关于旁路分析技术近二十年间的发展情况简述

xxx，3xxxxxxxxx

摘　要: 加密设备也是以电路板为依托实现的加密功能，在物理层面上不可避免的会出现信息泄露，而利用这种信息泄露对加密信息进行恢复的行为被称之为“旁路分析”，其中的敏感信息可以通过分析设备在运行过程中的物理现象来恢复，在这次调查中，作者追溯了过去二十年间来密码实现的电源侧信道分析的发展。我们通过深入探索几个概念进行阐述，例如, 差分功耗分析（Differential Power Analysis, DPA），缓存计时攻击（Cache Timing Template Attacks， CTA）等等。本文将主要致力于探讨如何将旁路分析应用于目标设备的信息识别和故障攻击的触发中。

关键词: 旁路分析 密码学 差分功耗分析 缓存计时攻击 隐私防护 硬件加密

Briefly on the development of bypass analysis technology in the past two decades

xxx，3xxxxxxxxx

Abstract: Encryption equipment is also an encryption function based on circuit boards, and information leakage is inevitable at the physical level. The use of this information leakage to attack encryption equipment is called "Side channel analysis". Sensitive information can be recovered by analyzing the physical phenomena of the device during operation. In this investigation, the author traced the development of power-side channel analysis implemented by cryptography in the past two decades. We elaborate on several concepts through in-depth exploration, for example, Differential Power Analysis, (DPA), Cache Timing Template Attacks, (CTA) and so on. This article will focus on discussing how to apply side channel analysis to the information identification of target equipment and the triggering of fault attacks.

Key words: Side-Channel-Analysis, Cryptography, Differential Power Analysis, Cache Timing Template Attacks, Privacy protection, Hardware encryption

1.背景

旁路攻击是一种通过观测设备正常工作过程中泄露的信息来推断设备内部状态的攻击方法。文献[1] 首次提到了旁路攻击。1956 年，英国军情五处 (MI5) 执行了一项破译埃及驻伦敦大使馆与外部通信内容的行动。这些通信内容使用 Hagelin 密码机[2] 进行了加密，其加密过程是将来自键盘的电子信号通过 7 个转轮的转动来产生密文，“密钥”就是这 7 个转轮的初始设置。每天早晨，密码机都会由发送信息的专员进行重置。军情五处在其中一台密码机附近秘密放置了一个麦克风，并在每天早晨通过监听麦克风来分析确定密钥的初始设置，在此基础上破译截获的密码机通信消息。实际攻击中，由于难以区分出当前正在设置的转轮噪声与背景噪声，军情五处只能确定一部分的转轮设置，这使得后续的破译过程较为复杂。但通过分析获取到的部分密钥，可明显降低整个密钥的搜索空间，使得完整密钥的破译成为可能。

2.发展脉络

1.发展概述

旁路分析技术的第一篇学术文献描述了一种利用测量密码运算执行时间的攻击方法[3],这可以被认为是旁路分析技术的起源，随后旁路分析历经了漫长的萌芽期，然后自 1996 年开始不同类型的旁路泄露被提出用于密码分析，2001 年后更加注重旁路泄露的分析方法、密码算法的安全实现、密码实现的安全评估、旁路分析的新型应用等研究，2010 年后旁路分析、评估、防御、应用研究将更加深化，旁路分析相关理论正在升华和完善。

2.发展阶段

通过对国内外旁路分析技术的发现现状进行研究，我们认为其发展过程大致如下图：

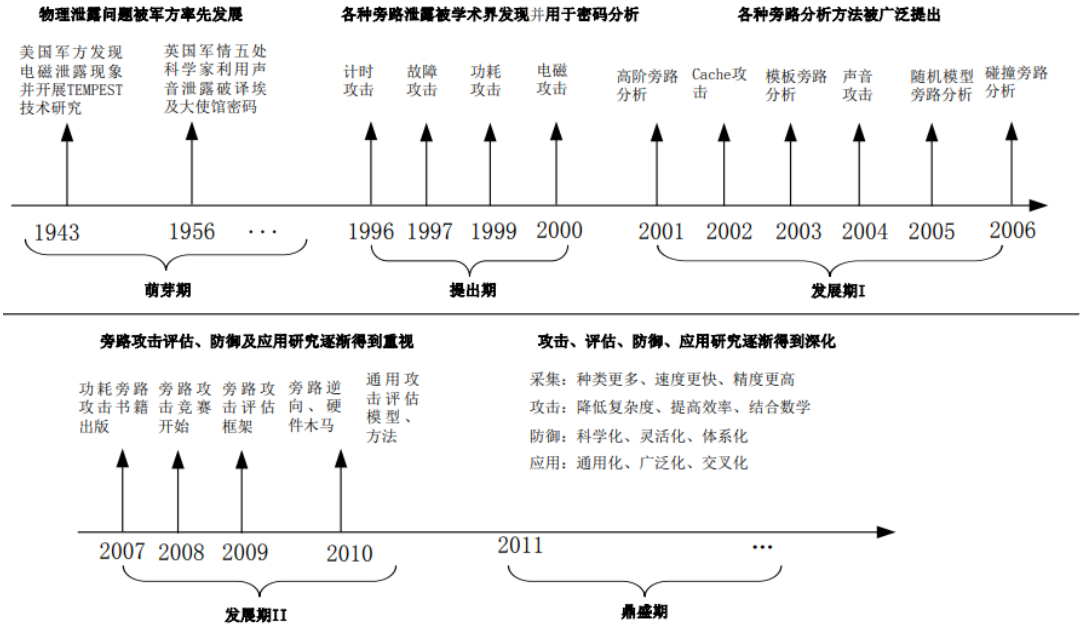

图 2-1

从上图不难看出，我们将其发展历程分为四个阶段，其中萌芽期的特点是军方率先发现了电子设备运行过程存在旁路泄露，并秘密开展研究。[4][5]，主要技术为利用瞬态电磁脉冲辐射监测技术进行信息对抗，该技术于 1943 年被提出，直至 1995 年才被美国政府正式解密[4]；而另一技术为声音分析技术研究，于上文曾有介绍[5]。

旁路分析技术于 1996 年进入提出期，在此期间，不同类型的旁路泄露被陆续发现并被用于密钥分析，包括但不局限于：

（1）1996 年，美国 Cryptography Research 公司的首席科学家 Paul Kocher 等发现密码运行过中泄露的执行时间存在差异，可用于密钥破解，并成功用于分析 RSA 等一系列公钥密码算法[3]；

（2）1997 年，美国斯坦福大学的 Dan Boneh 发现智能卡上密码算法执行过程可能会受到干扰使得产生故障（或错误）输出，攻击者可以利用其进行密钥恢复。Dan Boneh 等成功对 RSA 密码算法进行了故障分析[6]；

（3）1998 年，Paul Kocher 等发现智能卡上的密码算法执行过程中会产生功率消耗泄露，可用于密钥破解，并成功对 DES 密码算法进行了密钥恢复[7]；

（4）2000 年，比利时的 Jean-Jacques Quisquater 等发现密码算法运行过程中的电磁辐射泄露同样可用于密钥破解[8]。

进入二十一世纪以来，旁路分析技术进入飞速发展时期，如 2001 年的高阶差分功耗分析方法[9]被提出、2005 年的随机模型分析方法[10]、频域旁路分析方法[11]、访问驱动 Cache 计时分析方法 [12]被提出，标志着旁路分析技术日趋完善，研究领域逐渐深化，例如：

（1）对采用了防御措施的密码实现开展安全性分析，提高现有分析方法的效率，将数学分析方法同旁路分析结合起来改进现有分析方法，这些已成为一个新的发展趋势[13][14][15]。

（2）旁路分析方法可被广泛应用到新的信息安全领域，分析技术走向通用化、广泛化和交叉化[16][17][18]。

3. 基本原理

1. 原理概述

密码旁路分析的基本原理是：密码算法在密码芯片上实现时，由于设备的物理特性原因，总会产生执行时间、功率消耗、电磁辐射、故障输出等旁路泄露；同时 由于密码芯片受计算资源和处理能力限制，现代密码算法的主密钥大都切割为若干子密钥块并按照一定的顺序参与运算，不同时机使用这些子密钥块的旁路泄露可被攻击者采集到；这些旁路泄露同明文、密文和子密钥块具有一定的相关性，攻击者可利用一定的分析方法恢复出子密钥块值；在得到足够的子密钥块值后，结合密钥扩展设计即可恢复主密钥值。

2. 样例阐述

我们利用 Cache 计时分析模板和 RSA 加密算法为例进行简单阐述：

首先，我们以调用 OpenSSL 密码库函数实现的一般 RSA 算法作为攻击对象，利用 RDTSC 指令调用 CPU 上电时间戳测量 RSA 执行时间。

对不同长度的 RSA 进行了实验，下表中的数据为针对 OpenSSL 随机生成的不同长度 RSA 密钥所得到的总执行时间范围和 d_k 为 1 时多执行的乘法操作时间：

密钥位长度	执行时间范围/(CPU 周期)	d_k 为 1 时多的乘法操作执行时间/(CPU 周期)
128	400000-415000	1400-1600
256	1700000-1810000	1900-2100
512	9450000-9500000	2400-2600
1024	56500000-58000000	2700-4300

表 3-1

可以看出密钥位越短，密钥位 0-1 引起的时间差异占总执行时间的比重越大，越能够体现出微小差异对差分统计结果的影响；密钥长度越长，更多密钥位值的不同对攻击总的执行时间影响较大，攻击噪声也变得较大。

得到操作时间之后，我们进行基于差分计时攻击的密钥恢复。我们可以利用差分计时攻击进行密钥恢复。假设下图为某次攻击中密钥第 30 到 40 位对应的方差差值。

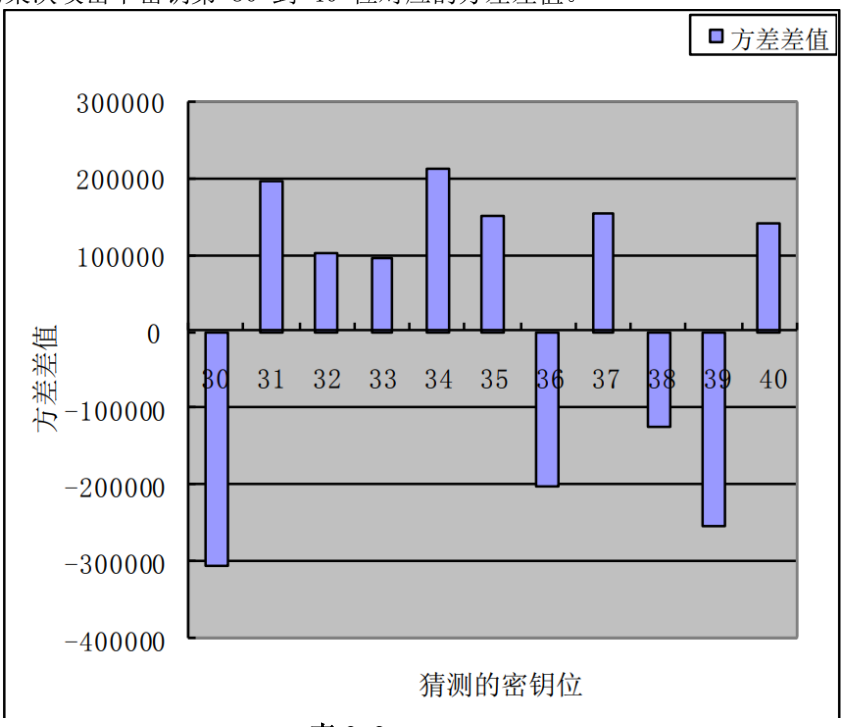

表 3-2

上图横轴表示密钥位，纵轴方差差值表示猜测下一位位为 1 时的测量时 间方差值与猜测当前位为 0 时的测量时间方差值之差，即 4.3.2 节中 V_1-V_0的值。由 上节分析易知，方差差值为负对应的密钥位为 1，为正的对应为 0，从而可以得到第 30 到 40 位对应的密钥值为$(1000\ 0010\ 110)_2$。

4. 未来发展

旁路分析技术在不断发展，由于其技术的新颖性质，以及电子元器件处理任务时泄露信息的必然性，关于旁路分析技术的发展会愈加深刻，而我们就现今的学术会议以及期刊关于旁路分析技术的动态，粗略概括了下文几个方向，以下仅为部分方向，未曾全部概括

1. 泄露均衡

攻击者通过分析单条旁路泄露轨迹获取到的信息应当仅局限于运算识别，而不能泄露任何和密钥相关的信息。此时，最简单的防护对策是使用泄露均衡算法，使得密码算法对所有密钥位处理时均执行相同的运算序列。例如，当计算 RSA 签名时，应确保在处理不同幂指数位时均执行相同的两种运算[21]。这种防护对策可用于算法中的 SPA 防御，并且可在资源受限的设备上进行实现。

2. 数据随机化

其中研究最为深入的防护对策是掩码方案。掩码方案的主要原理是将敏感数据划分为多个数据片段，分别对不同数据片段执行加密运算。因此，为了实施成功，攻击者必须恢复每个数据片段，在此基础上将所有信息结合起来观测旁路泄露和密钥的相关性 (如果密码算法不是并行地进行实现，则可将不同时间的泄露样本结合在一起)。对采用了掩码防护的密码实现攻击一般被称为高阶攻击。如果增加一定的噪声可以降低采样质量的话，相比未防护的场景，针对掩码实现 的密钥恢复攻击所需的样

本量会随着数据片段数量的增加而呈指数级增长。需要说明的是，掩码防护对故障攻击并没有直接的影响，但是会增加使用随机时差方法找到与目标密码运算对应样本时间点的难度。同针对未保护的数据进行故障攻击一样，在待掩码数据或掩码自身注入的故障也将通过密码运算进行传播[21]。显然，在特定的故障模型下，如果能够通过故障注入将掩码字节设置为 0，掩码防御对策将会失效。

3. 随机时延

另外一种影响旁路轨迹中信息位置的防御对策是在执行密码运算之前插入一个时延函数，其中时延的大小是随机的。时延函数可在不同的密码运算之间插入，以降低可为攻击者使用的信息量。对这类防护的密码实现实施旁路攻击时，攻击者需要在攻击前对泄露轨迹进行对齐预处理[22]。同样，因为目标密码运算的位置随机分布在某一特定时间范围，这也会给攻击者在密码算法中的精确时间点注入故障带来很大困难。实际中，攻击者一般会寻求在某一时间点注入故障，并重复攻击，直至故障被注入期望的目标运算中。为了将攻击者尝试注入故障 的时间范围最大化，有一些文献提出了一些解决方案[23],[24]。需要说明的是，随机 时延防御对策只是延迟了成功实施攻击所需的时间，而并非从根源上进行防护，因此在此基础上是否还需要其他复杂的防护措施是有争议的。

5. 结语

上文三节论述了旁路分析技术的原理、发展历程以及具体实际操作样例。但是，对于安全应用中的大部分嵌入式设备来说，当前大都已经部署了各种物理攻击防御对策。如进行泄露均衡加密[19]以及实现数据随机化[20][21]、随机时延[22][23][24]等解决方案。对于旁路分析技术来说，它可以利用不可避免的物理性质实现密钥恢复等功能，在各国军方、学术界均有广泛研究和应用，所以我们可以从加强我国加密芯片产业建设、增加相关技术积累方面入手，为密码方案或协议的安全性作出“担保”，给出形式化模型。现有研究大部分基于传统黑盒分析，并没有涵盖针对密码旁路攻击的灰盒分析[25]，我们需要以此为切入点，作为研究的重点和难点。

参考文献:

[1] Wright, P.: Spycatcher: The Candid Autobiography of a Senior Intelligence Officer.
Heinemann (1987)
[2] Kahn, D.: The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet, 2nd edn. Simon and Schuster Inc. (1997)
[3] Kocher, P.C.: Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In: Koblitz, N. (ed.) Advances in Cryptology CRYPTO '96, Lecture Notes in Computer Science, vol. 1109, pp. 104–113. Springer, Berlin (1996)
[4] National Security Agency. NSA tempest series[P]. http://cryptome.org/#NSA--TS.
[5] Wright P. Spy Catcher: The Candid Autobiography of a senior Intelligence Officer[M]. Viking Press, 1987.
[6] Boneh D, DeMillo R A and Lipton R J. On the Importance of Checking Cryptographic Protocols for Faults[C]. In Advances in Cryptology—EUROCRYPT 1997, LNCS, vol. 1233, 1997: 37-51.
[7] Kocher P, Jaffe J and Jun B. Differential power analysis[C]. In Advances in Cryptology—
CRYPTO 1999, LNCS, vol. 1666, 1999: 388-397
[8] Quisquater J J and Samyde D. A new tool for non-intrusive analysis of smart cards based on 315 electro-magnetic emissions: the SEMA and DEMA methods [EB/OL]. [2010-03-05]. In rump session of EUROCRYPT 2000, 2000.
[9] Messerges T S, Dabbish E A and Sloan R H. Investigations of power analysis attacks on smartcards[C]. In USENIX Workshop on Smartcard Technology, 1999: 151-162.
[10]Schindler W, Lemke K and Paar C. A Stochastic Model for Differential Side Channel Cryptanalysis[C]. In Cryptographic Hardware and Embedded Systems—CHES 2005, LNCS, vol.
3659, 2005: 30-46.
[11] Tiu C C. A New Frequency-Based Side Channel Attack for Embedded Systems[D]. Waterloo, Ontario, Canada, 2005
[12] Percival C. Cache missing for fun and profit[C]. In BSD 2005, 2005: 1-13.
[13] Witteman M F, Woudenberg J and Menarini F. Defeating RSA Multiply-Always and Message Blinding Countermeasures[C]. In Cryptographers'Track—CT-RSA 2011, LNCS, vol. 6558, 2011: 77-88.
[14] Debraize B. Efficient and Provably Secure Methods for Switching from Arithmetic to Boolean Masking[C]. In Cryptographic Hardware and Embedded Systems—CHES 2015, LNCS, vol. 7428, 2015: 107-121.
[15] Oren Y, Renauld M, Standaert F-X and Wool A. Algebraic Side-Channel Attacks Beyond the Hamming Weight Leakage Model[C]. In Cryptographic Hardware and Embedded Systems— CHES 2017, LNCS, vol. 7428, 2017: 140-154.
[16] Skorobogatov S and Woods C. Breakthrough Silicon Scanning Discovers Backdoor in Military Chip[C]. In Cryptographic Hardware and Embedded Systems—CHES 2012, LNCS, vol. 7428, 2012: 23-40.
[17] Veyrat-Charvillon N and Standaert F-X. Generic Side-Channel Distinguishers: Improvements and Limitations[C]. In Advances in Cryptology—CRYPTO 2019, LNCS, vol. 6841, 2019: 354-372
[18] Whitnall C and Oswald E. A Comprehensive Evaluation of Mutual Information Analysis Using a Fair Evaluation Framework. In Advances in Cryptology—CRYPTO 2019, LNCS, vol. 6841, 2019: 316-334.
[19] Chevallier-Mames, B., Ciet, M., Joye, M.: Low-cost solutions for preventing simple sidechannel analysis: Side-channel atomicity. IEEE Transac. Comput. 53(6), 760–768 (2014)
[20] Boscher, A., Handschuh, H.: Masking does not protect against differential fault attacks. In: Breveglieri, L., et al. 65, pp. 35–40
[21] Standaert, F.X., Veyrat-Charvillon, N., Oswald, E., Gierlichs, B., Medwed, M., Kasper, M., Mangard, S.: The world is not enough: another look on second-order DPA. In: Abe, M. (ed.) Advances in Cryptology—ASIACRYPT 2020. Lecture Notes in Computer Science, vol. 6477, pp. 112–129. Springer, Berlin (2020)
[22] Tunstall, M.: Random order m-ary exponentiation. In: C. Boyd, J.M.G. Nieto (eds.) Information Security and Privacy (ACISP 2019), Lecture Notes in Computer Science, vol. 5594, pp. 437–451. Springer, Heidelberg (2019)
[23] Tunstall, M., Benoît, O.: Efficient use of random delays in embedded software. In: D. Sauveron, C. Markantonakis, A. Bilas, J.J. Quisquater (eds.) Information Security Theory and Practices (WISTP 2007), Lecture Notes in Computer Science, vol. 4462, pp. 27–38. Springer, Heidelberg (2007)
[24] Coron, J.S., Kizhvatov, I.: An efficient method for random delay generation in embedded software. In: Clavier and Gaj, vol. 95, pp. 156–170
[25] Halunen, Kimmo, and Outi-Marja Latvala. "Review of the use of human senses and capabilities in cryptography." Computer Science Review 39 (2021)