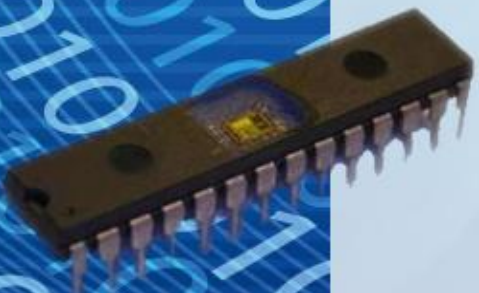
密码学与网络空间安全

王小云
清华大学
2016年3月24日



报告提纲

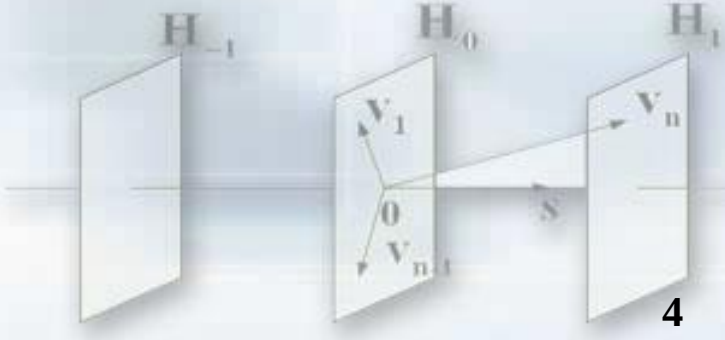
- 现代密码学的发展
- 网络空间安全的范畴
- 网络通信中密码安全事件
- 大数据与云计算安全
- 密码技术产业

报告提纲

- 现代密码学的发展
- 网络空间安全的范畴
- 网络通信中密码安全事件
- 大数据与云计算安全
- 密码技术产业

密码学发展的三个阶段

- 密码学是一个即古老又新兴的学科。密码学(Cryptology)一字源自希腊文"krypto's"及"logos"两字，直译即为"隐藏"及"讯息"之意
- 密码学发展的二个阶段
  - 古典密码（手工、机械阶段 -1949）
  - 现代密码（信息论:1949-1975）
    （计算机:1976-）



古典密码——Caesar 密码

- **Caesar 密码：公元前1世纪，古罗马Julius Caesar发明的，被用于高卢战争中，是一种单字母替代密码**
  - **对字母表中的每个字母用它之后的第3个字母代换**
  - **Caesar 密码 ： c=(m+ k) mod 26**

明文	ABCDEFGHIJKLMNOPQRSTUVWXYZ
密文	DEFGHIJKLMNOPQRSTUVWXYZABC

k=3

明文	Caesar was a great soldier
密文	FDHVDU ZDV D JUHDW VROGLHU

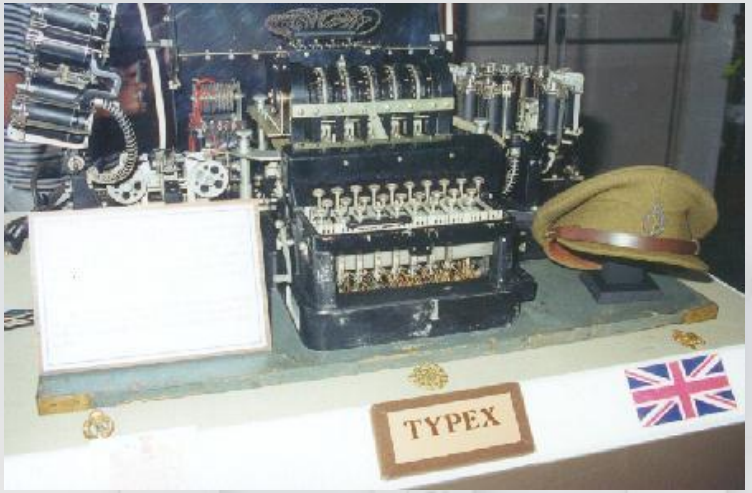
  - **攻击方法：猜测26种情况**

古典密码——ENIGMA密码

- Sigaba (美国)
- Typex (英国)
- Lorenz SZ 40/42 (德国陆军)
- Siemens and Halske T52 (德国空军、海军)
- 紫密码机 (日本)

德国防卫军使用的G型恩尼格玛密码机

日军使用的T型恩尼格玛密码机



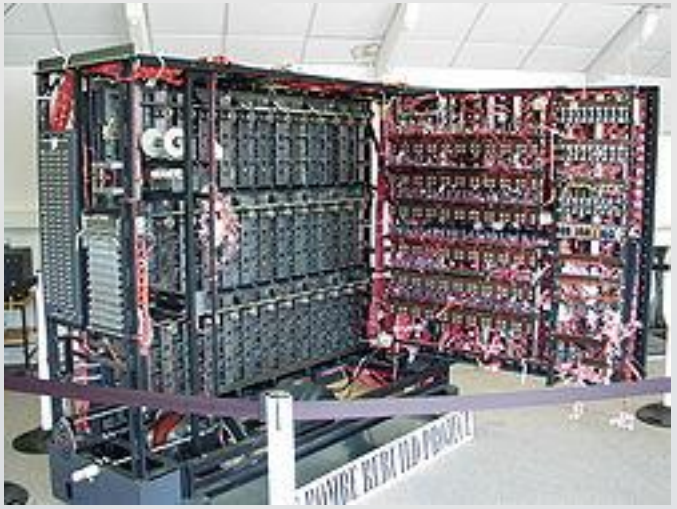
英国的TYPEX打字密码机

古典密码—— ENIGMA密码机的破解

二战期间，数学家雷耶夫斯基和图灵等采用数学方法破解了德军密码Enigma，改变了世界格局

雷耶夫斯基

图灵



破解Enigma设备Bombe

现代密码学的发展

- 1949年，Shannon发表《保密系统的信息理论》，提出熵的概念，建立了完善安全性为对称密码学建立了理论基础，密码学从艺术成为科学
- 1976年，Diffie和Hellman发表《密码学新方向》奠定了现代公钥密码学基础：基于因子分解、离散对数、背包问题(NP-C) 等数学难题设计公钥密码体制

2015年图灵奖获得者

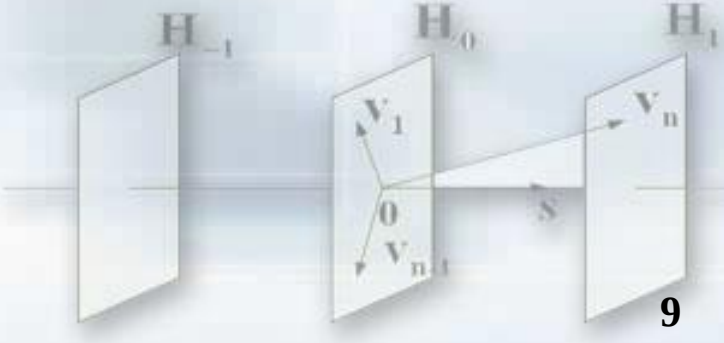
- 1976年美国公布：数据加密标准DES
- 1976年两项标志性成果意味着密码设计与分析全面进入了现代密码学阶段

信息论与完善安全

- **密码体制的完善安全性（Perfect Security)**
  - 1949：Claude E. Shannon, Communication Theory of Secrecy Systems

    H(K|(M,C))=H(K)

    H： 熵，信息量或者不确定性
  - 随机$K \in \{0,1\}^{128}$，猜测K的概率为$1/2^{128}$。信息量H(K)=128比特，强力攻击为2^{128}次猜测
- **问题：大明文、密钥空间，很难设计可证明的完善安全密码体制**



计算安全、多项式安全及密码设计

- **计算安全性（Computational Secure)**
  - 在各种攻击下，破解密码体制是计算时间内是不可能求解密钥k、从密文C求解明文M、伪造数字签名S(M)等。对称密码体制的设计：计算安全性， 不低于安全指标(如:多项式时间不可破解)
- **多项式安全（Goldwasser, Micali，1982）给定两个明文M_1、M_2，以及给定一个密文C，且C为其中一个明文的密文，在多项式时间内不能以大于1/2的实质性的概率区分C为那个明文的密文**

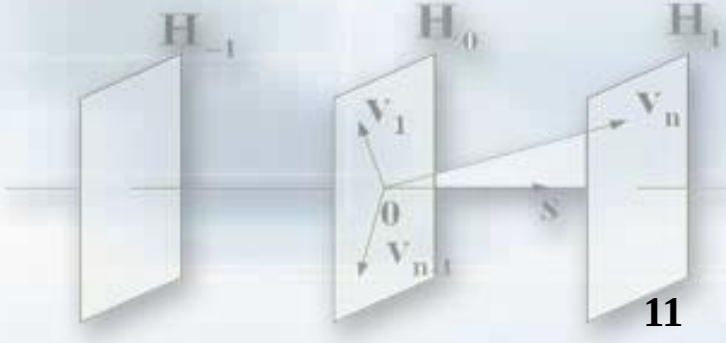
$$\Pr(A(C, M_1, M_2)=\text{正确明文})<1/2+1/P(k)$$

k：安全指数，P(k)为任意正系数多项式

计算安全、多项式安全及密码设计

计算机通信由一对一通信，发展为多对一通信

- **1976, Diffie, Hellman, New Directions in Cryptography**
- **单向陷门函数： C=F(M, Ke)　(K_d是K_e的陷门)**
  - 已知M与K_e计算C是容易的
  - 已知C计算M是困难的
  - 已知C与K_d计算M是容易的



现代密码特点

- 计算复杂性理论：NP-C，NP-Hard
- 数学难题：经典数学难题
- 量子信息:量子密码, 量子计算机
- 密码分析：多学科交叉
- 密码学的相关数学领域主要包括

数学是密码学的理论基石

Euclid – 300 B.C.

There are infinitely many primes:
2, 3, 5, 7, 11, 13, . . .

The greatest common divisor of two numbers is easily computed (using "Euclid's Algorithm"):
$\gcd(12, 30) = 6$

Pierre de Fermat (1601-1665)
Leonhard Euler (1707–1783)

Fermat's Little Theorem (1640):
For any prime p and any a, $1 \le a < p$:

$$a^{p-1} = 1 \pmod{p}$$

Euler's Theorem (1736):
If $\gcd(a, n) = 1$, then

$$a^{\phi(n)} = 1 \pmod{n},$$

where $\phi(n) = \#$ of $x < n$ such that $\gcd(x, n) = 1$.

Carl Friedrich Gauss (1777-1855)

Published *Disquisitiones Aritmeticae* at age 21

"The problem of *distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors* is known to be one of the most important and useful in arithmetic. . . . the dignity of the science itself seems to require solution of a problem so elegant and so celebrated."

William Stanley Jevons (1835–1882)

Published *The Principles of Science* (1874)

Gave world's first *factoring challenge*:

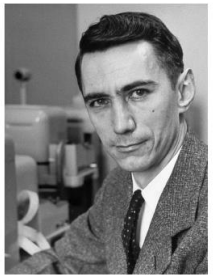
"What two numbers multiplied together will produce 8616460799 ? I think it unlikely that anyone but myself will ever know."

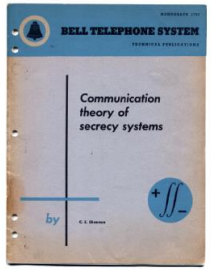
Factored by Derrick Lehmer in 1903. $(89681 * 96079)$

Alan Turing (1912–1954)

Developed foundations of theory of computability (1936).

Claude Shannon (1916–2001)





- "Communication Theory of Secrecy Systems" Sept 1945 (Bell Labs memo, classified).
- Information-theoretic in character—proves unbreakability of one-time pad. (Published 1949).

Ronald L. Rivest在On the growth of cryptography报告中介绍的1976年之前密码学家与数学家

基础密码算法

- 加密算法：机密性
  - 对称加密算法，如分组密码算法DES、AES等
  - 非对称加密算法（公钥密码体制如RSA、ECC等）
- 电子签名(数字签名）：可认证性，不可否认性
  - RSA、ECC等
- Hash函数：完整性，电子签名的不可否认性
  - 如MD5、SHA-1、SHA-2、SHA-3等

RSA: 1978, Rivest、Shamir和Adleman提出

ECC: 1985, Koblitz与Miller 独立提出

MD5：1991, Rivest设计

SHA-1、SHA-2、SHA-3 : 美国标准技术局公布的标准

RSA 密码体制的安全性——加密

$N = pq$ (其中 p、q 是大的素数)

公开: N, e, 公钥: e, $(e, \varphi(N)) = 1$

保密: p、q, $\varphi(N)$

私钥: d, $ed \equiv 1 \bmod \varphi(N)$

$\varphi(N)$=(p-1)(q-1): Euler函数

Attacker

获得e

无法通过e、c获得m

截取c

e

计算 获得明文
$m \equiv c^d \bmod N$

Alice

传送c

获得e

消息 $m \in \mathbb{Z}_N^*$
计算密文
$c \equiv m^e \bmod N$

Bob

RSA 密码体制的安全性——数字签名

$N = pq$ (其中 p、q 是大的素数)

公钥e满足$(e, \varphi(N)) = 1$

私钥d满足$ed \equiv 1 \bmod \varphi(N)$

无法通过多组(m, e, s)获得m', s'使得
$m' \equiv s'^{e} \bmod N$

Attacker

获取(m, e, s)

消息$m \in \mathbb{Z}_N^*$
计算签名
$s \equiv m^d \bmod N$

Alice

(m, e, s)

Bob

获得(m, e, s)
验证
$m \equiv s^e \bmod N$

密码学的重要性

安全通讯

机密性

完整性

有效性

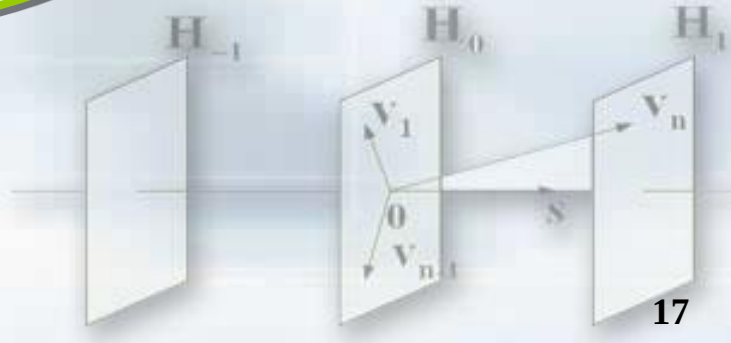
可认证性

不可否认性

密码学是信息安全的支撑，是网络通信与数据保密的重要保障

电子商务

军事



密码的重要性

密码跟安全通讯密不可分

- 信息通讯由单一的点到点通讯演化为全球化网络通讯
- 为提供全球约1万亿通讯设备的安全保障，密码算法与协议被广泛用于有线和无线通讯

计算机网络

物联网

4G手机网络

云计算

报告提纲

- 现代密码学的发展
- **网络空间安全的范畴**
- 网络通信中密码安全事件
- 大数据与云计算安全
- 密码技术产业

网络空间安全

- 2009年，美国成立网络司令部
- 2011年，美国国防部发布《网络空间国际战略》和《网络空间行动战略》
- 网络空间是继陆、海、空和太空领域后的第五大领域

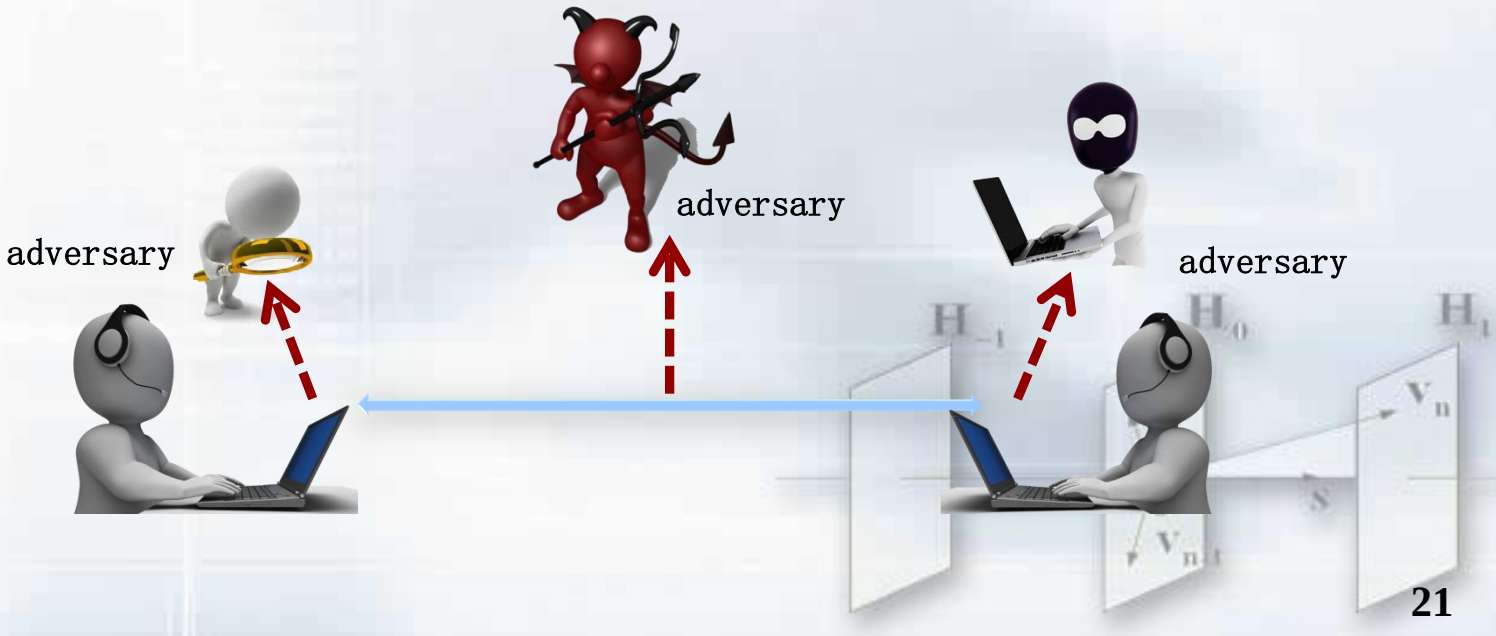
- 十八大报告指出
  - 高度关注海洋、太空、网络空间安全
  - 建设下一代信息基础设施，发展现代信息技术产业体系，健全信息安全保障体系，推进信息网络技术广泛运用

2014年2月27日，中央网络安全与信息化领导小组成立

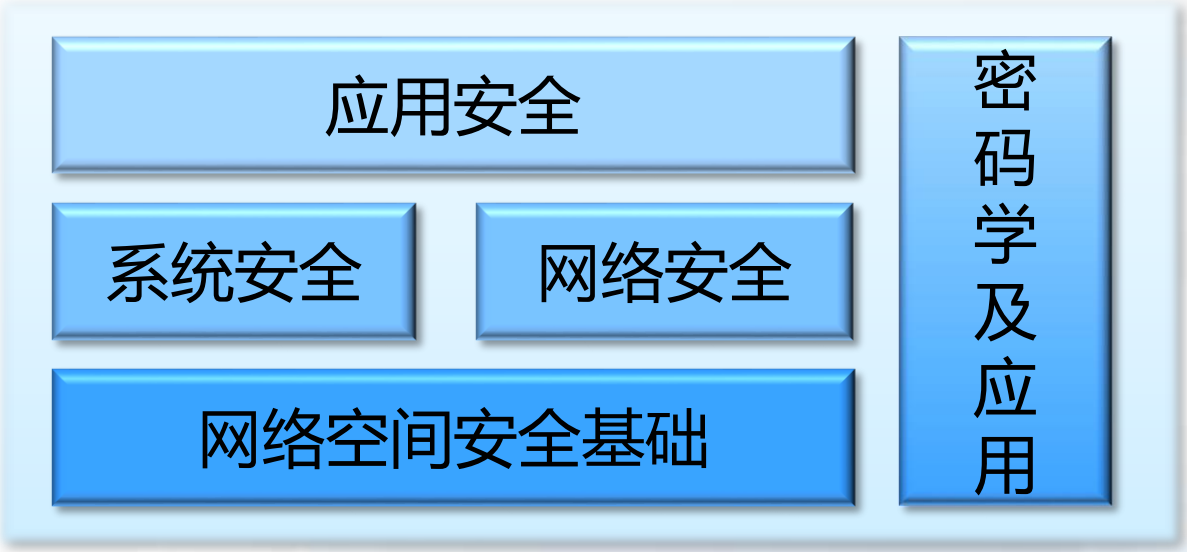
20

网络空间安全

- Cyberspace Security或简称Cyber Security
- 研究网络空间中的安全威胁和防护问题，即在有敌手（adversary）的对抗环境下，研究信息在产生、传输、存储、处理的各个环节中所面临的威胁和防御措施、以及网络和系统本身的威胁和防护机制



网络空间安全学科方向



- **安全基础**为其他方向的研究提供理论、架构和方法学指导
- **密码学及应用**是为系统/网络/应用安全提供密码安全机制
- **系统安全**保证网络空间中的单元计算系统的安全
- **网络安全**保证网络自身和传输信息的安全
- **应用安全**保证大型应用系统的安全，也是安全的综合应用

网络空间安全本科生课程模块（供参考）

应用系统安全课程模块

- 信息隐藏
- 物联网安全
- WEB安全
- 计算机数字取证
- 舆情分析及预警
- 数字版权保护技术
- 隐私保护技术
- 云计算安全
- 大数据安全
- 垃圾信息识别与过滤
- 数据存储与恢复
- 电子政务/电子商务安全

系统安全课程模块

- 数据库安全
- 可信计算
- 代码安全与漏洞挖掘
- 操作系统安全
- 芯片安全
- 恶意代码分析与防御
- 访问控制技术
- 物理安全
- 可靠性技术

网络安全课程模块

- IPv4/v6安全
- 无线通信安全
- 网络漏洞检测与防护
- VPN
- 通信网络安全
- 入侵检测与防御
- 网络安全协议
- 网络攻击与防护
- 防火墙技术

网络空间安全理论基础课程模块

- 网络空间安全导论
- 网络空间安全法律法规
- 网络空间安全管理基础
- 操作系统
- 数据库
- 程序设计语言
- 计算机网络
- 计算机组成
- 数论
- 信息论
- 计算复杂性

密码学及应用课程模块

- 密码协议
- 公钥密码数学基础
- 微积分
- 密码学
- 密码分析技术
- 量子密码
- 密码实现技术
- 高等代数
- 编码理论
- 概率论与数理统计

网络空间安全研究生核心课程（供参考）

学科 \ 层次	硕士	博士
网络空间安全基础	网络空间安全导论、网络空间安全理论基础、网络空间安全体系结构、网络空间安全管理与安全法律法规（安全评估准则与风险管理）	
	大数据分析及其安全应用、网络安全脆弱性分析与评估、网络安全态势感知与分析	安全形式化方法、网络空间对抗博弈与安全经济学
密码学及应用	应用密码学、对称密码、公钥密码、椭圆曲线密码、	
	密码实现技术、侧信道攻击与防护	格密码理论及应用、算法数论
系统安全	计算机系统安全导论、操作系统安全、软件安全、可信计算、芯片安全、虚拟化与云计算安全、分布式系统与大数据安全	
	软件逆向分析、计算机入侵检测技术、恶意代码检测与防护、数据恢复技术	移动计算安全
网络安全	网络安全基础、网络系统安全导论、网络安全技术、可信网络理论与设计、计算机通信网络与安全、无线网络安全、Internet安全协议与分析、网络安全协议与标准、网络安全协议分析技术、网络攻防对抗技术、网络系统应急响应、网络安全管理原理与技术	
	网络系统安全风险评估、网络系统入侵检测与预警技术	卫星通信安全、网络溯源取证
应用安全	应用系统安全导论、信息内容安全的理论与应用、嵌入式系统安全设计、移动互联网安全、云计算安全与隐私保护、物联网安全、大数据安全、国家关键信息基础设施安全	
	Windows安全原理与技术、计算机病毒原理、社会在线网络分析及应用	网络行为学、社会学与心理学

报告提纲

- 现代密码学的发展
- 网络空间安全的范畴
- **网络通信中密码安全事件**
- 大数据与云计算安全
- 密码技术产业

互联网中的安全隐患——棱镜计划

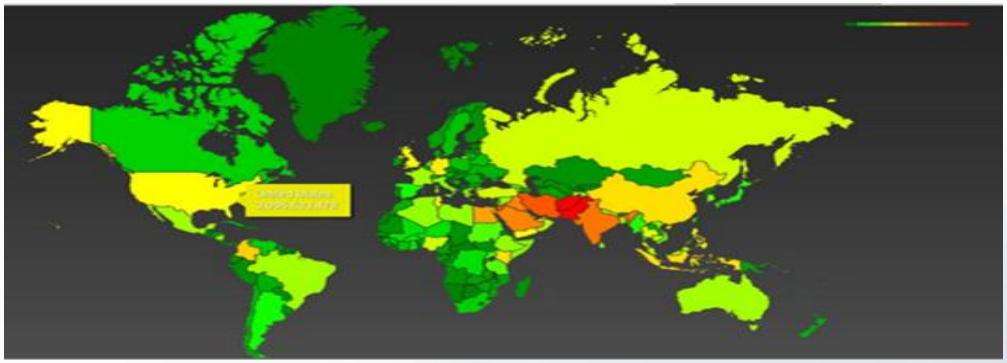
- 斯诺登事件
  - 2013年6月，被Edward Snowden公布
  - 棱镜计划（PRISM）：NSA自2007年起开始实施的绝密级电子监听计划

监听方式
语音通话
搜索记录
电子邮件
存储数据
文件传输
社交网络

Edward Snowden

互联网中的安全隐患——棱镜计划

- NSA收集信息统计
  - NSA监听各国情况：颜色越深，监听数量越大

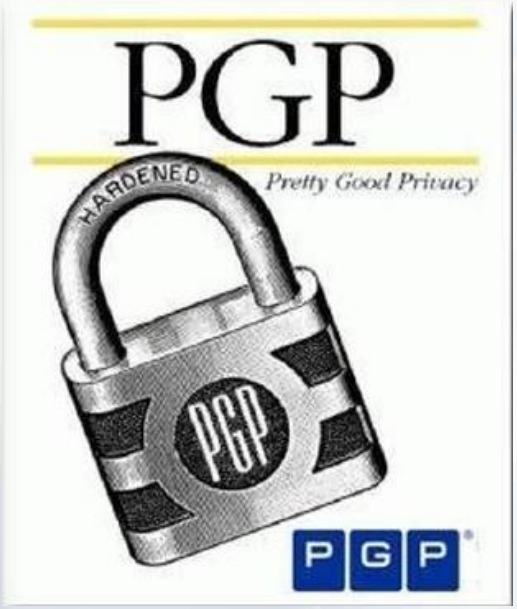


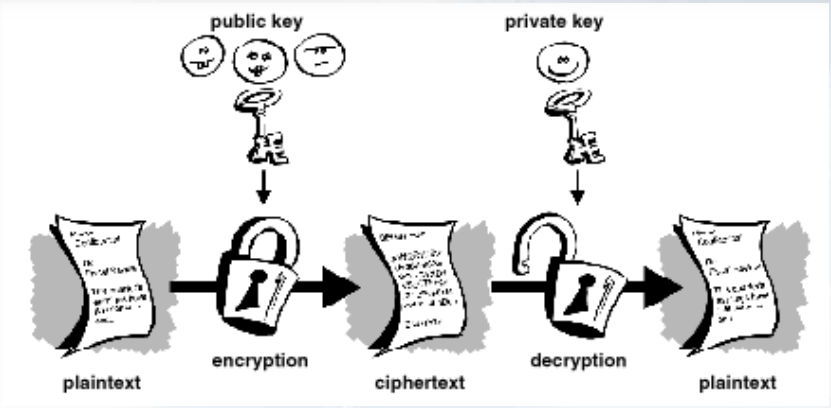
  - NSA每年收集2.5亿邮件地址
  - NSA一天收集到的电子邮件通讯薄
  - NSA一天可收集50亿手机位置

邮箱	数量
雅虎	444743
Hotmail	105068
Facebook	82857
Gmail	33697
其它	22881

互联网中的密码安全隐患

- **2012年2月，国际著名密码学家Lenstra团队公布广泛使用的基于RSA的X.509 证书和PGP密钥存在严重安全漏洞**
- **生成密钥的随机数生成器的种子空间不足，造成解密密钥关键信息发生碰撞，约有千分之二密钥不安全**





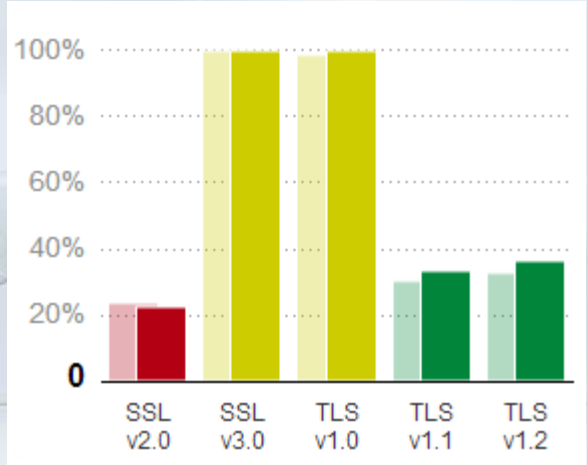
OpenSSL协议漏洞

密码协议实现漏洞攻击，OpenSSL“Heartbleed”漏洞

- 缺乏边界检查，导致内存泄漏

- 服务器上**64K**内存数据内容泄露
- 可能有安全证书、用户名与密码等

- 受影响的网站
  - TrustInet公司统计0.8%的网站受影响，包括Yahoo、Imgur等
- 建议漏洞修复



Ronald L. Rivest在On the growth of cryptography报告中介绍的密码攻击事件

Factorization of RSA-129 (April 1994)

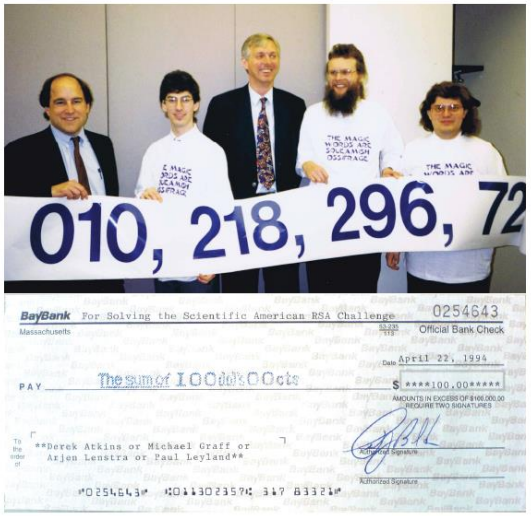
- RSA-129 =

  114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541

- Derek Atkins, Michael Graff, Arjen Lenstra, Paul Leyland: RSA-129 =

  3490529510847650949147849619903898133417764638493387843990820577 x 32769132993266709549961988190834461413177642967992942539798288533

- 8 months work by about 600 volunteers from more than 20 countries; 5000 MIPS-years.
- secret message:
  The Magic Words Are Squeamish Ossifrage



426-bit
大数分解

Factoring on a Quantum Computer?

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$|\alpha|^2 + |\beta|^2 = 1$

$\alpha|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ $\beta|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$

In 1994, Peter Shor invented a fast factorization algorithm that runs on a (hypothetical) *quantum computer* and works by determining multiplicative period of elements mod *n*.

- In 2001, researchers at IBM used this algorithm on a (real) quantum computer to factor $15 = 3 \times 5$.
- Recently (Dattani, 2014): 291311 = 557 x 523
- Dark clouds on horizon for RSA?

Hash Function Attacks

- In 2004 Xiaoyun Wang and colleagues found a way to produce *collisions* for MD5:

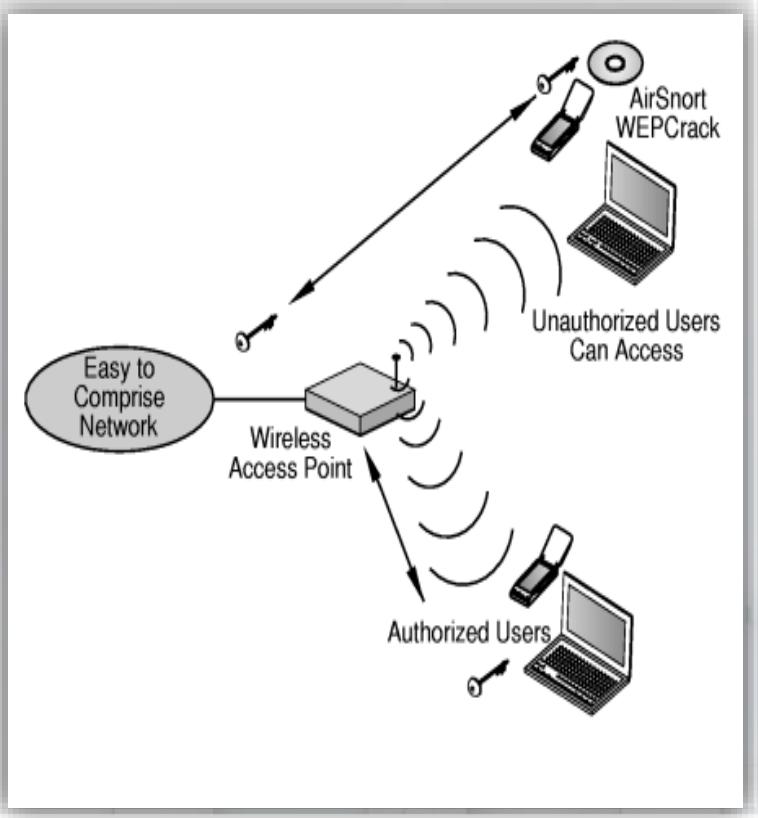
  $\mathrm{MD5}(file1) = \mathrm{MD5}(file2)$!!!

  Also for SHA-1 and many other hash functions. Major break!!
- So NIST ran a competition for new hash function standard (SHA-3 = Keccak).

https://people.csail.mit.edu/rivest/pubs/Riv11a.slides.pdf

无线网络中的密码安全问题

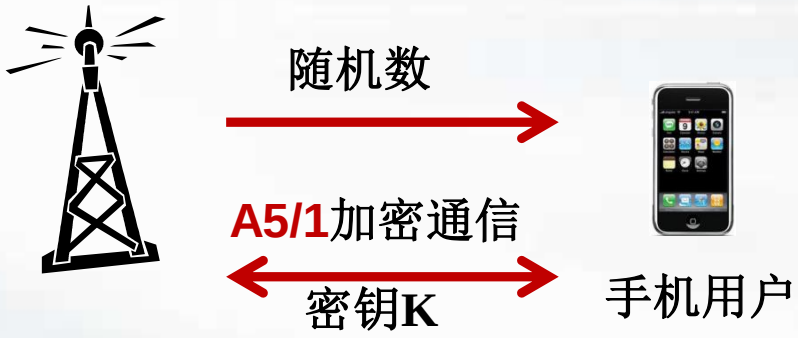
- 密码攻击：使用 AirSnort 软件等可以破解无线加密协议WEP加密的无线局域网WLAN，从而窃听用户数据
- WEP加密算法：采用RC4流密码进行加密
- 攻击原理：基于2001年Adi Shamir 等RC4密码分析结果



GSM手机通信中的安全问题

A5/1算法被破解：数据复杂度2TB，使用3-5分钟的通话明密文，可在几分钟内破解A5/1的密钥

[["GSM: SRSLY?". 26th Chaos Communication Congress (26C3)]]

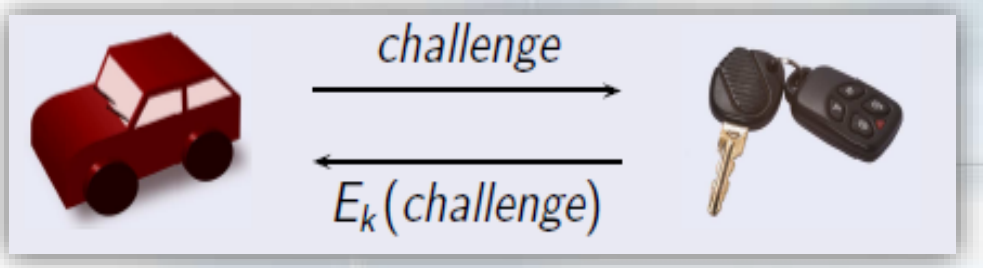


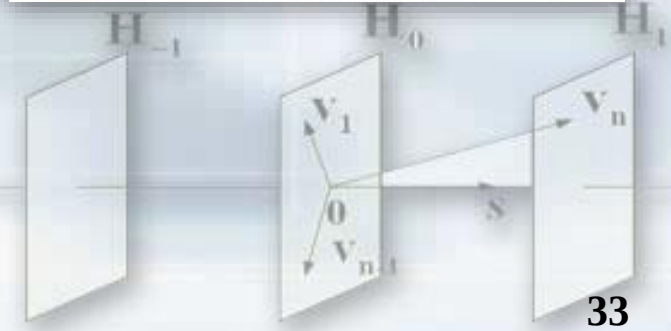
相同随机数R产生相同会话密钥！
通过手机的返回值计算密钥K，
对捕获的通讯数据进行解密

A5/1算法被替换为A5/3(Kasumi)算法，为达到兼容性，A5/1算法仍在使用，而且使用相同的密钥K。攻击者可冒充基站进行破解。

远程射频的密码安全问题

- 用于远程射频控制，如汽车钥匙等，大量采用Keeloq 算法加密。该算法原为保密算法，2006年被泄露
- Keeloq 算法攻击，Indesteege等，Eurocrypt 08
- Keeloq 算法的侧信道攻击，并成功获取密钥， Crypto 08， Paar等





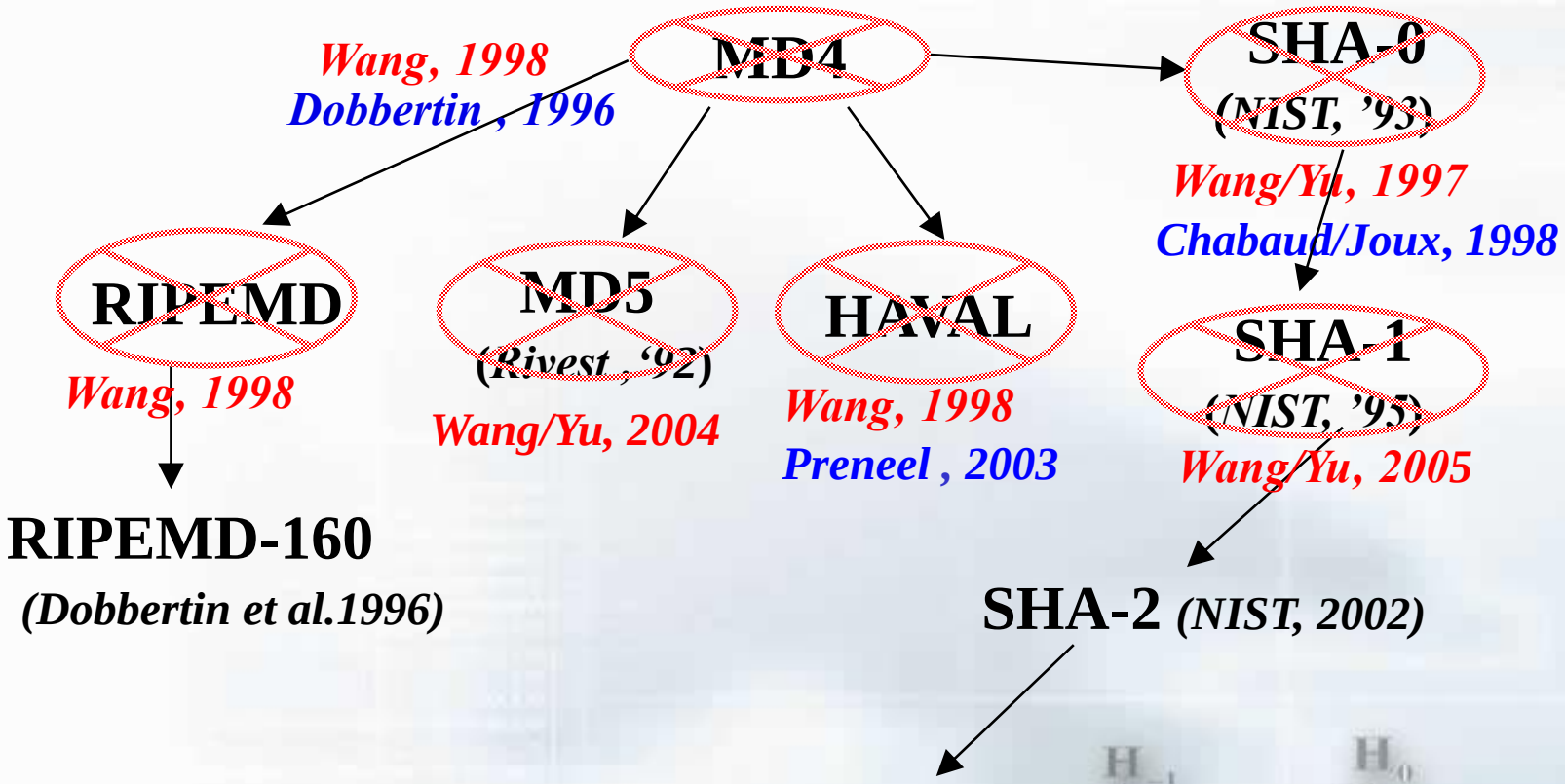
USB 安全令牌、智能卡的密码安全问题

- Prosecco 团队在 2012 年，通过对 RSA PKCS#1v1.5 消息填充的攻击，判定密文是否对应于某一个正确填充的明文，可以在短时间内恢复出明文

- 该攻击在一些基于 RSA PKCS#1v1.5 的密码设备得到了实际应用，比如 USB 安全令牌、智能卡等

- 利用这个攻击，在大约13分钟内恢复出 RSA 公司的 SecurID 800 令牌的密钥

国际通用Hash函数的碰撞攻击



2005年RSA大会宣布SHA1碰撞攻击视频

- 宣布SHA1攻击结果（7分钟视频）的五位密码学家：

  Adi Shamir：图灵奖获得者

  Ronald Rivest：图灵奖获得者

  Whitfield Diffie：2016年图灵奖得主，公钥密码学奠基人之一

  Burt Kalaski 和Paul Kocher

NIST启动新的杂凑函数标准SHA-3设计

举办两次国际 Hash函数研讨会

CSRC HOME > GROUPS > ST > HASH PROJECT

CRYPTOGRAPHIC HASH WORKSHOP

October 31-November 1, 2005

Original Call for Papers

Workshop Report

Program

NIST Gaithersburg, MD

Monday, October 31, 2005

8:15 AM - Bus departs Gaithersburg Holiday Inn for NIST

8:30 AM - 9:00 AM - Registration — Continental Breakfast

9:00 AM - 9:15 AM
Opening Remarks
Shashi Phoha, *Director, Information Technology Laboratory, NIST*
William Burr, *Manager, Security Technology Group, Computer Security Division, NIST*

9:15 AM - 9:45 AM
Keynote Speech: *Cryptanalysis of SHA-1 Hash Function* (ppt only)
Xiaoyun Wang, *Tsinghua University*

9:45 AM - 11:55 AM Session 1: Papers - Hash Collisions: Impacts and

现有Hash函数算法的安全性评估

SECOND CRYPTOGRAPHIC HASH WORKSHOP

August 24-25, 2006

Original Call for Papers

Workshop Report

Corwin Pavilion, UCSB Santa Barbara, CA

Unaccepted Papers

Thursday, August 24, 2006

1:00 PM - 5:00 PM - Registration (Corwin Pavilion Lobby)

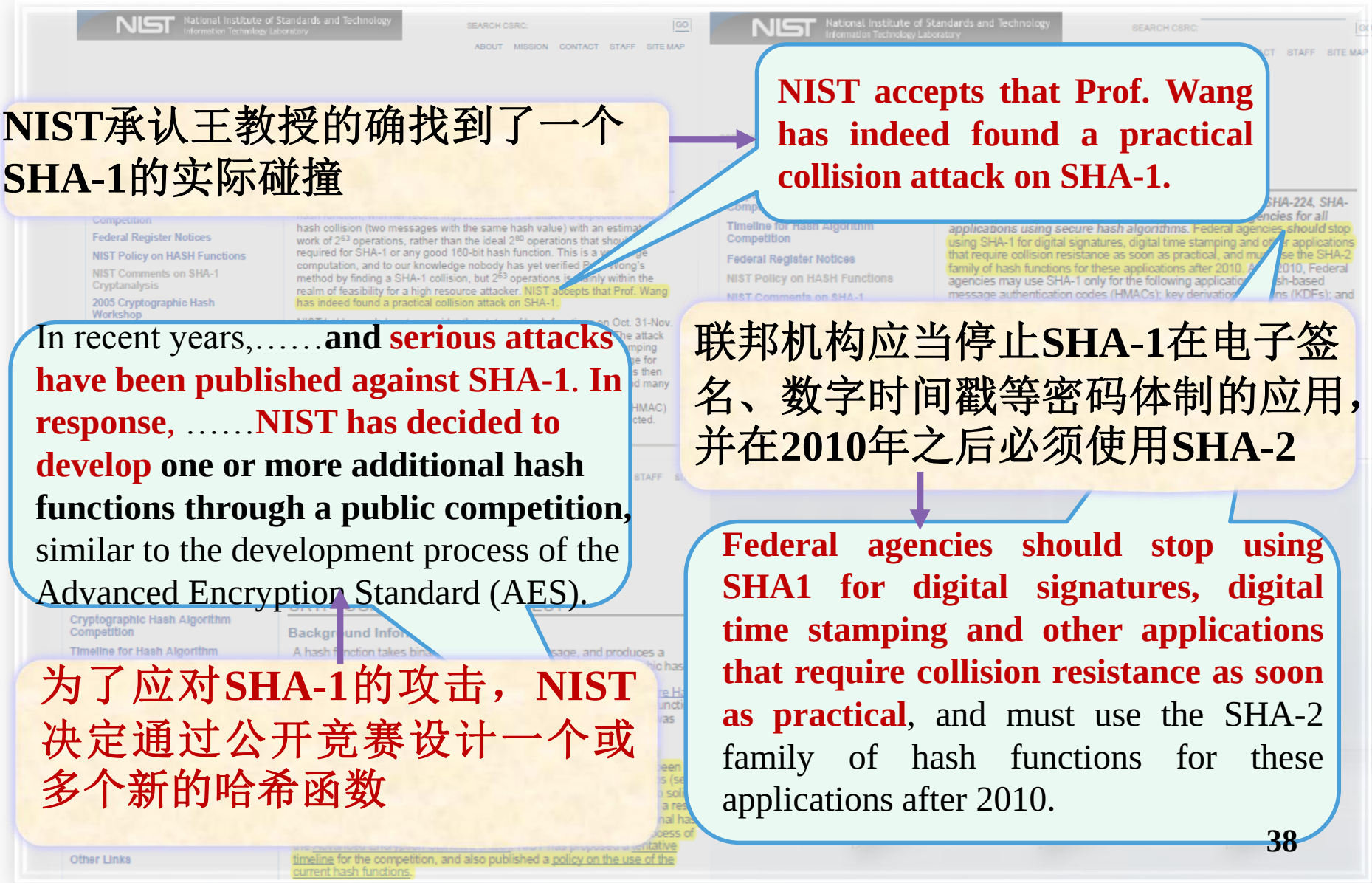
2:00 PM - 2:10 PM
Opening Remarks
William Burr, *National Institute of Standards and Technology*

2:10 PM - 3:15 PM Session 1: Papers - New Structures of Hash Functions
Session Chair: Lily Chen, *National Institute of Standards and Technology*

2:15 PM - 2:35 PM
A Framework for Iterative Hash Functions --- HAIFA [paper]
[presentation (.pdf)]
Orr Dunkelman, *Technion - Israel Institute of Technology*
Eli Biham, *Technion - Israel Institute of Technology*

新算法的征集办法讨论：多数赞成AES模式

为了应对王教授对SHA-1的攻击，NIST官方网站出台系列政策性文件



NIST承认王教授的确找到了一个SHA-1的实际碰撞

NIST accepts that Prof. Wang has indeed found a practical collision attack on SHA-1.

In recent years,……**and serious attacks have been published against SHA-1. In response, ……NIST has decided to develop one or more additional hash functions through a public competition,** similar to the development process of the Advanced Encryption Standard (AES).

联邦机构应当停止SHA-1在电子签名、数字时间戳等密码体制的应用，并在2010年之后必须使用SHA-2

为了应对SHA-1的攻击，NIST决定通过公开竞赛设计一个或多个新的哈希函数

Federal agencies should stop using SHA1 for digital signatures, digital time stamping and other applications that require collision resistance as soon as practical, and must use the SHA-2 family of hash functions for these applications after 2010.

Google应对策略

Gradually Sunsetting SHA-1

Friday, September 05, 2014

The SHA-1 cryptographic hash algorithm has been known to be considerably weaker than it was designed to be since at least 2005 — 9 years ago. Collision attacks against SHA-1 are too affordable for us to consider it safe for the public web PKI. We can only expect that attacks will get cheaper.

That's why Chrome will start the process of sunsetting SHA-1 (as used in certificate signatures for HTTPS) with Chrome 39 in November. HTTPS sites whose certificate chains use SHA-1 and are valid past 1 January 2017 will no longer appear to be fully trustworthy in Chrome's user interface.

SHA-1's use on the Internet has been deprecated since 2011, when the CA/Browser Forum, an industry group of leading web browsers and certificate authorities (CAs) working together to establish basic security requirements for SSL certificates, published their Baseline Requirements for SSL. These Requirements recommended that all CAs transition away from SHA-1 as soon as possible, and followed similar events in other industries and sectors, such as NIST deprecating SHA-1 for government use in 2010.

We have seen this type of weakness turn into a practical attack before, with the MD5 hash algorithm. We need to ensure that by the time an attack against SHA-1 is demonstrated publicly, the web has already moved away from it. Unfortunately, this can be quite challenging. For example, when Chrome disabled MD5, a number of enterprises, schools, and small businesses were affected when their proxy software — from leading vendors — continued to use the insecure algorithms, and were left scrambling for updates. Users who used personal firewall software were also affected.

We plan to surface, in the HTTPS security indicator in Chrome, the fact that SHA-1 does not meet its design guarantee. We are taking a measured approach, gradually ratcheting down the security indicator and gradually moving the timetable up (keep in mind that we release stable versions of Chrome about 6 – 8 weeks after their branch point):

Chrome 39 (Branch point 26 September 2014)

Sites with end-entity ("leaf") certificates that expire on or after 1 January 2017, and which include a SHA-1-based signature as part of the certificate chain, will be treated as "secure, but with minor errors".

The current visual display for "secure, but with minor errors" is a lock with a yellow triangle, and is used to highlight other deprecated and insecure practices, such as passive mixed content.

使用SHA-1证书的网站

Chrome浏览器将在2014年9月26日后停止对SHA-1证书的支持

Notice of AMS(美国数学学会)的评论

在2004年美密会上，王小云等由于对MD5的碰撞攻击得到了长久的欢呼……她们的攻击是对MD5的最后一击，意味着MD5出局

In 2005 the situation got worse. Wang, in collaboration with Yiqun Lisa Yin and Hongbo Yu, showed a collision attack on SHA-1 that took 2^{69} steps (instead of the expected 2^{80}) [14]; then Wang, in collaboration with Andrew Yao and Frances Yao, demonstrated a collision attack on SHA-1 that required only 2^{63} steps [15].

At a cryptography meeting in Santa Barbara, California, Xiaoyun Wang, Denggou Feng, Xuejia Lai, and Hongbo Yu **received a standing ovation for work showing collision attacks on MD5……. There had already been a move away from MD5, but this was the final blow.**

2005年情况更糟，王小云，尹依群，于红波等对SHA-1进行碰撞攻击，复杂度为2^{69}，随后，王，姚等又对结果进行了改进，复杂度为2^{63}。

AMS数学每月专栏 Mathematics and Internet Security

最近，作为安全Hash函数的支撑算法SHA-1被证明是易受攻击的，这个工作是由中国数学家王小云和她的团队完成的。……但是王小云和她的团队的进展表明了有些基于她开创的思想的巧妙变形能够威胁到现实中的系统。

介绍王小云的SHA-1攻击

L. Alberti

A. Turing

M.Rejewski

T. Elgamal

E. Friedman W. Friedman

2016年图灵奖得者

W. Diffie M.Hellman R. Merkle

三位图灵奖得主

A. Shamir, R. Rivest L. Adleman

量子算法提出者

P. Shor X. Wang

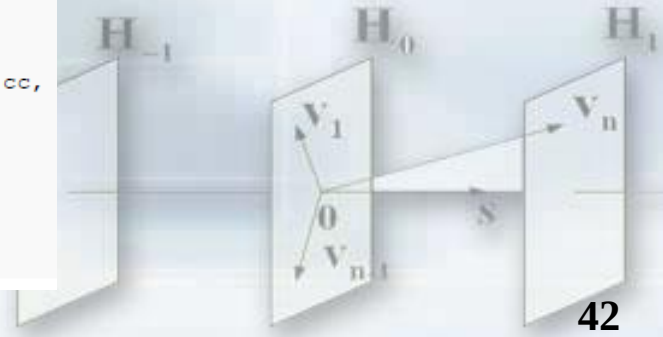
基于MD5随机碰撞的证书伪造

- X.509数字证书是国际电信联盟(ITU-T)制定的PKI(公钥密码基础设施)标准
- X.509定义了(但不仅限于)公钥证书、证书吊销清单、属性证书和证书路径验证算法等证书标准

X.509数字证书结构

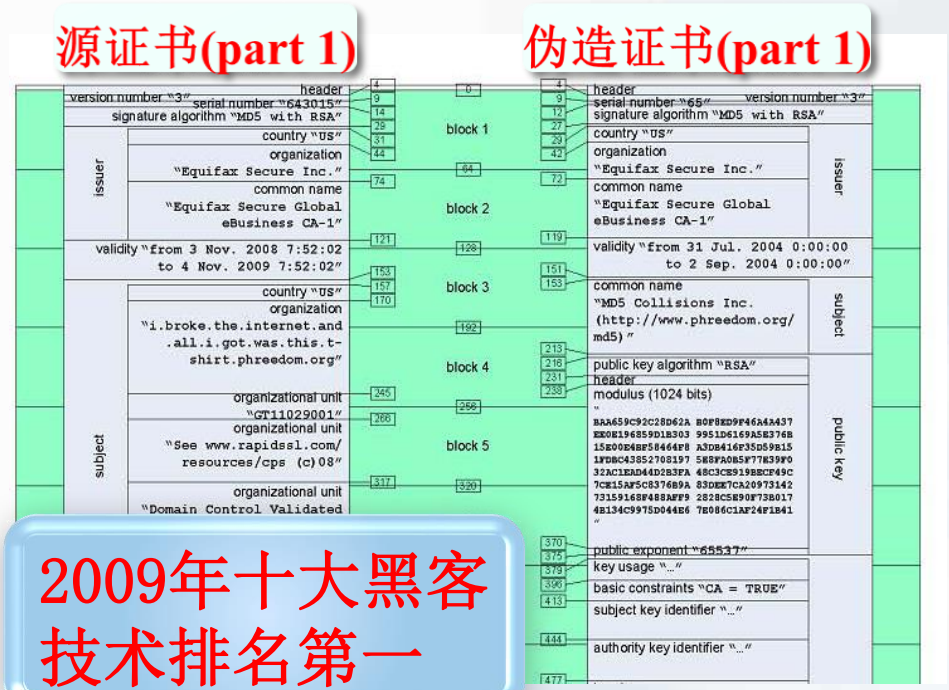
```
Certificate:
   Data:
       Version: 3 (0x2)
       Serial Number: 1 (0x1)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
               OU=Certification Services Division,
               CN=Thawte Server CA/emailAddress=server-certs@thawte.com
       Validity
           Not Before: Aug  1 00:00:00 1996 GMT
           Not After : Dec 31 23:59:59 2020 GMT
       Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
                OU=Certification Services Division,
                CN=Thawte Server CA/emailAddress=server-certs@thawte.com
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (1024 bit)
               Modulus (1024 bit):
```

采用MD5和RSA算法对证书签名



基于MD5随机碰撞的证书伪造

- 2005年Lenstra, Wang等给出同一个用户拥有不同公钥证书的伪造
- 2008年Sotirov, Stevens等在CCC大会上演示了通过MD5碰撞伪造的证书可以被浏览器当作是有效的、可信的证书



2009年十大黑客技术排名第一

Arjen Lenstra等[IJACT, 2012]MD5数字证书伪造论文基于王的工作建议

国际著名数学家、顶级密码学家，数域筛法和格基约化算法LLL的第一作者，768比特大整数分解和RSA-768挑战数的破解者之一。

Although Wang's random looking collision blocks by themselves do not pose any dange

虽然王找到的看起来随机的碰

First, **for any meaningful common prefix collision blocks (M; M') may be**

可以利用王的方法构造基于任

Given this message pair, **we modify a suggestion by Xiaoyun Wang (private**

根据王小云的改进建议，我们找到

This was suggested by Xiaoyun Wang be with this type of message difference the nu of bitconditions over the finnal two and a h

王小云建议利用这种类型的明文差分，最后两轮半的比特条

In [14] and [21] **it was shown how any exis MD5 collision, such as the ones originally presented by Xiaoyun Wang at the Crypt**

基于已有的MD5碰撞（例如王小云在Crypto 2004 的上提出的

This work benefited greatly from suggestions by Xiaoyun Wang

王小云对本工作的建议让我们受益匪浅。

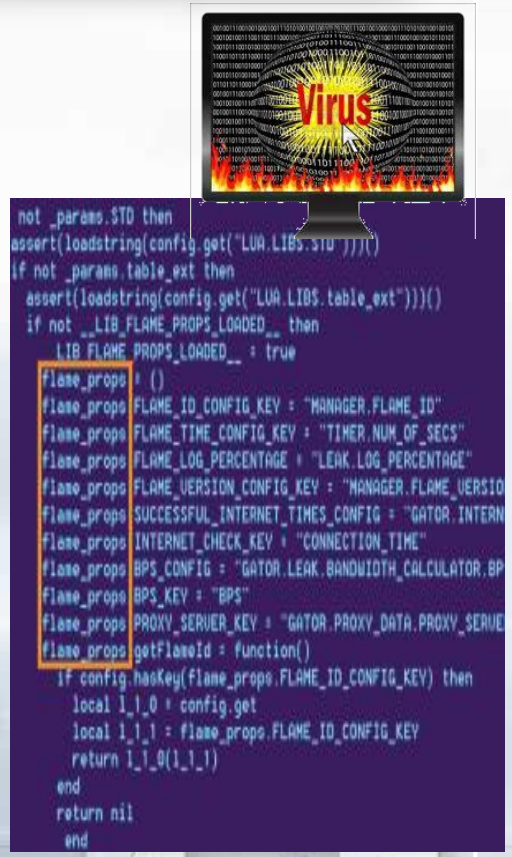
电子认证密码安全问题：数字证书的伪造

火焰病毒(Worm.Win32.Flame)

- 2012年5月，被俄罗斯安全专家发现
- 攻击范围

截获键盘输入
记录音频对话
获取截屏画面
监测网络流量

传送



- 搜集数据任务完成，自行毁灭，不留踪迹

电子认证密码安全问题：数字证书的伪造

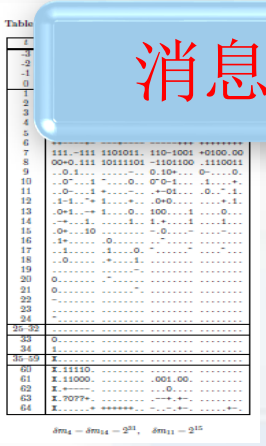
火焰病毒中的关键密码技术

微软终端服务器
许可服务证书签名的代码 (MD5)

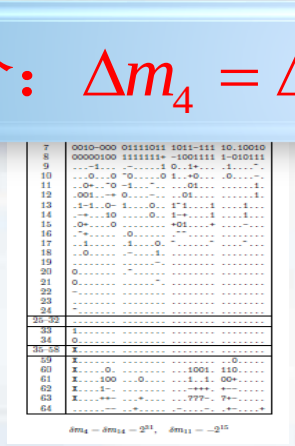
伪造证书
签名的病毒代码 (MD5)

- “火焰”采用选择前缀MD5碰撞攻击的新变体伪造证书，主体路线使用王小云等在Eurocrypt 05给出的路线

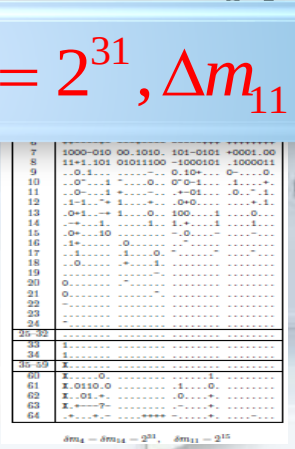
消息差分：$\Delta m_4 = \Delta m_{14} = 2^{31}, \Delta m_{11} = \pm 2^{15}$



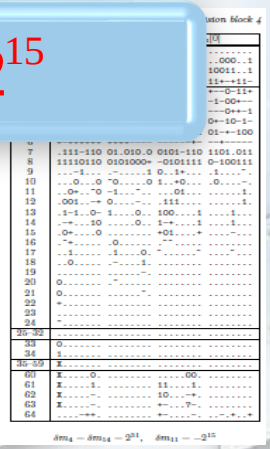
Block1



Block2



Block3



Block4

美国计算机应急小组应对策略

- 美国计算机应急小组（US-CERT）：发表了题为“MD5 vulnerable to collision attacks”

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Vulnerability Note VU#836068

MD5 vulnerable to collision attacks

Overview

I. Description

II. Impact

III. Solution

We are currently unaware of a practical solution to this problem.

Do not use the MD5 algorithm

Scrutinize SSL certificates signed by certificates using the MD5 algorithm

System: Affected

Vendor	Status	Date Notified	Date Updated
Microsoft Corporation	Unknown		2008-12-31
Mozilla	Unknown		2008-12-31
Verisign	Unknown		2008-12-31

MD5的碰撞弱点，使攻击者能够生成密码口令或者其他不合法的数据都能被认证。

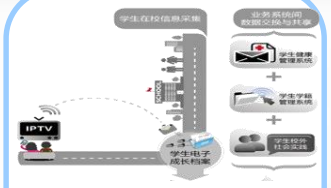
软件开发商，认证中心，网站和用户应该避免使用 **MD5算法**，以前的研究已经证明，从密码学的角度认为被破解的算法不再适合将来的应用

报告提纲

- 现代密码学的发展
- 网络空间安全的范畴
- 网络通信中密码安全事件
- **大数据与云计算安全**
- 密码技术产业

大数据

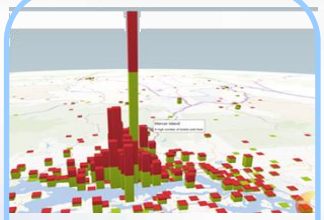
- 海量数据存储、传输、处理与利用（挖掘、开发等）
- 通常需要大型计算能力



教育信息系统

医疗卫生

监控系统



银行、证券

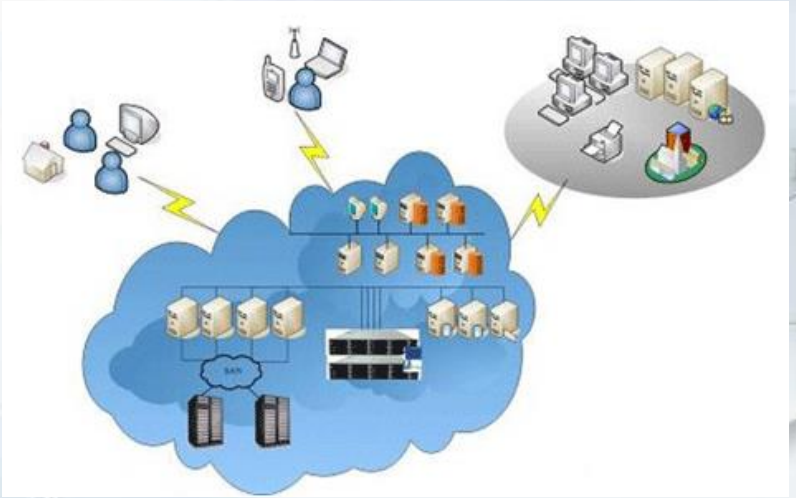
社交网络

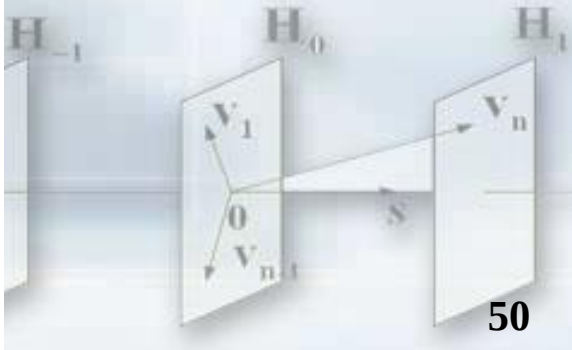
气候、天气

卫星导航

云计算

- 基于互联网的超级计算方式
- 共享软硬件资源和信息：存储资源、计算能力等
- 为用户提供所需的计算机服务：存储、计算等
- 云计算为大数据收集、存储、处理和利用提供基础设施和技术支持
  - 硬件资源：存储设施、计算能力
  - 软件资源：分布式数据库、分布式数据挖掘





云计算应用—Bitcoin挖掘

- **Bitcoin——基于计算资源货币**
  - 利用密码困难问题——SHA-2原像求解生成和交易

- **Cloud Mining、CPU、GPU、FPGA、 ASIC等方式计算**
- **值得思考的问题：世界计算能力的分布？**

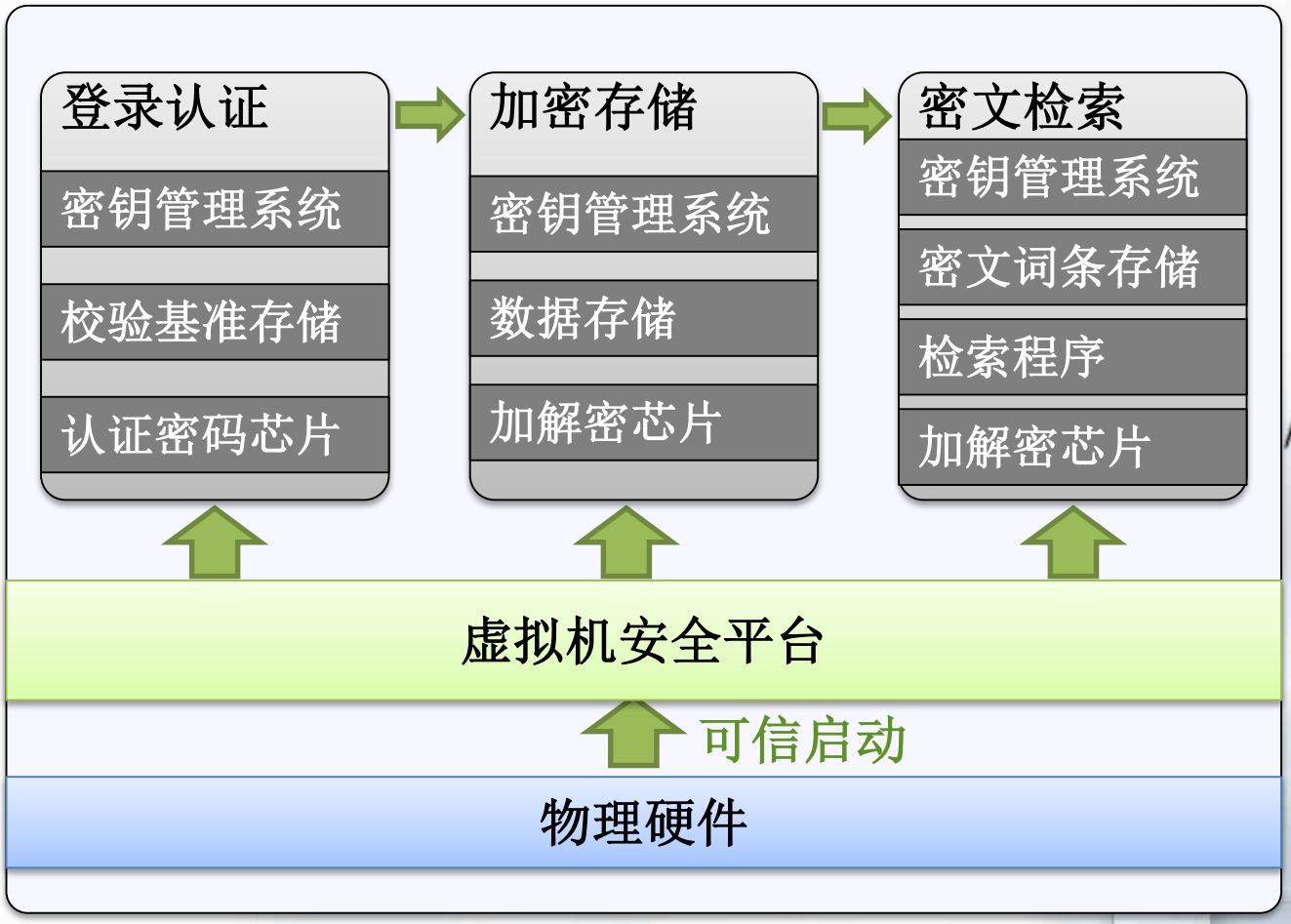
RANK	COUNTRY	NODES
1	United States	2953 (38.72%)
2	Germany	490 (6.53%)
3	United Kingdom	444 (5.02%)
4	Canada	441 (5.70%)
9	Australia	174 (2.28%)
10	Sweden	132 (1.73%)

More»

Map shows concentration of reachable Bitcoin nodes found in countries around the world.

比特币去中心化的电子认证技术近期受到国内外高度关注，拟被用于各种网络应用设计中

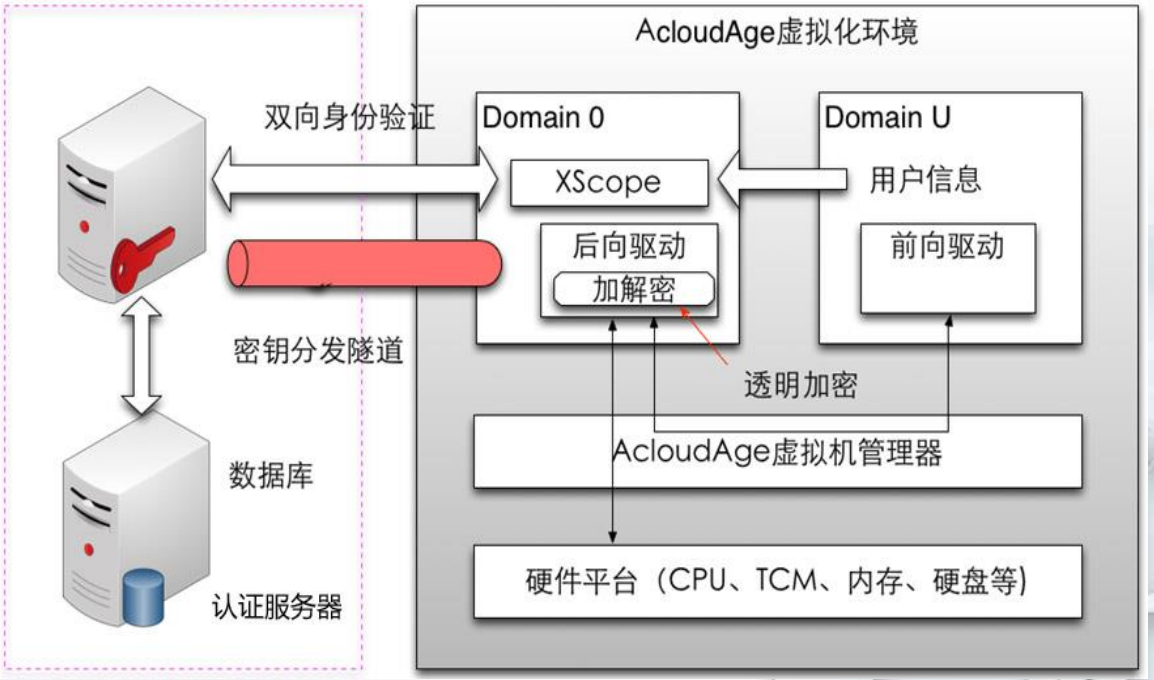
大数据的密码保障技术


登录认证
密钥管理系统
校验基准存储
认证密码芯片
加密存储
密钥管理系统
数据存储
加解密芯片
密文检索
密钥管理系统
密文词条存储
检索程序
加解密芯片
虚拟机安全平台
可信启动
物理硬件


安全传输

用户数据透明加解密

- 虚拟化平台下磁盘加密方案
  - 使用XTS模式，加解密算法能够并行处理
  - 加密模式与磁盘格式相结合，将磁盘地址作为唯一加密参数
  - 磁盘加解密对用户透明



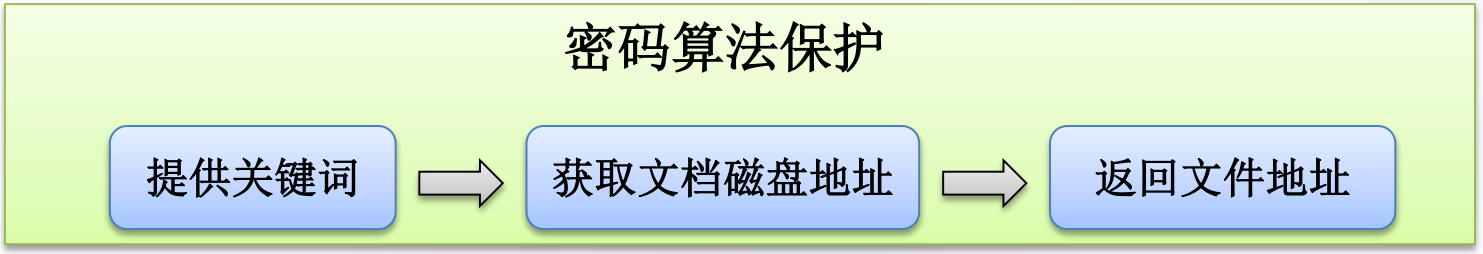
磁盘数据密文检索

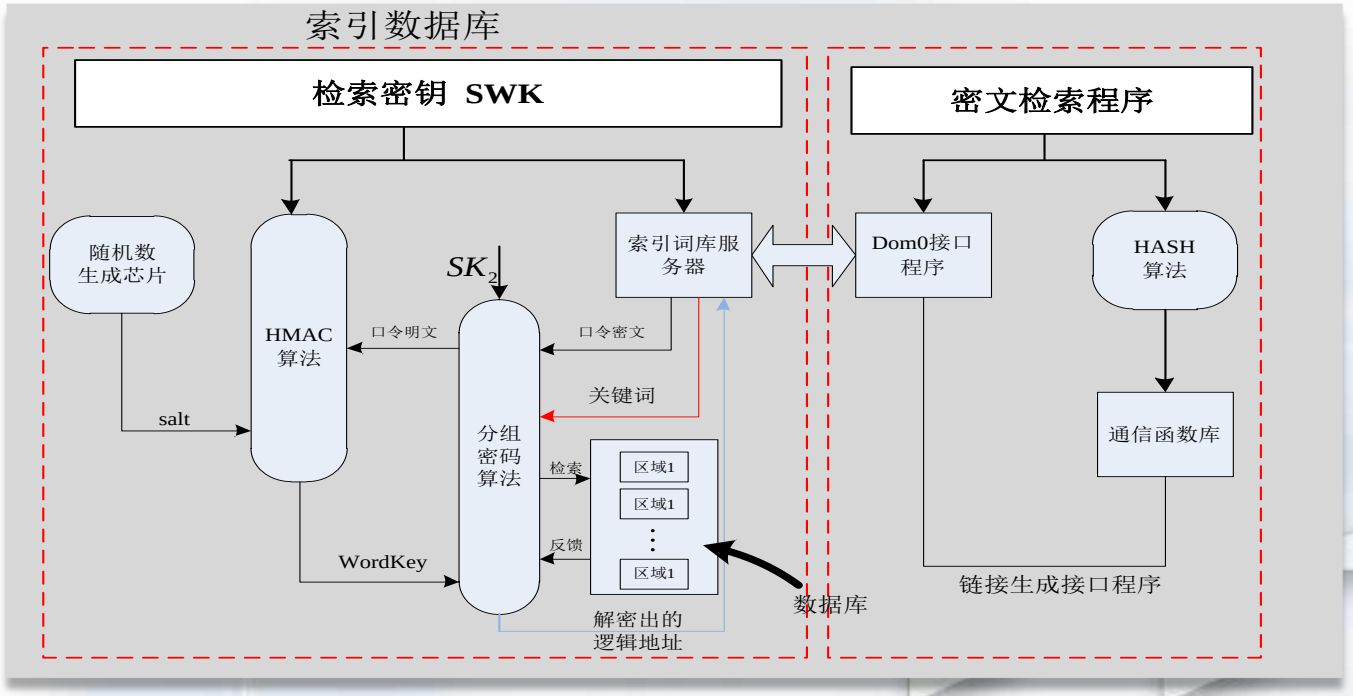
- 建立基于关键词的索引数据库，并对索引词条加密

用户名ID_1	WordKey 密钥生成参数 （salt）	密文词条	逻辑地址密文	……	逻辑地址密文	哈希值
		密文词条	逻辑地址密文	……	逻辑地址密文	哈希值
		……	……	……	……	哈希值
		密文词条	逻辑地址密文	……	逻辑地址密文	哈希值
用户名ID_2	WordKey 密钥生成参数 （salt）	密文词条	逻辑地址密文	……	逻辑地址密文	哈希值
		密文词条	逻辑地址密文	……	逻辑地址密文	哈希值
		……	……	……	……	哈希值
		密文词条	逻辑地址密文	……	逻辑地址密文	哈希值

磁盘数据密文检索

- 密文检索流程

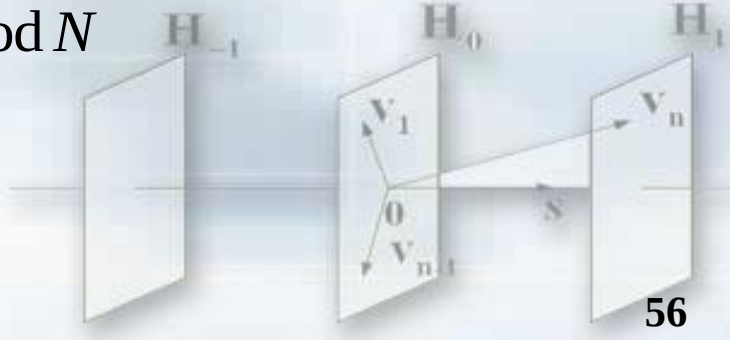




同态加密

- **同态加密的思想最早由Rivest等在设计RSA算法的过程中提出**
- **基础的RSA算法是满足乘法同态的加密算法：**
  - 给出RSA的公钥：$pk=(N,e)$，密文：$\{\psi_i \leftarrow \pi_i^{\mathrm{e}} \bmod N\}$
  - 在不解密的情况下可以对密文进行乘法操作，所得结果与用同一方法处理明文一致：

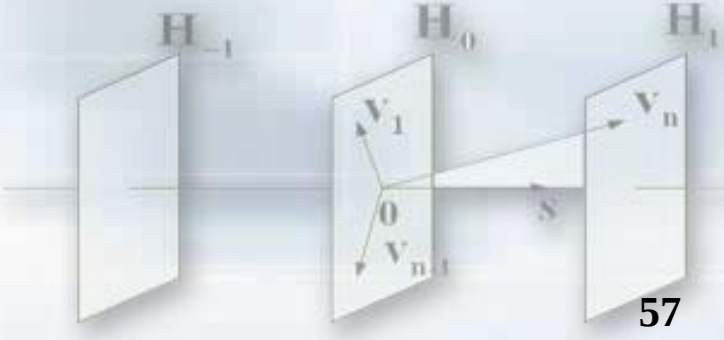
$$\prod_i \psi_i = (\prod_i \pi_i)^e \bmod N$$



同态加密

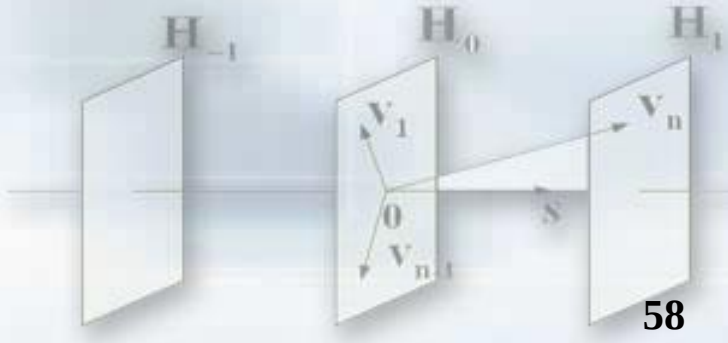
- **Rivest等进一步提出问题：是否存在一种具有全同态性质的加密方法，对任意操作（主要为加法和乘法操作）均满足以上性质，即对任意的** $c_i = \mathrm{Encrypt}(pk, m_i)$
  - 满足加法同态，即 $\sum_i c_i = \mathrm{Encrypt}(pk, \sum_i m_i)$
  - 满足乘法同态，即 $\prod_i c_i = \mathrm{Encrypt}(pk, \prod_i m_i)$

- **几类可行的全同态加密方法被提出：**
  - 基于理想格
  - 基于整数问题



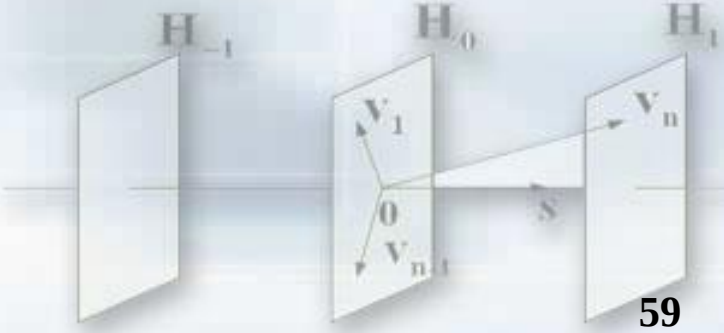
基于理想格的全同态加密

- **由Gentry于2009年在STOC发表的文章中提出**
- **其主要思想是：**
  - 密文 $\psi = \boldsymbol{v} + \boldsymbol{x}$ ，其中 $\boldsymbol{v}$ 是理想格， $\boldsymbol{x}$ 是由明文 π 加密的偏移向量
  - 根据理想格的性质，可将密文 ψ 视为多项式环 $Z[x]/f(x)$ 中元素的系数向量，因此满足加法和乘法同态
  - 其安全性基于固定环上理想格的CVP问题



基于整数问题的全同态加密

- **由Dijk等于2010年在EUROCRYPT发表的文章中提出**
- **其主要思想是：**
  - 对一个明文比特 $m \in \{0,1\}$ ，选择一个奇整数 $p \in [2^{\eta-1}, 2^{\eta})$ 为私钥，选择一组整数 $x_i = q_i p + 2r_i$ 作为公钥，其中 $q_i, r_i \in [2^{\gamma-1}, 2^{\gamma})$
  - 密文 c 由 m 与 x_i 中数个元素求和计算
  - 解密过程为 $m = (c \bmod p) \bmod 2$
  - 由于整数模运算的性质，方法满足加法及乘法同态
  - 其安全性基于大整数的因数分解问题



大数据引发的安全问题

- 存储、处理、开发等过程中面临诸多安全风险
- 个人隐私问题
  - 浏览记录、购物记录、朋友关系、刷卡习惯等
- 企业信息安全面临多重挑战
  - 电子邮件营销公司艾司隆(Epsilon)发生黑客入侵事件
  - 受害企业包括摩根大通、第一资本集团、万豪饭店、美国银行、花旗银行及电视购物网络等
- 国家安全受到信息战和网络恐怖主义威胁
  - “棱镜门”事件

报告提纲

- 现代密码学的发展
- 网络空间安全的范畴
- 网络通信中密码安全事件
- 大数据与云计算安全
- 密码技术产业

密码算法标准

- 国际密码算法标准：AES、RSA等
- 我国商用密码算法标准
  - SM4：分组加密算法，用于无线局域网产品
  - SM3：Hash函数算法 （王小云主持设计）
  - SM2：ECC公钥加密算法与签名算法

SM3的产业化应用


SM3
电子签名类
服务系统
计算机安全
登录系统
Password
计算机安全
通信系统
国家电网
数字证书
金融类
系统
中华人民共和国
社会保障卡
社会保障
系统
电子政务
安全云计算平台
和大数据
教育信息
系统

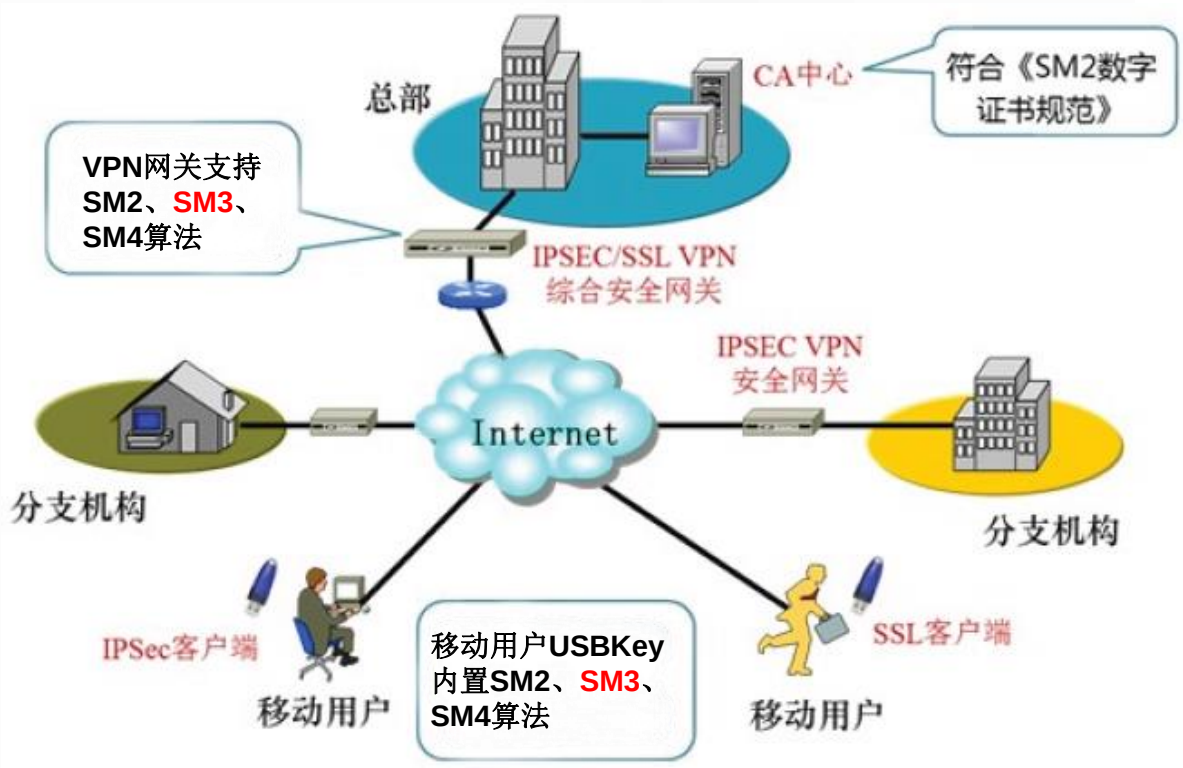
SM3的产业化应用

- **SM3被纳入我国22个重要行业规范中，涵盖计算机通信系统、数字证书、金融系统、国家电网、医疗保健、教育和交通系统等**
  - 含SM3具金融功能的社会保障卡与智能电表卡全国已普及推广
  - 经国家密码管理局审批的含SM3的密码产品640余款，其中224款销售3.4亿台（数据来源于国家密码管理局的统计数据）
  - 仅U盾超过5亿
- **SM3纳入操作系统中支持的Z32H320TC 系列芯片**
  - 支持TPM2.0的中国第一款芯片
  - 该芯片支持Windows 8/8.1, Redhat, Vmware等.
  - 该芯片集成于面向中国的Microsoft Surface Pro 3 pad

SM3申请ISO标准，与SHA-3等一起进入CD阶段

计算机网络安全通信

- 《IPSec VPN技术规范》等众多密码行业标准




国家商用密码管理办公室
www.oscca.gov.cn

国家密码管理局公告

（第 28 号）

现发布《IPSec VPN技术规范》等17项密码行业标准，自发布之日起实施。

标准编号及名称具体如下：

GM/T 0022-2014 《IPSec VPN技术规范》

GM/T 0023-2014 《IPSec VPN 网关产品规范》

GM/T 0024-2014 《SSL VPN技术规范》

GM/T 0025-2014 《SSL VPN 网关产品规范》

GM/T 0026-2014 《安全认证网关产品规范》

GM/T 0027-2014 《智能密码钥匙技术规范》

GM/T 0028-2014 《密码模块安全技术要求》

GM/T 0029-2014 《签名验签服务器技术规范》

GM/T 0030-2014 《服务器密码机技术规范》

GM/T 0031-2014 《安全电子签章密码技术规范》

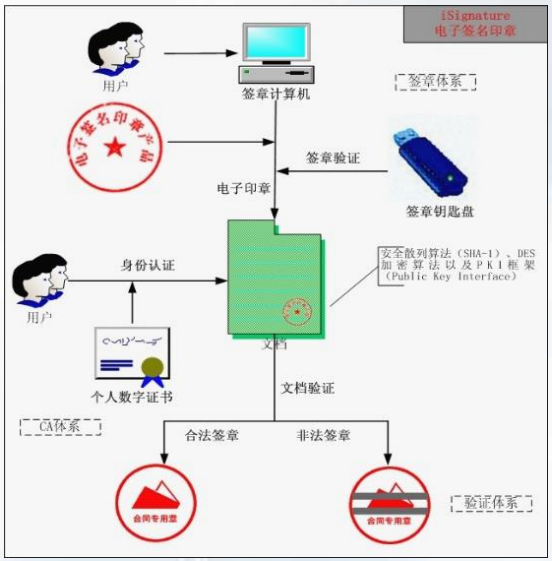
GM/T 0032-2014 《基于角色的授权管理与访问控制技术规范》

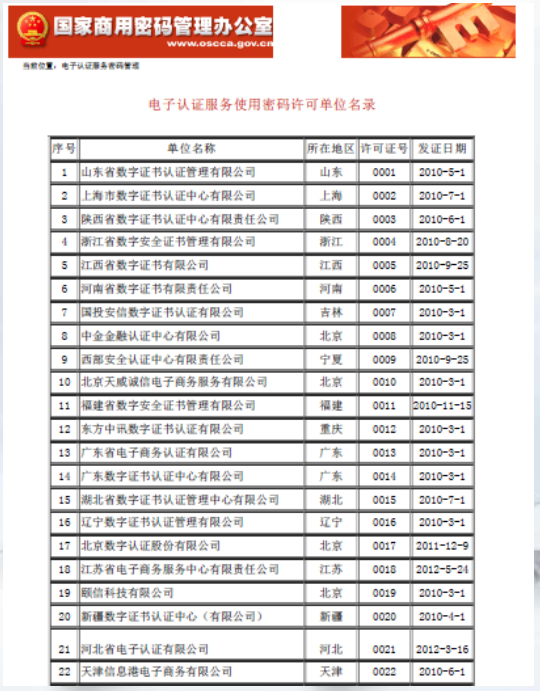
GM/T 0033-2014 《时间戳接口规范》

GM/T 0034-2014 《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》

电子认证

- 以数字证书(CA)为核心技术的加密技术，对传输的信息进行加密、解密、数字签名和数字验证
- 电子政务和电子商务中的核心环节
- 遍布24个省的38家单位获电子认证服务使用密码许可
  - 数字证书服务机构
  - 电子签章





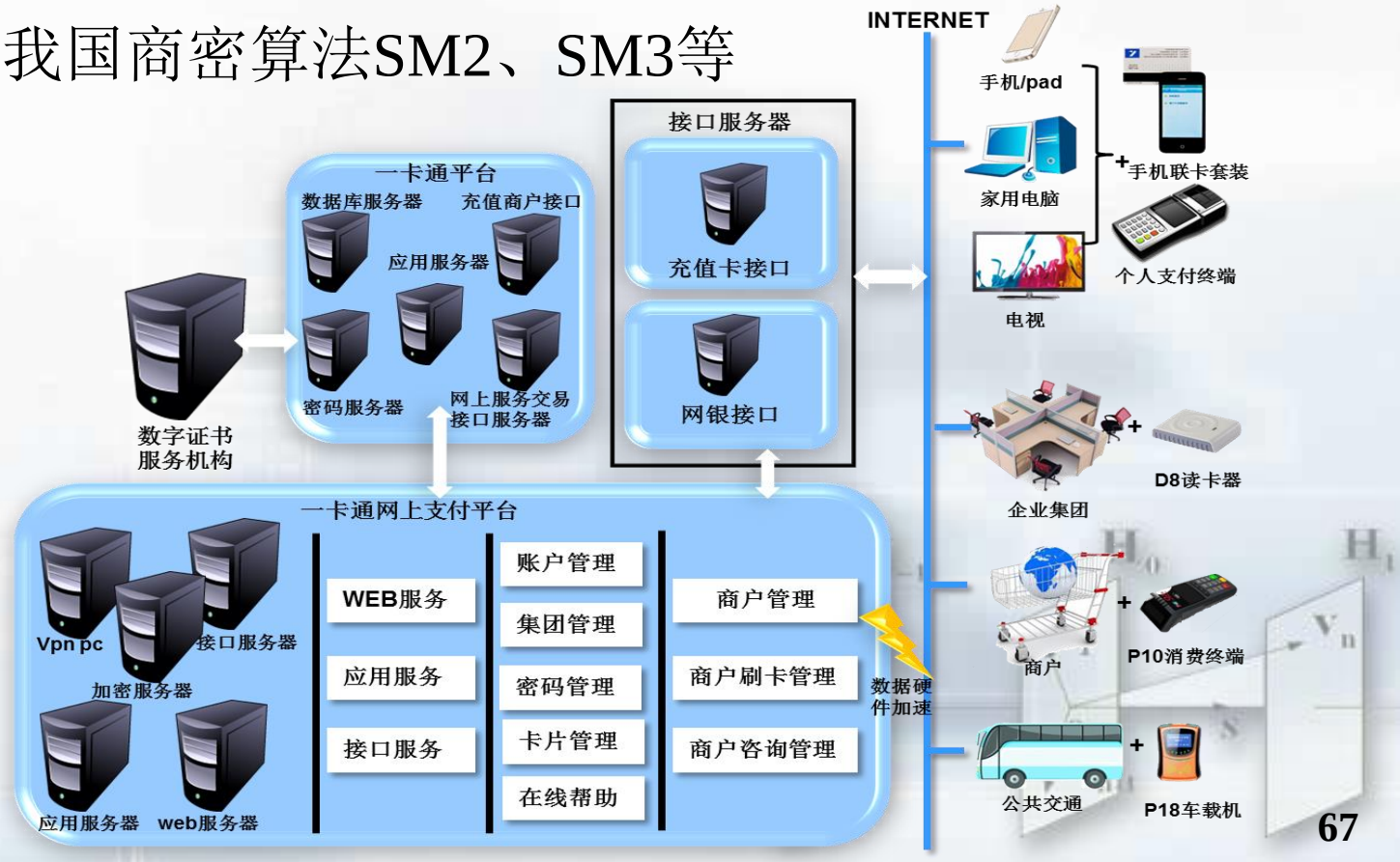
国家商用密码管理办公室
www.oscca.gov.cn

电子认证服务使用密码许可单位名录

序号	单位名称	所在地区	许可证号	发证日期
1	山东省数字证书认证管理有限公司	山东	0001	2010-5-1
2	上海市数字证书认证中心有限公司	上海	0002	2010-7-1
3	陕西省数字证书认证中心有限责任公司	陕西	0003	2010-6-1
4	浙江省数字安全证书管理有限公司	浙江	0004	2010-8-20
5	江西省数字证书有限公司	江西	0005	2010-9-25
6	河南省数字证书有限责任公司	河南	0006	2010-5-1
7	国投安信数字证书认证有限公司	吉林	0007	2010-3-1
8	中金金融认证中心有限公司	北京	0008	2010-3-1
9	西部安全认证中心有限责任公司	宁夏	0009	2010-9-25
10	北京天威诚信电子商务服务有限公司	北京	0010	2010-3-1
11	福建省数字安全证书管理有限公司	福建	0011	2010-11-15
12	东方中讯数字证书认证有限公司	重庆	0012	2010-3-1
13	广东省电子商务认证有限公司	广东	0013	2010-3-1
14	广东数字证书认证中心有限公司	广东	0014	2010-3-1
15	湖北省数字证书认证管理中心有限公司	湖北	0015	2010-7-1
16	辽宁数字证书认证管理有限公司	辽宁	0016	2010-3-1
17	北京数字认证股份有限公司	北京	0017	2011-12-9
18	江苏省电子商务服务中心有限责任公司	江苏	0018	2012-5-24
19	顺信科技有限公司	北京	0019	2010-3-1
20	新疆数字证书认证中心（有限公司）	新疆	0020	2010-4-1
21	河北省电子认证有限公司	河北	0021	2012-3-16
22	天津信息港电子商务有限公司	天津	0022	2010-6-1

安全支付

- 电子认证、网上银行、金融IC卡及移动支付
- 中国人民银行发布了《中国金融集成电路（IC）卡规范（V3.0）》
  - 支持我国商密算法SM2、SM3等



智能电网系统安全

- 智能电网连接着多种系统，智能仪表以及通信网络，将各种操作系统融合在一起，提供可视的，可监控的电网系统
- 对智能仪表、仪表数据管理平台，电网中的终端设备提供安全防护
- 采用我国商用密码算法SM2、SM3等

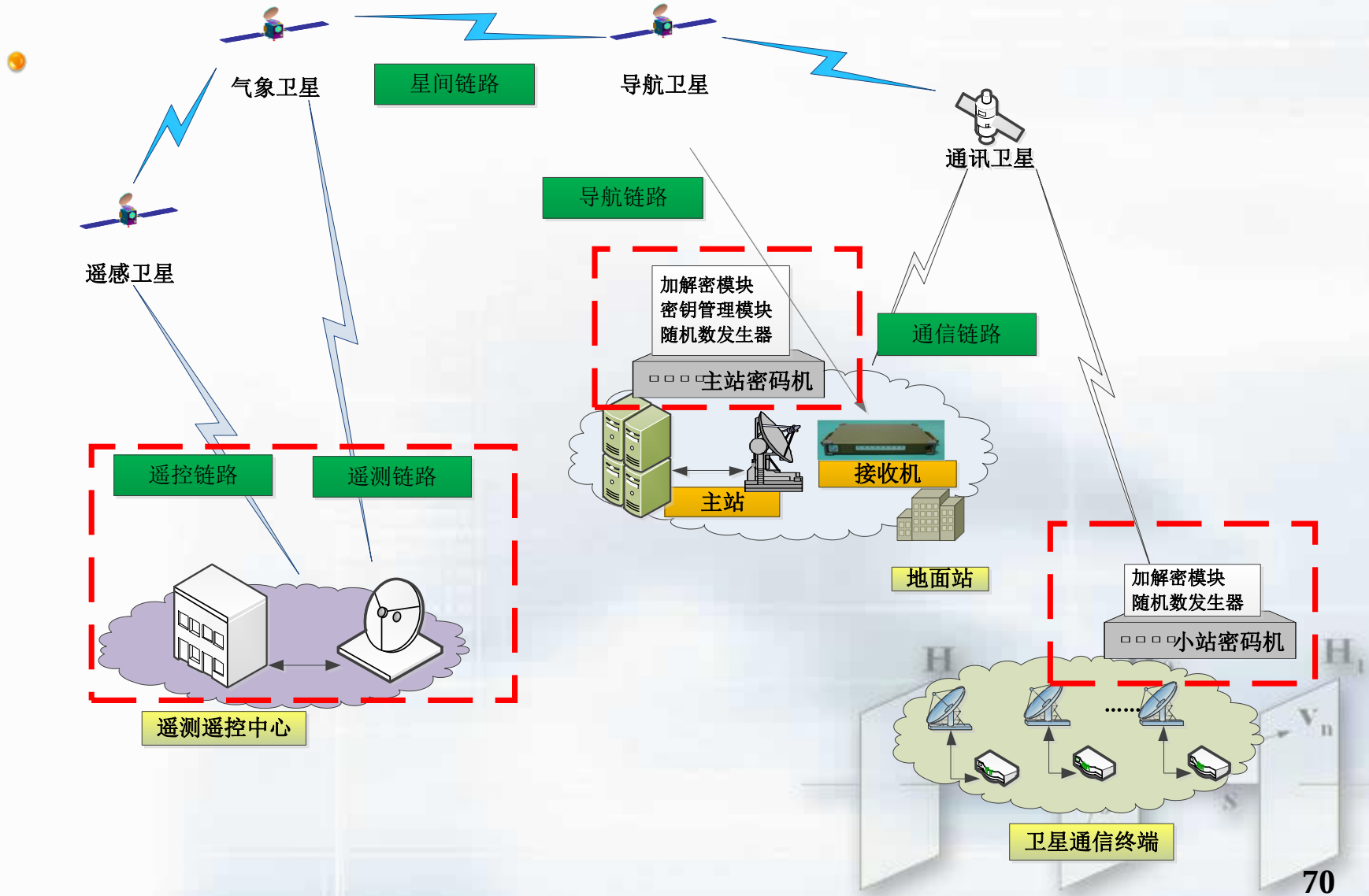
国家电网公司 STATE GRID CORPORATION OF CHINA

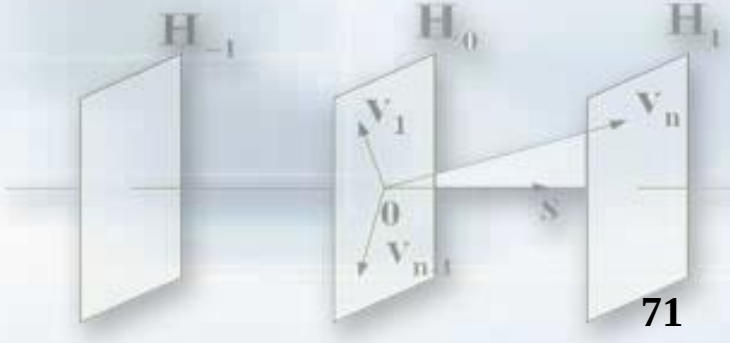
电网和核电网络是美国网络部队重点保护网络

教育系统安全

- 教育信息采集安全
  - 高校、高中、初中、小学
  - 互联互通
- 教育办公网络安全
  - 学籍管理、学校管理
- 教育资源保护
  - 远程教育
  - 在线课堂

卫星安全通信


气象卫星
星间链路
导航卫星
通讯卫星
导航链路
遥感卫星
加解密模块
密钥管理模块
随机数发生器
主站密码机
通信链路
遥控链路
遥测链路
主站
接收机
地面站
加解密模块
随机数发生器
小站密码机
遥测遥控中心
卫星通信终端


H-1
H0
H1
V1
Vn
0
Vn-1
S

谢 谢！