

CIS 2019

网络安全创新大会
Cyber Security Innovation Summit



揭开神“密”面纱 密码服务进万家

UNVAIL THE SECRECY OF SECRET BOOST THE SECRET AS A SERVICE

密码行业标准化技术委员会 委员
国家密码管理局总体专家组 专家



噫鸣智库 首席科学家
重庆大学 向宏
2019年·上海

CIS 2019

网络安全创新大会
Cyber Security Innovation Summit

- ① 青海长云暗雪山——《密码法》开启哪些机会之窗？
- ② 孤城遥望玉门关——密码服务如何支撑网络安全？
- ③ 黄沙百战穿金甲——密码服务有何内涵与外延？
- ④ 不破楼兰终不还——亟需哪些密码工程人才？



《密码法》开启哪些机会之窗？



 历史一瞬间

 瓦圣纳协定

 中美欧比较





“臣窃惟欧洲诸国，百十年来，由印度而南洋，由南洋而中国，闯入边界腹地，凡前史所未载，亘古所未通，无不款关而求互市。我皇上如天之度，概与立约通商，以牢笼之，合地球东西南朔九万里之遥，胥聚于中国，**此三千余年一大变局也。**”

同治十一年五月《复议制造轮船未可裁撤折》

甲午年间
清朝核密
被日破解



四千多年前
古埃及密码



三千多年前
中国的虎符



两千多年前
凯撒的密码



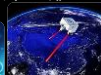
1939年
Enigma



1969年
DES加密



1978年
RSA加密



1984年
BB84协议



1994年
Shor 算法



2006年
关注PQC



2016年
PQC制标



密码体制每一次变革
都会颠覆Cyber生态圈

秋风宝剑孤臣泪
海外尘氛犹未息

落日旌旗大将坛
祝君莫作等闲看

李鸿章《临终诗》

五千年无大变 五十年已巨变



军品清单：各类武器
弹药共22类

军民两用清单：覆盖面更宽，包
括计算机信息安全技术等9大类



密码技术及其产品被瓦圣纳协定列为“Dual-Use Good”

对称加密密钥长度：56bit及以下

公钥加密密钥长度：512 bit及以下

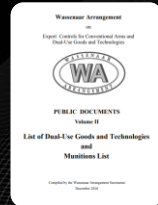


Suit B: 256 bit
Suit B: 2038 bit

掐脖子

- 瓦圣纳协定（Wassenaar Arrangement, WA），2005年签署
- 主要目的是控制“关键核心技术”（Dual-Use）出口
- 共计40个成员国（包括俄罗斯）
- 有无中国？

2⁵⁶与2²⁵⁶的区别
前者“秒杀”
后者“永生”



2018年将近250页
出口管制清单

一座蕞尔小城 卡住大国命脉



风景秀丽的瓦圣纳小镇
位于荷兰南部

中美欧密码法规比较

密码产品国内使用	密码产品进口	密码产品出口
无限制	无限制	严格限制
密码产品成员国使用	欧美关系	密码产品出口
无限制	美：密钥托管 欧盟：反对	瓦圣纳协定
商密产品/技术/服务定位	商密产品进出口管理	商密产品研发与应用
不得损害国家/社会/个人合法权益	国家安全：有 大众应用：无	从限制到放开/国内外一视同仁
商密通用服务	商密特殊服务	商密国内外对标
融入等保2.0	关键基础设施保护	鼓励各机构参与国际标准竞争





商密服务 三国演义
最佳实践 最佳策略



密码服务如何支撑网络安全



 壹鸣讲堂 密码与网络安全的昨天

 壹鸣视角 密码与网络安全的今天

 壹鸣展望 密码与网络安全的明天



密码与网络安全的昨天



恩智浦获颁国家密码管理局商用密码产品生产定点单位证书

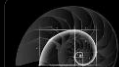
成为国家商用密码产品生产定点单位 承担商用密码产品生产任务

中国上海，2017年4月26日讯——恩智浦半导体（纳斯达克代码：NXP，以下简称“恩智浦”）今日宣布恩智浦（中国）管理有限公司正式获得国家密码管理局颁发的《商用密码产品生产定点单位证书》，成为国家商用密码产品生产定点单位暨首个获得国家证书的国际半导体企业。恩智浦将凭借其在安全半导体产品领域的技术优势，开展商用密码产品的研发和生产等系列活动，持续为中国本土信息安全提供全球领先的解决方案。



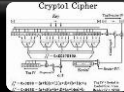
2010年
拉斯维加斯
黑帽大会破解
我损失惨重

The security of this
Cipher is closed to zero
该算法安全强度几乎为零



自然界中的
斐波那契曲线

被迫更换
数以亿计
各类卡片



密钥长度：48 bit
核心算法：斐波那契数列



物理安全

西门子公司
PLC840系列
高端数控
主要用协
S7/G代
形同裸
国产重盗
双重密码

工控安全



重庆大学密码应用高仿真测试环境 国密局工控安全专项

智慧城市

- 截止2018年年底，我国智慧城市试点数量：**789**个
- 华东夺得头筹、华北华中分布集中
- 以人为核心、跨区域/跨领域融合发展

噓鸣视角



智能交通



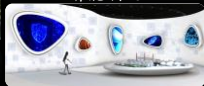
智慧能源



智慧城镇



智能制造



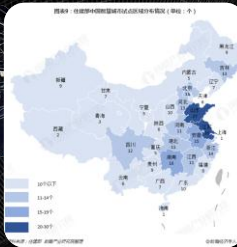
智慧环保

数字

镜像



数字孪生 赛博安全
分类服务 密码相连



2018智慧城市

China leads in blockchain startups

The publication states that blockchain is "one of the technologies which is anticipated to have a profound impact over the next 10-15 years," partly due to an increase of investment in blockchain startups. From €450 million in 2014 to €3.9 billion in 2017, it increased rapidly to €7.4 billion in 2018.

The report finds that in 2018, China has taken an impressive lead in the global number of DLT startups. China was the only reported nation to accelerate the number of startups from 2017-18. In 2018 over 130 companies started in China, almost double the number that were setup in the U.S.. Europe lagged behind with less than 20 per country. However, in terms of cumulative ventures, the U.S. still leads China by a small margin. In terms of sector focus, across the U.S., EU and Rest of World, over 70% of startups are in financial services or software.

报告摘要



2019年欧盟发布
《区块链的今天和明天》

欧美均认为 中国的企业
在这个领域 创新力强大
棒杀还是棒杀？



拜占庭共识
算法安全



区块链底层
密码安全性



联合国欧洲委员会2019发布
《区块链贸易白皮书》



美国国家档案馆2019发布
《区块链白皮书》

- 数字货币
- 智能合约



壹鸣视角 密码的内涵与外延

壹鸣惊人 密码作为服务

壹鸣观点 密码服务模型

密码服务的内涵与外延

为了规范密码应用和管理，促进密码事业发展，保障网络与信息安全，维护国家和社会公众利益，保护公民、法人和其他组织的合法权益，制定本法

—《中华人民共和国密码法》



□ 如何促进密码事业发展？



□ 如何用密码保障网络信息安全？



□ 如何用密码维护国家安全与社会公众利益？



□ 如何用密码保护公民、法人和其他组织的合法权益？



密码作为服务 (Cryptography as a Service, CaaS)



如何定义CaaS?



- 参照云服务: Cloud services refer to any IT services that are provisioned and accessed from a cloud computing provider. This is a broad term that incorporates all delivery and service models of cloud computing and related solutions
- 云服务是指任何来自于云计算服务提供商提供的IT服务
- Cryptography as a Service (CaaS) refer to any **Cybersecurity** services that are provisioned and accessed from a cryptography-service provider
- 密码服务是指由密码服务提供商 (国家授权机构、企业、法人团队等...) 提供的涉及网络安全的服务。

密码服务模型 (Models for CaaS)



与云服务模型对比



□ CSaaS: 密码模块/软件作为服务

□ CPaaS: 密码平台作为服务

□ ClaaS: 密码基础设施作为服务

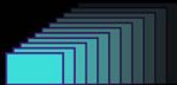


亟需哪些密码工程人才



壹鸣观点 从网络靶场到密码靶场

壹鸣展望 密码服务对人才的需求





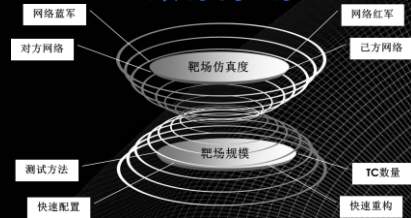
NCR的定位

- 模拟互联网
- 模拟军网（全球栅格、野战局域网）
- 模拟民网（电信、电网）

NCR的衡量标准

- 自动化：自动配置、普检、重置
- 伸缩性：虚拟技术
- 真实性：模拟人类行为
- 有效性：“时空”调控

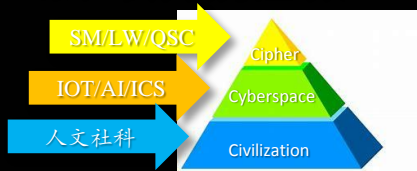
仿真度 灵活度



密码靶场（Cryptography Range）

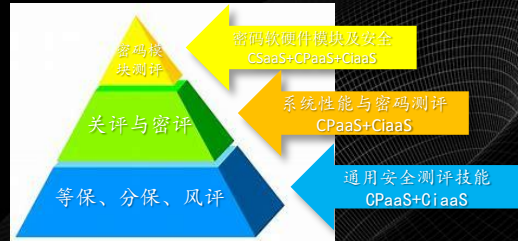
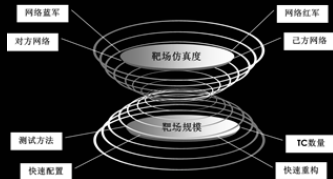
- 经典场景（云环境对密码子系统的攻防）
- 专用场景：ICS等高可靠、高时敏性网络对密码模块的适配性
- 未来场景：IOT/5G对不同密码体制的交互性

密码工程师培养模型刍议



3C金字塔知识模型

复合型、工程化、国际化



CXaaS测评技能模型

