2017 可信云大会
可信云标准新一代
客户满意是未来
Cloud Computing Summit 2017.7.25-26

《安全简史》

之“大数据隐私新视角”

杨义先，雷敏教授
北京邮电大学信息安全中心
灾备技术国家工程实验室
主任，副主任

没有网络安全就没有国家安全，没有网络安全人才，就没有网络安全，

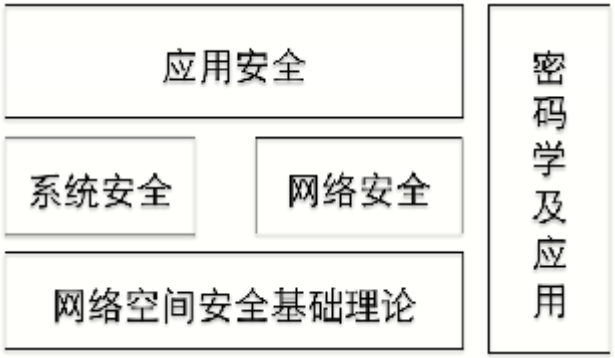
网络安全的竞争归根结底是人才的竞争。网络安全人才存在供需矛盾。

（1）数量不够。一个国家网络安全的实力，最终取决于它能否批量产生具备网络安全技能的技术人才。没有网络安全技术人才的充足保证，就没有网络安全的技术创新，也就没有国家网络安全的强有力保障。目前企事业单位对于网络空间安全人才求贤若渴。但我国高校开设信息安全专业只有将近100所，每年培养的人才只有万人，人才培养的数量无法满足社会的需求。

（2）匹配度不够。高校培养人才所具备的技能和社会对于信息安全人才所要求的技能匹配度不够，网络安全人才所掌握的技能和企事业单位网络安全人才的实际需求之间也存在较大鸿沟，高校的毕业生也无法快速的胜任企业各种所需的人才。

网络空间安全一级学科五个研究方向

2015年6月我国开始设立网络空间安全一级学科



（1）网络空间安全基础是支撑网络空间安全一级学科的基础，为网络空间安全其他研究方向提供理论遵循、技术架构和方法学指导，对建立相对独立的专业知识体系具有重要意义。

（2）密码学是一门集数学、信息论、计算机科学、复杂性理论等于一体的深度交叉与融合的学科，主要研究在有敌手的环境下的安全通信系统。

（3）网络安全研究网络空间中的网络所面临的各种威胁和防护手段，涉及网络安全风险分析、网络自身的安全防护、接入实体的安全管理和控制、以及端到端通信的安全，包括身份认证、访问控制、数据的保密性、完整性和可用性等安全服务，网络安全机制涉及预防、监测和应急响应等多个环节。

（4）“系统安全”学科方向主要研究网络空间上具有独立计算能力的计算机系统的安全性设计、开发、以及安全性测试评估的基本原理、方法和技术。

（5）应用安全技术是指为保障各种应用系统在信息的获取、存储、传输和处理各个环节的安全所涉及的相关技术的总称。

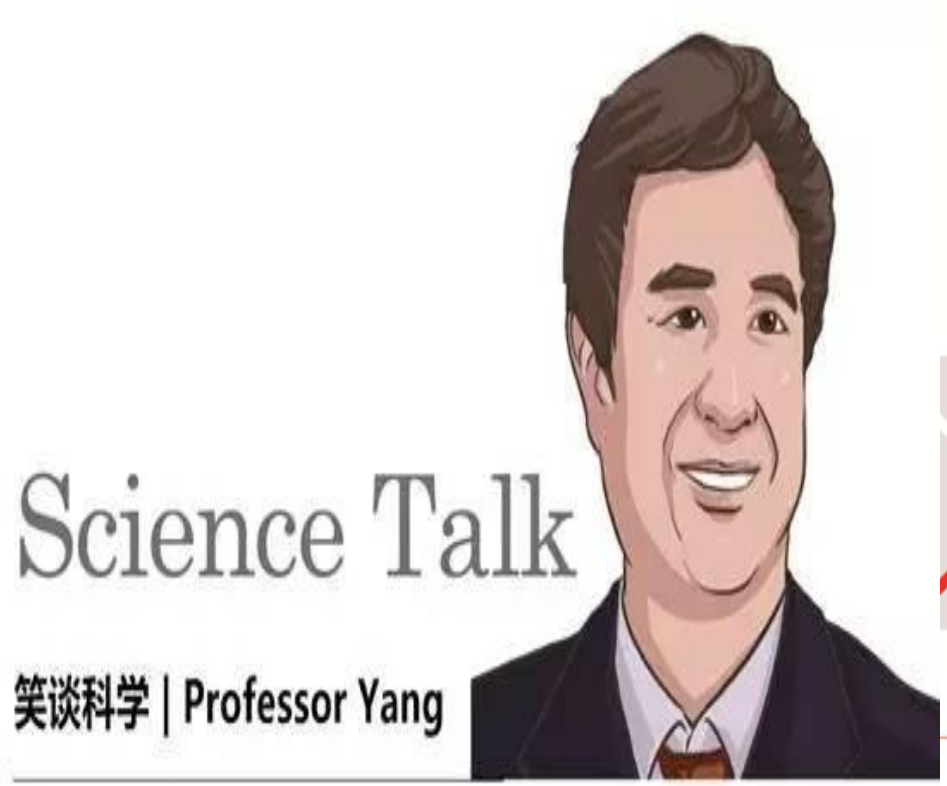
杨义先教授著作第一本：《安全通论》

但网络空间安全一级学科缺乏一套统一的基础理论支撑。

- 定位：顶天！为新设立的网络空间安全一级学科，建立一套统一的基础理论，改变安全界“盲人摸象、头痛医头，足痛治足”的现状。
- 榜样：香农《信息论》，将通信领域的各个分支，统一起来；仅用区区两个定理（信源编码定理、信道编码定理），就为现代通信竖起了“指路明灯”。
- 目的：刷新业界安全观！

《安全通论》《安全简史》作者

- 安全通论涉及的知识面非常宽，涉及博弈论、控制论、信息论、经济、管理、心理等多门学科。
- 既然想统一各学科分支、首先就必须了解，甚至精通这些分支。
- 无论从理论、技术、逻辑等，甚至从世界观和方法论方面来看，各安全分支差异太大，干脆写成科普。



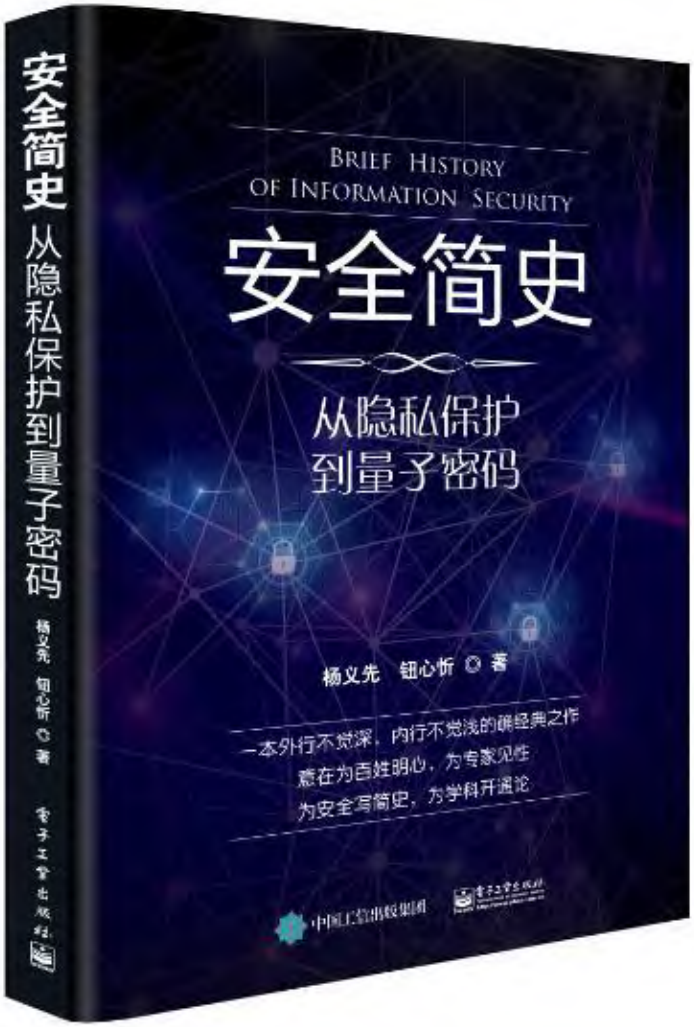
安全通论

- 《安全通论》
  - 定位：顶天！为网络空间安全学科，建立一套统一的基础理论，改变安全界“盲人摸象、头痛医头，足痛治足”的现状。
  - 榜样：香农《信息论》，将通信领域的各个分支，统一起来；仅用区区两个定理（信源编码定理、信道编码定理），就为现代通信竖起了“指路明灯”。
  - 目的：刷新业界安全观！

安全简史

- 《安全简史》
  - 定位：立地！外行不觉深，内行不觉浅。内容将涵盖信息安全的各主要分支。
  - 榜样：霍金的《时间简史》，布莱森的《万物简史》，格雷克的《信息简史》。它们不但出神入化，而且还能改变读者的世界观！
  - 目的：信息安全知识的全民科普！
  - 内容：共19章
- 两本书综合起来的梦想：为百姓明心，为专家见性；为安全写简史，为学科开通论

《安全简史》


安全简史
从隐私保护到量子密码
杨义先 钮心忻 著
BRIEF HISTORY
OF INFORMATION SECURITY
安全简史
从隐私保护
到量子密码
杨义先 钮心忻 著
一本外行不觉深，内行不觉浅的碎经典之作
意在为百姓明心，为专家见性
为安全写简史，为学科开遥论
中国工信出版集团

大数据与可信云

（1）大数据来源于人、来源于电脑、来源于大量的万物互联智能终端；物联网的终端设备产生了大量的数据，数据需要处理、运算和存储，促进云计算的快速发展。

（2）云计算是一种按使用的模式，这种模式提供可用的、便捷的、按需的服务，这些服务包括网络，服务器，存储，应用软件和服务，这些资源能够被快速提供。这些资源就像自来水和电力一样可以按需源源不断的提供。

（3）大数据+云计算的结合可以促进数据智能的发展，数据智能可以根据用户的行为和消费习惯的大数据，更加智能化的为用户推荐服务。

大数据造福，暴隐私遭灾

- 真的，在大数据面前，我们毫无隐私
- 你做过什么事，它知道；你有什么爱好，它知道；你生过什么病，它知道；你家住哪里，它知道；你的亲朋好友都有谁，它也知道……。反正，你自己知道的，它几乎都知道，或者说它都能够知道，至少可以说它迟早会知道。

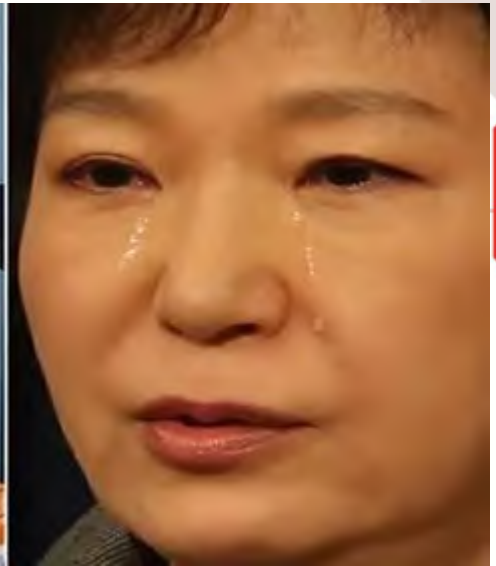
大数据造福，暴隐私遭灾

- 如果你对大数据隐私的这种魔幻能力印象不深的话，别急，请先听听下面这两位世界级大妈的真实故事。

大数据造福，暴隐私遭灾

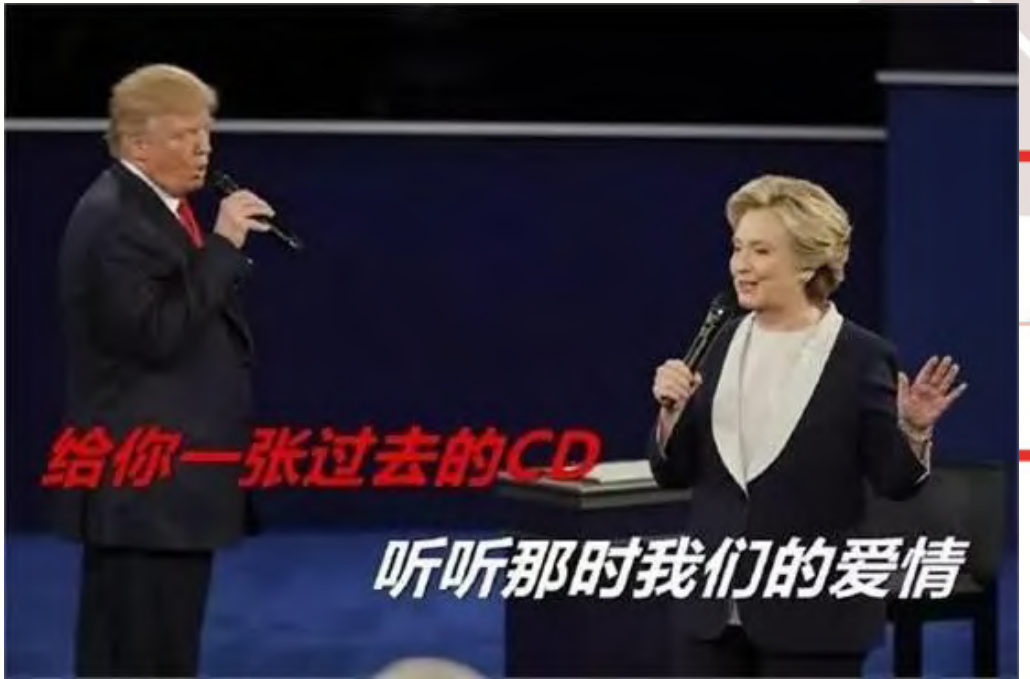
- 第1位：狗血韩剧的主人翁，朴大妈。本来好好地当着总统，正引导大韩民族实现“韩国梦”，民众支持率也高达33%。可是，当她的“萨德导弹”还未部署好时，自己却被来自网络的导弹击中，身败名裂





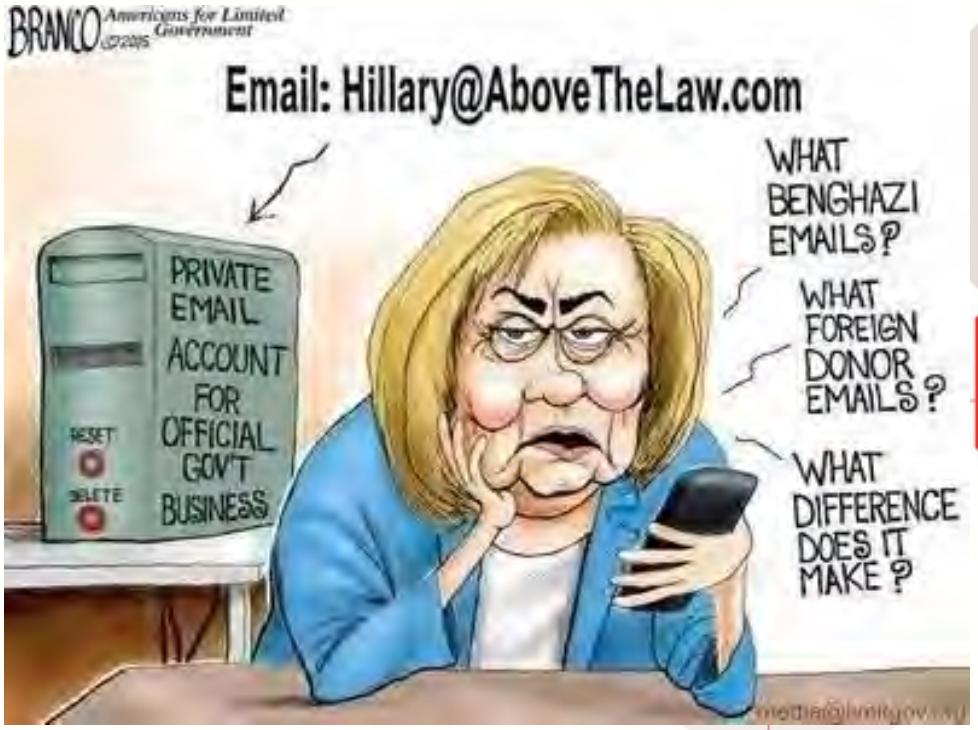
大数据造福，暴隐私遭灾

- 第2位：美剧女一号，希大妈！当然，按实际年龄你本该叫她奶奶的。为了一份工资并不高的岗位，七十多岁还不想退休的、风风火火的她，与另一位脱口秀开始了全面撕逼大战



大数据造福，暴隐私遭灾

- 正当她节节胜利，支持率比对方高出足足12%，胜券在握时，突然，有好事者揭露了她的一个隐私，于是，你懂的！



大数据造福，暴隐私遭灾

- 问：什么是大数据？
- 答：所谓大数据，就是由许多千奇百怪的数据，杂乱无章地堆积在一起的东西。比如，你主动在网上说的话、发的微博微信、存的照片、收发的电子邮件、留下的诸如上网纪录等行动痕迹等，都是大数据的组成部分。一句话，无论你是否喜欢，大数据它就在那里；无论主动还是被动，你都在为大数据做贡献。大数据是人类的必然！

大数据造福，暴隐私遭灾

- 问：大数据到底是靠什么法宝，咋知道那么多秘密的呢？
- 答：用行话说，它利用了“大数据挖掘”技术，采用了诸如神经网络、遗传算法、决策树方法、粗糙集方法、覆盖正例排斥反例方法、统计分析方法、模糊集方法等高大上的方法。大数据挖掘的过程，可以分为数据收集、数据集成、数据规约、数据清理、数据变换、挖掘分析、模式评估、知识表示等八大步骤。#@￥%&！*

大数据造福，暴隐私遭灾

- 是的，所谓的大数据挖掘，在某种意义上说，就是由机器自动完成的特殊“人肉搜索”而已。只不过，现在“人肉”的目的，不再限于抹黑或颂扬某人，而是有更加广泛的目的，比如，为商品销售者寻找最佳买家、为某类数据寻找规律、为某些事物之间寻找关联等等，总之，只要目的明确，那么，大数据挖掘就会有用武之地。

大数据造福，暴隐私遭灾

- 问：大数据隐私的当前局势如何？
- 答：必须承认，就当前的现实情况来说，“大数据隐私挖掘”的杀伤力，已经远远超过了“大数据隐私保护”所需要的能力。在大数据挖掘面前，当前人类还有点不知所措。这确实是一种意外，因为，自互联网诞生以后，在过去几十中，人们都不遗余力地将若干碎片信息永远留在网上；其中，每个碎片虽然都完全无害，可谁也不曾意识到，至少没有刻意去关注，当众多无害碎片融合起来，竟然后患无穷！

大数据造福，暴隐私遭灾

- 问：针对过去已经遗留在网上的海量碎片信息，如何进行隐私保护呢？
- 答：如果单靠技术，显然无能为力，甚至会越“保护”就越“泄露隐私”，因此，必须多管齐下。比如，从法律上，禁止以“人肉搜索”为目的的大数据挖掘行为；增加“网民的被遗忘权”等法律条款，即，网民有权要求相关网络删除“与自己直接相关的信息碎片”！

大数据造福，暴隐私遭灾

- 问：如何来保护自己的隐私呢？
- 答：法宝就是两个字：匿名！比如，澡堂着火了，美女们不顾一切冲出室外；才发现自己却是赤身裸体，慌乱中赶紧捂住下身。惊呆了的看门大爷，急中生智，高叫一声：捂脸！于是，一场大面积、情节恶劣的隐私泄露事件，就这样被轻松化解了。回放一下整个事件，关键在哪里呢？对，就是匿名！只要做好匿名工作，那么，对“大家都一样”的东西谈论什么“隐私泄露”，就是无本之木、无源之水了

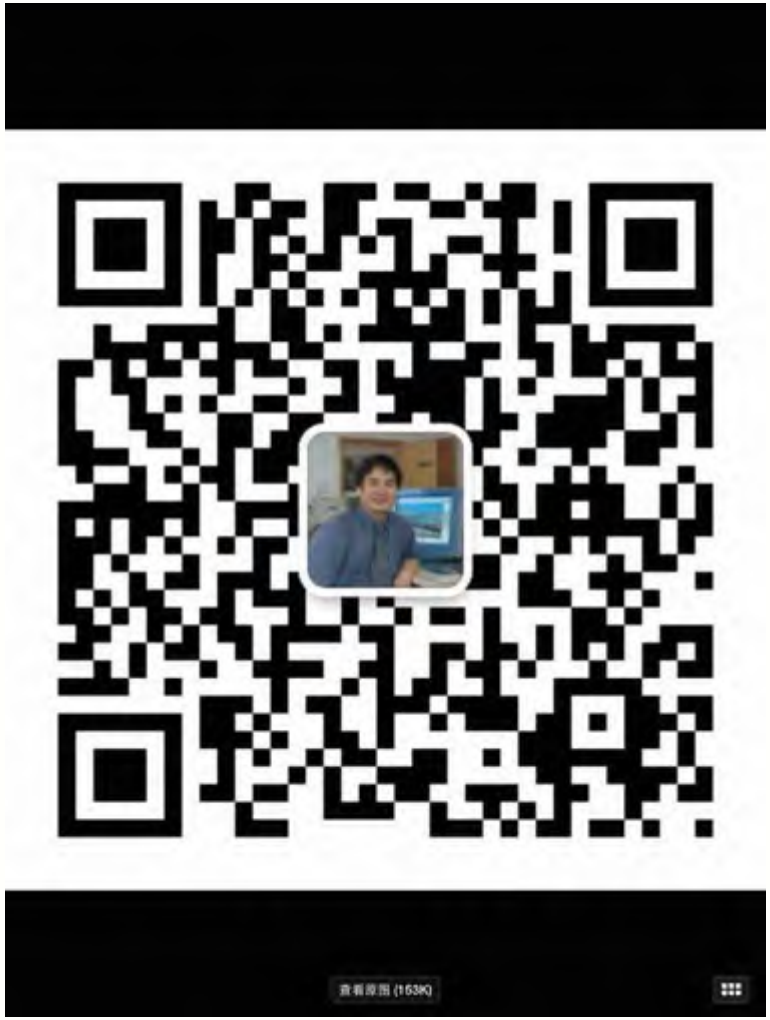
- 问：匿名的重点都有哪些呢？
- 答：身份匿名、属性匿名、关系匿名、位置匿名等。概括一下，
  - 在大数据之前，隐私保护的哲学是：把“私”藏起来，而我的身份可公开。
  - 大数据之后，隐私保护的哲学将变成：把“私”公开（实际上是没法不公开），而我的身份却被藏起来，即，匿名。

- 问：主要匿名技术都有哪些呢？
- 答：主要有三，1）基于数据失真的匿名技术
  - 假如你能够像孙悟空同志那样，一会儿是猫，一会儿成鸟，一会儿变蛇，一会儿为草，那么，除了观音菩萨之外，谁能知道你就是二师兄呢。你本来要上山，却偏要说下河；本来要杀鸡，却偏要说宰鹅；那么，谁会知道你到底要干什么，或者到底已经干了什么呢！

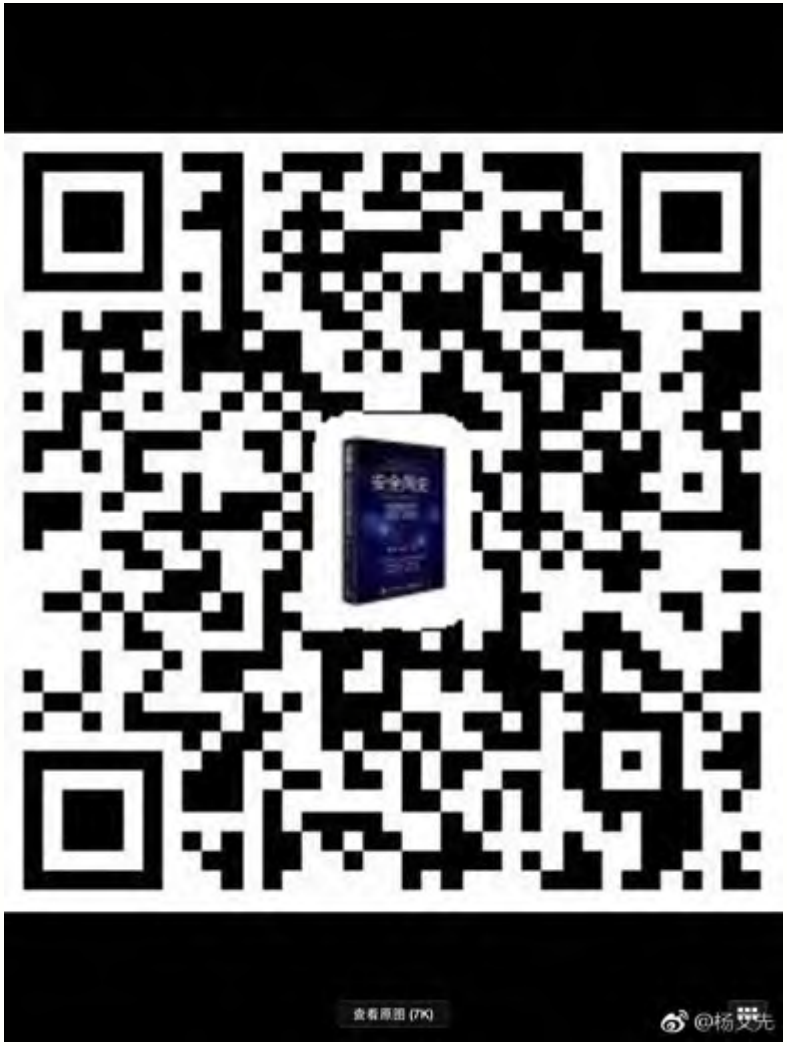
- 答（续）：匿名技术之2）：基于数据加密的匿名技术
  - 请你想想看，如果别人连你发布的信息都读不懂，他怎么会知道那是你的隐私；就算他知道是你的隐私，他又怎么知道隐私的具体内容，毕竟人人都有隐私嘛；如果他不知道你的隐私内容，那么，你就安心睡觉吧。

- 答（续）：匿名技术之3）：基于限制发布的匿名技术
  - 不该说的就别说，不该问的就别问，不该动的东西就别动，只要人人都严格按照规矩，老老实实地约束自己在网上的言行，那么，何愁隐私泄露

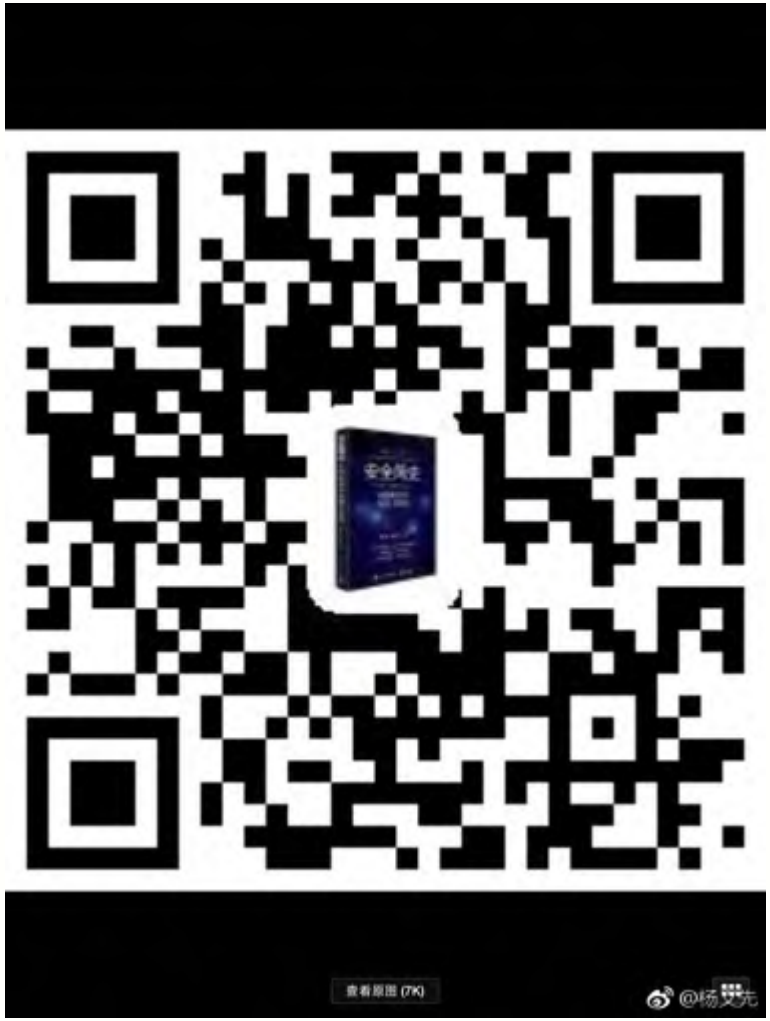
公众号：亦仙亦凡



通过京东购买《安全简史》



通过当当购买《安全简史》




谢谢！