同济区块链研究院
Tongji Blockchain Research Institute

国密介绍

同济区块链研究院

陈序

2021. 10. 30

Agenda

1.什么是国密算法

2.国密算法与国际算法区别

3.部分国密算法介绍

4.国密算法常见使用场景

Agenda

1.什么是国密算法

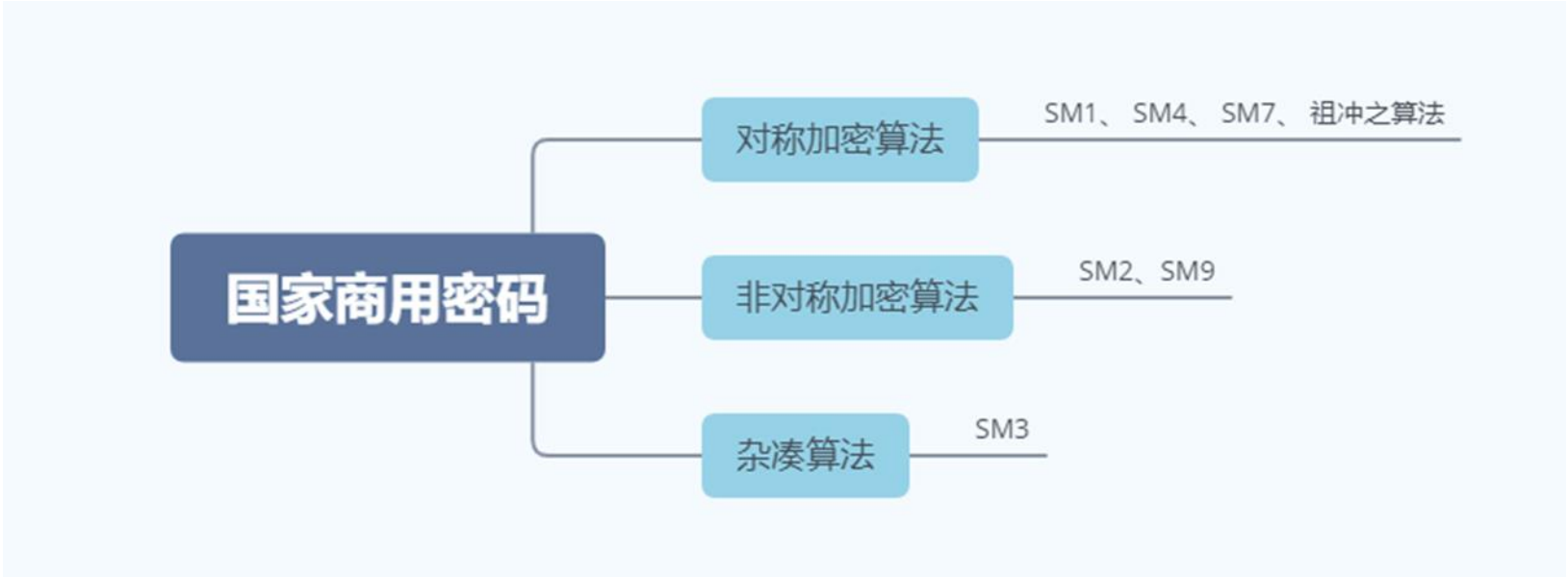
2.国密算法与国际算法区别

3.部分国密算法介绍

4.国密算法常见使用场景

什么是国密

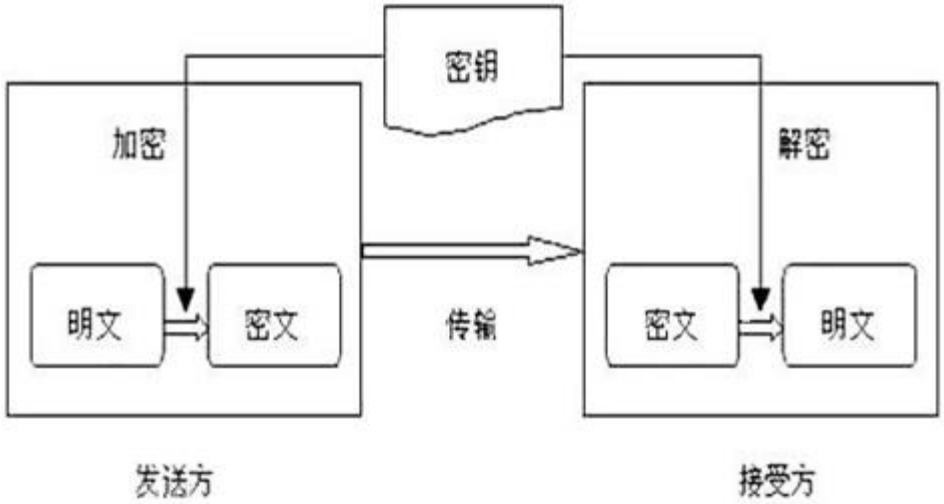
国密即国家密码局制定标准的一系列国产密码算法，其中包括了对称加密算法、椭圆曲线非对称加密算法、杂凑算法，具体包括SM1，SM2，SM3，SM4、SM9等算法。



对称加密算法

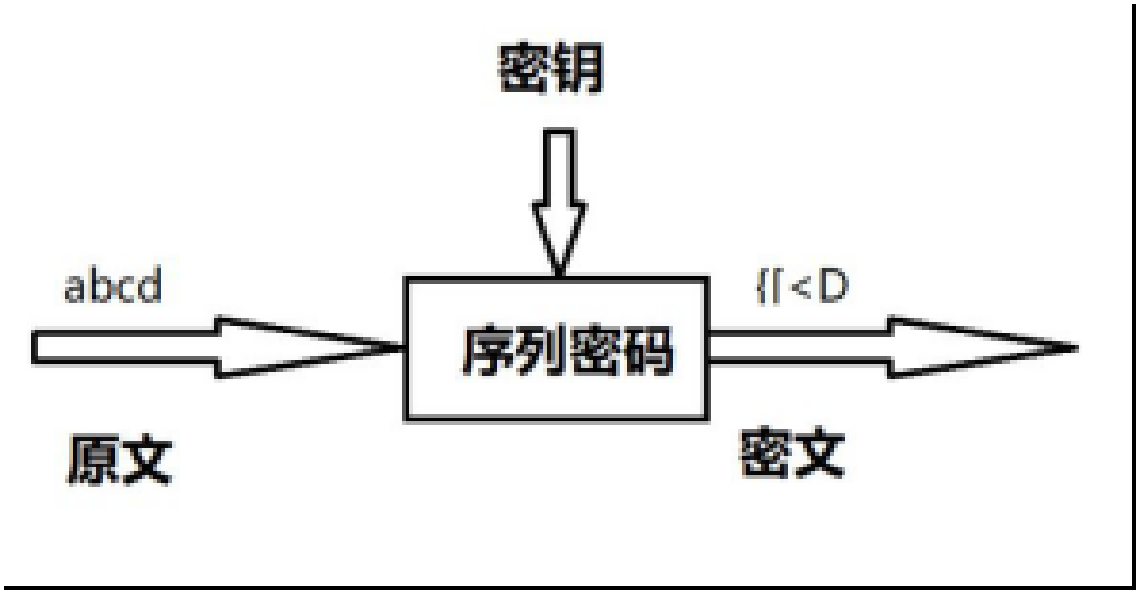
对称加密：采用单钥密码系统的加密方法，同一个密钥可以同时用作信息的加密和解密，也称为单密钥加密。

有序列加密、分组加密两种分类。



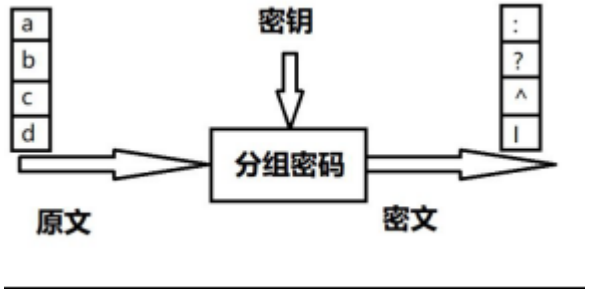
对称加密算法

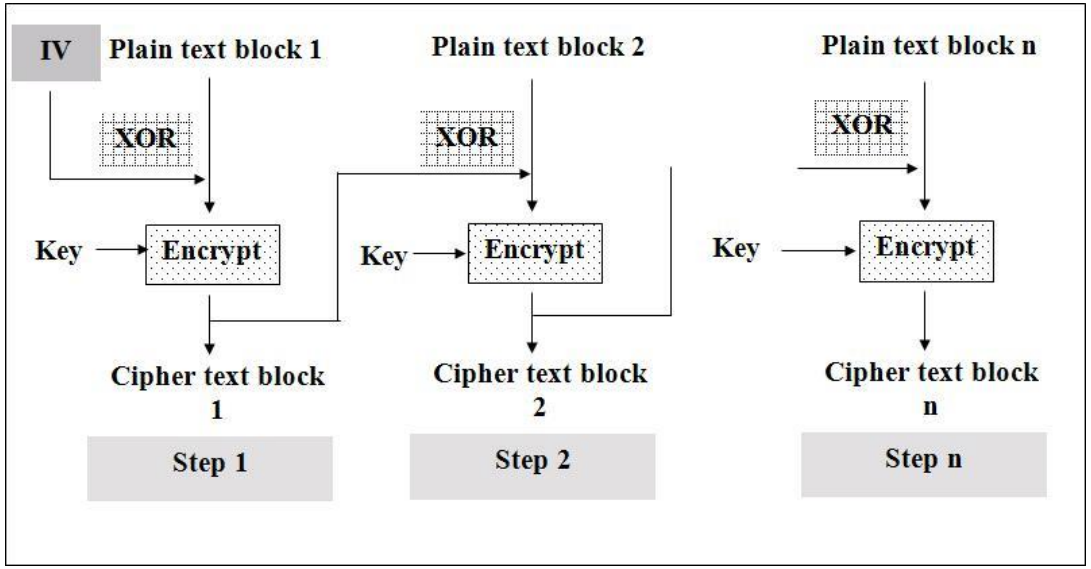
序列密码：用一个随机序列（**密钥流**）与明文序列按位叠加产生密文，用同一随机序列与密文序列叠加来恢复明文。又称流密码。



对称加密算法

分组密码：将原文消息分割成固定长度片段的对称密钥密码。又称块密码。有ECB,CBC,CFB,OFB等算法模式。





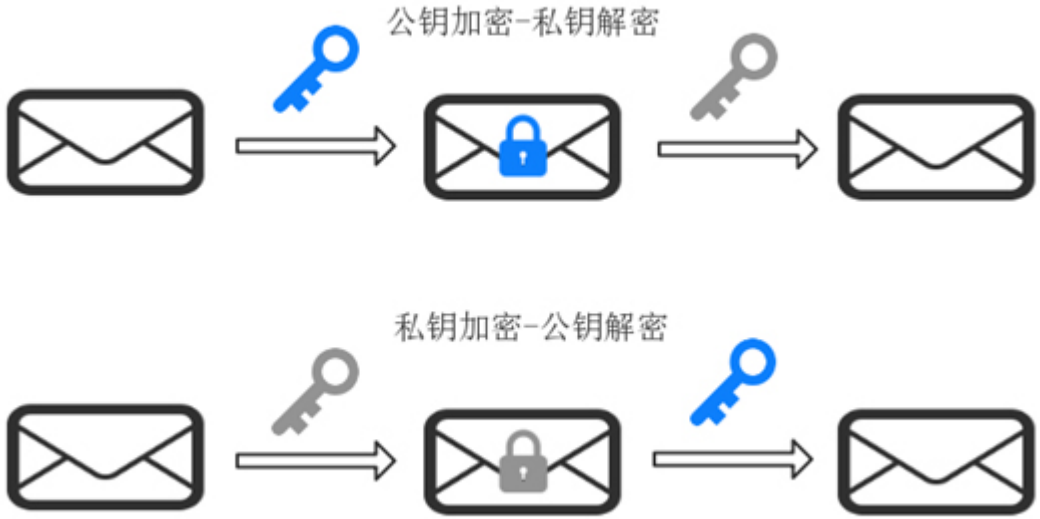
非对称加密算法

非对称加密算法：加密和解密使用的是两个不同的密钥。

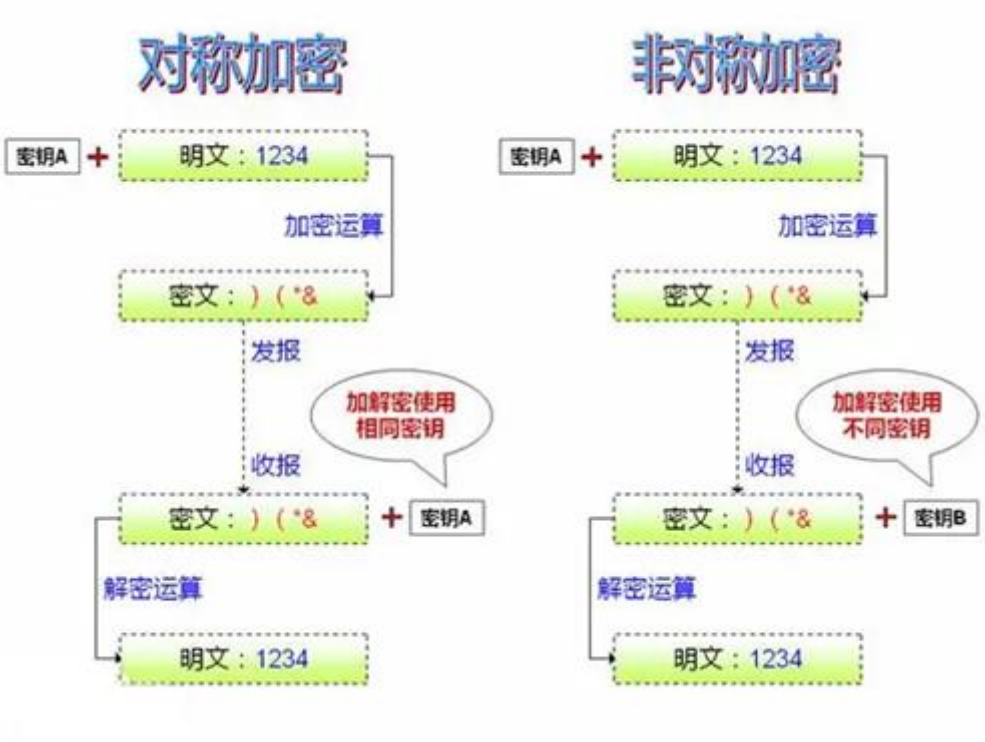
公开密钥（publickey:简称公钥）。

私有密钥（privatekey:简称私钥）。

非对称加密算法



非对称加密算法

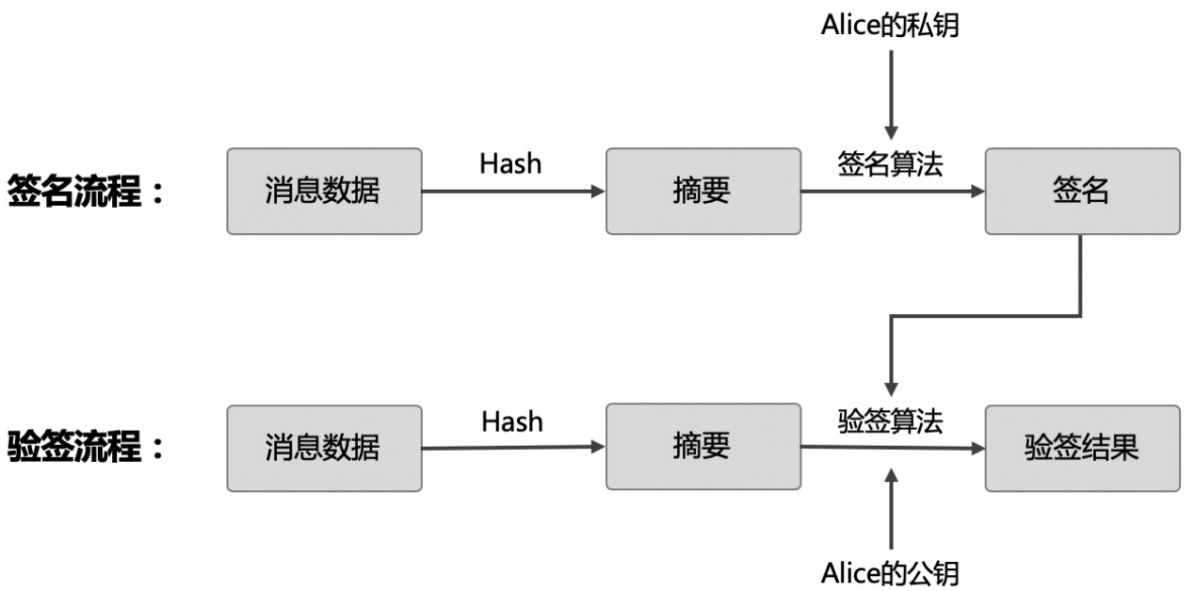

对称加密
密钥A
明文：1234
加密运算
密文：）（*&
发报
加解密使用
相同密钥
收报
密文：）（*&
密钥A
解密运算
明文：1234
非对称加密
密钥A
明文：1234
加密运算
密文：）（*&
发报
加解密使用
不同密钥
收报
密文：）（*&
密钥B
解密运算
明文：1234

数字签名

数字签名（又称公钥数字签名）是只有信息的发送者才能产生的别人无法伪造的一段数字串，这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明。

数字签名的全过程分两部分，签名与验证。

数字签名


Alice的私钥
签名流程：
消息数据
Hash
摘要
签名算法
签名
验签流程：
消息数据
Hash
摘要
验签算法
验签结果
Alice的公钥

杂凑算法

杂凑算法（Hash Function）是指把任意长的输入消息串变化成固定长的输出串的一种算法。又称哈希（Hash）算法，散列函数。

用于产生消息摘要，密钥加密等.

杂凑算法

表 11.1　密码学 Hash 函数 H 的安全性需求

需　求	描　述
输入长度可变	H 可应用于任意大小的数据块
输出长度固定	H 产生定长的输出
效率	对任意给定的 x，计算 $H(x)$ 比较容易，用硬件和软件均可实现
抗原像攻击（单向性）	对任意给定的 Hash 码 h，找到满足 $H(y)=h$ 的 y 在计算上是不可行的
抗第二原像攻击（抗弱碰撞性）	对任何给定的分块 x，找到满足 $y \neq x$ 且 $H(x)=H(y)$ 的 y 在计算上是不可行的
抗碰撞攻击（抗强碰撞性）	找到任何满足 $H(x)=H(y)$ 的偶对 (x,y) 在计算上是不可行的
伪随机性	H 的输出满足伪随机性测试标准

弱Hash函数：只满足以上前五个要求的Hash函数。

强Hash函数：满足以上前六个要求的Hash函数。

密码学算法

杂凑算法

不可逆，通过哈希值很难逆向推导出原数据

无冲突，原始输入不同，哈希值也不相同

计算速度快，同一算法其哈希值长度统一

典型算法：MD5，SHA，SM3

签名算法

保证信息传输的完整性

发送者的身份认证

防止抵赖发生

同属公钥体系，私钥签名，公钥验证

对称密码算法

加解密方共用一个密钥

加/解密速度快，但密钥分发比较困难

典型算法：DES，AES，SM4

非对称密码算法

通讯双方各有一对密钥（公钥和私钥）

公钥可以公开，分发给任何人

私钥保密，严格保存

公钥加密，只能用私钥解密

加/解密速度较慢，但无密钥分发问题

典型算法：RSA，ECC，SM2

Agenda

1.什么是国密算法

2.国密算法与国际算法区别

3.部分国密算法介绍

4.国密算法常见使用场景

国密与国际算法的区别

国密即国家密码局认定的国产密码算法，即国家商用密码。商用密码用于保护不属于国家秘密的信息，公民、法人和其他组织可以依法使用商用密码保护网络与信息安全。

国际算法是美国的安全局发布，是现今最通用的商用算法。

对称加密算法对比

对称加密算法	AES	国密SM4	3DES
计算结构	数据块长度和密钥长度都可变的分组加密RIJNDAEL算法	基本轮函数加迭代，含非线性变换	使用标准的算法和逻辑运算，先替换后置换，不含非线性变换
计算轮数	10/12/14轮	32轮	16*3轮
分组长度	128/192/256位	128位	64位
密钥长度/有效密钥长度	128位/112位	128位/128位	128位/112位
实现性能	软件、硬件实现都较快	软件、硬件实现都较快	软件慢、硬件快
安全性	较高	较高	较高

非对称加密算法对比

非对称加密算法（公钥算法）	ECC/国密SM2	RSA
计算结构	基于椭圆曲线	基于特殊的可逆模幂运算
计算复杂度	完全指数级	亚指数级
相同的安全性能下所需公钥位数	较少（160位ECC与1024位RSA具有相同安全等级）	较多
密钥生成速度	较RSA算法快100倍以上	慢
加解密速度	较快	一般
安全性难度	基于离散对数问题ECDLP数学难题	基于分解大整数的难度

杂凑算法对比

杂凑算法	国密SM3	SHA256
算法结构	Merkle-Damgard结构	基于特殊的可逆模幂运算
消息长度	2^64位	<2^64位
分组长度	512位	512位
摘要长度	256位	256位
计算步骤	64步	64步
加密速度	快	快

国密算法与国际算法对比

类型	国际算法	国密算法
对称加密算法	DES、AES	SM4
非对称加密算法（公钥密码算法）	RSA、ECDSA、ECDH	SM2
杂凑算法（消息摘要算法）	SHA256、MD5	SM3
传输层安全协议	TLS,SSL协议	TLS1.3-国密单证书（RFC8998） GM/T 0024和TLCP国密双证书TLS协议
数字证书	SHA-RSAEncrypt	SM2-with-SM3

Agenda

1.什么是国密算法

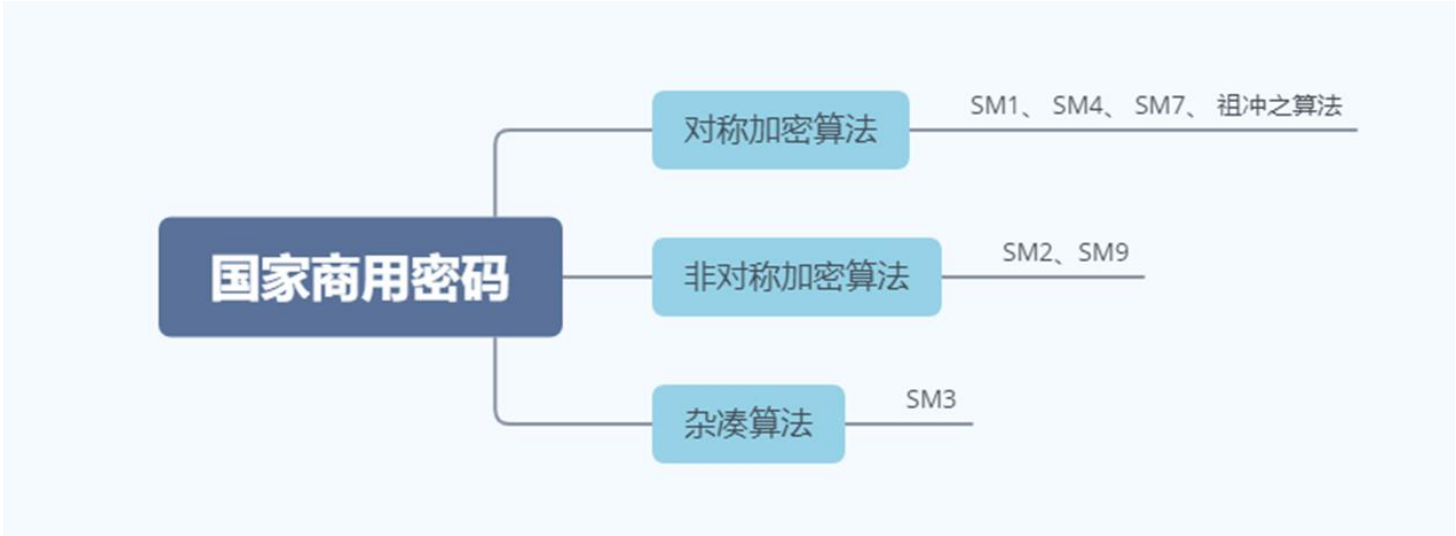
2.国密算法与国际算法区别

3.部分国密算法介绍

4.国密算法常见使用场景

对称加密算法

其中SM1、SM7算法不公开，调用该算法时，需要通过加密芯片的接口进行调用；



SM2

SM2算法由国家密码管理局于2010年12月17日发布，全称为椭圆曲线公钥密码算法，包括SM2-1椭圆曲线数字签名算法，SM2-2椭圆曲线密钥交换协议，SM2-3椭圆曲线公钥加密算法，分别用于实现数字签名密钥协商和数据加密等功能。

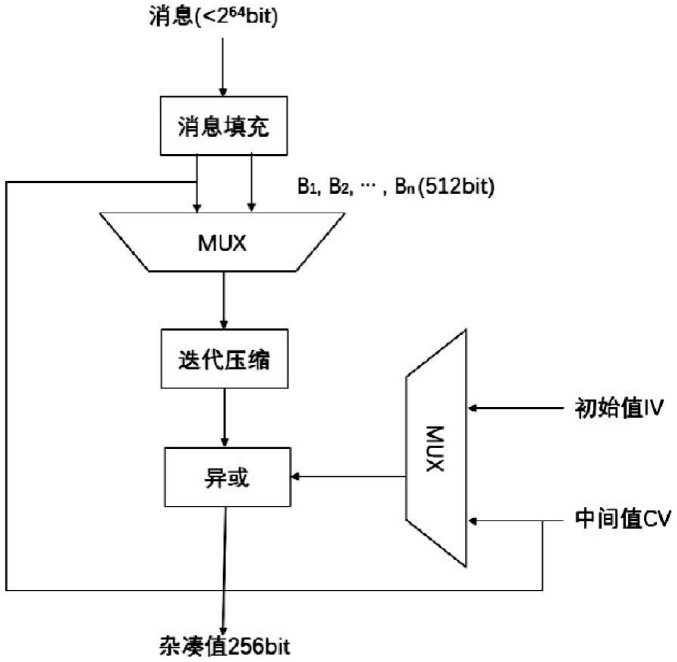
SM2算法与RSA算法一样，同属于非对称算法体系，是属于椭圆曲线加密（ECC）算法的一种，但与RSA算法不同的是RSA算法是基于大整数分解数学难题，SM2算法是基于椭圆曲线上点群离散对数难题。

相对于RSA算法，SM2算法具有以下优点：

- 安全性高。192位的SM2密码强度已经比RSA 2048位密码强度要高。
- 存储空间小。SM2算法的密码一般使用192－256位，RSA算法密码一般需要使用2048－4096位。
- 速度快。SM2在私钥运算上，速度远比RSA快得多。

SM3

SM3 算法是中国国家密码管理局在2010年公布的中国商用密码杂凑算法标准。



SM4

SM4算法是由国家密码管理局于2006 年1 月公布的用于用于实现数据的加密/解密运算的分组对称密码算法,是我国官方公布的第一个商用分组密码算法,SM4算法的密钥空间包含2128个密钥,数量庞大,破解难度大,算法安全性高。

SM9

SM9是国家密码管理局于2016年3月28日发布的一种标识密码标准，主要用于用户的身份认证。

SM9基于256位的BN椭圆曲线，使用素域 Fp 和有限域 Fp2 ， 双线性对使用R-ate。

SM9算法主要包括密钥部分和算法部分。

- 密钥部分：包括主密钥对(公钥和私钥)和用户私钥。
- 算法部分：包括签名验签算法、密钥封装解封算法、加密解密算法和密钥交换算法。

SM9—算法部分

SM9算法包括**签名验签**、**密钥封装解封**、**加密解密**和**密钥交换**四大部分。

- 签名算法：使用签名主公钥和签名者的签名私钥给数据签名。
- 验签算法：使用签名主公钥和签名者ID验证签名。
- 密钥封装算法：使用加密主公钥和密钥解封者(使用对称密钥的另一方)ID封装一个对称密钥。
- 密钥解封算法：使用加密主公钥和密钥解封者ID解出封装了的对称密钥。
- 加密算法：使用加密主公钥和解密者ID加密数据。
- 解密算法：使用解密者的加密私钥和解密者ID解密数据。
- 密钥交换算法：密钥交换双方使用加密主公钥、自己的加密私钥和双方的ID协商出一个共享密钥。

Agenda

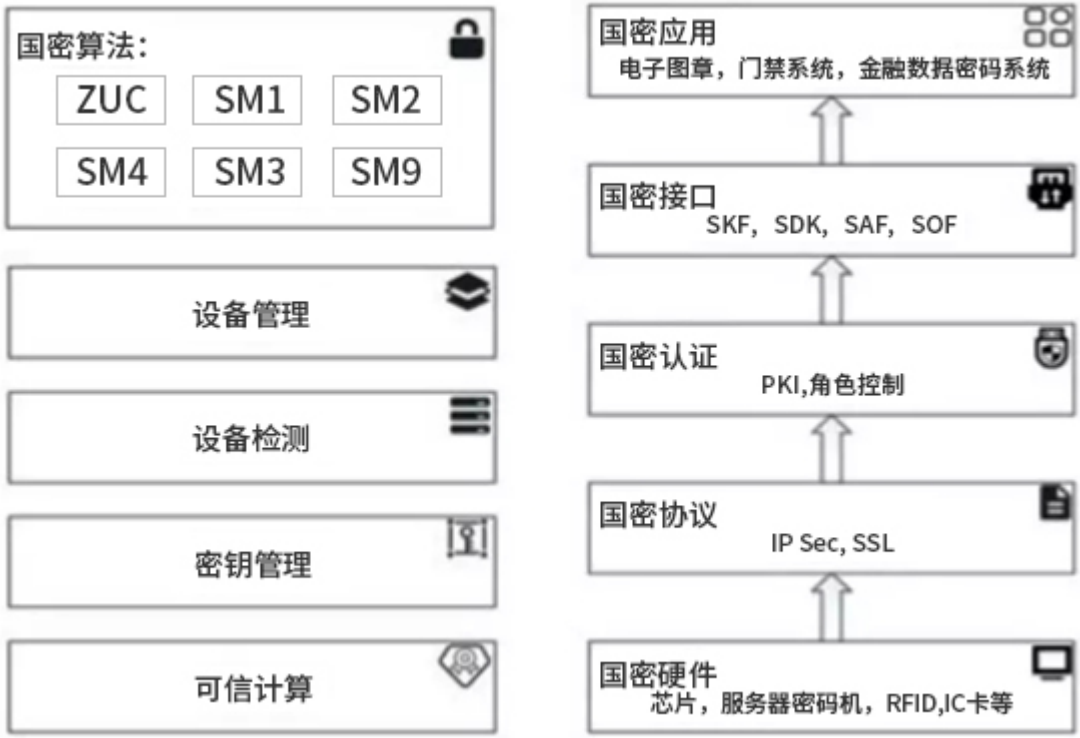
1.什么是国密算法

2.国密算法与国际算法区别

3.部分国密算法介绍

4.国密算法常见使用场景

国密标准体系


国密算法:
ZUC
SM1
SM2
SM4
SM3
SM9
设备管理
设备检测
密钥管理
可信计算
国密应用
电子图章，门禁系统，金融数据密码系统
国密接口
SKF，SDK，SAF，SOF
国密认证
PKI,角色控制
国密协议
IP Sec, SSL
国密硬件
芯片，服务器密码机，RFID,IC卡等

国密常见使用场景

商用密码的应用领域十分广泛，主要用于对不涉及国家秘密内容但又具有敏感性的内部信息、行政事务信息、经济信息等进行加密保护。比如：商用密码可用于企业门禁管理、企业内部的各类敏感信息的传输加密、存储加密，防止非法第三方获取信息内容；也可用于各种安全认证、网上银行、数字签名等。

●在门禁应用中，采用SM1算法进行身份鉴别和数据加密通讯，实现卡片合法性的验证，保证身份识别的真实性。

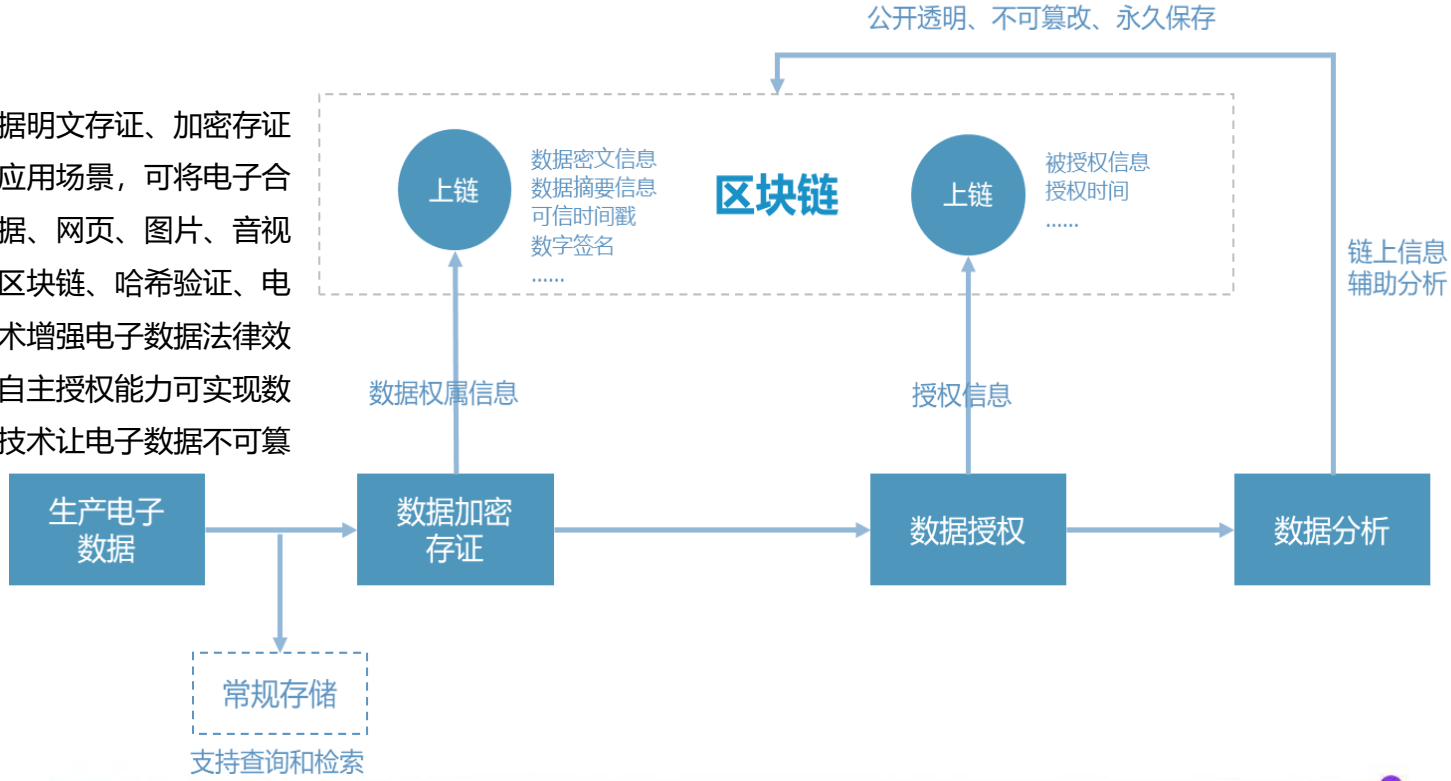
●SM3算法适用于商用密码应用中的数字签名和验证，消息认证码的生成与验证以及随机数的生成，可满足多种密码应用的安全需求。

●SM9算法不需要申请数字证书，适用于互联网应用的各种新兴应用的安全保障。如基于云技术的密码服务、电子邮件安全、智能终端保护、物联网安全、云存储安全等等。这些安全应用可采用手机号码或邮件地址作为公钥，实现数据加密、身份认证、通话加密、通道加密等安全应用，并具有使用方便，易于部署的特点，开启了普及密码算法的大门。

数据存证

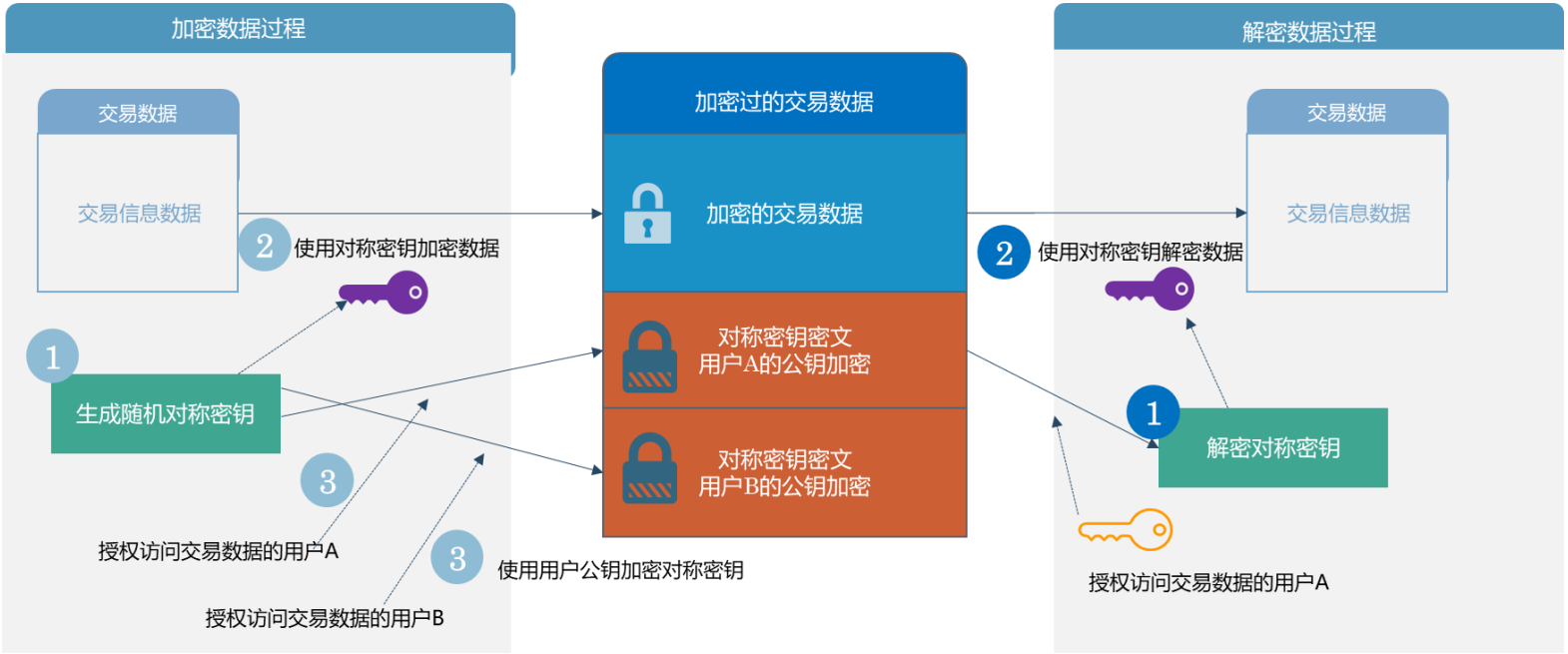
电子数据安全存证

区块链底层实现了电子数据明文存证、加密存证及授权功能，适用于多种应用场景，可将电子合同、电子协议、订单、票据、网页、图片、音视频等信息进行存证，通过区块链、哈希验证、电子签名、可信时间戳等技术增强电子数据法律效力；结合智能合约和数据自主授权能力可实现数据的共享和交易，区块链技术让电子数据不可篡改成为可能



数据加密存证

- 确保数据仅授权方可见
- 使用“对称加密和公钥加密”相结合的方式，只有授权用户能够用自己的私钥解密受保护的数据



国密在区块链中的改造

它更安全，国密对应的几个算法总体来说都比国际算法安全性更高。
它更规范，在政府及行业提出的区块链密码应用技术要求中，都提到需要支持国密算法。
基于国密改造的前两个优势：更安全、更规范，同时使用国家自主可控的算法，面对客户时更自信。

(1) 用 SM3 代替 SHA-256等作为默认的密码杂凑算法；

(2) 用 SM2 替代 ECDSA 签名算法；

(3) 用 SM2 证书代替 RSA、ECDSA 证书。

展望

区块链基于杂凑加密的匿名性能够很好保护用户隐私和证明唯一性，依托公钥/私钥的权限控制赋予数字资产丰富的管理权限。这些技术优势都为区块链的发展应用提供了大量创新空间。

密码技术作为区块链中的核心技术，必须实现自主可控。随着区块链技术在不同领域的推广，不同场景下的共识算法、签名方案、隐私保护、数据共享需求也不断变化，加强国产密码的相关应用研究与产品研制必将成为信息化安全建设的重要任务，相关成果也将在市场中体现其经济价值。

Thank You

chenxu
Tongji Blockchain Research Institute- Software Engineer
Chenxu@wutongchain.com