

# W3 6-2 Generic birthday attack

## 1、Generic attack on Collision resistance functions

记  $H: M \rightarrow \{0,1\}^n$  为一Hash函数, 且  $|M| \gg 2^n$

常规算法可以在  $O(2^{n/2})$  内找到一个hash碰撞, 算法如下

1. 在消息空间  $M$  内选择  $2^{n/2}$  条随机消息  $m_1, \dots, m_{2^{n/2}}$
2. 对于  $i = 1, \dots, 2^{n/2}$ , 计算  $t_i = H(m_i) \in \{0,1\}^n$
3. 找到一个碰撞  $t_i = t_j$ , 若未找到, 返回1

## 2、The birthday paradox

记  $r_1, \dots, r_n \in \{1, \dots, B\}$  为  $n$  个独立同分布整数 (independent identically distributed, iid)

定理: 若  $n = 1.2 \times B^{1/2}$  则  $\Pr[\exists i \neq j: r_i = r_j] \geq \frac{1}{2}$ , 证明如下

Proof: (for uniform indep.  $r_1, \dots, r_n$ )

$$\begin{aligned} \Pr[\exists i \neq j: r_i = r_j] &= 1 - \Pr[\forall i \neq j: r_i \neq r_j] = 1 - \left(\frac{B-1}{B}\right)\left(\frac{B-2}{B}\right) \dots \left(\frac{B-n+1}{B}\right) = \\ &= 1 - \prod_{i=1}^{n-1} \left(1 - \frac{i}{B}\right) \geq 1 - \prod_{i=1}^{n-1} e^{-i/B} = 1 - e^{-\frac{1}{B} \sum_{i=1}^{n-1} i} \geq 1 - e^{-\frac{n^2}{2B}} \\ &\quad \text{1-x} \leq e^{-x} \quad \frac{n^2}{2B} = 0.72 \Rightarrow 1 - e^{-0.72} = 0.53 > \frac{1}{2} \end{aligned}$$

Dan Boneh

## 3、Sample C.R. hash functions:

使用Crypto++ 5.6.0 [Wei Dai]

AMD Opteron, 2.2 GHz (Linux)

	<u>function</u>	<u>digest size (bits)</u>	<u>Speed (MB/sec)</u>	<u>generic attack time</u>
NIST standards	SHA-1	160	153	$2^{80}$
	SHA-256	256	111	$2^{128}$
	SHA-512	512	99	$2^{256}$
	Whirlpool	512	57	$2^{256}$

目前已知最好的找到SHA-1的碰撞的算法需要  $2^{51}$