# Hash Function Attack & Crptanalysis Survey

攻击Hash函数的主要目标是找到一对或更多对的碰撞消息。在目前已有的攻击Hash函数方案中，一些是一般的方法，可以攻击任何类型的Hash加密算法，例如生日攻击方法，另一些是特殊的方法，只能用于攻击某些特殊的Hash加密算法，例如中间相遇攻击适用于攻击具有分组链结构的Hash加密算法，修正分组攻击适用于攻击基于模算术的Hash加密算法。

生日攻击方法没有利用Hash函数的结构和任何代数弱性质，它只依赖于消息摘要的长度，即Hash值的长度。因此该攻击方法对Hash加密算法提出了一个必要的安全条件，即Hash值长度必须足够长。中间相遇攻击是生日攻击的一种变形，它不比较Hash值，而是比较链中的中间变量。修正分组攻击则是通过伪造消息和一个分组级联修正Hash结果并获得期望的值。

在EUROCRYPT 2005中，wang等运用了一种以模块化整数减法作为度量的差分攻击方法在15~60min中内发现了MD5的碰撞。EUROCRYPT 2007中，Stevens等表明可以用chosen-prefix collision的方法对MD5进行更有力的攻击。ASIACRYPT 2011中，Florian Mendel等分析了SHA-2的耐碰撞性。2013年，以先进新颖的SHA-1分析框架为基础，该团队又提出了对完整SHA-1的最佳碰撞攻击，该方法将SHA-1压缩函数的调用降低到了261次。CRYPTO 2017中,Stevens等最先展示了SHA-1碰撞的实例，并从理论上证明了SHA-1攻击的可行性。

针对RIPEMD系列，EUROCRYPT 2013, Franck Landelle等针对应用于RIMPED-128的双支Hash函数提出了一种新的密码分析方法。该方法能够通过在RIPEMD-128压缩函数的每个计算分支中放置一个非线性差分部分从而构建一条非常好的差分路径，极大地改进了已知结果。ASIACRYPT 2017中，Fukang Liu等从理论上计算了RIPEMD-160的越阶微分概率，并构建了一个30步的差分路径，首次实现了对圆形缩减RIPEMD-160的碰撞攻击，时间复杂度为270。进一步地，在2019年，该团队充分利用其消息扩展的弱点，提出了两种新的有效碰撞攻击框架。

同年，Leurent G.等提出了将碰撞攻击转化为选择前缀碰撞攻击的新技术并将改进的攻击技术应用于MD5和SHA-1，其结果表明，对于某些哈希函数，选择前缀碰撞攻击比以前预期的要容易得多，不比普通的碰撞攻击难多少。这也给业界和用户们发出了警告——必须尽快放弃使用SHA-1。另外，他们的研究也为新的研究方向开辟了道路，例如研究如何改善SHA-1碰撞攻击和如何将该策略应用于其他哈希函数等。

[1]William Stallings．密码编码学与网络安全：原理与实践【M】第二版．扬明等译．

[2] Liu F., Dobraunig C., Mendel F., Isobe T., Wang G., Cao Z. (2019) Efficient Collision Attack Frameworks for RIPEMD-160. In: Boldyreva A., Micciancio D. (eds) Advances in Cryptology – CRYPTO 2019. CRYPTO 2019. Lecture Notes in Computer Science, vol 11693. Springer, Cham

[3]Liu F., Mendel F., Wang G. (2017) Collisions and Semi-Free-Start Collisions for Round-Reduced RIPEMD-160. In: Takagi T., Peyrin T. (eds) Advances in Cryptology – ASIACRYPT 2017. ASIACRYPT 2017. Lecture Notes in Computer Science, vol 10624. Springer, Cham

[4] Wang X., Yu H. (2005) How to Break MD5 and Other Hash Functions. In: Cramer R. (eds) Advances in Cryptology – EUROCRYPT 2005. EUROCRYPT 2005. Lecture Notes in Computer Science, vol 3494. Springer, Berlin, Heidelberg

[5] Stevens M., Bursztein E., Karpman P., Albertini A., Markov Y. (2017) The First Collision for Full SHA-1. In: Katz J., Shacham H. (eds) Advances in Cryptology – CRYPTO 2017. CRYPTO 2017. Lecture Notes in Computer Science, vol 10401. Springer, Cham

Stevens M., Karpman P., Peyrin T. (2016) Freestart Collision for Full SHA-1. In: Fischlin M., [6]Coron JS. (eds) Advances in Cryptology – EUROCRYPT 2016. EUROCRYPT 2016. Lecture Notes in Computer Science, vol 9665. Springer, Berlin, Heidelberg

[7] Stevens, M., Lenstra, A.K., de Weger, B.: Chosen-prefix collisions for MD5 and colliding X.509 certificates for different identities. In: Naor, M. (ed.) EUROCRYPT 2007. LNCS, vol. 4515, pp. 1–22. Springer, Heidelberg (2007)

[8] Stevens, M.: New collision attacks on SHA-1 based on optimal joint local-collision analysis. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 245–261. Springer, Heidelberg (2013).

[9] Mendel F., Nad T., Schläffer M. (2011) Finding SHA-2 Characteristics: Searching through a Minefield of Contradictions. In: Lee D.H., Wang X. (eds) Advances in Cryptology – ASIACRYPT 2011. ASIACRYPT 2011. Lecture Notes in Computer Science, vol 7073. Springer, Berlin, Heidelberg

[10] Landelle F., Peyrin T. (2013) Cryptanalysis of Full RIPEMD-128. In: Johansson T., Nguyen P.Q. (eds) Advances in Cryptology – EUROCRYPT 2013. EUROCRYPT 2013. Lecture Notes in Computer Science, vol 7881. Springer, Berlin, Heidelberg

[11] Leurent G., Peyrin T. (2019) From Collisions to Chosen-Prefix Collisions Application to Full SHA-1. In: Ishai Y., Rijmen V. (eds) Advances in Cryptology – EUROCRYPT 2019. EUROCRYPT 2019. Lecture Notes in Computer Science, vol 11478. Springer, Cham

[12] Karpman, P., Peyrin, T., Stevens, M.: Practical free-start collision attacks on 76-step SHA-1. In: Gennaro, R., Robshaw, M.J.B. (eds.) CRYPTO 2015. LNCS, vol. 9215, pp. 623–642. Springer, Heidelberg (2015).

[13] Klima, V.: Tunnels in hash functions: MD5 collisions within a minute. Cryptology ePrint Archive, Report 2006/105 (2006).

[14] Leurent, G.: Analysis of differential attacks in ARX constructions. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 226–243. Springer, Heidelberg (2012).

[15] Stevens, M.: Attacks on hash functions and applications. Ph.D. thesis, Leiden University, June 2012