ICT-2007-216676 ECRYPT II

密码学 II 之欧洲特种网络

特种网络

信息和通信技术

D.SPA.7

ECRYPT2 算法和密钥规模年度报告（2008-2009）

提交时间：27、7、2009 交付使用时间：31、7、2009

项目开始时间：1、8、2009 周期：四年

通信联系作者：Katholieke Universiteit Leuven (KUL) 版本 1.0

在第 7 次规划框架下的欧洲授权基金项目		
传播级别		
PU	公开	X
PP	对其他项目参与者限制（包括委托服务）	
RE	限制可列出的资助小组（包括委托服务）	
CO	机密，仅仅对资助成员（包括委托服务）	

ECRYPT2 算法和密钥规模的年度报告（2008-2009）

编辑：Nigel Smart (BRIS)

过去和现在的参与者：

Steve Babbage (VOD), Dario Catalano (Catania), Carlos Cid (RHUL),
Benne de Weger (TUE), Orr Dunkelman (KUL), Christian Gehrmann (ERICS),
Louis Granboulan (ENS), Tanja Lange (RUB), Arjen Lenstra (EPFL),
Chris Mitchell (RHUL), Mats N¨aslund (ERICS), Phong Nguyen (ENS),
Christof Paar (RUB), Kenny Paterson (RHUL), Jan Pelzl (RUB),
Thomas Pornin (Cryptolog), Bart Preneel (KUL), Christian Rechberger (IAIK),
Vincent Rijmen (IAIK), Matt Robshaw (FT), Andy Rupp (RUB),
Martin Schl¨affer (IAIK), Serge Vaudenay (EPFL), Michael Ward (MasterCard)

27、7、2009

版本 1.0

摘　要

这个报告包括 ECRYPT2 特种网络（NoE）D.SPA.7 的官方文件，由欧洲信息社会技术项目资助的委员会第 7 框架计划资助。报告提供了获得授权的安全目标的密码推荐算法（例如分组密码，单向函数，签名体制）列表和推荐的规模和其他参数设置（应用方式）。因为在密码分析方面的可能的进展，基于项目周期的报告进行每年度的修改。这篇报告从第 6 框架项目（FP6）的 NoE 的早期的报告上进行构架。授权的算法或其他的变化不包括在这个报告里，不能作为特定的算法是不安全的参考，排除的原因仅仅是实际使用到期的限制（e.g 标准或缺乏实现）。

目录

第一章 简 介

为了在一个 IT 系统里保护信息资源，密码协议、算法和密钥用来获得特定的安全目标即信息资源保护。现在依赖通过安全目标制定的标准、公开安全架构获得安全目标典型的方法是什么。这种构架的典型例子是 IKE，IPsec，TLS，S/MIME 等。这是早先基于算法特征和协议的重要发展步骤，对普通公众（最大限度可能）保密。

当确认公开原则是正确的方法，对琐碎的任务也不是完全安全的难题，首先也需要决定算法和密钥对安全目标是适合的，更好一些的方法是使用不同的加密算法和大规模的密钥对每个信息使用四次。也许不同的方法，既然导致很坏的表现、复杂的管理和在一些条件下算法之间糟糕的实际安全。正如我们将要讨论的细节一样，安全是一个过程，而不是一个状态。特别的，公开有时是双刃剑，导致不同的已知攻击，普通用户对更高端的分析和保证他们的系统注册安全是困难的。更进一步，不容易明白不同优化注册的合成困难的效果，安全级别，当通过一个 nbit RSA 密钥去保护一个 K-bit AES 密钥，使用 RSA 底码优化 x？

这个报告的目的是提供范围更广泛，容易对密码算法，密钥和协议里的其他参数的推荐使用，例如这些上述的方法。特别的，报告包括了由欧洲第 7 界程序委员会（FP7）信息社会技术（IST）ECRYPT2 特种网络官方 D.SPA.7 的描述。当试着进行简单的推荐，我们也在相同的时间对更多面向技术的读者提供特别的参考，可以使用更多的背景信息。

既然密码领域是稳定进步的，这个报告里推荐的是一些每年的进展。

报告如下组成：这一章比较该报告和其他同类报告的区别。第二章我们对算法选择标准给出原理。接下来，在第三章，我们介绍一些概念和使用在贯穿整个报告的缩略语。那么，在第四章，我们在高级别讨论安全目标，方法去完成对不同类型攻击者的相关安全和非密码方面的重要，这是该报告的轮廓。剩下的报告分为三部分。第一部分提供密钥规模推荐，第二部分提供对称算法的使用推荐，第三部分最后处理非对称算法。

1.1 相关工作

第一部分报告里控制推荐算法和密钥规模不是轻而易举的事情。我们随后将综述更细节的上述工作，但现在，给出一个大致轮廓。

在[25]，对对称算法推荐的密钥规模是在1996年版本的，早已过时。比较近在[117，161]里对不同的攻击方式给出的推荐密钥规模和提供的对称/非对称等价规模的关系。一定程度上在[117]上简单的版本的分析，是面向发现非对称相同规模对称算法专门使用的，在[114，115]里可以发现。这些报告是非常普通的，不提供推荐算法。在[208]里可以发现一个数量级和不同推荐算法的比较。

美国 NIST 推荐算法和对美国联邦标准的密钥规模是通过FIPS的公开文件呈现的——一个在FIPS里出现的算法/密钥因此认为是“授权”。NIST也可以在特别公告（SP）开发指南/推荐。NESSIE 财团[155]，提供了一份推荐算法的文档，在一定程度上，也是密钥规模。一些在[155]里的算法已包括在该领域的标准里。

RSA实验室在[171]提供了一个在对称和非对称密钥规模相同价值的分析。最后，在[57]，可以发现算法和密钥规模推荐，但仅仅是针对签名体制。

比较上述工作，目前报告的瞄准了一个更宽的范围，包括算法原始类型，比较适合的密钥规模和其他参数设置。第二目标是不使用过多的技术语言提供一些容易理解的不同难题讨论。事实上，在该领域的专家发现在某些领域的文本不太正确（甚至是粗糙），

因此第三个目标是提供对更多技术条款的大量参考。正如提到的，至少对这分报告的年度进展提供更新的信息。

问题之间的区别也是重要的，最小的安全密钥规模是多少？并且，最小的密钥规模不是完全安全的？也就是与其试着发现一个很好的“陷门”，这肯定是不安全的，不如我们试着限制和讨论更多不同的安全级别，考虑更低安全级别，通过环境考虑分配合理的带宽或能量。也就是，要求保护的周期是重要的，是保护信息财产的价值。

第二章 算法选择标准

这份报告提供如下类别密码算法的清单。

- 对称类型:
  - 分组密码（和运算模式）
  - 流密码
  - 单向函数
  - 消息认证代码
- 非对称难题
  - 公钥加密
  - 签名体制
  - 公钥认证/身份识别体制
  - 密钥封装机制
  - 密钥协议和密钥分发

为什么包括一些算法，但没有包括另一些算法（有时甚至是知名算法）？选择的基础是安全和广泛使用。最基本的条件是包括标准化、成熟、广泛使用、安全算法。但是，在有些条件里，共同的使用，但是面向安全没有最优化的算法也包括在其中，在使用时进行校正。也有一些草案标准期望有附加接近未来使用的算法。

因此，事实上，一个特定的算法或变量不包括在内的，不能采用特定的算法不安全作为指示。排除的原因是作为提到的有限制的实际使用（例如，缺乏标准或调度）。相反的，包括不能保证在现在状态下特殊算法是安全的算法。当前的算法也许失败，有时比较吸引人，见[52]。

目前，包括不包括伪随机函数产生器，使用对称技术进行整体认证或更多密码协议元素。在有些基本算法条件的变化下，不同的RSA底码机制是由于他们大范围的使用和期望中的优点而被包括在其中的。

第三章、基本概念

3.1 概念

在整个报告里，如下的概念一直在使用：

$\log_b X$ 基是 b 的对数

log X $\log_2 X$

lnX $\log_e X$, e=2.7182…

|X| X 的规模，i.e. dlogXe

Z_m 模 m 的整数环

Z_{m} _ Z_m 乘法群

F_s s=P_n 元的有限域

请参考附录 A 的缩略语和缩略词。我们应该用国际标准算法对每个算法做参考。尽管他们在正规意义下是不标准的，可能密码标准整套说明最大的“顾客”是 IETF RFC。既然我们应该经常提到这些，我们希望澄清一次和多次缩略词使用。

Ipsec : IP 安全协议，RFC 2401，2402，2406
IKE：互联网密钥交换，RFC 2409
TLS： 传输层安全（TLS），RFC 2246
S/MIME：安全 MIME，RFC 3396，3850，3851
OpenPGP: RFC 2440,3156

上述标准和协议可以从 http://www.ietf.org/rfc.html 查询。

3.1.1 原型信息

对每个原型类型（分组密码，单向函数，签名体制，etc），我们仅仅给出非正式的、对各种原型是否安全的直观定义。许多不同的安全概念已经在文献里提出或使用，并且可以超过更深入的范围。更重要的实际使用，我们应该强调给出的安全概念的细节。对有兴趣的读者，我们常规指出每个 NESSIE 安全报告里每一章的特别综述，[156]。尽管我们的定义仅仅是非正式的，我们不应该使用任意的非标准的专业术语，因此对任意密码教科书，e.g.[137]，如果需要，应该可以提供更开阔的背景。

3.1.2 算法信息

包括在第 8 章到第 17 章的每个算法，在一个算法记录的每个代表形式有如下的形式和意义：

定义：参考固定的算法说明

参数：算法的参数特征，例如支持密钥和分组规模，同样要求算法运算模式的明确

说明，e.g. 实现算法的群。

安全：描述最新的安全特征。特别的对对称算法，有效的密钥规模，或，“如同声称的”，意味着是完整已知攻击。对非对称算法，对于应用，指出对安全和可能假设必须证明。

部署：使用算法涉及到标准和产品

实现：对实现或测试数据进行“参考”，如果这些已知。

公开分析：对公开分析进行参考，e.g. 研究文章/或最新进展，例如NESSIE，Cryptrec, etc, 可以使用。

已知漏洞：已知漏洞的参考和短期解释。

评价：任意附加信息，e.g. 缩略词，使用算法的 pros/cons，etc. 注意算法记录不必要穷尽。

第四章 安全目标和攻击者

我们在 IT 系统里介绍安全去满足特定希望的安全目标。与密码紧密相关的众所周知的安全目标是机密性、完整性和不可篡改性。安全级别决定了这些目标需要满足某重程度上的数量，例如，我们需要“有多强”的机密性，基于 IT 系统的威胁和冒险评估，任意简化要求如下形式的问题：

1、 怎样要求未来必须保持的安全级别？什么是保护资产的“生命周期”和/或“价值”（直接/间接）？
2、 强力攻击成功的密钥搜索是不可避免的，但是是否有更好的攻击？
3、 攻击模型是什么？（谁是攻击者？他/她们有什么资源？）
4、 在数据保护的生命周期这些资源是怎样进展的？
5、 在数据保护的生命周期密码分析程序是怎样开发的？

这个报告采用的方式是对第二点最新的状态进行的，假设至少的条件，推断密钥规模适合不同的安全级别，这是第一点就定义了的。如下我们将讨论更详细的意思。

在这样做之前，关于安全级别定义一些词，（1）同上，这是商业条款，可以指出所有安全分枝的金融影响。这里，更进一步指出“信誉”的价值是比直接典型更大的考虑。这是保护不同类型级别的消耗的整合，最后一人指出直到现在才希望决定安全级别。

4.1 安全过程

意识到安全是一个过程而不是一个状态是重要的。安全意味着使用和管理机制来保护：使攻击成本增高或探测不成功：使攻击很容易被探测。

响应：准备意味着应当成功攻击。

恢复：在遭到攻击后恢复系统到安全状态。

有时，也包括探测，密码的感觉非常类似保护（使用暗示需要破解系统对一个大规模的攻击进行阻止）

但是这里也讨论包括非技术的条款。

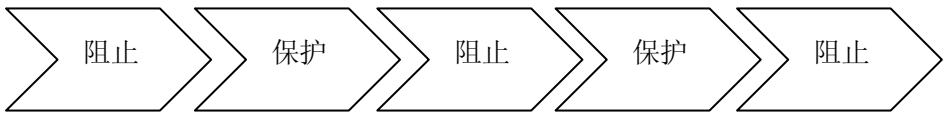

图4.1 安全过程

一个人可以验证在安全过程里的两个实现方法。失败的安全方法在阻止/保护失败安全投入了许多资源，这里，我们成为安全失败方法的对阻止/保护/恢复进行了努力，因此失败不能被唯一，但能够在另一方面恢复。正如我们将要看到的，不同的安全目标有时更适合这两种方法中的一种。

这个报告的部分目标是准备一些为了维持安全系统的安全过程的重要方法部分。但是，许多重要的过程方面也在范围之外，e.g.管理过程包括了密码密钥，例如在使用期限前密钥撤消和密钥代替。

4.2 安全级别

结束时，一个人应该关心攻击着破解安全需要多少时间，并且为了获得一个合理的成功机会，需要什么资源。破解开销（时间或金钱）必须比保护的开销（相似的度量）更大。例如，获得 1 美元的秘密可能花销 1 百万美元的机器，一人可能希望攻击者可以组织这些（除非他/她同时可以获得百万这样的秘密），类似的，如果信息仅仅对一段时间而言是“敏感的”，系统的破解要求一周攻击努力是可接受的。

需要怎样的安全级别是依赖安全目标的。指出上述的安全过程，如果仲裁机密性，常规没有太多可以从仲裁中恢复的信息。然而，如果我们害怕失去已掌握的不可拒绝攻击，恢复机智的几种合成也许是可行的，使用新算法和/或更长的密钥重新设计。因此，机密性常规是上述定义失败安全方法的自然安全目标，不可拒绝动机有时也用安全失败方法处理。

4.3 管理方面

当安全要求很高时，非密码的因素增加。例如，维持一个完整的系统安全级别，128 比特密钥，管理和社会方面趋向更多的密钥规模。我们不能认为关于想象非常高的安全级别是可能的，但我们希望加强这样一些非密码条款，同时使用背景里最弱的一个环节。报告因此简单的假设管理方法可以处理的适合希望的安全。在报告范围之外改变这样的密钥规模，期望回答的问题是：“我们使用 K 比特密钥，用类似这样的过程管理，什么是大概的密钥规模？”

4.4 攻击资源和莫尔斯定理的注记

攻击者怎样实现注册帐户？在 1996 年，[25]使用如下的分类。
“黑客”：使用 0$钱财和标准的 PC，或可能少于 FPGA 的硬件。
小组织：使用一个$10K 的钱财和 FPGA。
中等规模组织：使用$300K 的钱财和/或 FPGA/ASIC。
大规模组织：$10M 的钱财和 FPGA/ASIC。
情报组织：$300M 的钱财和 ASIC。
这样的分类是可能的而且现在仍然有效。

当安全是可以以超过几个月的长时间维持的，我们必须考虑攻击者可以根据最新的进展升级他/她的资源。有时讨论，但常规以可以接受的观点接受假设的莫尔斯定理。这个定理，现在常规引用为每年每平方英尺 $t\_2_{(t-1962)/1.5}$，在前几十年的“每美元的计算能力”有合理的进展。例如，[25]，FPGA系列的DES硬件攻击。这个FPGA系列的门数从1995年的1万门到2002年的十万门。

莫尔斯规则考虑希望的CPU速度锁，但对可能更相关的PC表现，在一定程度上的MIPS能力，似乎即使应用比“1.5”更大的常数，见[192]，工业专家似乎同意莫尔斯定理，在至少下一个十年和几十年仍然回发挥作用。因此，我们选择采用这个假设（如同[117]和先前的密钥规模研究）。然而，完全的新计算模型和硬件类型也需要随后考虑。

4.5 实现注记

密码算法能够更多或更少面临“实体”攻击，而不是密码漏洞攻击。也就是说，攻击能够以来实现错误或可利用的环境特征。例如，一些已知的攻击：密钥空间攻击、时间分析、差错分析、能量消耗分析等等。错误使用和管理差错能够导致仲裁。这个报告里推荐的是给出算法的假设可以合理实现、使用和管理，更进一步，在上述没有提及的边信道环境下运算。偶尔的，然而，我们也许指出这部分自然的缩略词说明。

PART I　普通密钥规模推荐

第五章 确定对称密码的密钥规模

对对称密码体制，在理论上，密钥规模的条件要求简单直观。如果密码体制对数据保护安全周期是可以预测的，攻击方式常规是强力密钥搜索猜测攻击，这种攻击的时间/成功率仅仅依赖计算能力（计算机的数量、特殊目的的硬件，etc），P，以及在他们的处理条件下的预测攻击方案。因此，我们选择一个 n-bit 密钥使得 $2_n/P$ 在某种程度上要比保护数据的周期更大一些。如果需要更长时间的保密周期，比如一年，应该把摩尔斯定理考虑进去。我们综述一些早期的推荐规模和一些（公开的）攻击，过去一些旧的推荐标准的判断。

我们的基础工作见[25]，在 1996 年 75 比特可以抗分析程度是“抗最严重的攻击”，90 比特可以保证 20 年的安全。这些方案见表 5.1，似乎通过定义最小安全维持几天到一年的安全是合理的。（最后一列是对不同攻击者在不同模型下的不同密钥恢复时间）有些方向是：

表 5.1：最严重攻击的最小对称密钥比特规模（1996）

攻击者	硬件成本	最小密钥规模	恢复时间
“黑客”	0 PC（S）	45	222 天
	$400 FPGA	50	213 天
小型组织	$10K FPGA	55	278 天
中型组织	$300K FPGA/ASIC	60	256 天
大型组织	$10M FPGA/ASIC	70	68 天
情报机构	$300M ASIC	75	73 天

这是非常合理而精确的方法。我们有一些最近攻击效果的数据，和一些硬件（FPGA 和 ASIC）的设计 。

5.1 基于攻击的 PC/软件

在 1999 年末，对这些目的的小团队都称为“黑客”在大约 3 周的时间里找到 48 比特 DES 密钥，使用相关普通计算机的小数据，作为屏保应用的部分密钥搜索，[5]。对表 5.1 应用摩尔斯定理，在 1999 年预测 48 比特密钥可以抗大约一年的黑客攻击。因此，比预测的攻击快 17 倍。另一方面，如果[25] 毫无疑问的包括这样的黑客分类攻击，我们随后给出新一些的数据。2002 年，在近 5 年大约 300,000 个人电脑的参与下[51]完成了 RC5 64 比特的挑战。（1997 年使用 3,000 台机器在 250 天里完成了 56 比特的挑战）问题是怎样介绍这样的结果，既然这些结果是 “黑客”使用相关的小资源处理的，通过现在的互联网进行连接。这是重要的条件，既然如果某人确实考虑黑客攻击，黑客密钥规模通过查表（至少 5-10 比特）需要一个非常大的增加。在另一方面，处理这些资源的争论是召集攻击的挑战类型。在另一方面 ，对普通的使用者，他/她最熟悉的部分攻击方式更经常使用各种类型的中间件。确实，[184]报告里称这是最普通的蠕虫。

在[53]里，互联网总的计算能力每年大约有 2^{85}。当攻击单独的 85 比特整个互联网实现花一年时间，还可以考虑更多的例子。

例如，假设使用密钥蠕虫搜索扩展到所有主机的 h 部分。假设也是这种蠕虫，为了避免探测，运行“秘密行动”模型，消耗每台主机的 C 部分 CPU 能量。（我们假设对所有简单的主机有相同的 CPU 能力）最后，假设采用一年前的 t 部分，蠕虫在抗病毒方式下是没有用的。对非常现实的 h,c,t 值（也就是说大约所有主机的 0.1-1%，在 1%的 CPU 能量下对抗病毒攻击有效），我们看到在某种程度上 56-64 比特的密钥是被限制的。

这些例子的研究导致我们对黑客使用分布式攻击需要介绍一个新的类型，也许可以从牺牲品机器上悄悄使用中等规模的CPU时间，我们希望加入这个类型的8比特分类。我们应该没有明确考虑大规模努力类型的挑战。

5.1.1 时间-内存-数据 配置协定

我们至少假设了强力密钥搜索是可能的攻击。这不是必须为真的，例如，如下的条件包括：

- 攻击者能够使用“离线”预处理步骤，产生大量的数据（e.g.在随机密钥下加密信息）
- 攻击者有大容量的存储能力
- 攻击者将能够观察在不同密钥条件下的大规模加密信息，足够攻击者破解这些密钥

在这个模型下的攻击是基于攻击者可以预先产生数据，存储在数据库里并且在观测数据和存储数据之间发现“幸运”碰撞。“幸运”典型依赖于密钥的规模，预先计算数据的总量，并且观察信息的数量，进行众所周知的生日碰撞攻击。从[53]总结的表 5.2 的一些普通、算法独立攻击的复杂度可以通过这样的时间-内存-数据配置进行协定。

表 5.2 普通 TMD 攻击配置协定

密钥规模	No. 密钥数据	时间	内存器	预处理
N	$2^{k/4}$	$2^{k/2}$	$2^{k/2}$	$2^{3k/4}$
N	$2^{k/3}$	$2^{2k/3}$	$2^{k/3}$	$2^{2k/3}$
N	$2^{k/2}$	$2^{k/2}$	$2^{k/2}$	$2^{k/2}$

例如，如果攻击者有 2^{43} 内存和 2^{85} 的预先计算过程，他能够使用 2^{84} 时间，在 2^{43} 的子集里获得诸如 128 比特的内存。

5.2 使用 ASIC 设计攻击

EFF 的 DES 攻击（a.k.a. “深度破解”），[63]，设计和构造需要花费大约 US$200K，1998 年仅仅需要 22 小时就可以恢复 56 比特 DES 密钥。表 5.1 预测在 1998 年，对专业的攻击者 2 天的时间可以恢复 61 比特密钥。经推断，深度攻击应该在 1 个月之内可以完成。表 5.1 因此是非常保守的估计。

在[31]（1999），一台$280M 的机器占据了五角大楼的一角，可以在几分钟内彻底还原 64 比特的 RC6 密钥。[25]数字的推断是非常合适这张图的。

最近，文献[49]（2006）推荐了一个对基于硬件流密码的 ASIC 设计目标。通过定义，

这种流密码容易通过硬件加速（硬件重复），使密钥搜索提速。而且，一些内在的流密码特征被抽取，e.g.仅仅产生一比特输出时，应该希望密钥的一半是可以被忽视的。这篇文章认为在 2010 年，使用$33M 的硬件在一月内可以还原 80 比特密钥。（另外，通过$8M 资金，密钥可以恢复） [25]在 1996 年的预测使用三倍的资金，两倍的时间还原 80 比特，是基本相同的消耗/时间的数量级。

5.3 使用 FPGA 设计攻击

如下，我们对基于 FPGA 设备使用的对称密码 DES 和 AES 穷尽密钥搜索攻击估计代价。对统计的基础，我们在下一节介绍使用面积-时间 DES 和 AES 的 FPGA 优化实现。我们评估的主要结果包括使用 FPGA 的 DES 密钥搜索是低成本和适度的工程专家的灵活处理。然而，在 AES 的条件下，强力攻击看来在未来的几十年里完全不可能实现。

我们关注 FPGA 更细节的原因是与 ASIC 对抗，FPGA 要求考虑更少的专家机制和 FPGA 开发环境的初始消耗是非常适度的（也许好几千美元与 100,000 美元的 ASIC 条件，见[56]）。我们应该强调，尽管，ASIC 比 FPGA 在大容量应用更有效。因此， AES 的密钥搜索机制条件下，应该使用尽量低成本的 ASIC。然而，希望消耗/实现的利益应该比 1-2 倍更好的效果，因此甚至一个基于 ASIC 密钥搜索攻击看来完全不合理。

5.3.1 存在的面积-时间 FPGA 效果实现

在[76]里，不同 AES 在 FPGA 上的实现是可以比较的。表 5.3 总结了相关的信息和相应的参考文献。

表 5.3 一些公开的 FPGA AES 实现的比较（128 比特密钥）

设计	设备	一片	分组 RAM	完全输入(Gbit/s)	Mbit/s/片
Gaj	XCV1000-6	12600	80	12.1	0.96
McLoone	XCV812E-8	2222	100	6.95	3.1
Standaert	XCV3200E-8	2784	100	11.77	4.2
Saggese	XVE2000-7	5810	100	20.3	3.4
Hodjat	XC2VP20-7	5177	84	21.54	4.0

显然的，[188]和[76]产生了在 FPGA 上的最好实现是面积-时间的折衷。11.77Gbit/s 和 21.54Gbit/s 是完全可以实现的。另一个贡献给出了 FPGA 对 DES 和 AES 的加速处理（[105]）。对 744M 字节/s 的处理，在单独 FPGA 上的 DES 要求 3.250CLB（注册逻辑分组）对完全的 2,500M 字节/s，AES 要求 5.350CLB 和 80 分组 RAM。从研究团队获得的其他结果是，可以使用的对称密码也有商业内核。“Helion AES 内核”在低成本 FPGA 上运算（Xilinx Spartan-3）和在四个不同级别上使用：一个 18Mbit/s 的“小内核”，使用 229M bit/s 的“标准内核”，一个使用大约 1 Gbit/s 的“快速内核”，和一个超过 10Gbit/s([75]) 的“Pipelined 内核”。

对 DES，Helion 提供了一个在 Xilinx FPGA（Virtes-II）上对单独 DES 和比 3DES（[75]）230Mbit/s 更多，比 640Mbit/s 使用更大数据率核心运算更快。

5.3.2 基于 FPGA 硬件的穷尽密钥搜索

对一个穷尽密钥搜索，所有可能的密钥使用 DES 或 AES 的 FPGA 硬件实现测试。假设明确-拥有密文文本，我们仅仅需要使用每个候选密钥加密一个单独的分组。所有基于[188,105]的结果，使用非管线实现（管线不同使用，因为我们仅仅使用特殊的密钥加密/解密单独的分组）

对 AES，我们每秒大约可以测试 9.2×10^7 密钥。对 DES，每秒可以检查 1.2×10^7 密钥。因此，使用单独的加密或解密单元，对 DES 和 AES 分别密钥穷尽搜索的平均时间是 3.1×10^{9s}(_98 年）和 1.9×10^{30s}(_5.9×10^{22} 年）。这些数据对 DES 和 AES 的密钥穷尽搜索是灵活的方向。

5.3.3 消耗估计

为了获得全面低成本，我们假设 FPGA 是高价格。例如，一个典型的低成本 FPGA Xilinx Spartan-3 FPGA(90nm 处理)现在大约$6.50（[209]）和包括大约 8,000 注册逻辑分组，因此可以适合 AES 和 DES。既然 5.3.1 的 FPGA 列表是与 Xilinx Spartan-3 不同的，如下的消耗计算方法不算抽象，而且是有根据的。

假设在一个月内进行密钥穷尽搜索，许多 FPGA 必须在一个簇内集成，实现每个密钥空间部分的密钥搜索。我们假设超过 100%的印制电路、电源配件等。更进一步的消耗，电能消耗和可能的冷却消耗应该考虑进去。在这些条件下，DES 可以在$13（FPGA 超过 100%）的 75 FPGA（包括两个 DES 机制）上进行破解，产生大约$1,000 的总消耗。

注意这些数据是基于平均密钥搜索的，即对一半的密钥空间搜索。性价比在估计里保持常数。这就意味着，例如，10 倍快速密钥搜索（3 天）应该要求密钥搜索机制，当然是 10 倍时间的代价（$10,000）。另外，我们应该强调这些估计比抽象的数据更重要。

对AES（128bit），一个平均密钥搜索的消耗分别是$\$4.6\times10^{24}$。甚至如果我们使用摩尔斯定理考虑（每1. 5年IC的成本减少2倍），2055年，这样的机制应该消耗$\$4.2\times10^{14}$。

然而，如果摩尔斯定理对这样的时间扇区是有根据的，基于半导体的计算方法 在各种物理限制下进行运算。然而，这些也有相关条款的消耗：甚至如果技术产生作用，制造水平得到提高，消耗降低，并且保持摩尔斯定理的预测。

5.3.4 相关 FPGA 领域的抗 DES 攻击研究

Hamer et al. ([69]) 的一篇文章描述了在可编程领域的DES破解硬件，称为“完全变形 2a”。一个完整的完成系统应该可以在1020天里以800百万密钥/秒的速度进行搜索。一个单独的单元由两种Altera 10K100 FPGA组成，每种有4MB内存的连接结构整个系统由16个这样的单元组成，希望消耗大约$60,000。

另外简单的密钥穷尽搜索机制，[111]提供了一个硬件FPGA的线性分析实现。作者完成了Matsui的原始攻击。最终攻击比Matsui的攻击效果差，但可以在单独的FPGA硬件上12-15小时进行破解。

[187]有一个通过穷尽密钥搜索对 DES 的攻击十分精确的估计。假设使用低成本的设备，例如从 Xilinx($ 12 p.p.) 3S1000 Spartan-3 和最近实现 DES 效率的结果看，在 3 天内完成 DES 破解大约需要$12,000。

在[113]（2006） 一个 e9,000 FPGA 设计，“COPACOBANA”在大约 9 天内可以破解 56 比特密钥。这是明显的（但不时任意重要的）比从上述 DES 机制里推断慢。因此，[50] 提出了一个类似流密码密钥穷尽的目标。

5.4 结论

通过上述的分析，我们的目标是在表 5.1 里加入大约 8 比特，同时加入安全边界的分布式攻击。ECRYPT 的对称密钥表在第 7 章里可以看到。

我们通过上述结论和在[117]里的工作进行快速“正规检查”。基于摩尔斯定理要求的密钥规模的研究，1982 年$50M 机器在 2 天里可以恢复 56 比特密钥，因此 56 比特密钥从那时起就完全不合适了。

现在 2008[117]推荐大约 75 比特的对称密钥，摩尔斯推断（加入 8 比特大约 1996[25]值）导致（2008）$300M 机器在 73 天里发现 83 比特密钥。在诱使返回（$50M,75-bit,2 天）机制在相同时间恢复 78 比特，或在大约 64 天时间恢复 83 比特密钥。因此通过我们的估计。

对 FPGA，表 5.1 预测在 2008，58 比特密钥给出了$400 FPGA 大约 200 天的保护设计。我们估计$12,000 可以限制 3 天里相同密钥规模的设备。花费$400 在 FPGA 上，可以给我们还原 58bit 密钥，如果可以等 90 天的时间。

5.4.1 边信道攻击

当考虑处理密码本难题时，不同的研究领域分析强调实现。非常难的密码难题是容易遭受攻击的。这样的边信道攻击实际上发现加密过程里的信息泄露，是否对不同的密钥/运算是不同的时间，不同的能量消耗曲线，甚至不同的内存访问周期。

时间攻击[109]是基于秘密运算平台的观察时间的。例如，考虑RSA加密不通过保护的使用平方或高次运算。在这种条件下，时间要求解密过程的步骤，当秘密指数大约两次1出现一个0。通过观察，解密过程时间是可能要求获取秘密指数的时间。通过使用特殊的密文和统计方法，可能恢复全部密钥。

算法运算时的高阶分析[110]跟随相似的观察互联信息的概念，但是使用能量消耗实现。例如，能量消耗显然可以使内存的bit 从0到1（或从1到0）比保持0比特消耗的能量多。这种攻击是智能卡、RFID 等特别设备使用的，攻击者可以通过设备容积的检测到能量消耗。总的研究数量是提供抗这种类型的保护，常规新的保护方法对这些攻击不产生新的作用。

Cache攻击[163]是特别的时间攻击条件。时间攻击规律常规抗非对称难题是有效的，他们常规抗对称算法是失败的，因此他们的执行时间是非常接近固定时间的（执行时间通过实际值加密是不相关的）。Cache攻击在算法加密前克服了测量Cache攻击状态的条款。通过观察所有的访问，在加密过程里可以探测到一个非常好的信息。这个领域最近的工作是使用现代CPU的TLB（Translation lookaside buffer）。值得一提的是，在Hyper Threading 计算模型 [162] 的条件下，最近 AES 的结果使未来 INTEL 的 CPU 指令需要AES加密。

不同的对抗活动建议克服这些攻击。大多是常规的方法（e.g. 维持一个加密方式下的 SHADOW 值，是不同的渠道能量消耗）和一些他们的算法说明。难题的分析抗这些攻击常规是非常难预测的（这样的攻击是基于说明实现的，不直接介入算法），有一

些基本的观察是真实的：真值表的使用，增加密码 Cache 攻击的受损程度。（攻击者可以尝试观察全部访问的表）。简单的运算看来比保护它容易（例如，取一个XOR运算的能量和32比特倍数的能量是常数）。

因此，对定义使用的模型用来分捡正确的密码问题是重要的，访问攻击者也许必须实现。更强的攻击也许数量上和边信道攻击是一样的，变成更贵的保护实现。

第六章 确定相应非对称密钥规模

对非对称密码学，问题更复杂，原因是：

- 无需大规模密钥实现
- 增加30年内发现的有效攻击（必须比强力攻击更有效）
- 我们最近看到对特殊目的密码硬件建议：比直接搜索机制更有效。对称和非对称机制

常规联合使用，e.g。非对称密钥是对称密钥的使用指南。因此，我们必须意识到一定程度的损失，常规有效的“安全”是与“弱链接”原理是一致的，我们需要发现非对称密钥规模的方式和对称密钥规模的预先说明相匹配。同时，我们希望避免过大的公共密钥。有些专业人士进行一些复杂的研究，而不是重复劳动，我们应该看到从这些材料里获取的结论。

6.1 内部系统等价

如下，RSA 常规对公钥体制，假设对整数因子分解难题是同等难度。我们类似的使用 DLOG 和 EC 指出常规基于离散对数的体制和安全椭园曲线组，相应的，都是素数阶的有限域。

对EC，最新的进展是 m-bit 规模的子集合等价 m/2 bits 对称密钥。事实上，考虑这些攻击的基本运算是一个椭园曲线指出的附加条件，可以试着和对称密钥相比，可能实际减少 8-12 bits 的 EC 密钥规模。

在 [117] 里可以查到，但在 [149,114] 里没有这项内容。作为常规推荐，我们提出如下简单的半规模原则。这也在[117]里注记到的，提供一些抗椭园密码分析的没有预先开发的保护，对实现没有严重的影响。在二进制域上的曲线常规推荐（见[207]）到轻度使用大规模密钥缓和特定的硬件攻击。而且，常规攻击在二进制条件下有时更有效。例如，所谓的 2^n 规模的二进制域 Koblitz 能够比 $\sqrt{2n}$ 的因子分解更快。当选择参数时，二进制域上的曲线常规要求其他形式的特殊关注。

根据最新进展，在规模是 2n 的域的素阶上解 DLOG 的难度为常数，对破解决 n-bit 的 RSA 渐近等式。在完全的时间里，DLOG 明显是更困难的。更进一步，DLOG 在小的子集里实现更标准的算法，那么这个子集合的规模在某种程度上是对称密钥定理等价的，也就是一半比特规模，抗 EC 条件下根据相同的普通攻击应用。值得注意的是在有限域上比一个椭园曲线同等安全，实现指数攻击是明显更贵的（不同的 10-40 倍数，以安全级别）实现，因此可以与实现相关。如果要求，通过少数比特对实践相同一半规模原理的简单应用减少子集合的规模，安排 n-bit 域和 n-bit RSA 相同安全，对 DLOG 基础体制的保守推荐。通过这些考虑，主要的条款是决定 RSA vs. 对称密钥等价。我们接下来综述一些这个领域的出版物。

6.2 现存指南的综述

通过任意的原因直到1982，假设 56bit 数据加密标准（DES）考虑“安全”，[117] 建议直到2012年，80比特对称密钥是安全的并且计算等价1120-1464 bit RSA/DLOG密钥

（以消费模式；HW/常规目的计算），140 bit DLOG 子集和149-165 bit EC 群（依赖分析过程的子进程）。分析是非常方法论的，可以使用起源于假设到脚本的密钥规模。

表 6.1：Lenstra-Verheul 推荐（假设“平均”消费模型/密码分析进程）

等价对称密钥规模	56	64	80	96
椭园曲线密钥规模	95	116	160	200
模长度（pq）/dlog 域	380	580	1300	2500
Dlog 子群	102	114	141	171

考虑更多的消耗（内存），[183] 争论在 2000 年，1024 比特 RSA 密钥相应 96 比特对称密钥。作为在[180]里的注记，这导致了 [117] 和 [183] 之间不同的 RSA 密钥生命周期的推断，第二给出了 1024-bit RSA 密钥比 30 年更长的生命周期。另一方面，在 [117] 里介绍的更坏的情况是 1024 比特密钥应该现在被分解了，但是认为任意密钥没有公开的记录，甚至接近被分解规模。

US， NIST 在 [149] 给出了一个表格，相应 1024 比特 RSA/DLOG 密钥和 160 比特 DLOG 子密钥和 EC 群，描述了 80 比特对称密钥。对 128 比特级别，推荐相应的 3072 和 256 比特密钥。直到 2010 年考虑 80/1024/160 比特级别是足够了的，提高 112/2048/224 比特，RSA

表 6.2：NIST 推荐

等价的对称密钥规模	80	112	128	192	256
椭园曲线密钥规模	160	224	256	384	512
模长度（pq）/dlog 域	1024	2048	3072	7680	15360
Dlog 子集	160	224	256	384	512

实验室和标准推荐在这里列出了。为了所有实践的目的，这在合理的协议下也获得了[117] 但不在与对称密钥运算比较下，EC 和 DLOG 子集里运算的代价。

最近在 [156] 里的 NESSIE 财团，对“中期”（5-10 年）安全推荐使用 1536 比特密钥长度的 RSA 和基于公钥体制的 DLOG，和 160 比特的椭园离散对数，建议 1536/80 等价，[117] 在线，对上述 EC 代价相同评价。这个推荐是基于 512 比特 RSA 密钥和 56 比特密钥等价的推断。然而，应该注意到，这个报告产生的条件，我们发现 NESSIE 推荐是基于精确的公式，导致某种程度 RSA 密钥过大。

在 [171] ，RSA 实验室实现基于代价的分析，获得了表 6.4 的等价密钥规模。计算破解时间假设机器能够在 100 秒里破解 56 比特密钥，然后相应进行扩展。机器栏目给出多少 NFS 筛法机制能够在假设$0.50/M 字节条件下假设购买$1 千万。

表 6.4 RSA 实验室分析

对称密钥	EC	RSA	时间	破解机制	内存
56	112	430	〈5 分	105	没有价值
80	160	760	600 月	4300	4Gb
96	192	1020	$3\cdot10^6$ 年	114	170Gb
128	256	1620	10^{16} 年	0.16	120Tb

IETF 推荐标准 RFC 3766[161](很大程度上基于[117]消耗模型变量)建议 80 比特对称密钥是与 1228 比特 RSA/DLOG 等价的，148 比特 DLOG 子群。特别的，给出表 6.5。

表 6.5 IETF RFC 3766 推荐

等价对称密钥规模	80	100	150	200	250
模长（pq）/dlog 域	1228	1926	4575	8719	14596
Dlog 子群	129	186	284	383	482

RSA 也在[206]里对短签名的生命周期进行推荐。这基于 100 折叠的安全

表 6.6 :[206]短 RSA 签名密钥生命周期边界

密钥规模	生命周期
512	1 小时
576	10 小时
640	4 天
704	30 天
796	8 月
1024	1 年

512 比特密钥要求 5 天的攻击效果。

所有上述报告的基础和讨论是要求保密的。有时讨论认证要求，可以比数据重新认证规律增加更大规模的密钥和更新的算法。例如签名，ETSI 报告 [57] “授权”密钥规模包括：1024 比特最小因子离散对数分解密钥和 160 比特椭园群的规模，但是授权在 5 年以后需要重新评估（例如有效期是 2001-2005）

6.2.1 ECTYPT 选择的方法

假设 n_{512} 是对称 (DES) 与 512bit RSA 等价密钥规模。与 NESSIE 类似和起源于讨论，ECRYPT 对基于 DLOG 基础体制的 RSA 因子分解的公钥规模推荐是基于 n_{512} 的统计和普通数域的复杂攻击的推论。数域筛法（GNFS），是计算整数和离散对数目前最快的方法。我们提到的方法是，基于 RSA 和因子分解假设等价。

特别的，对 N 的因子分解的 GNFS 运算时间估计是：

$$L(N) = Ae^{(C+o(1))(\ln N)^{\wedge 1/3}(\ln \ln N)^{\wedge 2/3}}$$

对一个常数 A，并且 C=（64/9）$^{1/3}$。我们应该假设对可以掌握的密钥规模是 o(1)级，可以作为 0 处理。从这一点，我们可以基于 L（512）= n_{512} ，这留给我们决定 n_{512} 数量的难题。从实际可以使用的经验值可以看到，RSA-512 的“抗攻击”比 DES-56 的 4-6 比特少一些。我们选择更多保守的值，例如，n_{512} = 50。

我们现在对有效的模 N 的 n-bit RSA 的不同密钥规模给出如下的表达式：

$$S(n) = (64/9)^{1/3} \log_2(e)(n\ln 2)^{1/3}(\ln(n\ln 2))^{2/3} - 14$$

对椭园曲线和离散对数 log 子群，如同上述讨论，我们应用“一半”规模的原理。

6.3 特殊目的硬件的操作

对一个（安全）对称难题，加速攻击时间是在几个目的的计算机上并行处理的，或者，构造一个特殊目的的密钥搜索机制。出于我们的知识结构，考虑最大的这种机制，是上述提到的 EFF 的深度攻击[63]。实际上考虑的是这样的硬件，甚至没有更进一步的提高，一个 64 比特密钥应该在少于一年的时间得到恢复。

同样对公钥（数论）体制，已提出了特殊目的分析硬件。

TWORL 设备和(光)TWINKLE 处理器，[178，179]，已经提出所谓的因子分解的筛步骤。看来应该感谢 TWIRL 严重威胁 512 比特 RSA 密钥（通过常规目的计算和非常小效果[5]的攻击）和构造一个 TWIRL 设备的构造消耗，以“合理的速度”分解 1024 比特 RSA 密钥和并行密钥搜索机制恢复 80 比特对称密钥进行比较。

Bernstein，[19]，提出了成为因子分解算法的矩阵步骤的大规模并行机制和称为基于密钥规模的因子分解的碰撞，要求作为大密钥的三次时间。随后的分析 [116]，然而，建议中等规模 17%的增加和仅仅在“最优”假设下的实现。

最后，[159]（1999），描述了硬件设计统计消耗$10M，可以在一个月时间破解在 2^{155} 域上的二进制椭园曲线。然而，既然设计比普通有限域更少消耗，避免的方法是不使用二进制域。在[207]，二进制域上统计椭园曲线，应该有8-10比特更大的密钥缓和这种硬件的效果。

考虑上述提到的机制的效果仅仅限制在密钥规模的范围，或限制碰撞，对这个报告的目的，我们应该在[159]讨论的机制考虑的特殊目的硬件。因此，我们提出关心的用户加入大约10比特。然而，对特殊硬件领域里的特殊目的的进展。我们没有办法在这个领域获得未来的进展。

6.4 量子计算

对整数因子分解和离散对数难题的两个棘手的假设可以破解，如果 Shor[181] 的量子证明可以构造出量子计算机。例如在这种机制下，整数 N 能够在 O（$\log_3 N$）步分解。然而我们对这样的设备的认识还相去甚远。在[193]，对因子“玩具”数 N=15 的分解时间是仅仅一秒之内。对对称密码算法，效果更加明显，甚至是毁灭性的。

Grover[65]通过普通搜索算法，密钥规模的效果仅仅达到一半。这种算法在小玩具实验里[40]已完成了。一个量子计算机应该也以复杂度 $2^{n/3}$[30]发现 n-bit 单向函数碰撞。

这个报告的推荐是假设大量量子计算机在最近不能成为现实。

第 7 章 推荐密钥规模文献

对上述讨论，ECRYPT2 推荐如下最小密钥规模防止不同的攻击。注意有一些最小规模，在几个月内给出保护。

表 7.1 对不同攻击者在比特范围内的最小对称密钥规模

攻击者	价格	硬件	最小安全
“黑客”	0	PC	53
	< $400	PC(s)/FPGA	58
	0	“中间件”	62
小型组织	$10K	PC(s)/FPGA	64
中型组织	$300K	FPGA/ASIC	68
大型组织	$10M	FPGA/ASIC	78
情报机构	$300M	ASIC	84

给定任意安全级别，把相应对称密码的密钥规模等价转化为非对称密钥规模。基于过程的讨论，我们提出如下的对称/非对称等价规模，见表 7.2。我们注意到 [114] 的表 1 的合理成分。

也许对现在开发的 RSA/DLOG 密钥规模的共同等价对称密钥规模，这可以从表 7.3 看到。注意 DLOG 和 EC 推荐素阶域。对 DLOG 体制的有效域，表可以需要修订考虑对 DLOG 在二进制域上进行更有效的修订。然而，我们没有意识到基于二进制域的离散对数现存的实际开发系统。

对 EC，对需要考虑的域的规模推荐二进制系统应该是 2p，p 是一个比特规模比群密钥规模稍大一些的素数。

如果另外 [159] 的特殊目的硬件考虑威胁，大致上另外 10 比特应该在这个条件下加入 EC 密钥规模。

表 7.3 等价密钥规模

安全（比特）	RSA	DLOG 域规模	DLOG 子域	EC
48	480	480	96	96
56	640	640	112	112
64	816	816	128	128
80	1248	1248	160	160
112	2432	2432	224	224
128	3248	3248	256	256
160	5312	5312	320	320
192	7936	7936	384	384
265	15424	15424	512	512

表 7.3 使用 RSA/DLOG 密钥的有效公共密钥规模

RSA/DLOG 密钥	安全（bits）
512	50
768	62
1024	73
1536	89
2048	103

7.1 推荐参数：非机密目标

上述最小要求希望在某个时间保持消息的机密。对其他安全目标，事情也许有一些不同。

7.1.1 不可篡改

恢复安全的概率是更好一些的，因为以规律的介入重新认证（和可能的攻击）可以假设逼近估计。因此，一些短密钥是可以接受的。

7.1.2 消息认证

基本上，相同的恢复机制在这里是可以应用的。第二，一些应用在这些可信数据仅仅在适时的条件下可信的，并且附加要求低安全的效果/带宽。

既然使用短密钥没有或常规很小的收获（从效果上看），上述推荐也保持认证密钥。假设选择足够大的密钥（使用安全协议/函数），主要威胁是“猜测”伪造攻击。（我们注意到有 MACs，基于 MACs 的 Carter-Wegman，这里可以保证这种攻击仅仅有一种可能）

对 MAC 目标，也许可以接受使用比 MAC 密钥规模短的值。在[70]，给出了一个 32 比特倍数的绝对最小目标。

一个甚至认证密钥也许在所谓相互认协议（MANA）的应用例子是相对短的。一个典型的应用是在两个使用小范围无线电的一次认证数据变化。在两个设备上选择一个（一次）PIN 作为密钥可以访问（使用物理边信道）。如果正确完成，伪造的概率可以明确评估，并且密钥能够有时允许比 16 比特标签和 160 比特标签更短。在细节条件下，注意这些值在相同的密钥重新使用条件下可以破解。见 [61] 更细节。应该注意到这种分析常规这样“物理逼近”条件下假设，部分使用特定攻击的规律。

常规条件下，当考虑最小接受标签规模，重要的是分析是否应用这种可能攻击的预言机制访问 MAC 证明机制。短标签应该在这种条件下使用。

7.1.3 用户认证

对用户认证（使用对称密钥挑战应答类型协议）应答长度的重要依赖有效认证的时间周期（会话长度）。如果一个攻击者幸运的猜测到一个应答，他将探测到重新认证（如果可以探测）。常规比伪造突发消息的影响更大。64比特的应答看来常规是最小的。一

个一次口令（OTP）产生典型过程 24-32 比特值，但是常规在长期的通信里使用，用户选择密钥（一个口令）。除非提出通信信道的物理安全（抗黑客攻击的安全），重要的是用户认证复制整型保护的会话密钥。也就是说，产生相同时间的应答，对相同挑战的整型保护的会话密钥和使用整型保护每个连续消息。使用合理的挑战保护应答，伪造应答的限制效果比短期拒绝服务攻击更有效。

7.1.4 单向函数

对安全单向函数的主要考虑是输出的规模。如果应用要求碰撞是难以发现的，输出必须是希望的安全级别的两倍。

这个条件下，使用数字前面。当对消息使用一个密钥单向认证，然而，输出也许经常如同上述被截断。

7.1.5 挑战随机数

所谓的挑战随机数（使用一次的数字）常规要求与安全级别符合的对称密钥的使用。这是因为基于生日攻击。例如，一个 n 比特挑战随机数（常规称为盐）用一个 k 比特对称密钥在大约（n+k）/2 比特的安全过程里，进行抗离线碰撞攻击。

7.2 安全级别

观察表 7.1 的安全级别，仅仅给出最基本的保证（几个月后），我们希望假如一些真实保护的边缘。在相同时间里，我们仅仅讨论，有一些使用特殊特征的应用，也许允许低安全边界要求，应该有可以获得一些简单的特定级别限制环境。我们因此可以定义一些安全级别和可以获得安全数量，在某些条件下，这个结果是可以接受的。也就是说，使用特定的密钥规模可以控制，我们应该更复合实际并且看到在有效条件下可以获得所谓安全的一些评估。

表7.4: 安全级别（对称等价）

安全级别	安全	保护（bits）	解释
1	32	个人适时攻击	仅仅接受认证标签规模
2	64	抗小组织的短期保护	在新系统里不使用机密数据
3	72	抗中等规模组织的短期保护 抗小组织的中期保护	
4	80	抗专门机构的极短期保护 抗小组织的长期保护	最小普通目的级别≤4 年保护
5	96	合法标准级别	2 密钥 3DES 的限制在 10^6 明文/密文 ≈ 10 年保护
6	112	中等规模保护	≈ 20 年保护，3 密钥 3DES
7	128	长期保护	好的常规的应用 ≈ 30 年保护
8	256	“预测未来”	抗量子密钥的好的保护

一个 80 bit 级别出现最小常规目的级别的知识，抗最有效和合理的攻击保护。然而，也可以进一步看到，32 和 64 比特级别应该对机密保护进行使用；32 比特密钥提供非机密相关攻击，对 64 比特提供仅仅不同的保护。不同的是，当这些级别也许是必要时的应用，如果对整数标签完全提供安全。当我们特定不考虑这个安全的级别应该提高，在相同重要的时间考虑进行一些窄带应用的影响，首先考虑这种短标签，使简单明确攻击成为可能。

对高和非常高的级别选择 112/128 在目前推断下是保守的。然而，既然存在很好证明标准元件支持这种级别，也看来可以合理定义，通过合理的对手攻击，当使用 80 和 128 比特密钥提供有效安全抗强力密钥搜索攻击（在对称难题条件下），应该注意到基于预先计算的攻击模型和大规模可用的存储，第 5.1.1 节里处理的攻击。考虑一个 80 bit 有效的实际破解，和 128 比特可能相应的有效 80 比特级别。作为首要简单的规则，应该选择双倍密钥从这样的攻击里减轻威胁。

7.3 怎样处理长期安全

在一些应用里，例如合法盲签名，固定秘密保护，应该需要非常高的安全级别。作为预先的讨论，获得和维持这样高的安全级别是困难的。除了非技术的因素，这个报告范围之外，更合理的要求，也出现了技术难题。也就是说，对分析发展技术是难以估计的。例如，一个 1024 比特整数，数域筛法比立方筛法方法更好，同时未来的提高应该有所不同。也就是说，甚至密钥规模的对下一个算法是有效的，比如 30 年，在这样的时间段，不能排除特定的算法更完善或可以完全破解。因此，我们采用怎样的分析过程进行考虑？在最后，如果分析对 RSA 有效，也就是说，对摩尔斯定理规律 20 年有效，应该不是合理假设，过程虽然短暂，可能对这样的想象轮廓更具争议，同时也更快（甚至在理论上更合理）。对所有实际目的（一个人可以还击的位置），我们可以在过去基于个人假设，假设未来的过程跟随这样的趋势。

在步骤里常规的进展（例如，从 QS 和 NFS 里提高），和超过大约 10 年的时间，在 ECRYPT2 参与者里常规的概念是推荐今天应该假设一个特别小的机密级别，也许特别是对非对称密码。

对所有没有考虑到的因素，对因为过程再次处理安全，可能还是维持消息认证和长时间的防篡改是可能的。通过保持分析和技术进展的数据，因为害怕更强的攻击，使用大密钥规模和不同的算法重新认证一个消息（存在签名）。

对消息认证的另一个方法是使用多个算法认证消息。例如，使用两个不同的算法签署一个消息，当且仅当两个签名都可以检查，并且考虑有效签名。重要的是密钥和参数常规随机产生和独立，并且，指出未来可能的进展，可能本质的算法是非常不同的。例如，如果量子计算机可以实现，使用 RSA 和离散对数技术不提供任意附加安全的算法，签署一个消息。某人可以考虑非对称和对称密钥的合成同时签署一个消息，并且加入基于整数的对称密钥。对机密，可能应用安全过程考虑更困难，一旦机密丢失，可以永远消失。然而，附加保护应该提供多重加密，抗使用有效“不同”算法。经典的一次体制应该可以应用非常安全的级别，假设可以解决密钥协议。

7.4 一个最后的注记：密钥使用原理

除了上述的推荐，重要的是意识到怎样使用其他参数的一些原理。

首先，一个随机原理必须如下：密钥必须随机或伪随即产生。如果比实际需要有更

少的少量密钥资源，伪随机函数应该用来获得要求数量的密钥。当然，我们不用声明比任意输入大小的随机数产生器更高的抗攻击机制。作为伪随机数产生器对合适的种子比特是关键的。这就是说，在实际应用里，可以经常看到。

第二，密钥扩展应用的原理：相同密钥应该对两个不同目的同时进行应用（对加密和整数保护使用不同的密钥）。更进一步，对称加密不用使用相同的变化输入（密钥，IV，etc）对不同消息过程进行双倍的处理。对整数保护，为避免重放,所有消息的安全是不同的（包括记数器）。这对其他的素数也持续推荐，在两个不同的体制下使用不用相同的签名密钥。

最后，对电子签名体制，怎样使用秘密密钥进行签名，应该不是太“重要”。首先没有安全消息底码体制，前面文件永远使用一些其他体制，包括合适的随机，见14章。

Part II　对称难题

第八章 分组密码

分组密码是一类密码算法：通过 n 比特密钥，把 b 比特分组变化到 b 比特。也就是说，通过两个算法，加密算法 E，解密算法 D，对所有 n 比特密钥 k，所有 b 比特分组 x 进行函数运算 D（k,E(k,x)）=x 。大多数算法支持一个分组规模，但是在许多条件下，可以支持几种密钥规模。

分组密码算法考虑一些安全特征。无须多说，一个要求是防止复杂度比 2^n 更好的密钥恢复攻击（e.g.差分 [21]，线性攻击 [124] etc）。对通常情况下更强的更强的安全概念，意味着什么？阅读者应该对人工智能熟悉，这些人能够通过和其他实体“对话”（键盘/屏幕），etc。这些实体可以是人或计算机。如果用户不能区分是否在和一个人或计算机对话，程序是人工智能的实现。在我们的条件下，攻击者获得明文，一个明文（从一个未知，随机密钥）的加密，或，一个随机 b 比特串。攻击者挑战猜测他得到的值，到这个过程结束，他可能选择要求加密的消息原语，在任意消息（除了挑战）。如果他不能成功过得去超过一半的概率，密码可以从随机预言里分离。如果密文仅仅看来是随机的，他们不应该得到关于明文的有用的消息泄露。在不同的安全概念里有许多已知不同关系和等价。

如果不是特殊的运算模式，见 8.4 节，注意分组密码应该不在列上使用。我们强调分组密码不提供整数保护，没有加入整型保护，可能会丧失机密 [18]。

分组规模也许在安全边界的上限定义。可以直接产生小的分组尺寸。也就是说，“不随机”行为也许可以在大约 $2^{b/2}$ 的加密分组后被探测到。这一章因此根据分组规模描述。

对一个分组密码算法特征扩展的讨论，见 NESSIE 评估报告，[156]。对更多分组密码明确的信息 [26] 。

8.2 64-bit 分组密码

8.2.1 DES

定义：NIST FIPS 46-3，[140]
参数：56-bit 密钥和 64-bit 分组规模
安全：不同密钥长度
使用范围：大范围，e.g. RFC 2406（IPsec）,RFC 2246(TLS)
实现：
公开分析：文章[21，24]（如下）
已知漏洞：假设差分分析[21]和线性分析[124]和扩展，通过 10-12 bit 进行有效密钥归约。然而，显然密钥规模已不合理
评论：NIST 2004 撤回

8.2.2 3DES

定义：NIST SP-800-67，[148]。（在 ISO/IEC 18033-3[89]标准化）
参数：112-bit 168-bit 密钥和64-bit分组
安全：因为3DES 的迭代结构，对3DES存在密钥搜索攻击，工作函数明显比密钥规定规模小。对三密钥3DES，工作函数可以减少到2^{112}运算（甚至在特定攻击模式下减少到2^{100}）运算次数。对两密钥3DES的工作函数可以由2^{112}降低到2^{120-t}，

如果攻击者可以获得使用相同密钥2t 明文/密文对（t>8）
使用范围：大范围，112bit 3DES 广泛的使用在金融系统里，168-bit 3DES使用在Ipsec，SSL/TLS，etc。
实现：
公开分析：Cryptrec 报告[46]
已知漏洞：结构特征的变化是众所周知的，但是可以容易回避
评论：[149]，112-bit 3DES 可以在 2010 年由 NIST 重新证实（通过上述讨论的基础，在 2^{40} 明文/密文对可以提供给一个攻击者条件下，提供 80 bit的安全），168-bit 3DES 推荐使用到 2030 (如果仅仅提供 112bit 安全)

8.2.3 Kasumi

定义：3GPP TS 35.202，[1]
参数：128-bit 密钥和 64-bit 分组
安全：如算法说明
范围：UMTS
实现：3GPP TS 35.203，35.204 [2,3] 包括测试数据
公开分析：评估报告[4]，文章[28]。一些已明确的可证安全相关线性和非线性分析[101]
已知漏洞：在[20]，一个相关密钥攻击要求_ 2^{54} 明文/密文对和_2^{76} 复杂度。相关密钥攻击的相关实现不推荐在 3GPP 使用
评价：MISTY-1 的变种，在 UMTS 里使用 Kasumi 证书

8.2.4 Blowfish

定义：见[177]
参数：32-448-bit 密钥 和 64-bit 分组
安全：如算法说明
范围：在 IPsec 注册表里使用。产品列表可以在[27]发现
实现：见[27]（包括测试向量）
公开分析：Vaudenay, [197]，发现弱密钥和已知明文攻击，但仅仅对减轮 Blowfish，见更近的文章 [102]。Rijmen, [168]，发现不能扩展到全部的密文。Schmidt 做了关于密钥体制的一些观察，[176]，对安全看来无效
已知漏洞：
评价：

8.3 128-bit 分组密码

8.3.1 AES

定义：NIST FIPS PUB 197，[143]（也在 ISO/IEC 18033-3[89] 里标准化，Suit-B[157] 的部分）

参数：NIST FIPS PUB 197， [143]（也在 ISO/IEC 18033-3[89] 里标准化，Suit-B[157] 的部分）
安全：如算法说明
范围：大范围，包括 TLS，S/MIME，IPsec，IEEE 802.11i，etc
实现：
公开分析：NIST 报告[152]，NESSIE 和 Cryptrec 报告[156, 46]
已知漏洞：
评论：提出了所谓的代数攻击是对 AES 的潜在攻击。当一些条款还非常难懂时，AES 不同考虑这种分析的脆弱性，到目前为止，AES 考虑了这种分析的脆弱。另外，AES 安全实现方面的漏洞是最难处理的过程（这些方面共享了密码学许多难题）。因此，当不直接和 AES 的密码强度相关时，抗未保护指令的 cache 时间攻击看来保持实际的威胁，至少当 AES 没有在可信环境下进行处理。另外的实现攻击没有 AES 可识别的密码弱点。对 AES 更多的信息见[10，53]。当 AES 远远比广泛使用的 128-bit 分组密码，没有意识到仅仅是这样的算法。如果希望使用一个帮助算法，应该立刻考虑使用 Camellia,[89]

8.4 运算模式

NIST 的分组密码算法运算模式说明见 [147]，[23]。一个标准使用的例子是 ISO/IEC 10116，[86]。另一个 NIST 的标准是[144，146]。

8.4.1 ECB 模式

加密比相等分组小的消息，否则会产生信息泄露。对相同的条件，给定密钥应该仅仅使用加密一个单独的消息。因为消息比分组小，消息底码必须填充分组，因此有超出带宽范围的危险。如果在密文里出现一个错位，解密出现垃圾错误繁殖。大约一半的明文会被改变。

8.4.2 CBC 模式

CBC 要求底码或上一分组的信息泄露，与 OFB 模式的最后分组信息泄露相同。导致[139]攻击。注意底码体制通常对边信道攻击是敏感的，攻击者可以对接收者和观察者诸如错误信息[196，138]。这也说明了完整性认证的重要性。如果分组密码算法安全，可以证明 CBC 模式安全[15]。

8.4.3 CTR 模式

CTR 模式是分组密码作为流密码使用的模式。可以抗[131]攻击，如果分组密码算法安全，CTR 模式安全[15]。

8.4.4 混合加密模式

随后在这篇报告里定义混合加密（密钥/数据封装模式，KEMs/DEMs），见 e.g. 16.2.1

节。合成了非对称密码和对称密码。混合体制有时证明安全，但要求对称密码难题的细致选择。推荐仅仅使用标准花后允许使用的算法。例如，标准ISO/IEC 18033-2[88] 说明一个DEM 使用 CBC （ISO / IEC 10116）和 根据 ISO/IEC 9797-2 产生的 MAC。 另外，ISO/IEC 19772 六项标准认证技术在2009年2月公布了。

第九章 流密码

9.1 简介

流密码是采用密钥产生(主要为实践目的)的长序列，密钥流。这个密钥流与明文合成为密文。最通常使用的密码应用，流密码是面向比特的模 2 明文（XOR），这称为二进制附加流密码。一些密码使用其他的合成运算，在某些条件下提供一些整型保护。注意明显的二进制附加比特自身没有整型保护；一个攻击者可以产生比特流。

二进制流密码应该总是使用整型保护。流密码有两个特点。同步流密码要求在外部方式下密钥流同步（e.g. 每个消息包括一个明确的同步值）。自同步流密码，允许临时的失步，可以自动的重新获得同步。本质上现在所有的实践使用流密码是同步的。

明显构造流密码的安全依赖于密钥流的“随机”，如果流与真随机不出现偏差，可以立刻获得安全。然而，一些流密码希望抗所有明显的攻击，但如果一个明显的攻击要求已知密钥流的大数据量，但这对实践安全可能不是灾难性的。

为什么选择一个流密码比选择一个分组密码更普通？通常的，可以有任意或所有如下的三个特征：

1、 流密码通常面向高速设计，限制要求的环境，因此许多流密码非常快而且“轻”（尽管注意到一些构造同时在历史上完全面向安全）
2、 流密码不要求消息底码，因此他们在关键应用提供带宽
3、 流密码对比特错误不进行扩展；加密后在密文里仅仅单独的变换

最后的动机可能是最有效的，如同注记，如果没有使用整型保护，意味着攻击者可以产生消息比特，整型保护应该同时抗应用错误同样的工作。但是，许多无线电系统的声音（没有整型保护）使用流密码，既然声音解码通常有高的容错率，但不能复制框架错误。

注意二进制附加流密码也许失去安全，如果相同的密钥（或更细致，相同的密钥流）使用两个不同的消息（产生所谓的两次一密）

对更广泛的流密码安全特征的讨论，见 NESSIE 评估报告[156]。

9.1.1 对伪随机数产生器的注记

本质上，任意流密码可以当作伪随机数产生器函数（PRNG）。

在 PRNG 和流密码之间有什么区别？单纯的看输出，使用一个流密码的强安全定义，没有真正的不同，两个输出与真随机没有明显的差异。实际上，通常有如下要求的一些不同：

- 流密码通常是归因于宽带存储（避免底码）或处理速度，否则可以仅仅使用分组密码的流密码模型。一个PRNG不能在速度非常慢的条件下经常使用。
- 如果提到的，对流密码明显的攻击不是太严重，但如果PRNG通常对其他密码产生密钥，可能完全是不同的过程。因此PRNG有可能对更强的安全要求。
- 流密码的密钥重新使用避免“过时”的密钥或进行同步，要求避免密钥流重新使用是容易理解的。一个PRNG也许可以“重新看到”提高内部结果的随机性，例如，对现存的状态“加入熵”，目前看来是流行而并不是科学。

9.1.2 eStream

如下可以看到，一些流密码包括这个报告，主要由于缺乏公开可以使用的流密码，这些流密码要满足安全要求。然而，ECRYPT 在 2008 年最后公开了安全流密码安全有效的进展，[55]。如下的流密码包括在文档里。

硬件实现密码全部支持 80bit 密钥和满足所有 80bit 安全级别。当 Salsa20 声称 256-bit 安全，当使用 256bit 密钥，所有其他的软件实现密码声称 128bit 安全。对更多信息，我们参考[55]。

F-FCSR-H

在最后的 eStream 的效果里，对 F-FCSR-H 进行了一个严重的攻击。因此，流密码 F-FCSR-H 从文献里挪走了。

表 9.1 eStream 文献

软件优化	硬件优化
HC-128	Trivium
Rabbit	Grain v1
Salsa20/12	MICKEY v2
SOSEMANUK	

9.2 RC4

定义：见[80，81]
参数：可变密钥规模
安全：没有公开的密钥恢复攻击，直接使用一个密钥流产生器，RC4 对攻击是高度敏感的，恢复重新使用密钥和重新初始化
范围：广泛使用，e.g. SSL/TLS，IEEE 802.11b，etc
实现：
公开分析：Cryptrec [46]，见 e.g.[80]
已知漏洞：应用不同的明显攻击，e.g.[122]。对重新使用密钥的特殊实现有一些密钥恢复攻击，[22]。描述恢复攻击可以见[130]。最先产生的密钥流对密码分析非常脆弱。实现 WEP 的最好的密钥恢复攻击是主动攻击[198]
评价：推荐去掉首先产生的512字节
然而，既然容易错误使用，ECRYPT2在普通流密码范围内不推荐使用RC4，

9.3 SNOW 2.0

定义：[90]
参数：128 和 256 比特密钥
安全：任意相关实践的攻击是已知的
范围：在 Display Port，[199]里使用
实现：
公开分析：NESSIE [155]。同时见[204，129，158]
已知漏洞：给出大约 2^{174} 比特的密钥流和 2^{174} 的工作，从真随机数，见[158]得到可能明显的 SNOW 2.0 输出。从 256-bit 密钥产生非平凡攻击，需要一定数量的密钥流。
评论：SNOW 2.0 是“SNOW”提交到 NESSIE 的加强版。SNOW 2.0，存在进一步的修订版本，“SNOW 3G”，已经被 ETSI SAGE 用于包括 3GPP UMTS 标准。SNOW 3G 主要的不同是第二个 S 盒抗未来可能的代数攻击的附加安全强度。

第十章 HASH 函数

10.1 简介

密码学单向函数广泛使用在计算机和网络安全领域里。他们在消息的规模范围内进行操作，产生一个固定规模的消息指纹，或摘要。依赖应用，一些或所有数字的安全特征从单向函数值 h(·)。我们声明的潜在特征是：抗预先构造攻击。当某人希望在某些点获得 x 值并且保持秘密直到最后，这样的特征应该是有用的。

二次抗预先构造攻击，这些特征也许用来防止某些方改变比特承诺值。

抗碰撞攻击：这个特征用来保护电子签名，抗伪造。

随机预言特征：函数 h(·) “作为”一个随机选择函数使用。

假设这个特征有时保持正规公钥安全的证明，可以证明公钥加密和签名体制安全。我们应该在 12.1 节讨论。

当某人能够构造函数的样本，抗碰撞攻击但不抗预先构造攻击，单向函数特征在对手面前的困难可以预计，通过找到一个最难的预先构造攻击任务。任意分析弱点缺乏条件下，仅仅强力攻击对攻击者是可以使用的。更细致的，如果 n 是单向输出，从安全函数希望的2^n 圈数操作，可以破解前两个特征（尽管减少增加可用目标的数量）和在 $2^{n/2}$ 操作下破解抗碰撞特征。因此，需要选择一个安全 h ，使用一个足够大的 n ，因此，这些数据可以满足依赖应用要求的“不灵活实践”。

从构造里可以非常清楚的认识到，没有单向函数在通常意义下敢声称“随机预言”，实际上，也确立了不固定的函数特征[34]。所谓的随机预言模型因此可以讨论，我们应该返回这些报告的非对称算法。

对更进一步的讨论单向函数的安全特征，见NESSIE 评估报告，[156]。对在明确单向函数信息，见[54，74]。

10.2 最近的进展

最近对 MD5/SHA 家族迭代单向函数的分析的许多进展在这个报告开始的第一版本就知道了[6，96，97，103，104，191，190，201，202，203]。

总而言之，MD5 已经认为被彻底破解了，SHA-1 提供仅仅非常小范围的安全。在两种情况下的碰撞可以已知 IVs 。这意味着消息认证的应用（是基于秘密密钥的 IVs ）没有直接威胁，一些关于更进一步可能升级的相关事物，见 11.2 节。同时，没有必要完全选择碰撞消息，也许会争论签名因此是安全的——只要可以发现随机碰撞。随后是非常乐观的假设。可以看到两个语句上构成公钥证书，在实际使用里是可读的对[36，47，118，190]。因此，使用 SHA-1 和特别 MD5 应该避免使用签名。更基础的假设是加强随机单向[68]。见[52]，有更多的讨论。注意，一些明显的技术目标提高/维护不能影响单向函数的安全。例如，简单体制，一些使用单向函数可能产生的相同输出[96]。

10.3 MD5

定义：RFC 1321，[170]

参数：128-bit 单向输出，主要输入规模 2^{64}-1 bit
安全：不抗碰撞。实际的碰撞能够在普通的PC上几秒时间找到
范围：大范围，在SSL/TLS，IPsec，etc
实现：在RFC 1321，[170]里提供C代码
公共分析：
已知漏洞：可以发现碰撞[191]，通过低计算复杂度，在 596 比特消息限制下构造。对公钥证书的碰撞已公开报道，[119，190]，对 MD5 使用口令恢复攻击已在具体实践，[120，175]。一个实际攻击产生一个证书认证证明，[191]。逆象攻击的复杂度是 $2^{124.4}$ [174]。更进一步的分析还在进行。
评价：MD5 应该在新的开发里不使用，应该在可能存在的应用里的推销。更进一步的评价可以通过 ECRYPT 描述单向函数，[52]

10.4 RIPEMD-128

定义：见 [169]
参数：128比特输出，最大输入规模 2^{64}-1 bit
安全：作为声明，碰撞要求2^{64} 迭代，然而，这已不合适了
范围：未知
实现：见 [169]
公开分析：
已知漏洞：
评论：当对RIPEMD 的碰撞在[201]里报道，RIPEMD 明显对RIPEMD-128 是不同的设计。然而，对减轮攻击，3轮RIPMD-128 的报道见[133]

10.5 RIPEMD-160

定义：ISO/IEC 10118-3，[87]（见[169]）
参数：160比特单向输出，最大输入规模 2^{64}-1 bit
安全：如同声明，碰撞搜索需要 2^{80} 压缩函数迭代。
范围：IPsec，IEEE 标准 1363，和 OpenPGP里的允许使用算法
实现：见 [169]
公开分析：Cryptrec 报告 [46]
已知漏洞：
评估：当在RIPEMD碰撞已经报告，RIPMD明显与RIPEMD-160设计不同，部分2-3轮攻击可以在[134]里查到。

10.6 SHA-1

定义：NIST FIPS 180-1 和 NIST FIPS 180-2，[141]。在 IEEE Std 1363，ISO/IEC 10118-3，etc里也包括了
参数：160-bit 单向输出，最大输入规模 2^{64}-1 bit
安全：不抗碰撞。还没有发现完全碰撞，但也许随时可以发现

范围：广泛使用（包括 IKE/IPsec）
实现：RFC 3174
公共分析：Cryptrec 报告 [46]
已知漏洞：
评价：使用2^{69}次运算可以发现SHA-1的碰撞，[202]，新结论甚至指一定程度的低复杂度，[135，121，203]。可以发现对完全的SHA-1 明确的碰撞。对SHA-1的明确的碰撞从80减少到70轮，[38]。在[39]里发现逆向攻击可以上升到45轮。
我们推荐在新的应用里抗使用SHA-1，从中等安全到高级安全应用签名可能逐步淘汰使用SHA-1。在消息认证里，e.g. HMAC，不立刻出现威胁，尽管可以发现一些警告，见节11.2

10.7 SHA-224，SHA-256

定义：NIST FIPS 180-2，[141]（也见Suite-B [157], ISO/IES 10118-3）
参数：224-bit 和 256-bit 相应的单向输出，最大输入规模是 2^{64}-1 bit
安全：如同说明；分别使用2^{112}和2^{128}次迭代发现碰撞搜索
范围：希望可以广泛使用
实现：
公开分析：Cryptrec 报告 [46]，也见[62,73]
已知漏洞：
评论：SHA上的碰撞已报道了。SHA 已类似，可以发现SHA-224，SHA-256的不同设计。SHA-224与SHA-256是有区别的，希望使用一个不同的IV和输出截断。说明SHA-256的说明变量在[125，133，210]里分析了。对24（从64圈）步的实际攻击在[83]里有报道

10.8 SHA-384，SHA-512

定义：NIST FIPS 180-2，[141]（同时可以见 Suite-B [157]）
参数：384-bit 和 512-bit 分别单向输出，最大输入规模是 2128-1 bit
安全：如同声明；相应要求 2^{192} 和 2^{256} 压缩函数碰撞
范围：没有声明。包括在 ISO 10118-3 里
实现：
公开分析：Cryptrec 报告 [46]
已知漏洞：
评论：SHA 上的碰撞已报道了。SHA 已类似，可以发现 SHA-384，SHA-512 的不同设计。SHA-384 与 SHA-512 是有区别的，希望使用一个不同的 IV 和输出截断。SHA-512 和 SHA-384 到 24（从 64 圈）步的实际攻击在 [83] 里有报道。

10.9 Whirlpool

定义： ISO/IEC 10118-3，[87] (见 [82])
参数 ：512-bit hash 输出，最大输入规模 $2^{256}-1$ bit
安全：如同声明；压缩函数的 2^{256} 迭代可以产生碰撞搜索

实现：见[82]
公开分析：NISSIE，[155]
已知漏洞：在 [136] 里已报道了 Whirlpool 的 4.5 减轮 2^{120} 碰撞攻击
评论：构造使用 AES 类型元件和对 MD 簇有不同

参考文献

[1] 3GPP TS 35.202, Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification, available from http://www.3gpp.org/ ftp/Specs/html-info/35202.htm.
[2] 3GPP TS 35.203, Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 3: Implementors' Test Data, available from http://www.3gpp.org/ftp/Specs/html -info/35202.htm.
[3] 3GPP TS 35.204, Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 4: Design Conformance Test Data, available from http://www.3gpp.org/ ftp/Specs/html-info/35204.htm.
[4] 3GPP TR 33.908, 3G Security; General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms, available from http://www.3gpp.org/ ftp/Specs/html-info/33908.htm.
[5] F. Almgren, G. Andersson, T. Granlund, L. Ivansson, and S. Ulfberg, How we Cracked the Code Book Ciphers, Report, 2000. Available via answers.codebook.org
[6] E. Andreeva, C. Bouillaguet, P.-A. Fouque, J. J. Hoch, J. Kelsey, A. Shamir and S. Zimmer, Second Preimage Attacks on Dithered Hash Functions, Proceedings of Eurocrypt 2008, LNCS 4965, pp. 270–288, Springer-Verlag.
[7] ANSI X9.19-1996, Financial Institution Retail Message Authentication.
[8] ANSI X9.62, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).
[9] ANSI X9.63, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography.
[10] The AES Lounge, http://www.iaik.tu-graz.ac.at/research/krypto/AES/index. php.
[11] K. Aoki, Y. Kida, T. Shimoyama, H. Ueda, Subject: SNFS274, Announcement, 24 Jan 2006.
[12] F. Bahr, M. Boehm, J. Franke, T. Kleinjung, Subject: RSA200, Announcement, 9 May 2005.
[13] M. Bellare, New Proofs for NMAC and HMAC: Security Without Collision-Resistance, Proceedings of Crypto 06, LNCS 4117, pp. 602–619, Springer-Verlag, 2006. 77 78
[14] M. Bellare, R. Canetti, and H. Krawczyk, Keying hash functions for message authentication, Proceedings Crypto 96, LNCS 1109, Springer-Verlag, 1996. Full paper available at http://www.cs.ucsd.edu/users/mihir/papers/hmac.html.
[15] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, A Concrete Treatment of Symmetric Encryption: Analysis of DES Modes of Operation, Proceedings of 38th IEEE FOCS, pp. 394–403, 1997.
[16] M. Bellare and A. Palacio, GQ and Schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks, Proceedings of Crypto'02, LNCS 2442, pp. 162–177, Springer-Verlag.
[17] M. Bellare and P. Rogaway, Optimal asymmetric encryption (how to encrypt with RSA), Proceedings of Eurocrypt'94, LNCS 950, pp. 92–111, Springer-Verlag.

[18] S. Bellovin, Problem Areas for the IP Security Protocols, Proceedings of the 6th Usenix Unix Security Symposium, pp. 1–16, 1996, available at www.research.att.com/esmb/papers /index.html
[19] D. Bernstein, Circuits for Integer Factorization: A Proposal, Manuscript, Nov. 2001. Available via http://cr.yp.to/papers.html.
[20] E. Biham, O. Dunkelman, and N. Keller, A Related-Key Rectangle Attack on the Full KASUMI, Proceedings of ASIACRYPT 2005, LNCS 3788, pp. 443–461, 2005.
[21] E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems, Journal of Cryptology, 4 (1991), 3–72.
[22] E. Biham and Y. Carmeli, Efficient Reconstruction of RC4 Keys from Internal States, Proceedings of FSE 2008, LNCS 5086, 2008.
[23] J. Black, Authenticated encryption, In “Encyclopedia of Cryptography and Security”, Springer-Verlag, 2005.
[24] D. Bleichenbacher, Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS#1, Proceedings of Crypto’98, LNCS 1462, pp. 1–12, Springer-Verlag.
[25] M. Blaze, W. Diffie, R. Rivest, B. Schneier, T. Shimomura, E. Thompson, and M. Wiener, Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security, Report of ad hoc panel of cryptographers and computer scientists, Jan. 1996. Available via http://www.crypto.com/papers/.
[26] The block cipher lounge, http://www2.mat.dtu.dk/people/Lars.R.Knudsen/bc.html.
[27] The Blowfish page, http://www.schneier.com/blowfish.html.
[28] M. Blunden and A. Escott, Related Key Attacks on Reduced Round KASUMI, Proceedings of FSE 2001, LNCS 2355, pp. 277–285, Springer-Verlag. 79
[29] M. Bod´en and S. Kowalski, Value based risk analysis: the key to successful commercial security targets for the Telecom Industry, Proceedings of 2nd Common Criteria Conference, 2002.
[30] G. Brassard, P. Hoyer, A. Tapp, Quantum cryptanalysis of hash and claw-free functions, ACM SIGACT, 28:2, 1997, 14–19.
[31] J. R. T. Brazier, Possible NSA Decryption Capabilities, Manuscript 1999, available via jya.com/nsa-study.htm
[32] D. R. L. Brown, Generic Groups, Collision Resistance, and ECDSA, available at http://eprint.iacr.org/2002/026/.
[33] M. Burmester, An almost-constant round interactive zero-knowledge proof, Information Processing Letters, 42:2, 81–87, 1992.
[34] R. Canetti, O. Goldreich, and S. Halevi, The Random Oracle Methodology, Revisited, In Proceedings of 30th Annual ACM Symposium on the Theory of Computing, pp. 209– 218, May 1998, ACM.
[35] C. De Canni´ere and C. Rechberger, Finding SHA-1 Characteristics: General Results and Applications, Proceedings of ASIACRYPT 2006, LNCS 4284, pp. 1–20, Springer- Verlag.
[36] C. De Canni´ere and C. Rechberger, SHA-1 collisions: Partial meaningful at no extra cost?, Presented at rump session of CRYPTO 2006.
[37] C. De Canni`ere and C. Rechberger, Finding SHA-1 Characteristics, NIST – Second Cryptographic Hash Workshop, 2006.

[38] C. De Canni`ere, F. Mendel and C. Rechberger, Collisions for 70-Step SHA-1: On the Full Cost of Collision Search, Proceedings of SAC 2007, LNCS 4876, pp. 56–73, Springer-Verlag.
[39] C. De Canni`ere and C. Rechberger, Preimages for Reduced SHA-0 and SHA-1, Proceedings of CRYPTO 2008, LNCS 5157, pp. 179–202, Srpinger-Verlag.
[40] I. L. Chuang, N. Gershenfeld, and M. Kubinec, Experimental Implementation of Fast Quantum Searching, Physical Review Letters, 80:15 (1998), 3408–3411.
[41] S. Contini and Y. L. Yin, Forgery and Partial Key-Recovery Attacks on HMAC and NMAC Using Hash Collisions, Proceedings of ASIACRYPT 2006, LNCS 4284, pp. 37– 53, Springer-Verlag.
[42] D. Coppersmith, M. Franklin, J. Patarin and M. Reiter, Low-Exponent RSA with Related Messages, Proceedings of Eurocrypt ’96, LNCS 1070, pp. 1–9, Springer-Verlag.
[43] J.-S. Coron, M. Joye, D. Naccache and P. Paillier, New Attacks on PKCS #1 v1.5 Encryption, Proceedings of Eurocrypt 2000, LNCS 1807, pp. 369–379, Springer-Verlag.
[44] J.-S. Coron, M. Joye, D. Naccache and P. Paillier, Universal Padding Schemes for RSA, Proceedings of Crypto 02, LNCS 2442, pp. 226–241, Springer-Verlag. 80
[45] R. Cramer and V. Shoup, Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack, Cryptology ePrint Archive, Report 2001/108, 2001.
[46] Cryptrec report annual 2002, available at http://www.ipa.go.jp/security/enc/CRYPTREC/ fy15/doc/ c02e\ report2.pdf.
[47] M. Daum and S. Lucks, Attacking Hash Functions by Poisoned Messages, “The Story of Alice and her Boss”, available at http://http://th.informatik.uni-mannheim.de/People/lucks/ HashCollisions/.
[48] A.W. Dent. Proofs of security for ECIES. Chapter III of Advances in Elliptic Curve Cryptography, pp 41–46, Cambridge University Press, 2005.
[49] I. Devlin and A. Purvis, A fundamental evaluation of 80 bit keys employed by hardware oriented stream ciphers, Workshop record of SHARCS 2006, www.ruhr-unibochum. de/itsc/tanja/SHARCS/
[50] I. Devlin and A. Purvis, Assessing the Security of Key Length, Workshop record of SASC 2007, sasc.crypto.rub.de/program.html
[51] distributed.net, Project RC5, available via http://www.distributed.net/rc5/.
[52] ECRYPT NoE, Recent Collision Attacks on Hash Functions: ECRYPT Position Paper, ECRYPT document STVL-ERICS-2-HASH STMT-1.1, Feb. 2005, available at http: //www.ecrypt.eu.org/documents/STVL-ERICS-2-HASH\ STMT-1.1.pdf.
[53] ECRYPT NoE, AES Security Report, ECRYPT deliverable D.STVL.2, Jan 2006, available at http://www.ecrypt.eu.org/documents/D.STVL.2-1.0.pdf.
[54] ECRYPT NoE, eHash home page, http://ehash.iaik.tugraz.at.
[55] ECRYPT NoE, eStream home page, http://www.ecrypt.eu.org/stream.
[56] EFF, Website of the electronic frontier foundation. http://www.eff.org/descracker.html.
[57] ETSI TS 102 176, Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures, ETSI, Nov 2004.
[58] P.-A. Fouque, G. Leurent, P. Q. Nguyen, Full Key-Recovery Attacks on HMAC/NMACMD4 and NMAC-MD5, Proceedings of Crypto 2007, 4622, pp. 13–30,

Springer-Verlag.
[59] E. Fujisaki, T. Okamoto, D. Pointcheval, and J. Stern, RSA-OAEP is secure under the RSA assumption, Proceedings of Crypto'01, LNCS 2139, pp. 260–274, Springer-Verlag.
[60] C. Gaj et al., Fast Implementation and Fair Comparison of the Final Candidates for Advanced Encryption Standard Using Field Programmable Gate Arrays, In CT-RSA 2001, LNCS 2020, pp. 84—99.
[61] C. Gehrmann and K. Nyberg, Security in Personal Area Networks, In C. Mitchell (Ed.): Security for Mobility, IEE 2003. 81
[62] H. Gilbert and H. Handschuh. Security analysis of SHA-256 and sisters, Proceedings of SAC 2003, LNCS 3006, pp. 175–193, Springer-Verlag.
[63] J. Gilmore (Ed.), Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design, Electronic Frontier Foundation, O'Reilly & Associates, 1998.
[64] L. Granboulan, How to repair ESIGN, Proceedings of SCN '02, also available at http://eprint.iacr.org/2002/074, 2002.
[65] L. K. Grover, A fast quantum mechanical algorithm for database search, Proceedings of the 28th ACM STOC, pp. 212–219, 1996.
[66] L. C. Guillou and J.-J. Quisquater, A "paradoxical" identity-based signature scheme resulting from zero-knowledge, Proceedings of Crypto'88, LNCS 403, pp. 216–231, Springer-Verlag, 1988.
[67] L. C. Guillou and J.-J. Quisquater, A practical Zero-Knowledge protocol fitted to security microprocessor minimizing both transmission and memory, Proceedings of Eurocrypt' 88, LNCS 330, pp. 123–128, Springer-Verlag.
[68] S. Halevi and H. Krawczyk. Strengthening Digital Signatures via Randomized Hashing. Proceedings of Crypto 2006, LNCS 4117, pp. 41–59, Springer-Verlag.
[69] I. Hamer and P. Cho, DES Cracking on the Transmogrifier 2a, In C¸. K. Ko¸c and C. Paar (Eds.), Cryptographic Hardware and Embedded Systems, 1st International Workshop, CHES 1999 Proceedings, LNCS 1717, pp. 13–24. Springer-Verlag.
[70] H. Handschuh and B. Preneel, Minding your MAC algorithms, Draft 2004, Submitted to ISB Journal.
[71] H. Handschuh and B. Preneel, Key-Recovery Attacks on Universal Hash Function based MAC Algorithms, Proceedings of Crypto 2008, LNCS 5157, pp. 144–161, Springer- Verlag.
[72] D. Harkins and D. Carrel, The Internet Key Exchange (IKE), RFC 2409, IETF.
[73] P. Hawkes, M. Paddon, and G. Rose, On corrective patterns for the SHA-2 family, Cryptology ePrint Archive, Report 2004/207, August 2004. http:// eprint.iacr.org/
[74] Hash function lounge, paginas.terra.com.br/informatica/paulobarreto/hflounge.html
[75] Helion, Website: http://www.heliontech.com/.
[76] A. Hodjat and I. Verbauwhede, A 21.54 gbits/s fully pipelined AES processor on FPGA, In Proceedings of the IEEE Symposium on Field-Programmable Custom Computing Machines.
[77] J. Hoffstein, J. Pipher, and J. H. Silverman, NTRU: A Ring-Based Public Key Cryptosystem, In Proceedings of ANTS III, LNCS 1423, pp. 267–288, Springer-Verlag, 1998.
[78] J. H°astad, Solving Simultaneous Modular Equations of Low Degree, SIAM J. of Computing, 17, 336–341, 1988. 82

[79] J. H°astad and M. N¨aslund, The security of all RSA and discrete log bits, J. ACM 51:2, 187–230 (2004).
[80] http://www.weizmann.ac.il/eitsik/RC4/rc4.html
[81] http://burtle.burtle.net/bob/rand/isaac.html
[82] http://planeta.terra.com.br/informatica/paulobarreto/WhirlpoolPage.html
[83] S. Indesteege, F. Mendel, B. Preneel and C. Rechberger, Collisions and other Non-Random Properties for Step-Reduced SHA-256, Proceedings of SAC 2008 (to appear).
[84] ISO/IEC 9797-1:1999, Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher.
[85] ISO/IEC 9798-5:2004, Information technology — Security techniques — Entity authentication — Part 5: Mechanisms using zero knowledge techniques.
[86] ISO/IEC 10116:2006, Information technology — Security techniques — Modes of operation for an n-bit block cipher.
[87] ISO/IEC 10118-3:2004, Information technology — Security techniques — Hashfunctions — Part 3: Dedicated hash-functions.
[88] ISO/IEC 18033-2:2006, Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric Ciphers.
[89] ISO/IEC 18033-3:2005, Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers.
[90] ISO/IEC 18033-4:2005, Information technology — Security techniques — Encryption algorithms — Part 4: Stream ciphers.
[91] IEEE Std 1363-2000, Standard Specification for Public-Key Cryptography.
[92] T. Iwata. On the Impact of Key Check Value on CBC MACs. Seminar 09031 on “Symmetric Cryptography”, Schloss Dagstuhl, January 2009.
[93] D. Johnson, A. Menezes, and S. Vanstone, The Elliptic Curve Digital Signature Algorithm (ECDSA), Submission to NESSIE.
[94] J. Jonsson, Security proofs for the RSA-PSS signature schemes and its variants, available at http://eprint.iacr.org/2001/053/, 2001.
[95] J. Jonsson, B. Kaliski, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, RFC 3447, IETF.
[96] A. Joux, Multicollisions in iterated hash functions, application to cascaded constructions, Proceedings of Crypto 04, LNCS 3152, pp. 306–316, Springer-Verlag, 2004.
[97] A. Joux and T. Peyrin, Hash functions and the (amplified) boomerang attack, ECRYPT Hash Workshop, Barcelona, Spain, 2007.83
[98] A. Joux, D. Naccache, E. Tho´e, When e-th Roots Become Easier Than Factoring, Proceedings of Asiacrypt 2007, LNCS 4883, pp. 13–28, Springer-Verlag.
[99] B. Kaliski, Hash Function Firewalls in Signature Schemes, RSA Conference 2002, LNCS 2271, pp. 1–16, Springer-Verlag.
[100] B. Kaliski, TWIRL and RSA Key Size, Available via www.rsasecurity.com/rsalabs
[101] J. S. Kang, S. U. Shin, D. Hong, and O. Yi, Provable security of KASUMI and 3GPP encryption mode f8, Proceedings of ASIACRYPT 2001, LNCS 2248, pp. 255–271, Springer-Verlag.
[102] O. Kara and C. Manap, A New Class of Weak Keys for Blowfish, Proceedings of FSE 2007, LNCS 4593, pp. 167–180, Springer-Verlag.

[103] J. Kelsey and B. Schneier, Second Preimages on n-Bit Hash Functions for Much Less than 2n Work, Proceedings of EUROCRYPT 2005, LNCS 3494, pp. 474–490, Springer-Verlag.
[104] J. Kelsey and T. Kohno, Herding Hash Functions and the Nostradamus Attack, Proceedings of EUROCRYPT 2006, LNCS 4004, pp. 183–200, Springer-Verlag.
[105] T. Kerins, E. Popovici, A. Daly and W. Marnane, Hardware encryption engines for e-commerce, In Proceedings of Irish Signals and Systems Conference, ISSC 2002, pp. 89–94.
[106] J. Kim, A. Biryukov, B. Preneel, and S. Hong, On the Security of HMAC and NMAC Based on HAVAL, MD4, MD5, SHA-0 and SHA-1, Proceedings of SCN, LNCS 4116, pp. 242–256, Springer-Verlag.
[107] T. Kivinen and M. Kojo, More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE) RFC 3526, IETF.
[108] N. Koblitz, A. J. Menezes, Another Look at “Provable Security”, Journal of Cryptology, 20:1 (2007), 3–27, Springer-Verlag.
[109] P. C. Kocher, Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems, Advances in Cryptography, Proceedings of CRYPTO 1996, LNCS 1109, pp. 104–113, Springer-Verlag, 1996.
[110] P. C. Kocher, J. Jaffe, B. Jun, Differential Power Analysis, Advances in Cryptography, Proceedings of CRYPTO 1999, LNCS 1666, pp. 388–397, Springer-Verlag, 1999.
[111] F. Koeune, G. Rouvroy, F.-X. Standaert, J.-J. Quisquater, J.-P. David and J.-D. Legat, A FPGA Implementation of the Linear Cryptanalysis, In 12th International Conference on Field Programmable Logic and Applications (FPL 2002), Montpellier, France.
[112] H. Krawczyk, M. Bellare, and R. Canetti, HMAC: Keyed-Hashing for Message Authentication, IETF RFC 2104, available at http://www.ietf.org/rfc/rfc2104.txt?number=2104
[113] S. Kumar, C. Paar, J. Pelzl, G. Pfeiffer, A. Rupp, and M. Schimmler, How to Break DES for e8,980, Workshop record of SHARCS 2006, www.ruhr-unibochum.de/itsc/tanja/SHARCS/ 84
[114] A. K. Lenstra, Unbelievable security; matching AES security using public key systems, Proceedings of Asiacrypt 2001, LNCS 2248, pp. 67–86, Springer-Verlag, 2001.
[115] A. K. Lenstra, Key Lengths, Chapter 114, of The Handbook of Information Security, Wiley 2005.
[116] A. K. Lenstra, A. Shamir, J. Tomlinson, and E. Tromer, Analysis of Bernstein’s factorization circuit, Proceedings of Asiacrypt 2002, LNCS 2501, pp. 1–26, Springer-Verlag, 2002.
[117] A. K. Lenstra and E. R. Verheul, Selecting Cryptographic Key Sizes, Journal of Cryptology 14:4, 255–293, 2001.
[118] A. K. Lenstra and B. de Weger, On the Possibility of Constructing Meaningful Hash Collisions for Public Keys, Proceedings of ACISP 2005, LNCS 3574, pp. 267–279, Springer-Verlag, 2005.
[119] A. K. Lenstra, X. Wang, and B. de Weger, Colliding X.509 Certificates based on MD5-collisions, http://www.win.tue.nl/˜bdeweger/CollidingCertificates/
[120] G. Leurent, Message Freedom in MD4 and MD5 Collisions: Application to APOP, Proceedings of FSE 2007, LNCS 4593, pp. 309–328, Springer-Verlag.

[121] C. McDonald, P. Hawkes and J. Pieprzyk. SHA-1 collisions now 252. Eurocrypt 2009 Rump session, http://eurocrypt2009rump.cr.yp.to/ 837a0a8086fa6ca714249409ddfae43d.pdf.
[122] S. Maitra and G. Paul, New Form of Permutation Bias and Secret Key Leakage in Keystream Bytes of RC4, Proceedings of FSE 2008, LNCS 5086, pp. 250–266, Springer-Verlag, 2008.
[123] J. Manger, A chosen ciphertext attack on RSA Optimal Asymmetric Encryption Padding (OAEP) as standardized in PKCS #1 v2.0, Proceedings of Crypto 2001, LNCS 2139, pp. 230–238, Springer-Verlag.
[124] M. Matsui, Linear cryptanalysis method for DES cipher, Proceedings of EUROCRYPT 93, LNCS 765, pp. 386–397, Springer-Verlag.
[125] K. Matusiewicz, J. Pieprzyk, N. Pramstaller, C. Rechberger, and V. Rijmen, Analysis of simplified variants of SHA-256, Proceedings of WEWoRC 2005, LNI P-74, pp. 123–134, 2005.
[126] U. Maurer, Towards the Equivalence of Breaking the Diffie-Hellman Protocol and Computing Discrete Logarithms, Proceedings of CRYPTO ’94, LNCS 839, pp. 271–281, Springer-Verlag.
[127] U. Maurer and S. Wolf, Diffie-Hellman, Decision Diffie-Hellman, and Discrete Logarithms, Proceedings of ISIT ’98, IEEE Information Theory Society, pp. 327, 1998.
[128] U. Maurer and S. Wolf, The Relationship Between Breaking the Diffie-Hellman Protocol and Computing Discrete Logarithms, SIAM J. Comp., 28:5 (1999), 1689–1721. 85
[129] A. Maximov and T. Johansson, Fast Computation of Large Distributions and Its Cryptographic Applications, Proceedings of Asiacrypt 2005, LNCS 3788, pp. 313–332, Springer-Verlag, 2005.
[130] A. Maximov and D. Khovratovich, New State Recovery Attack on RC4, Proceedings of Crypto 2008, LNCS 5157, pp. 297–316, Springer-Verlag.
[131] D. A. McGrew and S. R. Fluhrer, Attacks on Additive Encryption of Redundant Plaintext and Implications on Internet Security, Proceedings of SAC 2000, LNCS 2012, pp. 14–24, Springer-Verlag, 2001.
[132] McLoone et al., High Performance Single-Chip FPGA Rijndael Algorithm Implementations, In Workshop on Cryptographic Hardware and Embedded Systems — CHES 2001, Paris, France, 2001, LNCS.
[133] F. Mendel, N. Pramstaller, C. Rechberger, and V. Rijmen, Analysis of Step-Reduced SHA-256, Proceedings of FSE 2006, LNCS 4047, pp. 126–143, Springer-Verlag.
[134] F. Mendel, N. Pramstaller and C. Rechberger, Improved Collision Attack on the Hash Function Proposed at PKC’98, Proceedings of ICISC 2006, LNCS 4296, pp. 8–21, Springer-Verlag, 2006.
[135] F. Mendel, C. Rechberger and V. Rijmen, Update on SHA-1, Presented at Rump Session of CRYPTO 2007.
[136] F. Mendel, C. Rechberger, M. Schl¨affer and S.S. Thomsen. The Rebound Attack: Cryptanalysis of Reduced Whirlpool and Grøstl, Proceedings of FSE 2006, LNCS 5665, pp. 260–276, Springer-Verlag, 2006.
[137] A. Menezes, P. C. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997.
[138] C. J. Mitchell, K. G. Paterson, and A. Yau, Padding Oracle Attacks on the CBC-mode

encryption with random and secret IVs, Proceedings of Fast Software Encryption (FSE) 2005, LNCS 3557, pp. 308–329.
[139] C. J. Mitchell and V. Varadharajan, Modified forms of cipher block chaining, Computers and Security 10, pp. 37–40, 1991.
[140] NIST, Data encryption standard (DES), FIPS PUB 46-3, available at http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
[141] NIST, Secure hash standard, FIPS PUB 180-2, available at http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf
[142] NIST, Digital Signature Standard (DSS), FIPS PUB 186-2, Available at http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf
[143] NIST, Advanced Encryption Standard, FIPS PUB 197, available at http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[144] NIST, Recommendation for Block Cipher Modes of Operation, SP 800-38, http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf 86
[145] NIST, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, SP 800-38B, http://csrc.nist.gov/publications/nistpubs/800-38b/sp800-38b. pdf
[146] NIST, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, SP 800-38D, http://csrc.nist.gov/publications/nistpubs/800- 38D/SP-800 -38D.pdf
[147] NIST, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, SP 800-38C, http://csrc.nist.gov/publications/nistpubs/ 800-38c/sp800-38c.pdf
[148] NIST, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, SP 800-67, http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf
[149] NIST, Recommendation for Key Management — Part 1: General SP 800-57, May 2006, http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1- revised2 Mar08-2007.pdf
[150] NIST, Cryptographic Algorithms and Key Sizes for Personal Identity Verification, April 2005, available via csrc.nist.gov/publications/nistpubs/800-78/sp800-78-final.pdf
[151] NIST, PlutoPlus: An IKE Reference Implementation for Linux, available at http://ipsec-wit.antd.nist.gov/newipsecdoc/pluto.html
[152] J. Nechvatal, E. Barker, L. Bassham, W. Burr, M. Dworkin, J. Foti, and E. Roback, Report on the Development of the Advanced Encryption Standard (AES), available at http://csrc.nist.gov/CryptoToolkit/aes/round2/r2report.pdf
[153] P. Q. Nguyen and I. Shparlinski, The insecurity of the digital signature algorithm with partially known nonces, Journal of Cryptology, 15, 151–176, 2002. Also available at ftp://ftp.ens.fr/pub/dmi/users/pnguyen/PubDSA.ps.gz.
[154] P. Q. Nguyen and I. Shparlinski, The insecurity of the elliptic curve digital signature algorithm with partially known nonces, Design, Codes and Cryptography, 2002. Also available at ftp://ftp.ens.fr/pub/dmi/users/pnguyen/PubECDSA.ps.gz.
[155] NESSIE consortium, Portfolio of recommended cryptographic primitives, Feb. 2003, available via http://www.cryptonessie.org/
[156] NESSIE consortium, NESSIE Security report, available at https://www.cosic.esat. kuleuven. ac.be/ nessie/deliverables/D20-v2.pdf

[157] National Security Agency. NSA Suite B Cryptography. http://www.nsa.gov/ia/ programs/suiteb cryptography/index.shtml.
[158] K. Nyberg and J. Wall´en, Improved Linear Distinguishers for SNOW 2.0, Proceedings of FSE 2006, LNCS 4047, pp. 144–162, Springer-Verlag, 2006.
[159] P. C. van Oorschot and M. J. Wiener, Parallel Collision Search with Cryptanalytic Applications, Journal of Cryptology 12:1 (1999), 1–28. 87
[160] H. Orman, The Oakley Key Determination Protocol RFC 2412, IETF.
[161] H. Orman and P. Hoffman, Determining Strengths For Public Keys Used For Exchanging Symmetric Keys, IETF RFC 3766/BCP 86, April 2004.
[162] D. A. Osvik, A. Shamir, E. Tromer, Cache Attacks and Countermeasures: The Case of AES, Proceedings of CT-RSA 2006, LNCS 3860, pp. 1–20, Springer, 2006.
[163] D. Page, Theoretical Use of Cache Memory as a Cryptanalytic Side-Channel, Technical report CSTR-02-003, Department of Computer Science, University of Bristol. June 2002. Available online at http://www.cs.bris.ac.uk/Publications/pub master.jsp?id=1000625
[164] RSA Labs, PKCS# 1: RSA Cryptography Standard, available at http://www.rsasecurity. com/rsalabs/node.asp?id=2125
[165] B. Preneel and P. C. van Oorschot, A key recovery attack on the ANSI X9.19 retail MAC, Electronics Letters, 32:17 (1996), 1568–1569. Available at http://www.scs.carleton. ca/epaulv/papers/pubs.html
[166] C. Rechberger and V. Rijmen, On Authentication Using HMAC and Non-Random Properties, Proceedings of Financial Cryptography 2007, LNCS 4886, pp. 119–133, Springer-Verlag.
[167] C. Rechberger and V. Rijmen, New Results on NMAC/HMAC when Instantiated with Popular Hash Functions, Journal of Universal Computer Science (JUCS), Special Issue on Cryptography in Computer System Security, 14:3, 2008, 347–376.
[168] V. Rijmen, Cryptanalysis and design of iterated block ciphers, PhD thesis, October 1997.
[169] RIPEMD, http://www.esat.kuleuven.ac.be/ebosselae/ripemd160.html
[170] R. Rivest, The MD5 Message-Digest Algorithm, IETF RFC 1321, available at http://www.ietf.org/rfc/rfc1321.txt?number=1321
[171] RSA Labs, A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths, RSA Labs Bulletin #13, available at www.rsasecurity.com/rsalabs/
[172] SECG. Standards for Efficient Cryptography Group. SEC1: Elliptic Curve Cryptography version 2.0, http://www.secg.org.
[173] Saggese et al., An FPGA-Based Performance Analysis of the Unrolling, Tiling, and Pipelining of the AES Algorithm, In FPL 2003, LNCS 2778, pp. 292–302, Springer- Verlag.
[174] Y. Sasaki and K. Aoki. Finding Preimages in Full MD5 Faster Than Exhaustive Search. Proceedings of EuroCrypt 2009, LNCS 5479, pp. 134–152, Springer-Verlag.
[175] Y. Sasaki, L. Wang, K. Ohta, N. Kunihiro, Security of MD5 Challenge and Response: Extension of APOP Password Recovery Attack, Proceedings of CT-RSA 2008, LNCS 4964, pp. 1–18, Springer-Verlag. 88
[176] D. Schmidt, On the Key Schedule of Blowfish, Manuscript 2005, available at http://eprint.iacr.org/2005/063.
[177] B. Schneier, Description of a New Variable-Length Key, 64-Bit Block Cipher

(Blowfish), Proceedings of FSE 1994, LNCS 1008, pp. 191–204, Springer-Verlag, 1994.
[178] A. Shamir, Factoring Large Numbers with the TWINKLE Device (Extended Abstract), Manuscript, 2000.
[179] A. Shamir and E. Tromer, Factoring large numbers with the TWIRL device, Proceedings of Crypto 2003, LNCS 2729, pp. 1–26, Springer-Verlag, 2003.
[180] R. Shipsey, How long. . . ?, NESSIE Report NES/DOC/RHU/WP3/015/a, available via https://www.cosic.esat.kuleuven.ac.be/nessie/reports/phase1/rhuwp3-015.pdf
[181] P. W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM J. Sci. Statist. Comput., 26 (1997).
[182] V. Shoup, A proposal for an ISO standard for public key encryption, Cryptology ePrint Archive, Report 2001/112, 2001. http://eprint.iacr.org/
[183] R. D. Silverman, A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths, RSA Laboratories Bulletin #13, April 2000.
[184] E. Skoudis and L. Zeltser, Malware: Fighting Malicious Code, Prentice Hall, 2003.
[185] N. P. Smart, How Secure are elliptic curves over composite extension fields?, Proceedings of Eurocrypt ’01, LNCS 2045, pp. 30–39. Springer-Verlag, 2001.
[186] JH. Song, R. Poovendran, J. Lee, The AES-CMAC-96 Algorithm and Its Use with IPsec, RFC4494, IETF, 2006.
[187] F. X. Standaert, Secure and Efficient Use of Reconfigurable Hardware Devices in Symmetric Cryptography, Ph. D. thesis, Facult´e des sciences appliqu´ees, Universit´e catholique de Louvain.
[188] Standaert et al., Efficient Implementation of Rijndael Encryption in Reconfigurable Hardware: Improvements and Design Tradeoffs, In Workshop on Cryptographic Hardware and Embedded Systems — CHES 2003, Cologne, Germany, 2003, LNCS 2779, pp. 334–350.
[189] J. Stern, D. Pointcheval, J. Malone-Lee, and N. P. Smart, Flaws in Applying Proof Methodologies to Signature Schemes, Proceedings Crypto 2002, LNCS 2442, pp. 93–110, Springer-Verlag. Also available at http://www.di.ens.fr/ epointche/pub.php?reference= MaPoSmSt02
[190] M. Stevens, A. K. Lenstra and B. de Weger, Chosen-Prefix Collisions for MD5 and Colliding X.509 Certificates for Different Identities, Proceedings of EUROCRYPT 2007, LNCS 4515, pp. 1–22, Springer-Verlag.89
[191] M. Stevens, A. Sotirov, J. Appelbaum, A. Lenstra, D.Molnar, D.A. Osvik and B. de Weger. Short chosen-prefix collisions for MD5 and the creation of a rogue CA certificate. Proceedings of Crypto 2009, LNCS 5677, Springer-Verlag.
[192] I. Tuomi, The Lives and Death of Moore’s Law, Available via http://www.firstmonday.dk/issues/issue7 11/tuomi/
[193] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, Experimental realization of Shor’s quantum factoring algorithm using nuclear magnetic resonance, Nature 414 (2001), 883–887.
[194] S. Vaudenay, Hidden collisions on DSS, Proceedings of Crypto’96, LNCS 1109, pp. 83– 88, Springer-Verlag, 1996.
[195] S. Vaudenay, The Security of DSA and ECDSA, Proceedings of PKC’03, LNCS 2567, pp. 309–323 Springer-Verlag, 2003.
[196] S. Vaudenay, Security Flaws Induced by CBC Padding — Applications to SSL,

IPSEC,. . . Proceedings of Eurocrypt'02, LNCS 2332, pp. 534–545, Springer-Verlag, 2002.
[197] S. Vaudenay, On the weak keys of Blowfish, Proceedings of FSE'96, LNCS 1039, pp. 27–32, Springer-Verlag, 1996.
[198] S. Vaudenay and M. Vuagnoux. Passive-Only Key Recovery Attacks on RC4, Proceedings of SAC 2007, LNCS 4876, pp. 344-359, Springer-Verlag, 2007.
[199] VESA, DisplayPort Specification. Available at www.vesa.org
[200] L.Wang, K. Ohta and N. Kunihiro, New Key-Recovery Attacks on HMAC/NMAC-MD4 and NMAC-MD5, Proceedings of Eurocrypt 2008, 4965, pp. 237–253, Springer-Verlag.
[201] X.Wang and D. Feng, X. Lai, and H. Yu, How to Break MD5 and other Hash Functions, Proceedings of Eurocrypt'05, LNCS 3494, pp. 19–35, Springer-Verlag, 2005.
[202] X. Wang, Y.L. Yin, and H. Yu, Finding Collisions in the Full SHA-1, Proceedings of Crypto'05, LNCS 3621, pp. 17–36, Springer-Verlag, 2005.
[203] X. Wang, New Collision search for SHA-1, Manuscript, presented at rump session of Crypto'05.
[204] D. Watanabe, A. Biryukov, and C. De Canni´ere, A Distinguishing Attack of SNOW 2.0 with Linear Masking Method, Proceedings of SAC 2003, LNCS 3006, pp. 222–233, Springer-Verlag, 2004.
[205] Weil descent page, http://www.cs.bris.ac.uk/enigel/weil descent.html
[206] B. Weis, The Use of RSA Signatures within ESP and AH, IETF draft http://www.ietf.org/internet-drafts/draft-ietf-msec-ipsec-signatures-03.txt, Nov 2004.
[207] M. J. Wiener, Performance Comparison of Public-Key Cryptosystems, RSA Crypto-Bytes 4:1 (1998), 1–5.90
[208] L. C. Williams, A Discussion of the Importance of Key Length in Symmetric and Asymmetric Cryptography, Available via http://www.giac.org/practical/gsec/Lorraine Williams GSEC.pdf
[209] Xilinx. Xilinx Press Release #03142. Available at http://www.xilinx.com/prs rls/ silicon spart/03142s3 pricing.htm.
[210] H. Yoshida and A. Biryukov, Analysis of a SHA-256 Variant, Proceedings of SAC 2005, LNCS 3897, Springer-Verlag, pp. 245–260.

缩略语：

附件 A

缩略语在文件里有更详细的说明：

3GPP	3rd Generation Partnership Project
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
ASIC	Application-Specific Integrated Circuit
CCA	Chosen Ciphertext Attack
CDH	Computational Diffie-Hellman Assumption
CMA	Chosen Message Attack
CPU	Central Processing Unit

CRT	Chineese Remainder Theorem
DDH	Decisional Diffie-Hellman Assumption
DES	Data Encryption Standard
DH	Diffie-Hellman
DLOG	Discrete Logarithm
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
FPGA	Field Programmable Gate Array
EC	Elliptic Curve
ECC	Elliptic Curve Cryptography
EFF	Electronic Frontier Foundation
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standard
HW	Hardware
TLB	Translation Lookaside Buffer
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Taskforce
IEC	International Electrotechnical Commission
IKE	Internet Key Exchange
ISO	International Standardization Organization
IP	Internet Protocol
IV	Initialization Value
KEM	Key Encapsulation Method
KDF	Key Derivation Function
MAC	Message Authentication Code
MD	Message Digest
MIME	Multipurpose Internet Mail Extensions
MIPS	Mega/Million Instructions Per Second
NESSIE	New European Schemes for Signatures, Integrity and Encryption
NFS	Number Field Sieve
NIST	National Institute of Standards and Technology
NIST	SP NIST Special Publication
OAEP	Optimal Asymmetric Encryption Padding
PK	Public Key
PKCS	Public Key Cryptography Standard
PRNG	Pseudo-random Number Generator
PSS	Probabilistic Signature Scheme
QS	Quadratic Sieve
RFC	Request For Comments (see www.ietf.org)
ROM	Random Oracle Model
RSA	Rivest-Shamir-Adleman cryptosystem
SHA	Secure Hash Algorithm
TLS	Transport Layer Security
UMTS	Universal Mobile Telecommunication System

WTLS	Wireless TLS
ZK	Zero Knowledge