管理子系统生成根密钥，将其导入安全模块，在门禁卡发卡时，通过使用对称加密算法对根密钥进行密钥分散，实现一卡一密

金融系统

由于加密大部分数据的密钥需要频繁更改，例如每天或每次会话更改一次，这些密钥不适用于通过人工分发，因为代价太高。所以一般将密钥分成两类，数据密钥（DK，有时也称为会话密钥）、密钥加密密钥（KEK），前者保护数据，后者保护前者

分发有两种方式，点到点结构和基于密钥中心的结构

点到点需要手工建立KEK，因为在大型网络中变得极难处理

基于密钥中心的结构又分为两种，密钥转换中心（KTC）、密钥分发中心（KDC），前者DK由通信发起方产生，后者KD由KDC产生

对称密钥管理

五、密钥管理

公钥基础设施概念

公钥基础设施（PKI）是基于公钥密码技术实施的具有普适性的基础设施，可用于提供信息的保密性、信息来源的真实性、数据的完整性和行为的不可否认性，主要解决公钥属于谁的问题

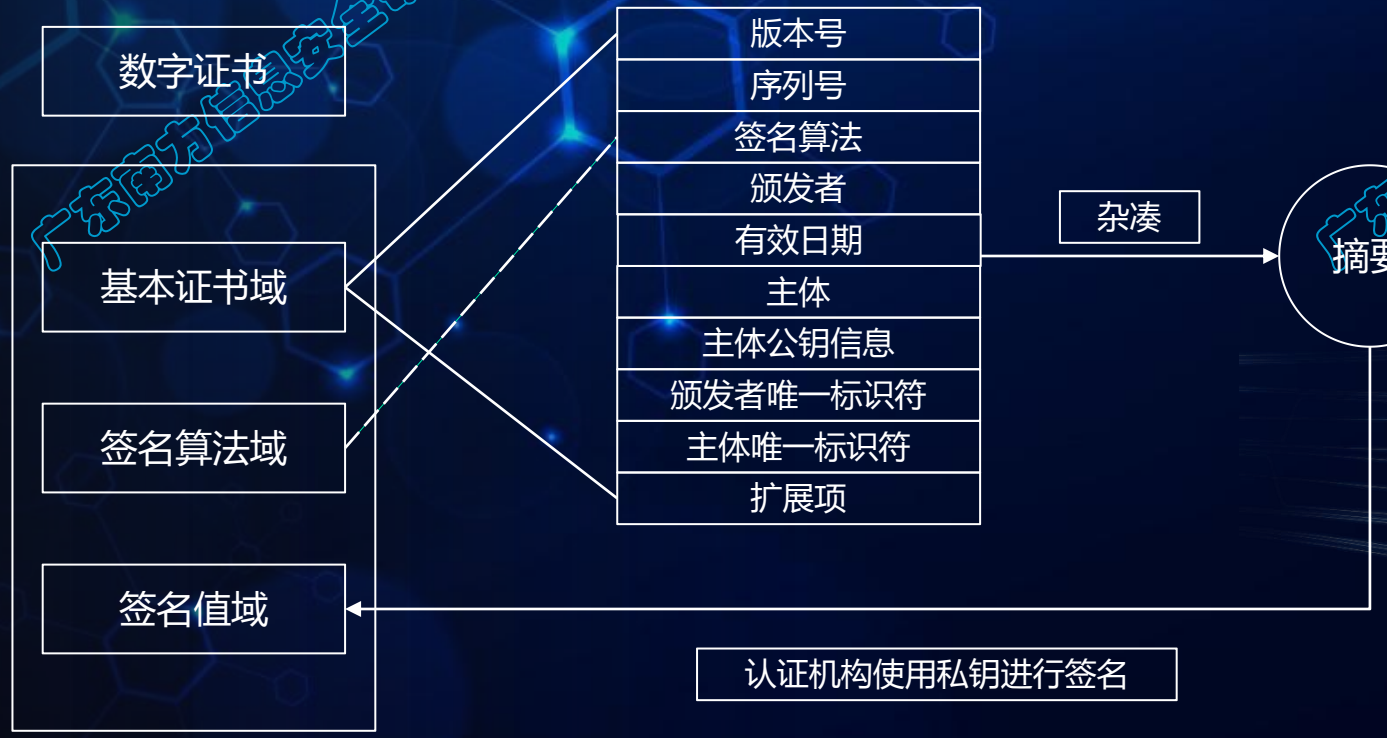
PKI系统组件
证书认证机构（CA），一个PKI可能有多级CA
证书持有者，身份信息和公钥会出现在自己证书中，也称为用户
依赖方，使用其它人的证书来实现安全功能的通信实体
证书注册机构（RA），作为CA与申请者的交互接口，专门负责检查和管理
资料库，用于实现证书分发，负责存储所有的证书
证书撤销列表，包含了当前所有被撤销的证书
在线证书状态协议，一种实时检查证书撤销状态的协议标准
轻量目录访问协议，一种开放的应用协议，提供访问控制和维护分布式信息的目录信息
密钥管理系统（KM），为PKI系统的其他实体提供专门的密钥服务

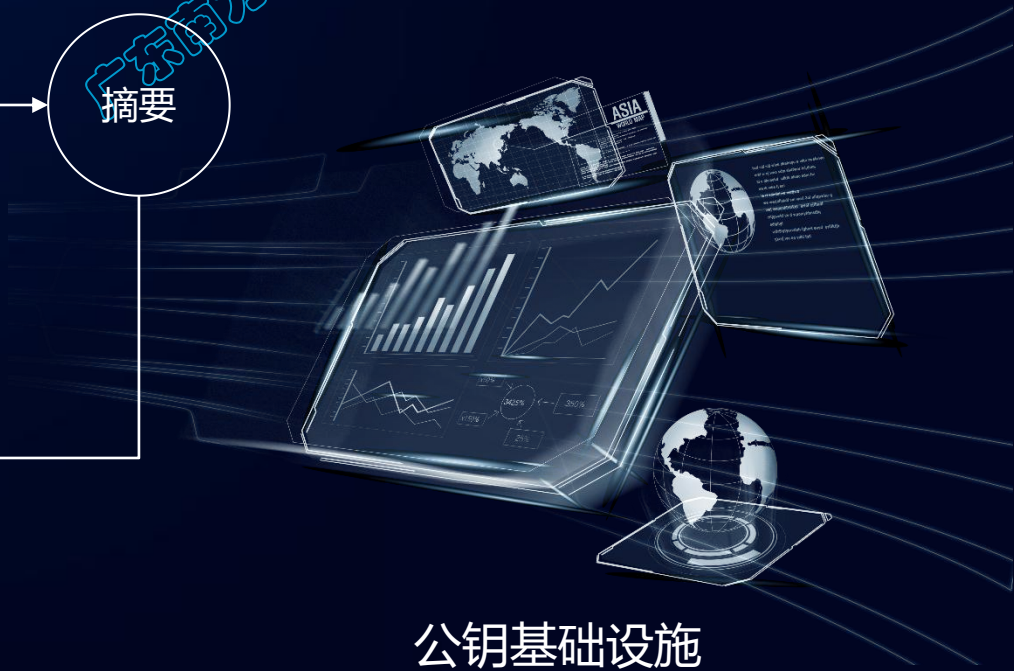
公钥基础设施

五、密钥管理

数字证书结构

数字证书也称公钥证书，包括基本证书域、签名算法域、签名值域三个域构成





公钥基础设施

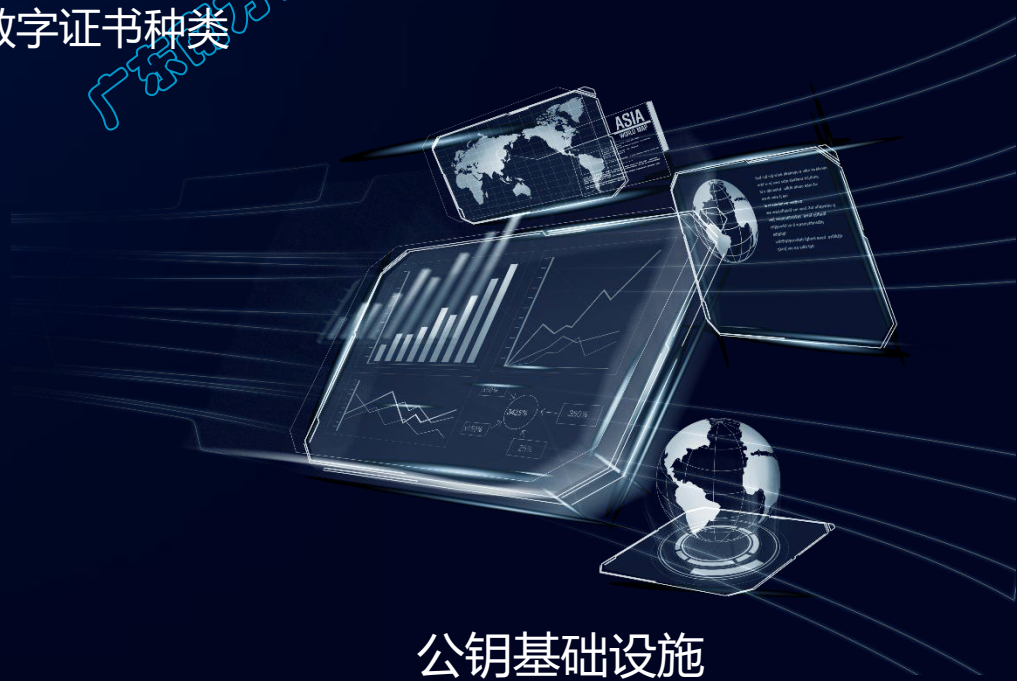
五、密钥管理

数字证书的生命周期

证书的产生
主要包括密钥生成、提交申请、审核检查和证书签发四个步骤
密钥生成，证书申请者在本地生成一个公私密钥对
提交申请，证书申请者向CA或RA提交申请材料
审核检查，CA或被授权的RA审核，判断真实性，审定可签发的数字证书种类
证书签发，包括证书的签署和证书的发布

证书的使用
证书获取、验证使用、证书存储

证书的撤销
证书的生命不一定会持续到失效日期



公钥基础设施

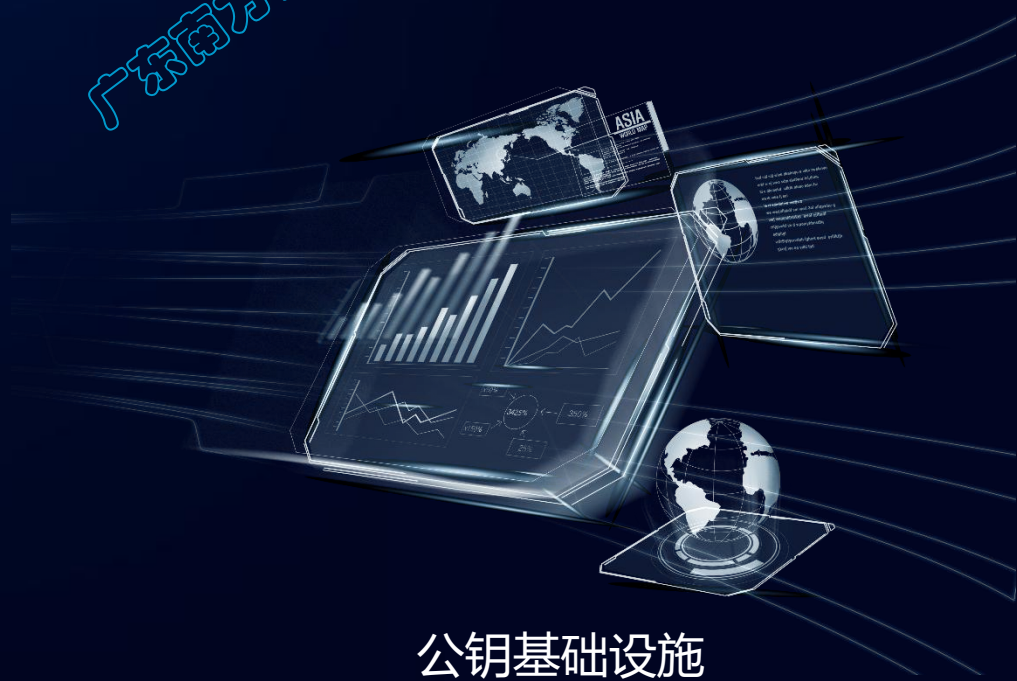
五、密钥管理

数字证书的生命周期

证书更新
需要CA签发新证书，更新后证书与原证书的内容基本一样，不同处仅在序列号、生效和失效日期

证书的归档
PKI系统必须支持对曾有数据的归档处理

双证书系统
用户同时具有两个私钥，分别称为签名私钥和加密私钥
签名私钥由用户在本地生成并专有掌握
加密私钥由可信机构生成并和用户共同掌握



公钥基础设施

六、密码协议

广东南方信息安全研究院

六、密码协议

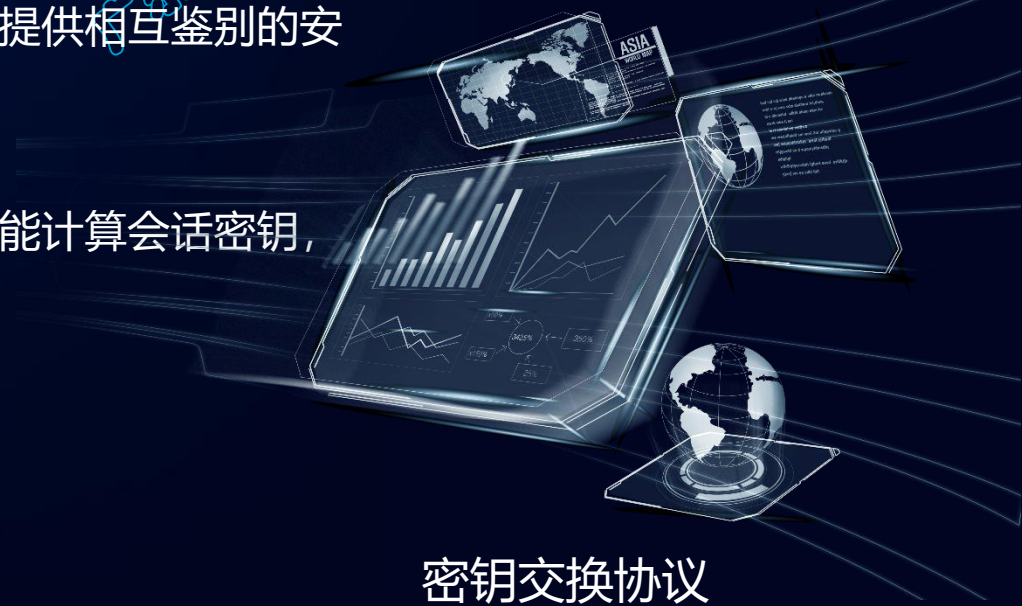
密钥交换协议概念及典型

在使用对称密码进行保密通信前，必须向通信双方分发密钥使得双方共享密钥，然而在公钥密码出现前，通信双方建立共享密钥是一个困难的问题
密钥交换协议旨在让两方或多方在不安全的信道上协商会话密钥，从而建立安全的通信信道

Diffie-Hellman协议
只能提供建立会话密钥的功能，并不能抵抗中间人攻击，也不能提供相互鉴别的安全保障

MQV协议
交互过程中用到了双方的公钥信息，只有拥有相应私钥的用户才能计算会话密钥，从而达到隐式鉴别

SM2密钥交换协议
MQV的一个变种



密钥交换协议

六、密码协议

实体鉴别协议概念及分类

用于证实某个实体就是他所声称的实体，待鉴定的实体通过表明它确实知道某个秘密来证明其身份

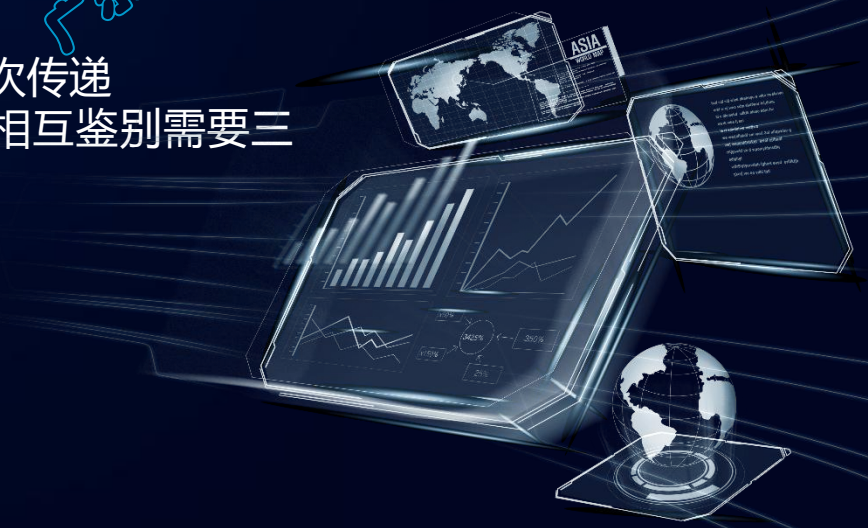
单向鉴别分为一次传递鉴别和两次传递鉴别

相互鉴别分为两次传递鉴别、三次传递鉴别和更多次传递鉴别

如果采用时间和序号，单向鉴别只需要一次传递，相互鉴别需要两次传递
如果使用随机数的“挑战-响应”方法，单向鉴别需要两次传递，相互鉴别需要三次或四次传递

一次传递鉴别，采用对称加密算法、密码校验函数、数字签名技术

两次传递鉴别，为了防止重放攻击，采用“挑战-响应”机制



实体鉴别协议

六、密码协议

综合密码协议

IPSec协议和SSL协议是两个较为综合的密码协议，支持采用多种密码技术为通信交互中的数据提供全面安全保护

IPSec协议工作在网络层

SSL协议工作在应用层和传输层

综合密码协议举例

六、密码协议

IPSec协议

它是国际组织 IETF以RFC形式公布的一组IP密码协议集，其基本思想是将基于密码技术的安全机制引入IP协议中，实现网络层的安全

它为网络层上的通信数据提供一套协议集合，包括IKE协议、认证头（AH）协议、封装安全载荷（ESP）协议和用于网络身份鉴别及加密的一些算法等

从流程上分为两个环节
IKE是第一个环节，完成通信双方的身份鉴别、确定IPSec安全策略和密钥
第二个环节是使用数据报文封装协议和IKE中协定的IPSec安全策略和密钥，实现对通信数据的安全传输

AH和ESP协议可以工作在传输模式或隧道模式下，
传输模式一般用于端到端的应用场景，只有IP载荷部分被保护，对IP头不做改动
隧道模式对整体IP数据报文提供加密和认证功能，并在此基础上添加新的IP头，一般用于创建虚拟专用网（VPN）隧道链路

综合密码协议举例

六、密码协议

IPSec协议

IKE协议
IKE协议用于鉴别通信双方身份、创建安全联盟（SA）、协商加密算法以及生成共享会话密钥等，
SA是IPSec的基础，协定的内容包括数据封装协议、IPSec工作模式、密码算法等安全策略和密钥
SA是单向的，一个SA为单一通信方向上传输的数据提供一种安全服务，若使用多个服务保护数据流，应该创建多个SA来分别实现不同服务

ISAKMP是IKE的核心协议，其核心功能是创建和维护SA
分为两个阶段，
第一阶段是主模式，即新建ISAKMP，并实现身份鉴别和密钥交换，得到工作密钥（用于保护二阶段协商过程）
主模式是一个身份保护的交换
第二阶段是快速模式，使用以建的ISAKMP提供保护，实现通信双方的IPSec SA的协商，确定安全策略和会话密钥
会话密钥有两个，分别用于通信数据加密，以及完整性校验和数据源身份鉴别

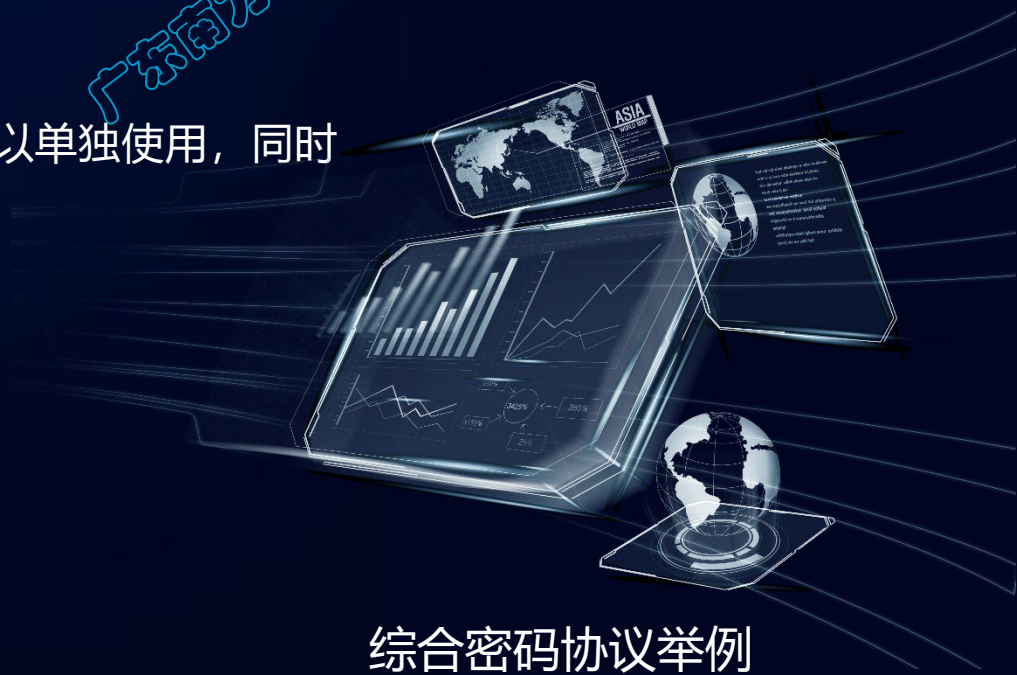
综合密码协议举例

六、密码协议

IPSec协议

AH协议
提供数据源身份鉴别、完整性和抗重放等安全功能，不提供任何保密性服务
AH使用MAC对IP数据报文进行认证，最常用的是HMAC

ESP协议
与AH相比，增加了对数据报文的加密功能
ESP可以与AH结合使用，由AH提供数据源身份鉴别服务，也可以单独使用，同时选择保密性和数据源身份鉴别服务



综合密码协议举例

六、密码协议

SSL协议

它是网景通信公司在推出Web浏览器时提出的，旨在保证经Web传输的重要或敏感数据的安全性，是由多协议组成的两层协议集合，工作于应用层和传输层之间

上层有4个协议
握手协议，实现了服务端和客户端之间的相互身份鉴别、交互过程中密码套件（密码算法的集合）与密钥的协商
密码规格变更协议，用于通知对方其后的通信消息将用刚刚协商的密码规格及相关联的密钥来保护
报警协议，用于关闭连接的通知，以及对整个连接过程中出现的错误进行报警
HTTP，可为超文体传输协议提供安全服务

下层是记录层协议
发挥了SSL“承上启下”的作用

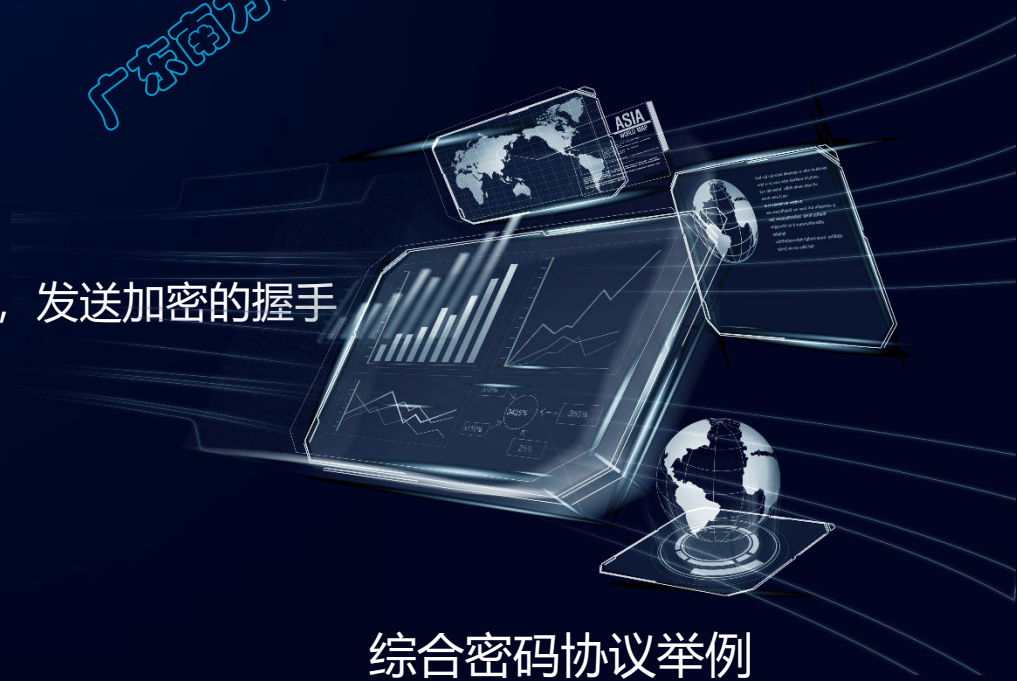
综合密码协议举例

六、密码协议

SSL协议

握手协议
主要作用有两点
一是通信双方对彼此进行身份鉴别
二是协商连接会话所需的密码参数（密码算法和密钥）

四步工作流程
客户端向服务端发送Hello消息，服务端回应Hello消息
身份鉴别和密钥交换
若服务端发送一个证书请求消息，客户端必须返回一个证书消息
客户端发送密码规格变更消息，并立即使用刚协商的算法和密钥，发送加密的握手结束消息



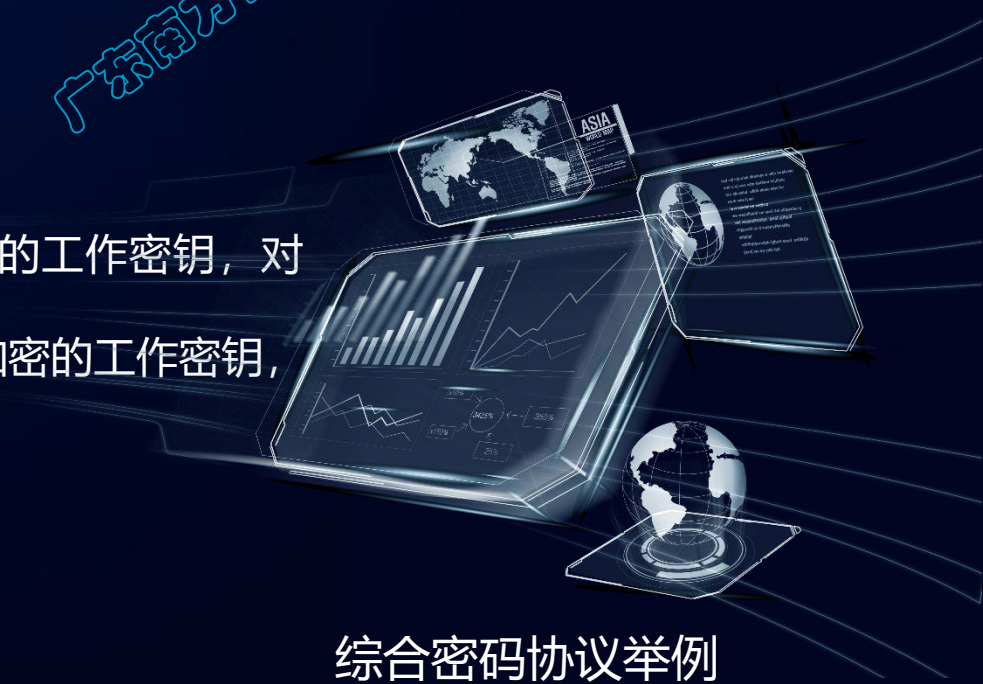
综合密码协议举例

六、密码协议

SSL协议

记录层协议
当客户端和服务端握手成功后，待传输的应用数据通过记录层协议封装，并得到保密性和完整性保护，接收到这些信息的实体要将该过程逆向执行一遍，从而获取原始数据

五步工作流程
数据分段
数据压缩
数据添加MAC，使用握手协议中协定的密码杂凑算法和用于校验的工作密钥，对每块明文计算MAC
对数据和MAC加密，使用握手协议中协定的对称密码算法和用于加密的工作密钥，对压缩数据和与之相关的MAC进行加密
附加SSL记录报头



综合密码协议举例

七、密码功能实现示例

七、密码功能实现示例

保密性

完整性

真实性

不可否认性

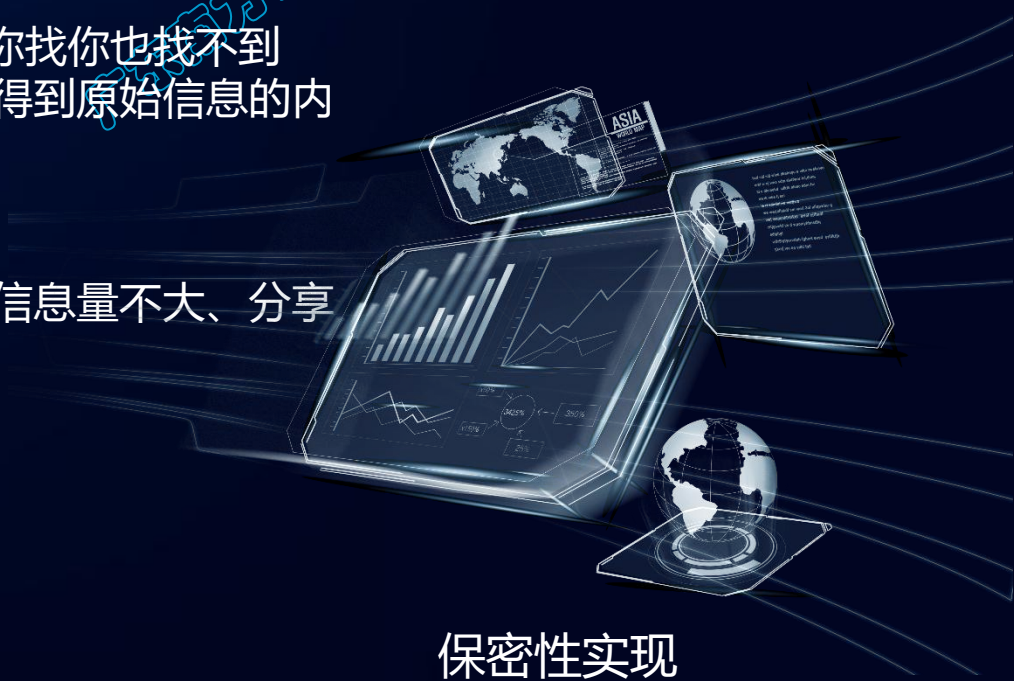
七、密码功能实现示例

保密性实现目的和方法

目的是避免信息泄露或暴露给未授权的实体

有三种基本方法
一是访问控制，防止敌手访问敏感信息，简单说，就是不让你找
二是信息隐藏，避免敌手发现敏感信息的存在，简单说，就是让你找你也找不到
三是信息加密，允许敌手观测到信息的表示，但是无法从表示中得到原始信息的内容或提炼出有用的信息，简单说，就是找到了你也看不懂
其中加密，是实现保密性的主要机制

公钥密码技术加密和解密方式灵活，但计算成本高，主要应用于信息量不大、分享方式复杂的信息保密性保护，如密钥协商或加密传输
对称密码技术，主要应用于大量信息传输或存储的保密性保护
公钥密码技术可以为对称密码应用提供密钥协商或安全传输支撑



保密性实现

七、密码功能实现示例

完整性实现的目的和方法

数据完整性保护的目的在于保护信息免受非授权实体的篡改或替代
包括有意或无间的损坏

有两种基本方法
一是访问控制，限制非授权实体修改被保护的数据
二是损坏-检测，这种方法无法避免数据损坏，但能确保这些损坏能够被检测出来，并能够被纠正或报警

消息鉴别码实现完整性
对称密码和杂凑算法都可以用于消息鉴别码的生成，只确保完整，不能防止伪造

数字签名实现完整性
基于公钥密码的数字签名，既实现完整性，还能实现不可否认性

完整性实现

七、密码功能实现示例

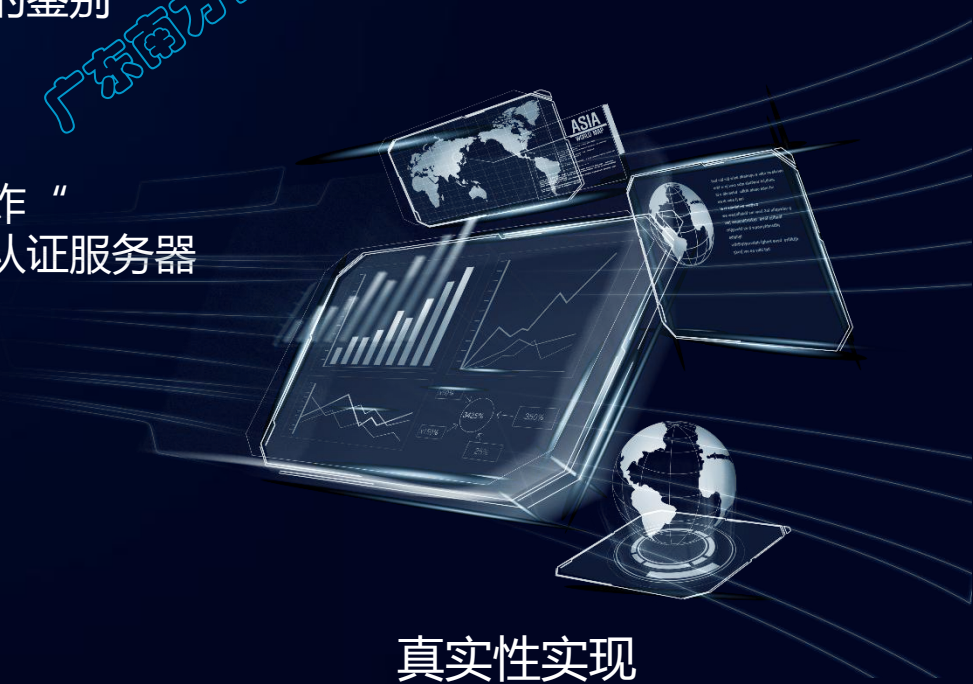
真实性实现的基本方法

实现信息来源真实性的核心是鉴别

基于密码技术的鉴别机制
基于声称者知道某一秘密密钥这一事实，实现验证者对声称者身份的鉴别

最简单的方法是声称者和验证者共享一个对称密钥

但如果每一对声称者和验证者都共享一对密钥，将会导致“密钥爆炸”
这个问题可以引入认证服务器来解决，包括在线认证服务器和离线认证服务器



真实性实现

七、密码功能实现示例

鉴别机制

基于静态口令的鉴别机制

静态口令或者个人识别码（PIN）是最常用的鉴别信息之一，也是很多人口中的“密码”

直接使用口令鉴别有许多脆弱点，最严重的是外部泄露和口令猜测，以及窃听、重放攻击，用密码技术可以有效提升口令鉴别过程中的安全性，主要在口令传输过程中的进行保护

基于动态口令的鉴别机制

动态口令的使用主要用于抵抗重放攻击

声称者拥有一个存储秘密值的动态令牌，采用密码算法，将秘密值、时间戳和其他一些信息作为输入，计算动态口令

基于生物特征的鉴别机制

与静态口令面临的问题相同，也容易受到窃听和重放攻击，所以一般不直接用于远程鉴别，而只用于设备对自然人的鉴别，身份验证后，设备再使用密码技术与应用服务器进行安全交互

真实性实现

七、密码功能实现示例

不可否认性实现的基本方法

使用不可否认功能，虽然不能防止通信参与方否认通信交换行为的发生，但是能够在产生纠纷时提供可信证据，有利于纠纷解决，主要通过数字签名技术来实现

起源的不可否认

使用发起者的数字签名
发起者对要保护的数据用自己的私钥进行签名，并将其发给接收者，签名就是不可否认证据的主要内容
使用可信第三方数字签名
可信第三方可以作为发起者的担保，发起者把数据传递给可信第三方，由第三方签名

不可否认性实现

七、密码功能实现示例

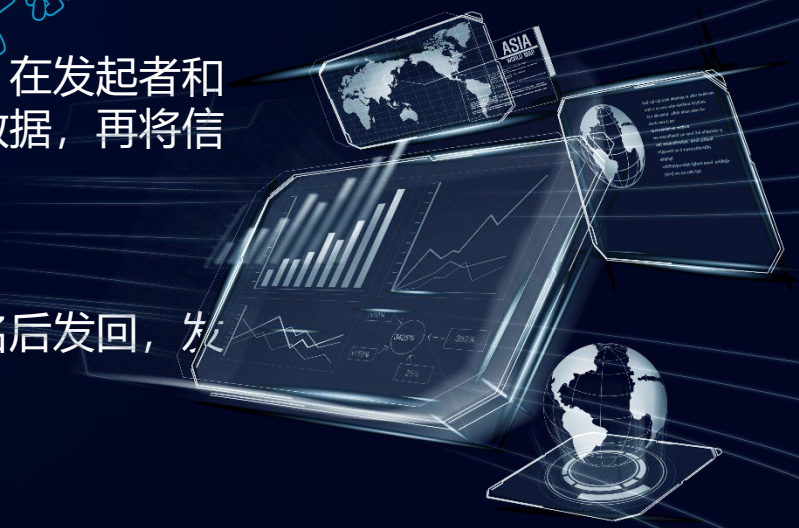
不可否认性实现的基本方法

传递的不可否认

使用接收者的数字签名
接收者收到消息后，产生一个确认信息送回给发起者

使用可信传递代理
接收者签名不能防止接收者阅读了信息内容但是拒绝生成证明的情况，在发起者和接收者之间介入一个可信传递代理，代理接到信息首先生成不可否认数据，再将信息转发给接收者

使用两阶段传递
发送者在发送消息之前，先发送一个预接收消息给接收者，接收者签名后发回，发送者再将完整消息发给接收者，接收者再进行签名回传



不可否认性实现


谢谢聆听