网络安全创新大会
Cyber Security Innovation Summit

愿加密与你同在

曾瑞丰　亚洲诚信 解决方案总监

愿加密与我同在

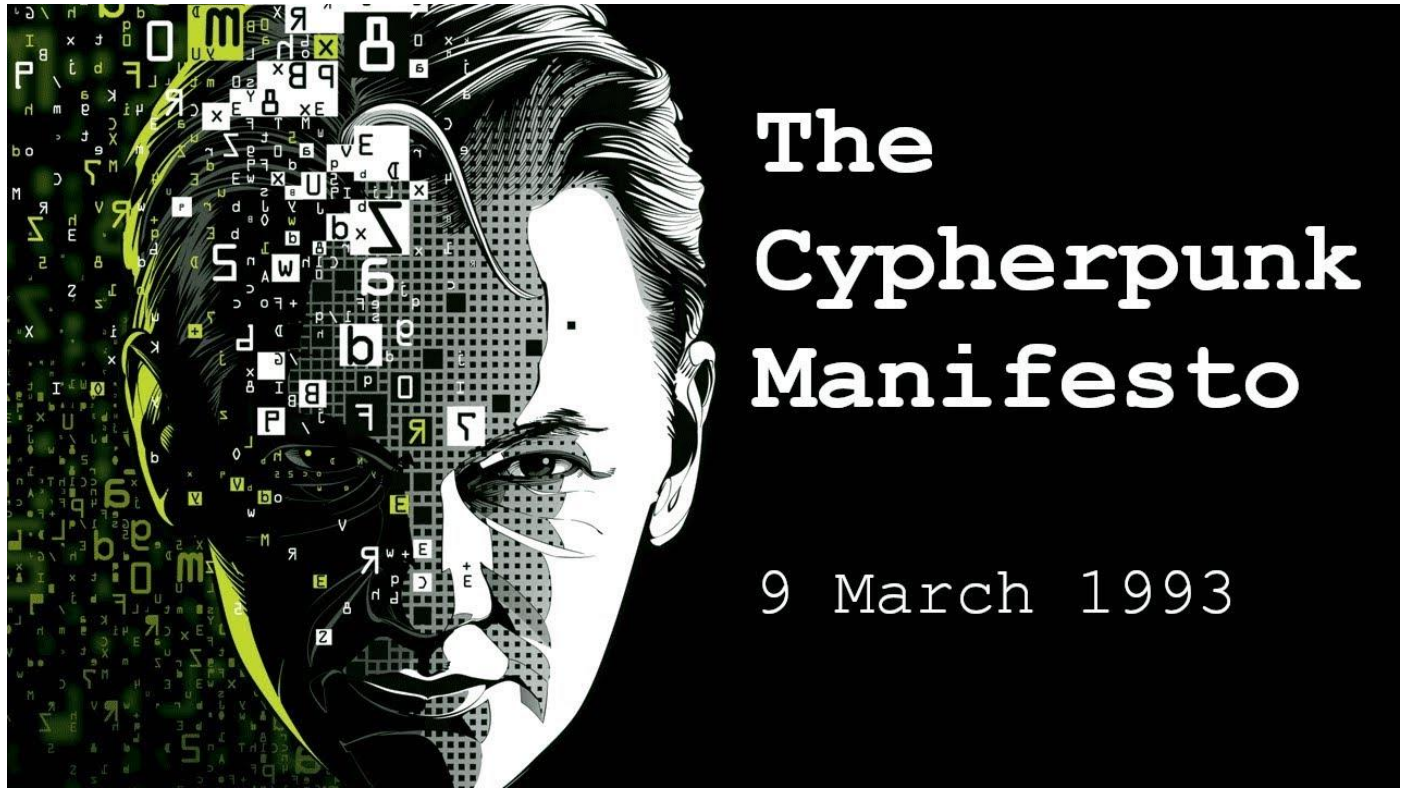
- 今天，几乎每个人都可以在我们口袋里随身设备中获得几乎不可破解的加密技术。
- 数据加密是个人信息隐私安全的关键技术，它保障数据在不安全环境中的安全存储和通信。
- 未来，随着大数据、脑机接口、人工智能的蓬勃发展，加密技术将与我们同在。

现代加密技术的本质

通过数据加密，发送的信息变成一堆乱码（图片来源 / 海洛创意）

- 从数学角度讲，加密的本质是一种数学变换函数
- 密码系统就是由 明文、密文、加密算法、解密算法、密钥 五种元素组成
- 确保密码系统可靠性的两个要点
  - 算法的安全性
  - 密钥的安全性

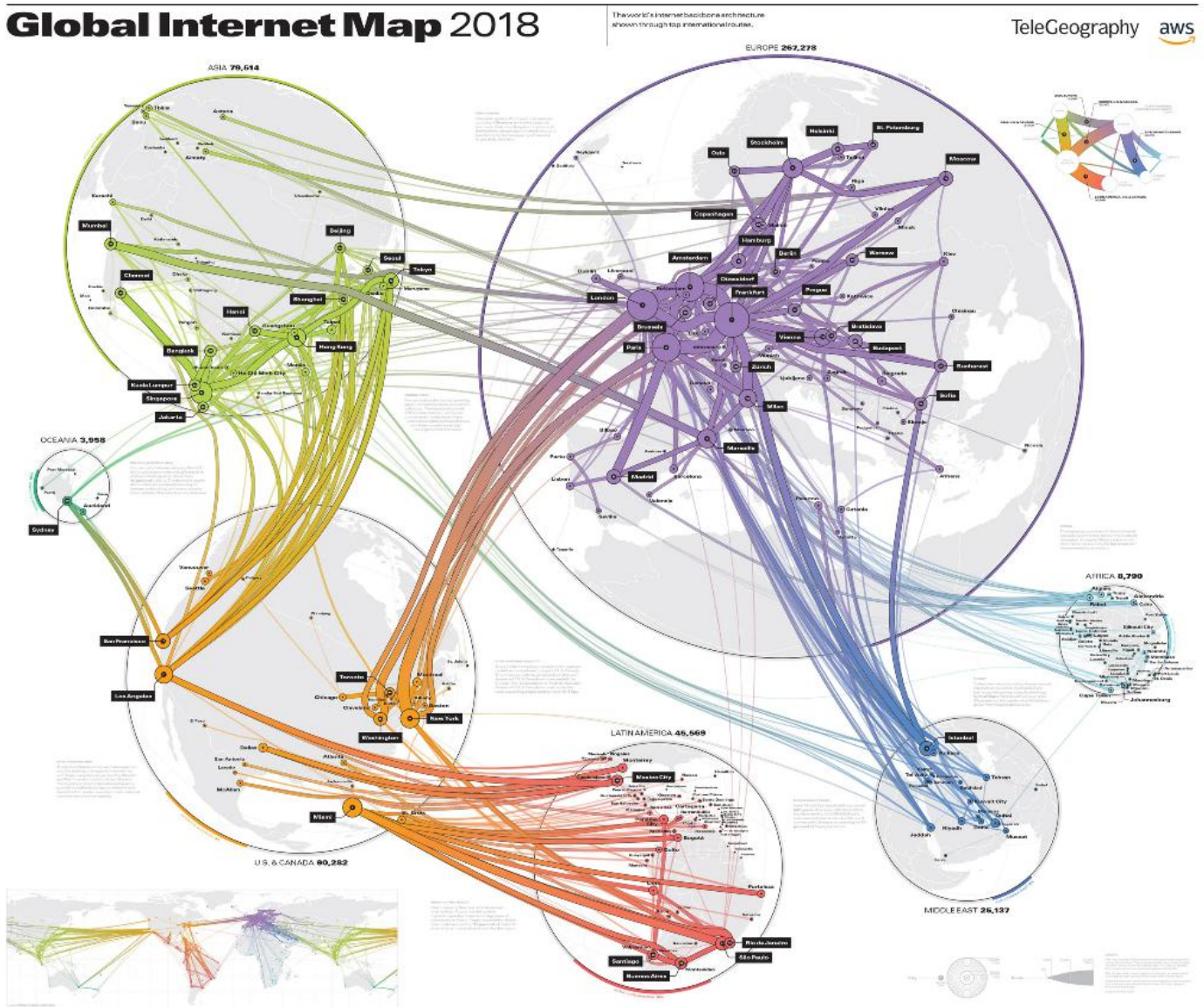
密码朋克宣言

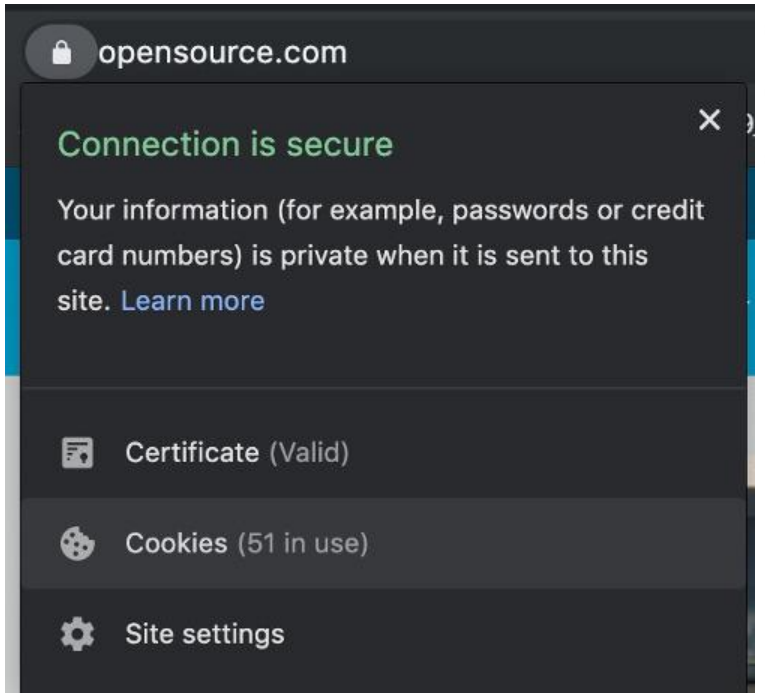


https://www.activism.net/cypherpunk/manifesto.html

- 在电子时代，隐私是开放社会的必要条件。
- 隐私是有选择地将自己透露给世界的权力。
- 在一个开放的社会中，隐私需要密码学。如果我说了些什么，我希望只有我想让其知道的人能够听到。如果我说话的内容可以让全世界都知道，我就没有隐私了。
- 加密是表示对隐私的渴望。

互联网加密技术TLS





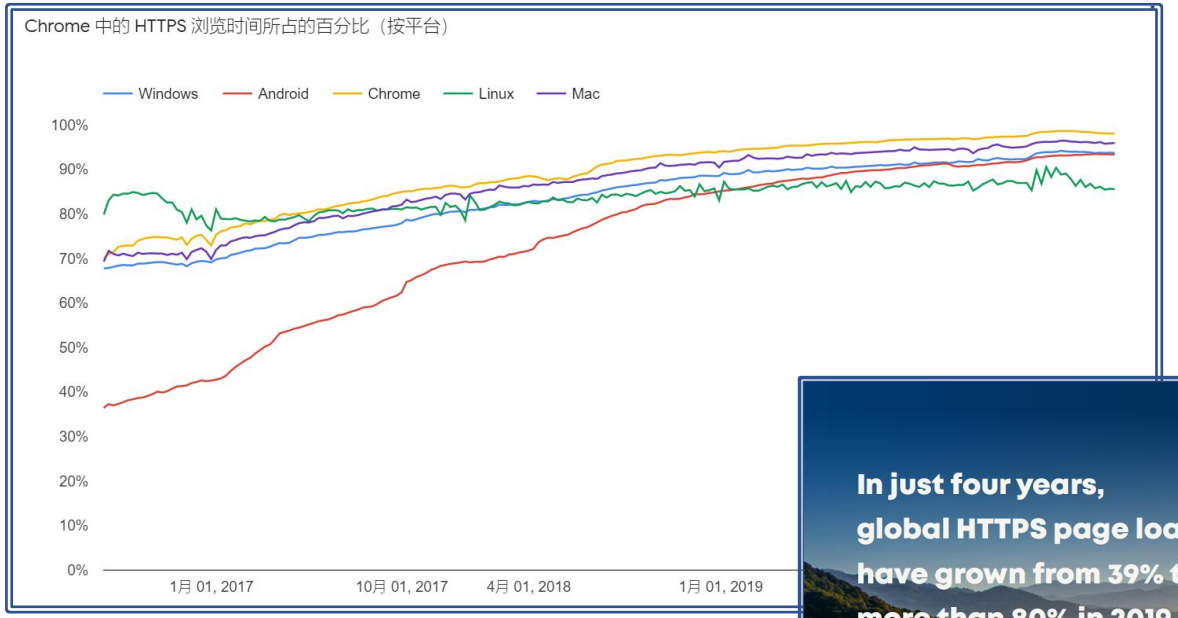
- 在开放的互联网世界用加密来保护我们的隐私
- 通过TLS加密技术确保数据传输安全

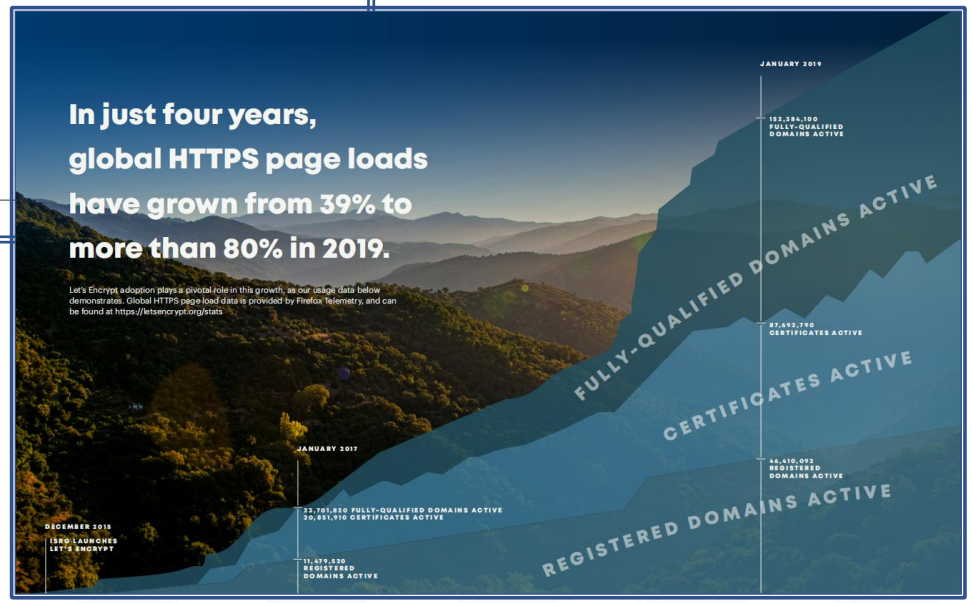
互联网加密技术HTTPS

GLOBAL APPLICATION
TOTAL TRAFFIC SHARE

1. **YOUTUBE:** 2019: 8.69% **2020: 15.94% (+7.25%)**
2. **NETFLIX:** 2019: 12.87% **2020: 11.42% (-1.45%)**
3. **HTTP:** 2019: 3.61% **2020: 6.57% (-2.96%)**
4. **BITTORRENT:** 2019: 7.75%% **2020: 5.23% (-2.52%)**
5. **FACEBOOK:** 2019: 3.37% **2020: 3.68% (+0.37%)**
6. **HTTP MEDIA STREAM:** 2019: 13.76% **2020: 3.64% (-10.12%)**
7. **GOOGLE:** 2019: 1.23% **2020: 2.91% (+1.68%)**
8. **WORDPRESS:** 2019: 0.10% **2020: 2.88% (+2.78%)**
9. **INSTAGRAM:** 2019: 2.64% **2020: 2.72% (+0.08%)**
10. **FACEBOOK VIDEO:** 2019: 2.46% **2020: 2.29% (+0.17%)**

➢ HTTPS 是使用最为广泛的加密技术

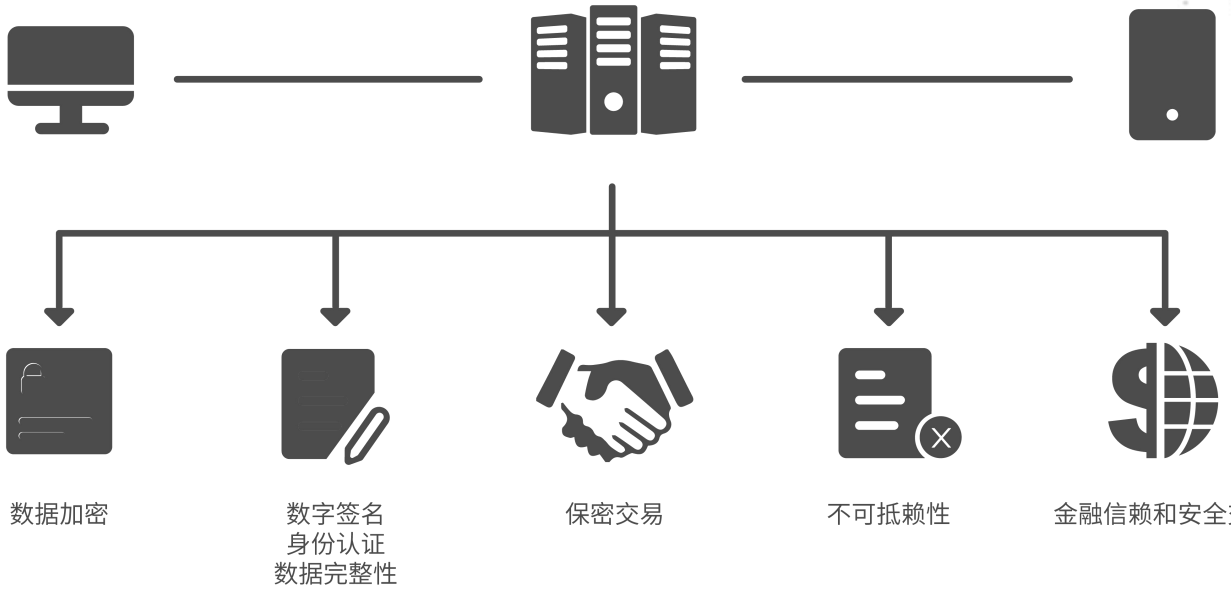




https://transparencyreport.google.com/https/overview

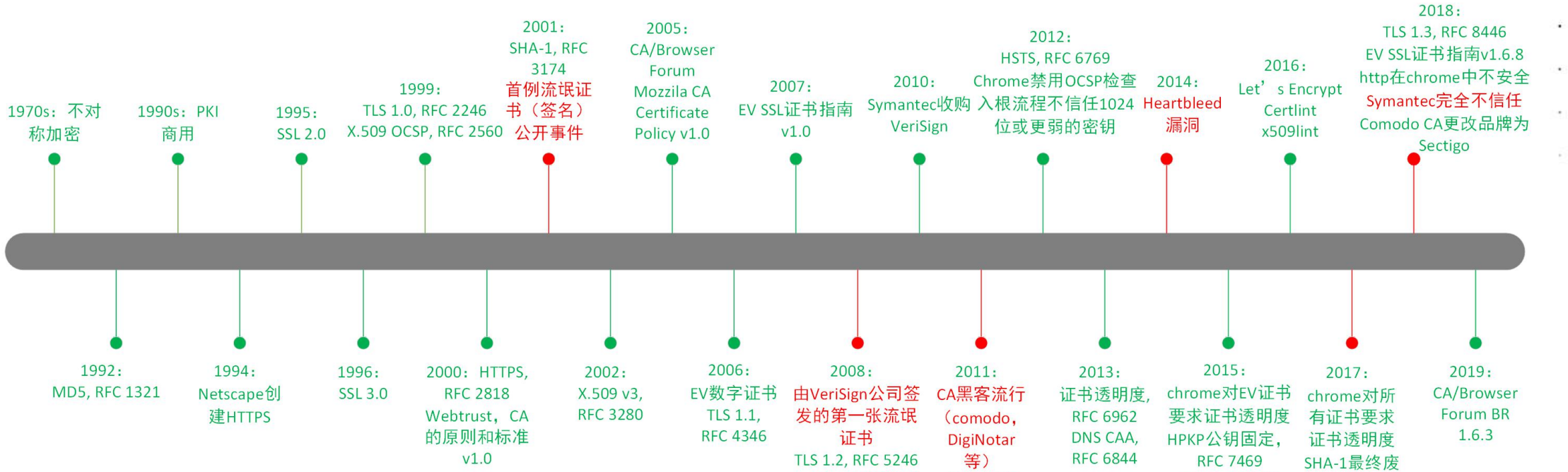
互联网安全的核心机制-PKI系统

以PKI为基础的安全网络



当通过浏览器访问网站时：服务器在TLS握手过程中出具证书；浏览器验证证书链的有效性；如果验证通过，则协商会话秘钥，继续通信；如果不通过，弹出告警。

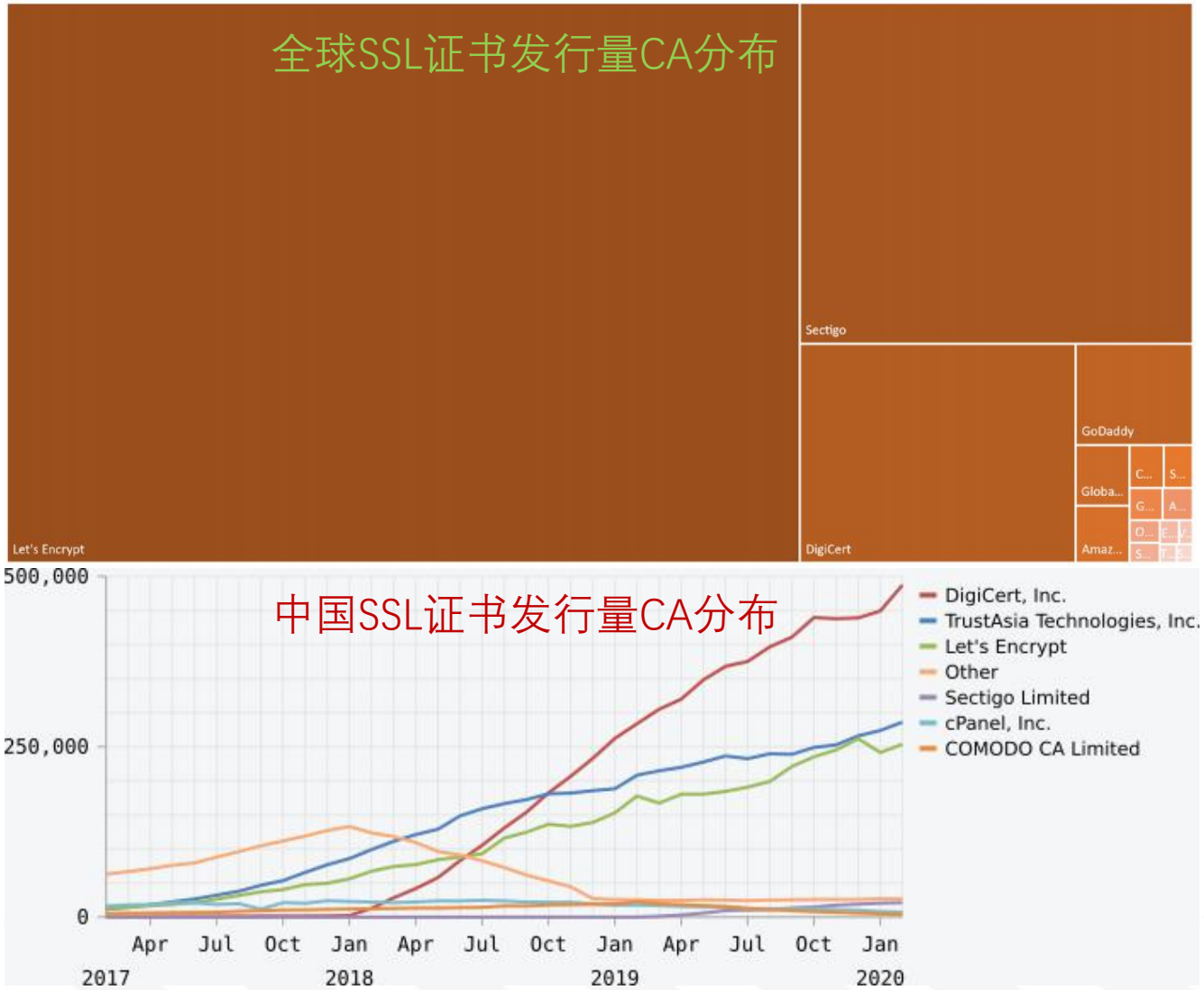
现代PKI系统的涅槃



- PKI（公钥基础设施）系统是现有的加密技术中效率最好的系统
- 不断的技术升级，监管升级，以及自我修正

正确的使用网站加密技术

Web PKI 安全生态问题



- 从安全的角度来看，市场上CA的碎片化是一个优点，而不是一个bug
- 像对手一样思考，你可以解密所有的流量--如果你有像Let's Encrypt这样的CA的私钥
- LE是一个非营利组织，没有收入；SSL证书是免费的。没有人失去任何东西；没有 "皮肉之苦"
- 以隐私安全为首位。要避免 "免费 "和 "方便 "的诱惑

RSA算法证书是当前国内主流HTTPS应用安全的基础

网络安全创新大会
Cyber Security Innovation Summit

MySSL.com统计显示我国99%网站都是在使用的RSA SSL证书
大量关键信息基础设施的密码使用规范不符合国密要求

https://www.taobao.com 淘宝网 Taobao.com

https://www.jd.com 京东

https://weixin.qq.com 微信

https://weibo.com 微博

https://user.95516.com 中国银联 China UnionPay

https://mybank.icbc.com.cn ICBC 工银

https://ebsnew.boc.cn 中国银行 BANK OF CHINA

https://www.baidu.com 百度

https://www.12306.cn 中国铁路12306 12306 CHINA RAILWAY

https://gd.ac.10086.cn 中国移动 China Mobile

gzdata.com.cn 云上贵州 Guizhou-Cloud Big Data

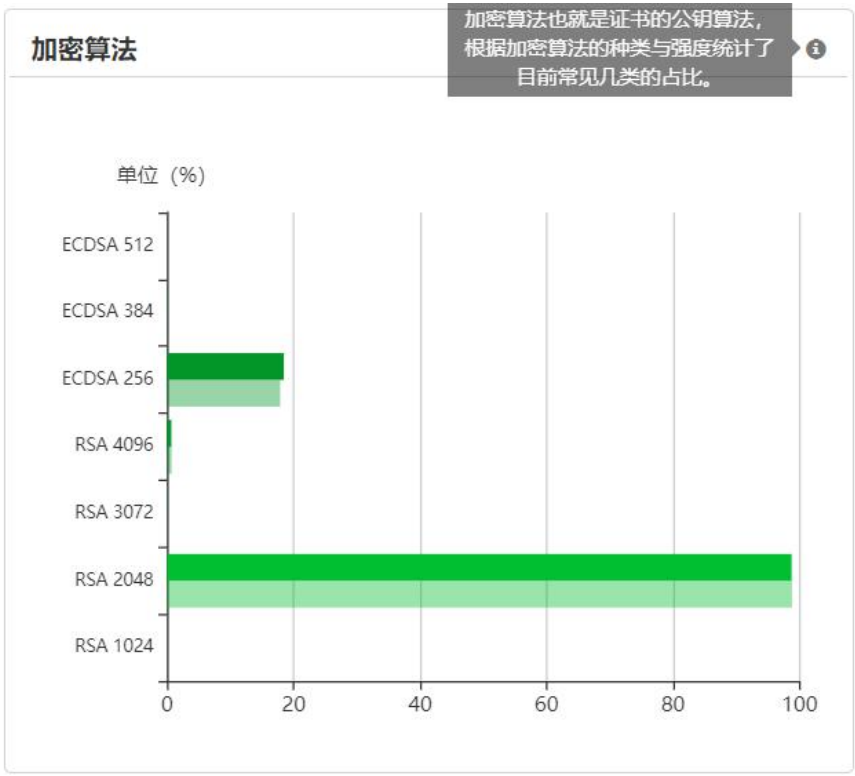
https://www.pku.edu.cn 北京大学 PEKING UNIVERSITY

https://www.alipay.com 支付宝 ALIPAY

https://www.tenpay.com 财付通

https://ibsbjstar.ccb.com.cn 中国建设银行 China Construction Bank

https://www.ctrip.com Ctrip 携程



加密技术后门

1. 到目前为止，RSA算法并未发现任何缺陷。
2. RSA公司推出的BSafe安全软件，提供了RSA加解密，以及密钥自动产生等功能。
3. 但是BSafe软件产生密钥所使用的算法Dual_EC_DRBG，已经被研究人员确认为是可能存在后门的算法。事实上这已经意味着BSafe软件产生的密钥并不安全了（这在2007年）。但RSA算法还是安全的。
4. 目前最新的进展是，斯诺登披露的文件证明了，美国国家安全局（NSA）通过贿赂RSA公司，使其在BSafe安全软件中采用Dual_EC_DRBG算法。而Dual_EC_DRBG则是NSA精心设计的留有后门的算法

强者需要透明 弱者需要隐私

Council of the
European Union

Brussels, 24 November 2020
(OR. en)

13084/1/20
REV 1

LIMITE

JAI 999
COSI 216
CATS 90
ENFOPOL 314
COPEN 329
DATAPROTECT 131
CYBER 239
IXIM 122

NOTE

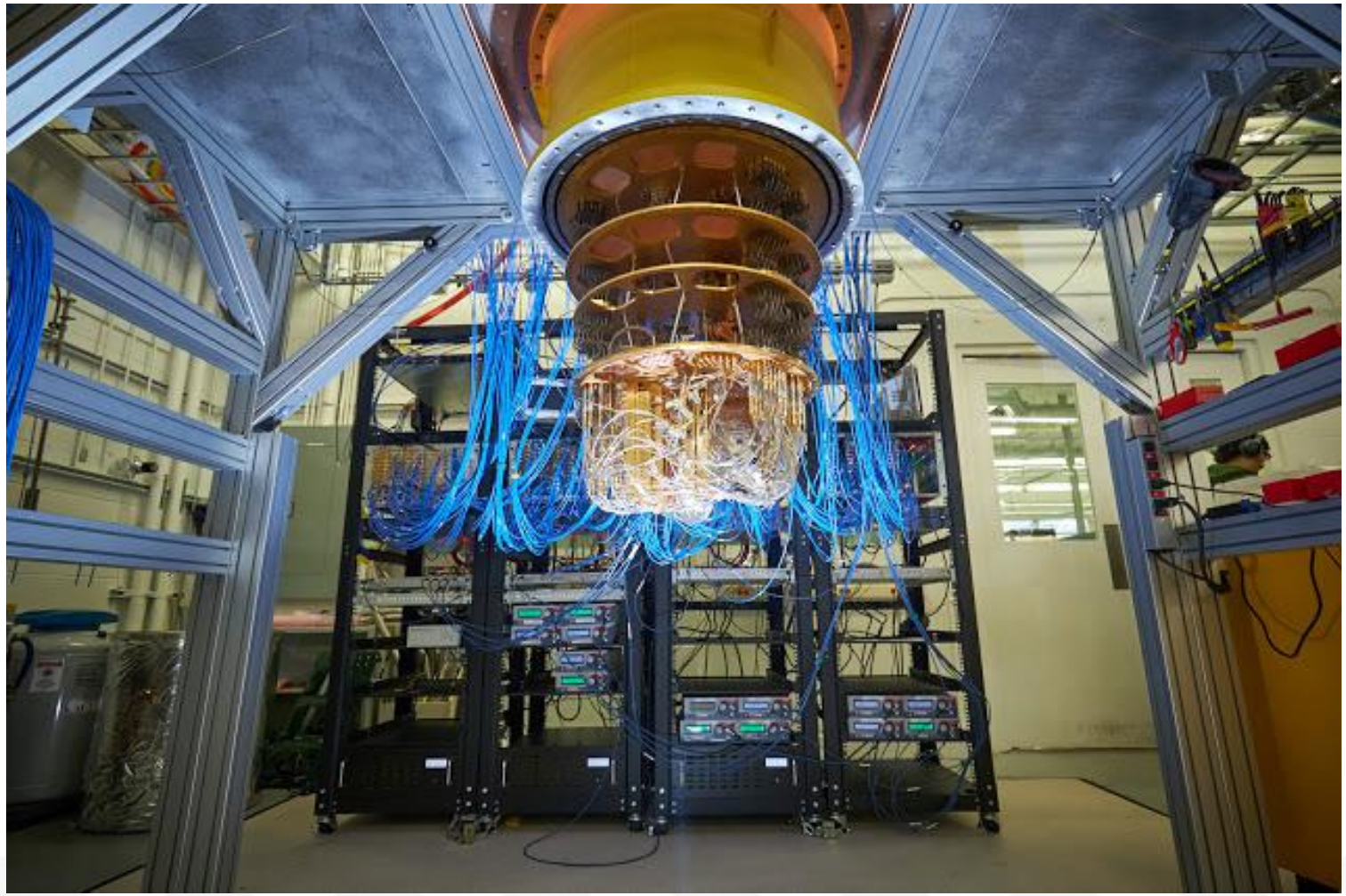
From:	Presidency
To:	Delegations
No. prev. doc.:	12863/20
Subject:	Council Resolution on Encryption - Security through encryption and security despite encryption

- scientists4crypto 致欧盟委员会的学术函
- 通过加密保障安全，不加密就没有安全可言!
- 我们承认端对端加密给调查人员带来了挑战，但我们要强调的是，"不顾加密方法，但还是安全 "是一个欺骗性的概念。在信息安全和方便合法调查访问之间不存在 "平衡 "。
- 没有人是一座孤岛

--Johe Donne

https://sites.google.com/view/scientists4crypto/start

“量子霸权”的到来



量子计算机时代正式开启了，2019年10月份谷歌宣布实现了量子霸权，说实在的还是挺震撼，他们首次在实验中证明了量子计算机对于传统架构计算机的优越性：在世界第一超级计算机 需要计算 1 万年的实验中，谷歌的量子计算机只用了 200秒。

密码算法安全级别对比

安全级别	对称密码算法		哈希摘要算法		公钥密码算法			
					RSA算法		ECC椭圆曲线算法	
	经典环境	量子环境	经典环境	量子环境	经典环境	量子环境	经典环境	量子环境
40bit	DES		MD5	SHA1		不可用		不可用
64bit	RC4	AES128 SM4	SHA1					
80bit	3DES	AES192		SHA256 SM3	1024		160	
128bit	AES128 SM4	AES256	SHA256 SM3	SHA384	3072		256 (SM2)	
192bit	AES192		SHA384	SHA512	7680		384	
256bit	AES256		SHA512		15360		512	

密码算法安全级别对比

密码学应用	不完整举例	潜在应对策略
非对称密钥数据加密和数字签名	RSA，DSA，ElGamal，ECDSA，SM2	替换为抗量子算法
密钥交换	Diffie-Hellman密钥交换	替换为抗量子算法
数字证书	X.509，国密证书	替换为抗量子算法
加密通信	TLS，HTTPS，IPsec	替换为抗量子算法
硬件可信执行环境	SGX	替换为抗量子算法
对称密钥数据加密	AES，DES，SM4	增大安全参数值
数据摘要和哈希	SHA-3，HMAC，SM3	增大安全参数值
随机数生成器	RNG	不受直接影响
密钥生成和派生算法	KDF	不受直接影响

根据美国国家标准与技术研究院（NIST）分析，量子计算机对于非对称密码学体系冲击最大。用来构造公钥密码算法的经典计算困难性问题，如大数分解困难问题、离散对数困难问题、椭圆曲线上的离散对数困难问题，在量子计算机上均有有效的破解算法——Shor算法及其变体。这些攻击会具体影响到现在的公钥加密、数字签名、数字证书、密钥交换等的安全性。

NIST 后量子密码算法标准征集

	Signatures		KEM/Encryption		Overall
Lattice-based	CRYSTALS-DILITHIUM DRS FALCON pqNTRUSign qTESLA	5	Compact LWE CRYSTALS-KYBER Ding Key Exchange EMBLEM and R.EMBLEM FrodoKEM HILA5 KCL KINDI LAC LIMA Lizard LOTUS NewHope NTRUEncrypt NTRU-HRSS-KEM NTRU Prime Odd Manhattan Round2 SABER Three Bears Titanium	21	26
Code-based	pqsigRM RaCoSS	2	BIG QUAKE BIKE Classic McEliece DAGS HQC LAKE LEDAkem LEDApkc Lepton LOCKER McNie NTS-KEM Ouroboros-R QC-MDPC KEM RLCE-KEM RQC	16	18
Multi-variate	DualModeMS GeMSS Gui HiMQ-3 LUOV MQDSS Rainbow	7	CFPKM DME	2	9
Symmetric/ Hash-based	Gravity-SPHINCS Picnic SPHINCS+	3			3
Other	Post-quantum RSA-Signature WalnutDSA	2	Giophantus Guess Again Mersenne-756839 Post-quantum RSA-Encryption Ramstake SIKE	6	8
Total		19		45	64

网络安全创新大会
Cyber Security Innovation Summit

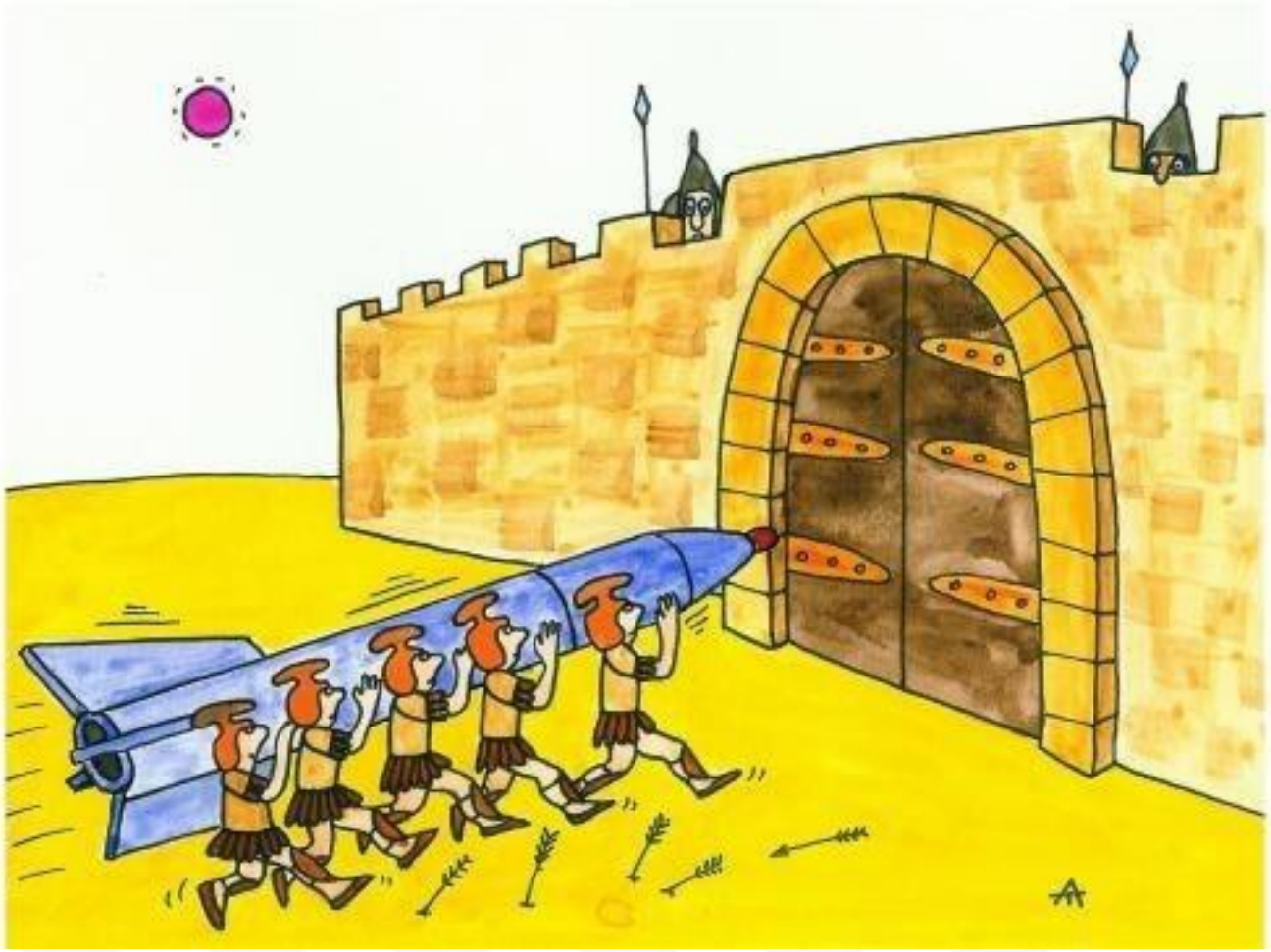
第三轮挑选

Public-Key Encryption/KEMs
Classic McEliece
CRYSTALS-KYBER
NTRU
SABER

Digital Signatures
CRYSTALS-DILITHIUM
FALCON
Rainbow

预计2021年底前确定标准
倒计时12个月

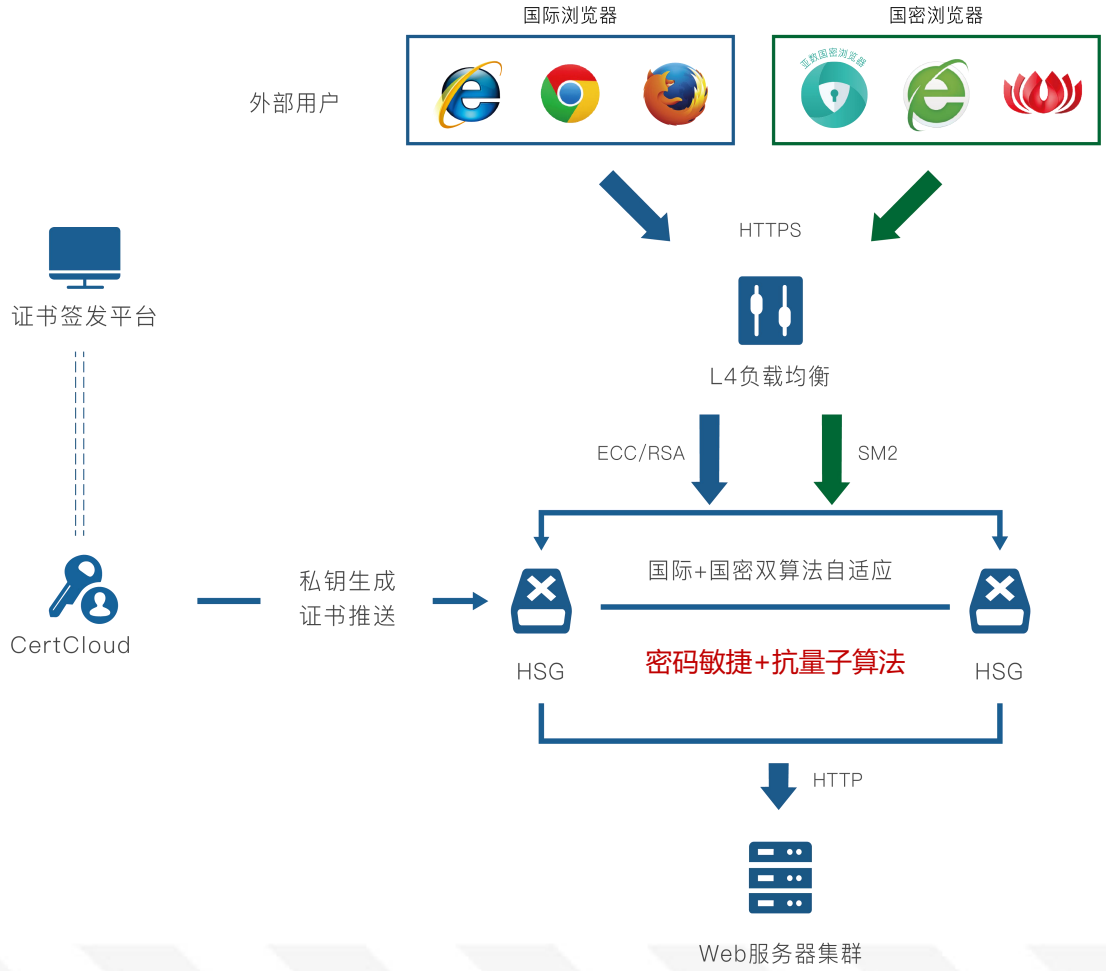
现有国密算法的抗量子计算对策



现状：
中国密码学会开展了两轮全国密码算法设计竞赛，通过国内科研团队开创符合中国特色的抗量子计算密码算法。

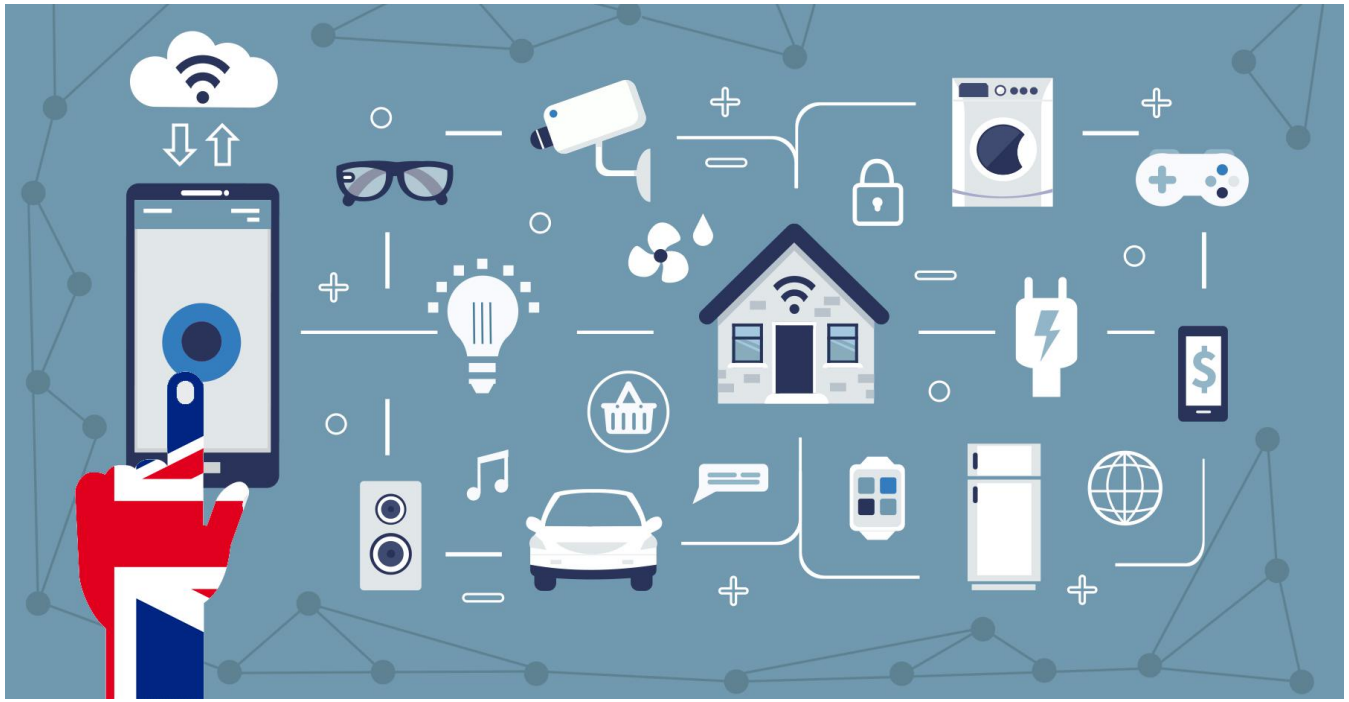
对策：
部署密码敏捷性平台，在实用化量子计算机到来的时候，我们可以灵活地切换到抗量子国密算法或者抗量子国际标准算法上。从而实现在后量子时代达到安全标准的目的。

我们是如何在CertCloud和HSG上实现加密敏捷性



- 我们是把加密服务从Web服务层**抽取**出来，然后**集中**到HSG上。这样，加密和应用就实现了一定程度的**剥离**。
- CertCloud和HSG连接，实现证书的管理、自动化部署，自动化监测，当发现密码机制弱点时快速切换。
- HSG设备应对密码规范的变迁，已经提供了SM2/RSA/ECC/多算法同步兼容，可以进一步提供抗量子算法的兼容和加速。
- CertCloud和HSG的整合除了实现证书自动化管理和SSL卸载的功能外，是一个在SSL/TLS领域的加密敏捷性平台。

全连接，全加密，IOT安全与加密



- 加密应该是每个物联网设备的核心，以达到数据在存储和传输中都完全加密的状态
- 数据存储在服务器上，必须控制每一个能够访问数据的人，并且对数据加密。这样才能保证数据的隐私性和排他性。
- 可穿戴设备和医疗设备直接关联我们的身体信息
- 用加密技术来阻止爬虫获取数据

令人震惊的事实

- 98%的物联网设备流量都是未加密的。
- 攻击者如果成功绕过第一道防线和已建立的黑客控制中心能够监听未加密的网络流量，收集个人或机密信息。

未来已来，加密与你同在

智能义肢，脑机接口把人类的物质本源与互联网连接。

加密技术让我们能自由的生存于赛博空间

网络安全创新大会
Cyber Security Innovation Summit

THANKS

Ralph.zeng@trustasia.com