量子计算机的威胁被夸大，决战在 30 年后

郁 昱

一、CT-RSA 会议召开

本人参加了于 2 月 12-17 日在旧金山举办的 RSA Conference 2017 会议，并在密码学家分论坛（Cryptographer’s Track）上做了大会报告，介绍了此次在 CT-RSA 2017 会议论文集上发表的署名单位摩石实验室的文 章“Ridge-Based Profiled Differential Power Analysis”。

该文将基于岭回归的机器学习方法引入旁路攻击中，解决了线性回归等同类方法在建模过程中出现的过拟合 (overfitting) 问题，模拟实验和芯片软硬件实现都验证了该攻击不仅在对传统工艺芯片的功耗分析攻击上优于以往同类方法，且能很好的适应纳米级工艺密码芯片的非线性泄露的功耗特征，是未来基于差分功耗分析 (DPA) 的旁路攻击的新发展方向。在同一个论坛上，来自我国中科院软件所吴文玲团队和中科院信工所荆继武团队的研究人员分别介绍了他们在基于旁路攻击的保密信号恢复和随机数生成的熵估计方面的研究成果。

二、后量子密码专家观点

此次密码学分论坛的一个热门议题是后量子密码，举办方特地组织了一个多小时的座谈讨论 (panel discussion)，本次讨论由前国际密码学会主席比利时鲁汶大学的 Bart Preneel 教授主持，参加嘉宾包括图灵奖获得者 Adi Shamir 教授、斯坦福大学 Dan Boneh 教授、滑铁卢大学的 Michele Mosca 教授和思科 (Cisco Systems) 的 Scott Fluhrer。本人对本次讨论的内容进行了总结，具体内容如下：

1. Bart Prennel

Bart Prennel 介绍了目前量子计算机发展的形势，指出量子计算机日益成为计算机科学家甚至普遍民众热议的话题，也被是认为是对现代密码学的一个重要威胁，且美国国家标准与技术研究院 (NIST) 于今年开始征集后量子密码算法并将在五年后发布相应的标准。

2. Adi Shamir

Adi Shamir 教授称，考虑到时机还未成熟，暂时不会担忧量子计算机的发展对目前的安全体系带来毁灭性影响。在他看来，不仅 NSA 在研究量子计算机，很多国家政府、学术机构和商业实验室都对此展开了研究，一旦技术成熟，这些机构会发出足够的预警，目前还没到这个阶段。他还谈到了是否应该马上转移到后量子密码的问题，他认为马上换用新的算法，究竟会变得更安全还是不安全需要一定的时间来验证。最后，Shamir 教授指出，今年是 RSA 算法发明 40 周年，一个安全的算法是经得起时间考验的。

3. Scott Fluhrer

Scott Fluhrer 对量子计算机持乐观态度，他认为量子计算机好比登月，虽然非常困难，但是最终都会实现，且这个困难任务可以分解成许多可定义的步骤，再逐一实现。他倡导从现在开始，按照“10 年内造出可用的量子计算”这一假设去安排接下来的工作。

4. Danel Boneh

Danel Boneh 教授表示，当工业界的朋友问及现在如何应对量子计算机时，我的建议是等待 NIST 的标准制定，目前大家更应该关心缓冲区溢出、SQL 注入、CSS 这一类的传统安全漏洞。Boneh 根据自己对 Shor 量子算法的了解，预计分解 2048 比特的 RSA 需要 200 多万的量子比特。并指出按照目前的量子计算机的制造水平，即使我们乐观地假设摩尔定律适用于量子计算机，那也需要三十多年才能造出一台分解 RSA-2048 的量子计算机，且 Shor 算法的高串行性会给量子计算机带来一些其它的技术难度和挑战。最后，Boneh 认为等到量子计算机造出来的那一天，抵抗量子计算机的后量子算法肯定已经部署到实际应用中，因此量子计算机的主要应用领域不是密码学，而是模拟计算和人工智能等其他领域。

5. 其它

最后，几位专家建议，在过渡阶段，最保险的方案还是结合经典密码学与后量子密码学，比如在做密钥交换时，用 Diffie-Hellman 和后量子密钥交换协议分别协商出一个密钥，然后把这两个密钥作比特异或得到最终的密钥。

三、延伸阅读

1. http://mt.sohu.com/it/d20170220/126756016_481676.shtml

2. http://netsecurity.51cto.com/art/201702/530936.htm

3. http://bluereader.org/article/211783673

4. http://soft.yesky.com/security/469/108518469.shtml

5. https://baijiahao.baidu.com/po/feed/share?wfr=spider&for=pc&contex t= %7B%22sourceFrom%22%3A%22bjh%22%2C%22nid%22%3A%22news_4264515563681606832%22%7D

让密钥丢失不再致命

郑 东

随着信息和互联网技术的发展，承载各类密码算法的软硬件系统被广泛应用在政府、军工、金融、通信等领域。在这些系统中，密码算法通常以硬件电路或软件程序的形式进行物理实现，而算法的密钥占有十分重要的地位，需要进行安全地保护。例如在加密系统中，只有合法用户才能够进行机密文件的解密操作。目前，大部分密码系统都假设用户可以安全地保护密钥。但是，近年来出现了各种各样的侧信道攻击证明，这种假设很难在现实情况下满足，系统在实际运行过程中会出现密钥泄漏的问题。通过观察和测量密码算法运行的功耗、能量、时间、电磁辐射、声音等物理信息以及通过物理手段干扰硬件运行的各类错误注入手段，攻击者可以获取密钥的部分信息。此外，随着新技术的不断发展，智能手机等移动设备的普及，越来越多的数据加密系统被用于各种安全较差的环境中，密钥泄漏问题更加突出。与解决一个数学难题相比，攻击者获取一个系统的部分密钥信息更加容易。因此，密钥的泄漏已成为威胁一个密码系统安全的重要因素之一。目前已存在一些能部分解决密钥泄漏问题的方法，例如具有前向安全的密码系统、密钥隔离技术、入侵回弹技术和代理重加密技术等。最近提出的利用泄漏函数定义的抗泄漏密码学是解决密钥泄漏问题的最有力技术之一。因此，研究抗泄漏密码方案具有重要的理论意义和实际应用价值。

通俗来讲，抗泄漏是指攻击者即使获得密钥的部分信息，仍然可以保证密码系统的安全。要设计安全的抗泄漏密码学方案，首先要确定一个合适的安全模型，来描述泄漏攻击过程中敌手能够获取哪些信息。近年来，提出了一些重要的泄漏模型及抗泄漏密码方案：

★ 2004 年，国际上提出首个一般化泄漏模型，即“唯计算才会产生泄漏”模型 [1]。该模型要求，一个密码系统在运行过程中，攻击者只能从当前参与计算的内存中获取泄漏信息，而不能从未参与计算的内存中获取任何信息。近年来，围绕该模型提出的密码方案主要有抗泄漏流密码和通用抗泄漏编译器。不幸的是，还有很多泄漏攻击是静态存储泄漏，与“唯计算才会泄漏”这一假设相矛盾。典型的基于静态存储泄漏的攻击是冷启动攻击。

★为了捕获冷启动攻击，密码学家又提出了有界泄漏模型。该模型假设敌手可以获取有限长度的秘密信息，设计者利用一定的伪随机数提取技术来保证密码方案在泄漏了部分秘密信息后，攻击者仍然难以恢复完整的密钥。特别地，有界密钥泄漏模型可以涵盖相对泄漏和有界恢复泄漏这两种类型的泄漏攻击。2012 年，Naor 和 Segev[2] 证明了所有基于哈希证明系统的方案都是抗相对泄漏的。2013 年，刘胜利等 [3] 提出基于特殊通用哈希函数的泄漏量与消息空间独立的公钥加密方案。同年，秦宝东和刘胜利 [4] 提出不依赖双线性配对运算的高泄漏比率的公钥加密方案。

★一种更具有普遍性的泄漏模型是辅助输入模型。它并不限制敌手获取信息的长度，而只是要求攻击者通过泄漏信息无法恢复完整密钥。针对辅助输入泄漏攻击，2014 年 Yuen 等 [5] 提出一种允许密钥和随机数同时泄漏的基于身份加密方案，2016 年 Komargodski[6] 提出一种抗辅助输入泄漏的单向函数。

★上述泄漏模型存在一个共同的缺点，即在密码方案设计之初，必须预估泄漏量的可能上限，再根据该上限设计相应的密码方案，以保证方案在系统整个生命周期内的安全。为了克服该限制条件，连续泄漏模型应运而生。该模型假设敌手能够连续获得当前私钥的任意信息，只要两次成功的密钥更新之间所泄漏的信息量不超过一定限制，而在系统生命周期内泄漏的信息总量是无限制的。2014 年 Ananth 等 [7] 设计了一个抗连续泄漏的交互式证明协议。2016 年 Koppula 等 [8] 提出第一个抗连续泄漏的确定性公钥加密方案。

★ 以上泄漏模型又称为事前泄漏，即仅考虑泄漏发生在挑战密文出现之前，从而限制了一些侧信道攻击的种类。为此，Halevi 和 Lin[9] 针对公钥加密方案提出了事后泄漏模型，即攻击者在知道挑战密文之后仍能够进行私钥泄漏攻击。

在抗泄漏密码学研究方面，国外起步较早，经过近十年的发展，已经形成比较完善的设计方法和理论体系，提出了许多具有影响力的抗泄漏模型。我国对抗泄漏领域的研究起步相对较晚，主要还是引进和借鉴国外相关技术和理论。但是，随着国家对网络空间和信息安全产业的高度重视，国内高校和研究机构在该领域投入的人力和物力逐年增大，研究发展速度很快并取得了一定的成果。

图 1 和图 2 分别展示了中国和欧美国家近五年在密码学领域顶级会议上发表的论文情况以及国内在抗泄漏密码学领域取得的学术成果数量。从中可以看出，国内在该领域的研究呈现上升趋势，但是与欧美国家相比具有