大数据利用中的密码安全态势与法律趋势

马民虎

西安交通大学信息安全法律研究中心

2017-09-22

大数据时代数据大爆炸

- 行为数据化
- 决策数据化
- 安全数据化

目录

大数据利用中的安全新态：密码再生

大数据变革

安全边界模糊

密码

数据安全新态

- 全球化整合
- 跨界联动
- 智能自动化
- ……

- 加密大搜索
- 动态数据加密
- 静态数据加密

大数据利用中的安全新态：密码再生

国密局商密办领导：

网络安全关系国家安全、社会稳进和人民利益，**网络安全的新态势、新需求、新发展，都需要密码发挥不可替代的重要作用**

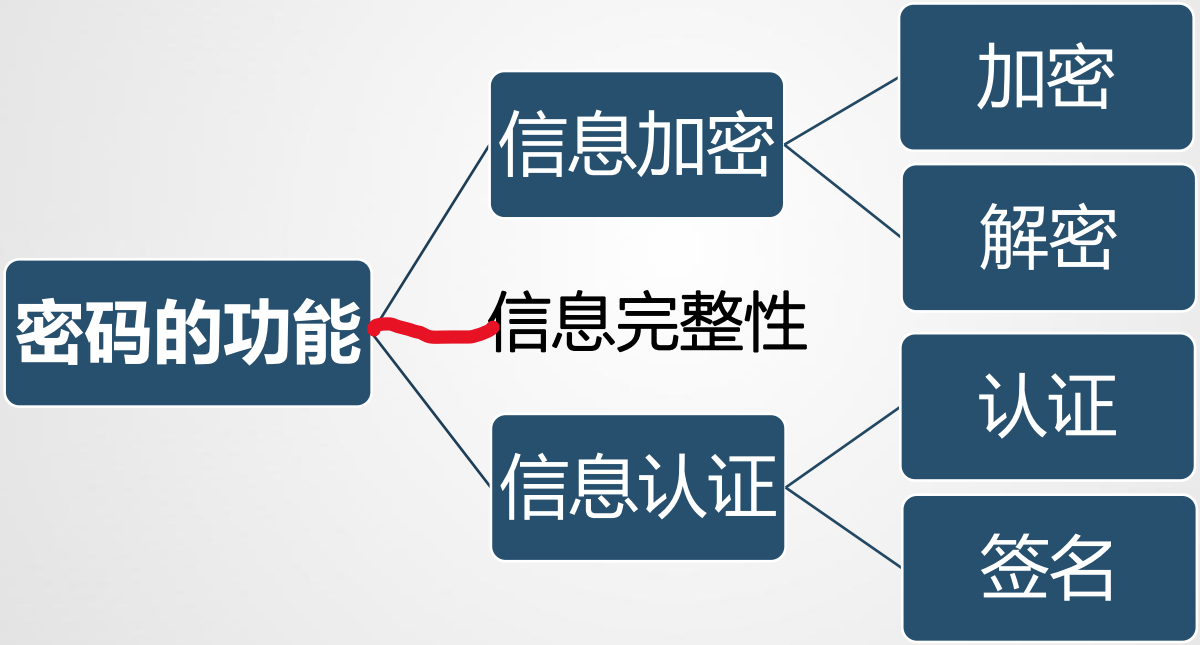
倡导新的安全理念，就是要通过密码实现可信互联、安全互通，贯彻习总书记提出的平等、创新、共享、安全的互联网发展理念

推动建立新的安全体制，要树立总体国家安全观为统领，以密码为核心技术为基础支撑的网络体系安全观

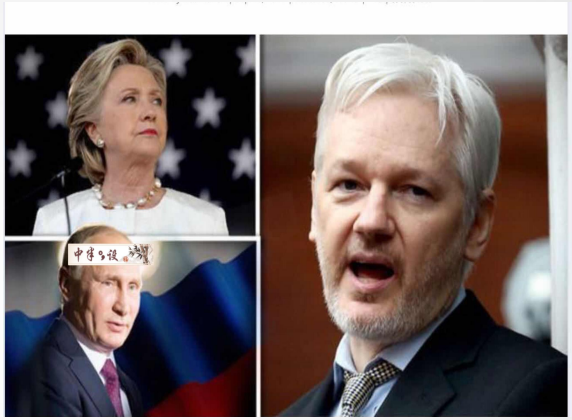
创建新的安全环境，构建起以密码为基础支撑的系统的、完善的网络安全保障体系

1

大数据利用中的安全新态：密码再生

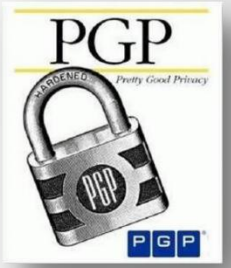


大数据利用中的安全态势：大泄密



2

大数据利用中的安全态势：密码漏洞



2012年**2**月，国际著名密码学家**enstra**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。

2014年4月7日，OpenSSL协议“心脏出血”漏洞服务器上64K内存数据内容泄露，可能包括安全证书、 用户名与密码等。

2

大数据利用中的安全态势：密码滥用

2 大数据利用中的安全态势：证书被盗

2

大数据利用中的安全态势：可信粒度结构化

国家可信 

 企业可信

产品/服务可信 

 人员可信

2 大数据利用中的安全态势：虚拟货币威胁

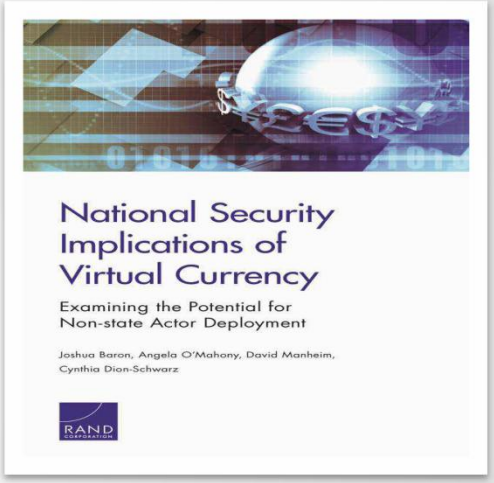
包括恐怖组织的亚国家集团在利用虚拟货币

目的在增强其经济和政治能力

美国NSA早在2015年开始对其进行研究

兰德公司利用网络威胁六级框架对恐怖分子部署虚拟货币进行了分析

从另一方面可以看出这次勒索软件事件是一次攻击预演

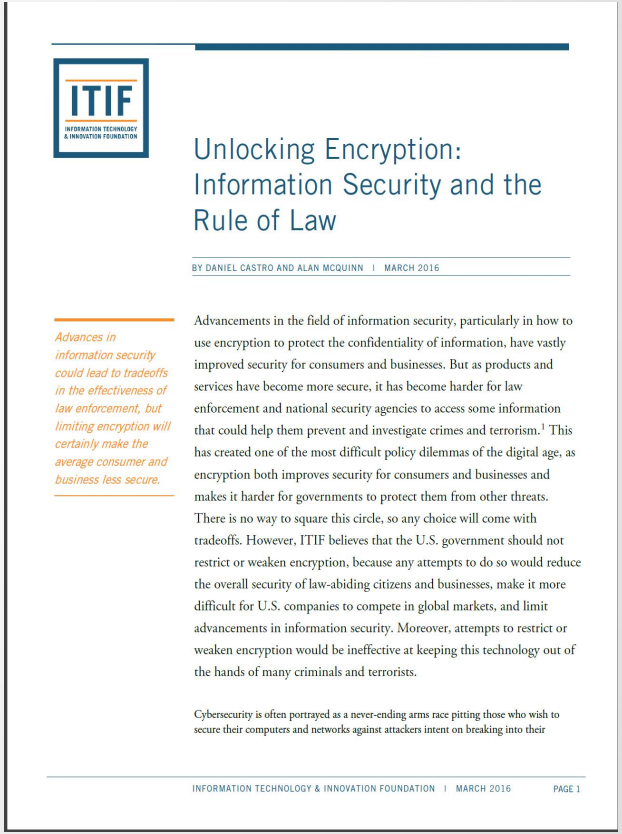


2

大数据利用中的安全态势：法律争议焦点

密码技术作为实现信息安全的有效方法，在整个数据生命周期中发挥着不可替代的保障作用。通过数据加密、消息认证和数字签名等方式，能在不安全的环境下对通信和存储的数据施加保护，以防止未经授权的访问、篡改、伪造、抵赖等行为。

密码技术的“泛在化”商业利用会削弱执法机构的执法能力。算法标准化和技术开源化造成密码技术可以被更加便利地获得和使用，密码技术既可以被善意地用于信息安全保护，也可以被恶意地用于掩盖犯罪证据，阻碍执法机构的调查。



ITIF
INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Unlocking Encryption: Information Security and the Rule of Law

BY DANIEL CASTRO AND ALAN MCQUINN | MARCH 2016

Advances in information security could lead to tradeoffs in the effectiveness of law enforcement, but limiting encryption will certainly make the average consumer and business less secure.

Advancements in the field of information security, particularly in how to use encryption to protect the confidentiality of information, have vastly improved security for consumers and businesses. But as products and services have become more secure, it has become harder for law enforcement and national security agencies to access some information that could help them prevent and investigate crimes and terrorism.[1] This has created one of the most difficult policy dilemmas of the digital age, as encryption both improves security for consumers and businesses and makes it harder for governments to protect them from other threats. There is no way to square this circle, so any choice will come with tradeoffs. However, ITIF believes that the U.S. government should not restrict or weaken encryption, because any attempts to do so would reduce the overall security of law-abiding citizens and businesses, make it more difficult for U.S. companies to compete in global markets, and limit advancements in information security. Moreover, attempts to restrict or weaken encryption would be ineffective at keeping this technology out of the hands of many criminals and terrorists.

Cybersecurity is often portrayed as a never-ending arms race pitting those who wish to secure their computers and networks against attackers intent on breaking into their

INFORMATION TECHNOLOGY & INNOVATION FOUNDATION | MARCH 2016 PAGE 1

3

国际大数据利用中的密码法律新动向

数据加密存储

- 我国2017年《网络安全法》第21条
- 美国内华达州2010年《加密法》（ sb227 ）

密码进出口管控

- 美国工业安全局《出口管理条例》
- 澳大利亚2015年《国防贸易管控法修正案》及其《国防和战略物资清单》
- 新加坡2013年《战略物资（管控）命令》
- 以色列2007年《国防出口管控和实施规则》
- 我国国家安全法（国家安全审查）
- 我国网络安全法（国家安全审查等）
- 我国出口管控法（正在制定中）

通信解密

- 欧盟enisa 2016年提交理事会《关于信息社会密码重要性》的建议
- 美国2014年Apple v. FBI
- 英国2016年《调查权管理法》
- 我国反恐法第18条

禁止性规定

- 越南2011年《密码法》
- 中国2017年《密码法（草案征求意见稿）》

4 我国大数据利用的密码法律战略思考

法律理念

- 总体国家安全观

法律原则

- 安全与发展原则
  - 积极规范与促进应用（电子政务、关键基础设施、产品与服务管理）
  - 发展保障（人才、奖励、标准化、学术交流）
- 密码分类分级原则
  - 核密、机密、普密、商密
  - 关键基础设施与等保
- 谁加密谁解密原则
  - 协助解密

4 我国大数据利用的密码法律战略思考

密码安全保障

- 基础设施建设安全审查
- 密码应用安全性评估
- 人的可信保障
- 密码保障能力建设
- 密码监测认证

密码安全

- 禁止密码滥用
- 禁止密码攻击

密码危机管控

- 泄密、漏洞危机协同联动机制

密码出口管制

- 出口对象、再出口

大数据时代数据安全权利边界模糊甚至崩溃，密码保护措施是必然的选择

密码保障性与脆弱性并存，对密码自身的保护也成为数据安全法律设计的必然考虑

密码的两用属性决定了分类管理在综合性法律框架中的战略挑战性

我国密码法立法为世界密码法学界提出了中国方案，具有价值和意义

谢 谢 !

THANK YOU