SHA 家族

SHA （Secure Hash Algorithm，译作安全散列算法） 是美国国家安全局 （NSA） 设计，美国国家标准与技术研究院 （NIST） 发布的一系列密码散列函数。正式名称为 SHA 的家族第一个成员发布于 1993年。然而现在的人们给它取了一个非正式的名称 SHA-0 以避免与它的后继者混淆。两年之后， SHA-1，第一个 SHA 的后继者发布了。 另外还有四种变体，曾经发布以提升输出的范围和变更一些细微设计： SHA-224, SHA-256, SHA-384 和SHA-512 （这些有时候也被称做 SHA-2）。

SHA-0 和 SHA-1

最初载明的算法于 1993年发布，称做安全散列标准 （Secure Hash Standard），FIPS PUB 180。这个版本现在常被称为 "SHA-0"。它在发布之后很快就被 NSA 撤回，并且以 1995年发布的修订版本 FIPS PUB 180-1 （通常称为 "SHA-1"） 取代。根据 NSA 的说法，它修正了一个在原始算法中会降低密码安全性的错误。然而 NSA 并没有提供任何进一步的解释或证明该错误已被修正。1998年，在一次对 SHA-0 的攻击中发现这次攻击并不能适用于 SHA-1 — 我们不知道这是否就是 NSA 所发现的错误，但这或许暗示我们这次修正已经提升了安全性。SHA-1 已经被公众密码社群做了非常严密的检验而还没发现到有不安全的地方，它现在被认为是安全的。SHA-0 和 SHA-1 会从一个最大 2^64 位元的讯息中产生一串 160 位元的摘要然后以设计 MD4 及 MD5 讯息摘要算法的 MIT 教授 Ronald L. Rivest 类似的原理为基础来加密。

SHA-0 的密码分析

在 CRYPTO 98 上，两位法国研究者展示了一次对 SHA-0 的攻击 （Chabaud and Joux, 1998）：散列碰撞可以复杂到 2^61 时被发现；小于 2^80 是理想的相同大小散列函数。

2004年时，Biham 和 Chen 发现了 SHA-0 的近似碰撞 — 两个讯息可以散列出相同的数值；在这种情况之下，142 和 160 位元是一样的。他们也发现了 SHA-0 在 80 次之后减少到 62 位元的完整碰撞。

2004年8月12日，Joux, Carribault, Lemuet 和 Jalby 宣布了完整 SHA-0 算法的散列碰撞。这是归纳 Chabaud 和 Joux 的攻击所完成的结果。发现这个碰撞要复杂到 2^51，并且用一台有 256 颗 Itanium2 处理器的超级电脑耗时大约 80,000 CPU 工作时 。

2004年8月17日，在 CRYPTO 2004 的 Rump 会议上，Wang, Feng, Lai, 和 Yu 宣布了攻击 MD5、SHA-0 和其他散列函数的初步结果。他们对 SHA-0 攻击复杂到 2^40，这意味着他们攻击的成果比 Joux 还有其他人所做的更好。该次 Rump 会议的简短摘要可以在 这里找到，而他们在 sci.crypt 的讨论，例如： 这些结果建议计划使用 SHA-1 作为新的密码系统的人需要重新考虑。

更长的变种

NIST 发布了三个额外的 SHA 变体，每个都有更长的讯息摘要。以它们的摘要长度 （以位元计算） 加在原名后面来命名："SHA-256","SHA-384" 和 "SHA-512"。它们发布于 2001年的 FIPS PUB 180-2 草稿中，随即通过审查和评论。包含 SHA-1 的 FIPS PUB 180-2，于 2002年以官方标准发布。这些新的散列函数并没有接受像 SHA-1 一样的公众密码社群做详细的检验，所以它们的密码安全性还不被大家广泛的信任。2004年2月，发布了一次 FIPS PUB 180-2 的变更通知，加入了一个额外的变种 "SHA-224"，定义了符合双金钥 3DES 所需的金钥长度。Gilbert 和 Handschuh （2003） 研究了新的变种并且没有发现弱点。

SHAd

SHAd 函数是一个简单的相同 SHA 函数的重述：

SHAd-256（m）=SHA-256（SHA-256（m））。它会克服有关延伸长度攻击的问题。

应用

SHA-1, SHA-224, SHA-256, SHA-384 和 SHA-512 都被需要安全散列算法的美国联邦政府所应用，他们也使用其他的密码算法和协定来保护敏感的未保密资料。FIPS PUB 180-1 也鼓励私人或商业组织使用 SHA-1 加密。Fritz-chip 将很可能使用 SHA-1 散列函数来实现个人电脑上的数位版权管理。

首先推动安全散列算法出版的是已合并的数位签章标准。

SHA 散列函数已被做为 SHACAL 分组密码算法的基础。

SHA-2

NIST发布了三个额外的SHA变体，这三个函数都将讯息对应到更长的讯息摘要。以它们的摘要长度（以位元计算）加在原名后面来命名：SHA-256，SHA-384和SHA-512。它们发布于2001年的FIPS PUB 180-2草稿中，随即通过审查和评论。包含SHA-1的FIPS PUB 180-2，于2002年以官方标准发布。2004年2月，发布了一次FIPS PUB 180-2的变更通知，加入了一个额外的变种SHA-224″，这是为了符合双金钥3DES所需的金钥长度而定义。SHA-256和SHA-512是很新的杂凑函数，前者以定义一个word为32位元，后者则定义一个word为64位元。它们分别使用了不同的偏移量，或用不同的常数，然而，实际上二者结构是相同的，只在循环执行的次数上有所差异。SHA-224以及SHA-384则是前述二种杂凑函数的截短版，利用不同的初始值做计算。这些新的杂凑函数并没有接受像SHA-1一样的公众密码社群做详细的检验，所以它们的密码安全性还不被大家广泛的信任。Gilbert和Handschuh在2003年曾对这些新变种作过一些研究，声称他们没有找到弱点。