Cryptanalysis of Hash Functions

Lars R. Knudsen

Department of Mathematics, Technical University of Denmark

lars@ramkilde.com, www.ramkilde.com

ECRYPT Summer School, Samos 2007

Agenda

- Birthday attack(s)
- Random collisions versus meaningful collisions
- Differential cryptanalysis
  - Block ciphers
  - Hash functions
- Attack examples
  - exploiting weaknesses of underlying block ciphers
  - another birthday attack
  - generalised birthday attacks
  - structural attacks

Birthday attack on hash functions

Hash function $H : \{0,1\}^* \to \{0,1\}^n$

- choose $k = \sqrt{2} \cdot 2^{n/2}$ randomly chosen, distinct inputs
- compute hash values for all k inputs

Prob(at least one collision) =

$$p \approx 1 - \exp\left(-\frac{k(k-1)}{2 \cdot 2^n}\right) \approx 1 - e^{-1} \simeq 0.63$$

Intuition: probability two random n-bit values equal is 2^{-n}
number of pairs of elements is $k(k-1)/2 \simeq 2^n$

Birthday attack - more collisions

Hash function $H : \{0,1\}^* \to \{0,1\}^n$

- choose k randomly chosen, distinct inputs
- compute hash values for all k inputs

1 collision expected with $k = \sqrt{2} \cdot 2^{n/2}$
2 collisions expected with $k = \sqrt{2}\sqrt{2} \cdot 2^{n/2}$
t collisions expected with $k = \sqrt{t}\sqrt{2} \cdot 2^{n/2}$

Intuition: probability two random n-bit values equal is 2^{-n}
number of pairs of elements is $k(k-1)/2 \simeq t2^n$

Random collisions versus meaningful collisions

Birthday attack - realistic messages?

Hash function $H : \{0,1\}^* \to \{0,1\}^n$

- m_1 message, m_2 fraudulent message
- choose variations $m_1(i)$ of m_1 for $i = 1, \ldots, 2^{n/2}$
- choose variations $m_2(j)$ of m_2 for $j = 1, \ldots, 2^{n/2}$
- compute hash values for all messages
- find (i, j) such that $H(m_1(i)) = H(m_2(j))$
- number of pairs (i, j) is 2^n

Random collisions

Short-cut collisions often on random-looking messages

Criticism often heard: ...not realistic... no need to worry

However added complexity of making messages meaningful often small, e.g., Dobbertin on MD4

Random collisions can sometimes be used to make meaningful collisions

Collisions in Postscript - Daum-Lucks 2005

Applicable to iterated hash functions

Notation: (S1)(S2)eqT1T2ifelse

Meaning: If $S1 = S2$ then $T1$ else $T2$

Find random messages S1 and S2 which collide under hash function

Construct PS1 and PS2 for arbitrary T1 and T2

PS1: ...(S1)(S2)eqT1T2ifelse...

PS2: ...(S2)(S2)eqT1T2ifelse...

Differential cryptanalysis

Differential cryptanalysis - Biham-Shamir 1990

- chosen plaintext attack, proposed for block ciphers
- data x combined with key k: $x \otimes k$
- define difference of data x_1 and x_2 as

$$\Delta(x_1, x_2) = x_1 \otimes x_2^{-1}$$

- difference invariant after combination of key

$$\begin{aligned}&\Delta(x_1 \otimes k, x_2 \otimes k)\\ &= x_1 \otimes k \otimes k^{-1} \otimes x_2^{-1} = \Delta(x_1, x_2)\end{aligned}$$

- Definition of *difference* relative to cipher (often exor)

Differential cryptanalysis

$$m_1 \longrightarrow \overset{k_0}{\oplus} \longrightarrow u_1 \longrightarrow \boxed{F} \longrightarrow v_1 \longrightarrow \overset{k_1}{\oplus} \longrightarrow c_1$$

$$m_2 \longrightarrow \overset{k_0}{\oplus} \longrightarrow u_2 \longrightarrow \boxed{F} \longrightarrow v_2 \longrightarrow \overset{k_1}{\oplus} \longrightarrow c_2$$

- $m_1 \oplus m_2 = \alpha$ implies $u_1 \oplus u_2 = \alpha$
- assume $u_1 \oplus u_2 = \alpha$ implies $v_1 \oplus v_2 = \beta$ with probability p
- then $m_1 \oplus m_2 = \alpha$ implies $c_1 \oplus c_2 = \beta$ with probability p

Example: $F : \{0,1\}^4 \rightarrow \{0,1\}^4$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$F(x)$	6	4	12	5	0	7	2	14	1	15	3	13	8	10	9	11

- consider inputs x and y where y is the bitwise complement of x
- such inputs have difference $x \oplus y = 15$
- 2 inputs of difference 15 $\rightsquigarrow$ 2 outputs of difference 13 in 10 of 16 cases
- we say that $\Delta = 15 \overset{F}{\to} \Delta = 13$ with probability 10/16
- probability computed over all inputs (keys)

x	y	$F(x)$	$F(y)$	$F(x) \oplus F(y)$
0	15	6	11	13
1	14	4	9	13
2	13	12	10	6
3	12	5	8	13
4	11	0	13	13
5	10	7	3	4
6	9	2	15	13
7	8	14	1	15
8	7	1	14	15
9	6	15	2	13
10	5	3	7	4
11	4	13	0	13
12	3	8	5	13
13	2	10	12	6
14	1	9	4	13
15	0	11	6	13

Differentials

$$m_1 \longrightarrow \overset{k_0}{\oplus} \longrightarrow \boxed{F} \longrightarrow \overset{k_1}{\oplus} \longrightarrow \boxed{F} \longrightarrow \overset{k_2}{\oplus} \longrightarrow \boxed{F} \longrightarrow \overset{k_3}{\oplus} \longrightarrow c_1$$

$$m_2 \longrightarrow \overset{k_0}{\oplus} \longrightarrow \boxed{F} \longrightarrow \overset{k_1}{\oplus} \longrightarrow \boxed{F} \longrightarrow \overset{k_2}{\oplus} \longrightarrow \boxed{F} \longrightarrow \overset{k_3}{\oplus} \longrightarrow c_2$$

- find differences with high probabilities through whole cipher
- $\Delta m = \alpha_0 \xrightarrow{F} \alpha_1 \xrightarrow{F} \alpha_2 \xrightarrow{F} \cdots \xrightarrow{F} \alpha_r = \Delta c$
- $\alpha_{i-1} \xrightarrow{F} \alpha_i$ with prob p_i, $\alpha_0 \xrightarrow{F^r} \alpha_r$ with prob $p = \prod_{i=1}^{r} p_i$
- probability of differential taken as average over all keys

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1	-	-	6	-	-	-	-	2	-	2	-	-	2	-	4	-
2	-	6	6	-	-	-	-	-	-	2	2	-	-	-	-	-
3	-	-	-	6	-	2	-	-	2	-	-	-	4	-	2	-
4	-	-	-	2	-	2	4	-	-	2	2	2	-	-	2	-
5	-	2	2	-	4	-	-	4	2	-	-	2	-	-	-	-
6	-	-	2	-	4	-	-	2	2	-	2	2	2	-	-	-
7	-	-	-	-	-	4	4	-	2	2	2	2	-	-	-	-
8	-	-	-	-	-	2	-	2	4	-	-	4	-	2	-	2
9	-	2	-	-	-	2	2	2	-	4	2	-	-	-	-	2
10	-	-	-	-	2	2	-	-	-	4	4	-	2	2	-	-
11	-	-	-	2	2	-	2	2	2	-	-	4	-	-	2	-
12	-	4	-	2	-	2	-	-	2	-	-	-	-	-	6	-
13	-	-	-	-	-	-	2	2	-	-	-	-	6	2	-	4
14	-	2	-	4	2	-	-	-	-	-	2	-	-	-	-	6
15	-	-	-	-	2	-	2	-	-	-	-	-	-	10	-	2

Differential cryptanalysis for hash functions

Example: block cipher based hash function

- Matyas-Meyer-Oseas $h_i = e_{h_{i-1}}(m_i) \oplus m_i$
- find high-probability differential for e such that $\alpha \xrightarrow{e} \alpha$
- assume m and $m' = m \oplus \alpha$ are such that

  $$e_{h_{i-1}}(m) = e_{h_{i-1}}(m') \oplus \alpha,$$

  for some value of h_{i-1}
- but then $h_i = h'_i$, and there is a collision!

Differential cryptanalysis - encryption vs hashing

	Encryption	**Hashing**
key to e	fixed, no control of attacker	not fixed, under (some) control of attacker
find pairs satisfying differential	check ciphertexts	check after each round early abort strategy
nature of differential	any	special form
workload to find differential should be	$< 2^n$	$< 2^{n/2}$

Attacks - examples

Attacks - weaknesses in block cipher

- FEAL, high-probability differentials
- SAFER, weakness in key-schedule exploitable for hash functions
- DES, weak keys
- $\cdots\cdots\cdots$

DES: Data Encryption Standard

- 1977: publication of FIPS 46 (DES)
- complementation property:

$$\forall\, p, k : c = \mathsf{DES}_k(p) \Longleftrightarrow \bar{c} = \mathsf{DES}_{\bar{k}}(\bar{p})$$

- 4 weak keys: $\mathsf{DES}_k(\mathsf{DES}_k(p)) = p, \ \forall\, p$
- Best differential $2r$ rounds
  - average probability over all keys: $(1/234)^r$
  - probability for subspace of keys: $(1/146)^r$

Compression functions using DES

- Davies-Meyer: $h_i = e_{m_i}(h_{i-1}) \oplus h_{i-1}$
- Matyas-Meyer-Oseas: $h_i = e_{h_{i-1}}(m_i) \oplus m_i$
- Complementation property leads to collision for both
- DES reduced to 15 rounds:
  - encryption: $\alpha \to \alpha$, probability 2^{-55} (Biham-Shamir)
  - hashing: $\phi \to \phi$, can be found in time 2^{26} (Rijmen, Knudsen, Preneel)

AR Hash - double block hash mode (1992)

$$\begin{aligned} h_i^1 &= m_i \oplus e_{k_1}(m_i \oplus h_{i-1}^1 \oplus h_{i-2}^1 \oplus \eta) \\ h_i^2 &= m_i \oplus e_{k_2}(m_i \oplus h_{i-1}^2 \oplus h_{i-2}^2 \oplus \eta) \end{aligned}$$

- k_1, k_2 fixed keys
- $e_k : \{0,1\}^n \to \{0,1\}^n$
- $\eta = 01234 \cdots EF$, constant
- hash result $2n$ bits
- Collisions $2^{n/2}$, preimages 2^n, Damgård-Knudsen & Preneel (93)

An implementation of AR Hash

European bank, keys chosen as

$$k_1 = 0000000000000000 \text{ and } k_2 = 2A41522F4446502A$$

If $e_{k_1}(x) = x$, x is called a fixed point (for $e_{k_1}()$)

Weak key in DES has 2^{32} fixed points. k_1 weak

Damgaard-Knudsen (93):

- Strong attack if $\exists\, z$ s.t. z and $e_{k_2}(z)$ fixed points for $e_{k_1}()$
- Implementation showed two such values z_1, z_2
- For any m it holds that $AR(m) = AR(z_1 \mid m) = AR(z_2 \mid m)$

Preimage attack on Rabin's scheme

$$h_0 \longrightarrow \overset{\overset{m_1}{\downarrow}}{\boxed{e}} \longrightarrow \overset{\overset{m_2}{\downarrow}}{\boxed{e}} \longrightarrow \cdots\cdots\cdots \longrightarrow \overset{\overset{m_{t-1}}{\downarrow}}{\boxed{e}} \longrightarrow \overset{\overset{m_t}{\downarrow}}{\boxed{e}} \longrightarrow h_t$$

- Given (h_0, h_t) $\qquad e : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$
- Choose arbitrary values of $m_1, m_2, \ldots, m_{t-2}$, compute h_{t-2}
- For $2^{n/2}$ values of $m_{t-1}(i)$ compute $e_{m_{t-1}(i)}(h_{t-2})$
- For $2^{n/2}$ values of $m_t(j)$ compute $e^{-1}_{m_t(j)}(h_t)$
- Find match (i, j), thus $m_1, m_2, \ldots, m_{t-2}, m_{t-1}(i), m_t(j)$ hash to h_t

Davies-Price variant of Rabin's scheme

$$h_0 \longrightarrow \overset{m_1}{\underset{}{\boxed{e}}} \longrightarrow \overset{m_2}{\boxed{e}} \longrightarrow \cdots\cdots\cdots \longrightarrow \overset{m_{t-1}}{\boxed{e}} \longrightarrow \overset{m_t}{\boxed{e}} \longrightarrow h_t$$

$$h_t \longrightarrow \overset{m_1}{\boxed{e}} \longrightarrow \overset{m_2}{\boxed{e}} \longrightarrow \cdots\cdots\cdots \longrightarrow \overset{m_{t-1}}{\boxed{e}} \longrightarrow \overset{m_t}{\boxed{e}} \longrightarrow h_{2t}$$

- Cycle through message blocks twice
- Hash of $m_1, \ldots, m_t$ is h_{2t}
- Attack more complicated ?? Complexity 2^n ??
- Coppersmith 1985 to follow...

Another birthday attack - precomputation

$$h_0 \rightarrow \overset{m_1}{\boxed{e}} \rightarrow \overset{m_2}{\boxed{e}} \underset{z\uparrow}{\rightarrow} \overset{m_3}{\boxed{e}} \rightarrow \overset{m_4}{\boxed{e}} \underset{z\uparrow}{\rightarrow} \overset{m_5}{\boxed{e}} \rightarrow \overset{m_6}{\boxed{e}} \rightarrow \cdots\cdots \rightarrow \overset{m_{t-1}}{\boxed{e}} \rightarrow \overset{m_t}{\boxed{e}} \rightarrow h_t$$

$$h_t \rightarrow \overset{m_1}{\boxed{e}} \rightarrow \overset{m_2}{\boxed{e}} \rightarrow \overset{m_3}{\boxed{e}} \rightarrow \overset{m_4}{\boxed{e}} \rightarrow \overset{m_5}{\boxed{e}} \rightarrow \overset{m_6}{\boxed{e}} \rightarrow \cdots\cdots \rightarrow \overset{m_{t-1}}{\boxed{e}} \rightarrow \overset{m_t}{\boxed{e}} \rightarrow h_{2t}$$

- Find (m_3, m_4) s.t. $h_2 = h_4 = z$ (arbitrary z), complexity $2^{n/2}$

Another birthday attack - precomputation

$$h_0 \rightarrow \overset{m_1}{\boxed{e}} \rightarrow \overset{m_2}{\boxed{e}} \underset{z\uparrow}{\rightarrow} \overset{m_3}{\boxed{e}} \rightarrow \overset{m_4}{\boxed{e}} \underset{z\uparrow}{\rightarrow} \overset{m_5}{\boxed{e}} \rightarrow \overset{m_6}{\boxed{e}} \rightarrow \cdots\cdots \rightarrow \overset{m_{t-1}}{\boxed{e}} \rightarrow \overset{m_t}{\boxed{e}} \rightarrow h_t$$

$$h_t \rightarrow \overset{m_1}{\boxed{e}} \rightarrow \overset{m_2}{\boxed{e}} \rightarrow \overset{m_3}{\boxed{e}} \rightarrow \overset{m_4}{\boxed{e}} \rightarrow \overset{m_5}{\boxed{e}} \rightarrow \overset{m_6}{\boxed{e}} \rightarrow \cdots\cdots \rightarrow \overset{m_{t-1}}{\boxed{e}} \rightarrow \overset{m_t}{\boxed{e}} \rightarrow h_{2t}$$

- Find $2^{n/8}$ pairs (m_3, m_4) s.t. $h_2 = h_4 = z$, complexity $2^{n/2+n/16}$

Another birthday attack - precomputation

$$h_0 \rightarrow \overset{m_1}{\boxed{e}} \rightarrow \overset{m_2}{\boxed{e}} \underset{z\uparrow}{\rightarrow} \overset{m_3}{\boxed{e}} \rightarrow \overset{m_4}{\boxed{e}} \underset{z\uparrow}{\rightarrow} \overset{m_5}{\boxed{e}} \rightarrow \overset{m_6}{\boxed{e}} \underset{z\uparrow}{\rightarrow} \cdots\cdots \rightarrow \overset{m_{t-1}}{\boxed{e}} \rightarrow \overset{m_t}{\boxed{e}} \rightarrow h_t$$

$$h_t \rightarrow \overset{m_1}{\boxed{e}} \rightarrow \overset{m_2}{\boxed{e}} \rightarrow \overset{m_3}{\boxed{e}} \rightarrow \overset{m_4}{\boxed{e}} \rightarrow \overset{m_5}{\boxed{e}} \rightarrow \overset{m_6}{\boxed{e}} \rightarrow \cdots\cdots \rightarrow \overset{m_{t-1}}{\boxed{e}} \rightarrow \overset{m_t}{\boxed{e}} \rightarrow h_{2t}$$

- Find $2^{n/4}$ pairs (m_3, m_4, m_5, m_6) s.t. $h_2 = h_4 = h_6 = z$

Another birthday attack - precomputation

$$h_0 \rightarrow \overset{m_1}{\boxed{e}} \rightarrow \overset{m_2}{\boxed{e}} \underset{z\uparrow}{\rightarrow} \overset{m_3}{\boxed{e}} \rightarrow \overset{m_4}{\boxed{e}} \underset{z\uparrow}{\rightarrow} \cdots\cdots \underset{z\uparrow}{\rightarrow} \overset{m_9}{\boxed{e}} \rightarrow \overset{m_{10}}{\boxed{e}} \underset{z\uparrow}{\rightarrow} \cdots\cdots \rightarrow \overset{m_t}{\boxed{e}} \rightarrow h_t$$

$$h_t \rightarrow \overset{m_1}{\boxed{e}} \rightarrow \overset{m_2}{\boxed{e}} \rightarrow \overset{m_3}{\boxed{e}} \rightarrow \overset{m_4}{\boxed{e}} \rightarrow \overset{m_5}{\boxed{e}} \rightarrow \overset{m_6}{\boxed{e}} \rightarrow \cdots\cdots \rightarrow \overset{m_{t-1}}{\boxed{e}} \rightarrow \overset{m_t}{\boxed{e}} \rightarrow h_{2t}$$

- Find $2^{n/2}$ pairs $(m_3, m_4, m_5, m_6, m_7, m_8, m_9, m_{10})$ s.t. $h_2 = h_{10} = z$

Another birthday attack - precomputation

$$h_0 \rightarrow \overset{m_1}{\boxed{e}} \rightarrow \overset{m_2}{\boxed{e}} \underset{z\uparrow}{\rightarrow} \overset{m_3}{\boxed{e}} \rightarrow \overset{m_4}{\boxed{e}} \underset{z\uparrow}{\rightarrow} \cdots \rightarrow \overset{m_{10}}{\boxed{e}} \underset{z\uparrow}{\rightarrow} \cdots \rightarrow \overset{m_{18}}{\boxed{e}} \underset{z\uparrow}{\rightarrow} \cdots \rightarrow \overset{m_t}{\boxed{e}} \rightarrow h_t$$

$$h_t \rightarrow \overset{m_1}{\boxed{e}} \rightarrow \overset{m_2}{\boxed{e}} \rightarrow \overset{m_3}{\boxed{e}} \rightarrow \overset{m_4}{\boxed{e}} \rightarrow \overset{m_5}{\boxed{e}} \rightarrow \overset{m_6}{\boxed{e}} \rightarrow \cdots\cdots \rightarrow \overset{m_{t-1}}{\boxed{e}} \rightarrow \overset{m_t}{\boxed{e}} \rightarrow h_{2t}$$

- Find $2^{n/2}$ pairs $(m_{18}, m_{17}, m_{16}, m_{15}, m_{14}, m_{13}, m_{12}, m_{11})$ s.t. $h_{18} = h_{10} = z$

Another birthday attack - Coppersmith 1985

$$h_0 \to \overset{m_1}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_2}{\overset{\downarrow}{\boxed{e}}} \underset{z\,\uparrow}{\to} \overset{m_3}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_4}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_5}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_6}{\overset{\downarrow}{\boxed{e}}} \to \cdots\cdots \to \overset{m_{t-1}}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_t}{\overset{\downarrow}{\boxed{e}}} \to h_t$$

$$h_t \to \overset{m_1}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_2}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_3}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_4}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_5}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_6}{\overset{\downarrow}{\boxed{e}}} \to \cdots\cdots \to \overset{m_{t-1}}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_t}{\overset{\downarrow}{\boxed{e}}} \to h_{2t}$$

- Given (h_0, h_{2t})
- Find (m_1, m_2) to get $h_2 = z$, complexity $\sqrt{2^n}$

Another birthday attack - Coppersmith 1985

$$h_0 \to \overset{m_1}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_2}{\overset{\downarrow}{\boxed{e}}} \underset{z\,\uparrow}{\to} \overset{m_3}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_4}{\overset{\downarrow}{\boxed{e}}} \underset{z\,\uparrow}{\to} \cdots \to \overset{m_{10}}{\overset{\downarrow}{\boxed{e}}} \underset{z\,\uparrow}{\to} \cdots \to \overset{m_{18}}{\overset{\downarrow}{\boxed{e}}} \underset{z\,\uparrow}{\to} \cdots \to \overset{m_t}{\overset{\downarrow}{\boxed{e}}} \to h_t$$

$$h_t \to \overset{m_1}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_2}{\overset{\downarrow}{\boxed{e}}} \underset{\uparrow}{\to} \overset{m_3}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_4}{\overset{\downarrow}{\boxed{e}}} \to \cdots \to \overset{m_{10}}{\overset{\downarrow}{\boxed{e}}} \to \cdots \to \overset{m_{18}}{\overset{\downarrow}{\boxed{e}}} \underset{\uparrow}{\to} \cdots \to \overset{m_t}{\overset{\downarrow}{\boxed{e}}} \to h_{2t}$$

- From h_{2t} compute backwards to h_{t+18} (arbitrary $m_{19}, \ldots$)
- Compute h_{t+2}

Another birthday attack - Coppersmith 1985

$$h_0 \to \overset{m_1}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_2}{\overset{\downarrow}{\boxed{e}}} \underset{z\,\uparrow}{\to} \overset{m_3}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_4}{\overset{\downarrow}{\boxed{e}}} \underset{z\,\uparrow}{\to} \cdots \to \overset{m_{10}}{\overset{\downarrow}{\boxed{e}}} \underset{z\,\uparrow}{\to} \cdots \to \overset{m_{18}}{\overset{\downarrow}{\boxed{e}}} \underset{z\,\uparrow}{\to} \cdots \to \overset{m_t}{\overset{\downarrow}{\boxed{e}}} \to h_t$$

$$h_t \to \overset{m_1}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_2}{\overset{\downarrow}{\boxed{e}}} \underset{\uparrow}{\to} \overset{m_3}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_4}{\overset{\downarrow}{\boxed{e}}} \to \cdots \to \overset{m_{10}}{\overset{\downarrow}{\boxed{e}}} \underset{\to\leftarrow}{\to} \cdots \to \overset{m_{18}}{\overset{\downarrow}{\boxed{e}}} \underset{\uparrow}{\to} \cdots \to \overset{m_t}{\overset{\downarrow}{\boxed{e}}} \to h_{2t}$$

Do meet-in-the-middle attack on 2nd chain using

- $2^{n/2}$ pairs $(m_3, m_4, \ldots, m_9, m_{10})$ s.t. $h_2 = h_{10} = z$
- $2^{n/2}$ pairs $(m_{18}, m_{17}, \ldots, m_{12}, m_{11})$ s.t. $h_{18} = h_{10} = z$

Another birthday attack - Coppersmith 1985

$$h_0 \to \overset{m_1}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_2}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_3}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_4}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_5}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_6}{\overset{\downarrow}{\boxed{e}}} \to \cdots\cdots \to \overset{m_{t-1}}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_t}{\overset{\downarrow}{\boxed{e}}} \to h_t$$

$$h_t \to \overset{m_1}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_2}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_3}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_4}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_5}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_6}{\overset{\downarrow}{\boxed{e}}} \to \cdots\cdots \to \overset{m_{t-1}}{\overset{\downarrow}{\boxed{e}}} \to \overset{m_t}{\overset{\downarrow}{\boxed{e}}} \to h_{2t}$$

- preimage attack on one-chain Rabin $\approx 2^{n/2}$
- preimage attack on two-chains Rabin $\approx 2^{n/2+n/16}$ using multi-collisions!

Sum of hash functions?

- Assume $f, g : \{0,1\}^* \to \{0,1\}^n$ are ideal hash functions
- Consider the hash function
$$h(x, y) \stackrel{\text{def}}{=} f(x) \oplus g(y)$$
- Is h at least as strong as both f and g ??

Generalised birthday attack - Wagner 2002

$$\left.\begin{array}{l} 2^{n/3} \text{ values } x_i \\ \\ 2^{n/3} \text{ values } x_j \end{array}\right\} \begin{array}{l} 2^{n/3} \text{ pairs } (x_i, x_j): \\ f(x_i) \oplus f(x_j) = (**0) \end{array}$$

$$\left.\right\} \begin{array}{l} \text{one tuple } (x_i, x_j, y_k, y_\ell): \\ f(x_i) \oplus f(x_j) = \\ g(y_k) \oplus g(y_\ell) \end{array}$$

$$\left.\begin{array}{l} 2^{n/3} \text{ values } y_k \\ \\ 2^{n/3} \text{ values } y_\ell \end{array}\right\} \begin{array}{l} 2^{n/3} \text{ pairs } (y_k, y_\ell): \\ g(y_k) \oplus g(y_\ell) = (**0) \end{array}$$

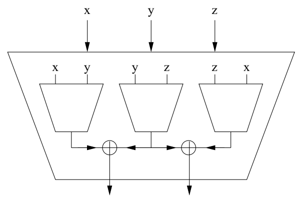
Generalized birthday attack (2)

- $h(x, y) = f(x) \oplus g(y)$
- hence we found

$$\begin{aligned} f(x_i) \oplus f(x_j) &= g(y_k) \oplus g(y_\ell) \\ &\text{or} \\ f(x_i) \oplus g(y_k) &= f(x_j) \oplus g(y_\ell) \end{aligned}$$

- collision for h in time approximately $2^{n/3}$

Nandi et al, 2005



$2n$-bit result

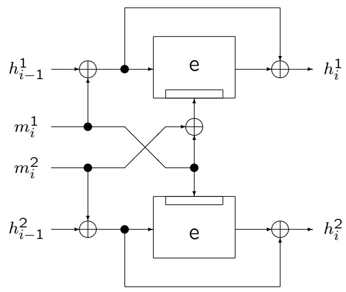
Collisions require $\geq 2^{2n/3}$ operations (proof, ideal cipher model)

Knudsen-Muller (2005)

- collision in $2^{2n/3}$, preimages in time 2^n
- truncation to $2s$ bits: collisions in $2^{2s/3}$, preimages in 2^s

Structural attacks

Parallel-DM, hash results $2n$ bits



Attacks on Parallel-DM - preimage attack

- given $h_t = (h^1_t, h^2_t)$ and h_0.
- find x, y such that $e_x(y) \oplus y = h^1_t$ (brute-force)
- repeat 2^n times:
  - compute a value of h^1_{t-1} from arbitrary $m_1, \ldots, m_{t-1}$
  - choose m^1_t, m^2_t, such that computation of h^1_t is $e_x(y) \oplus y$
- we have 2^n messages all with partial hash value h^1_t
- one message is expected to hash to h^2_t in 2nd half

NB. If t is unknown, fix it to value > 1

Attacks on Parallel-DM - collision attack

- choose arbitrary x, y, compute $e_x(y) \oplus y = h^1_t$
- repeat $2^{n/2}$ times:
  - compute a value of h^1_{t-1} from arbitrary $m_1, \ldots, m_{t-1}$
  - choose m^1_t, m^2_t, such that computation of h^1_t is $e_x(y) \oplus y$
- we have $2^{n/2}$ messages all with partial hash value h^1_t
- two of these messages are expected to collide also in 2nd half

SMASH - Knudsen 2005

Compression function built from one bijective mapping

$$f : \{0,1\}^n \rightarrow \{0,1\}^n$$

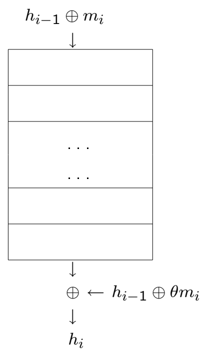
Regard the h's and the m's as elements in GF(2^n)

Let θ be element in GF(2^n), but not 0 or 1

Compression function

$$h_i \;=\; f(h_{i-1} \oplus m_i) \oplus h_{i-1} \oplus \theta m_i$$

SMASH - outline



Problems ?

$$h_i \;=\; f(h_{i-1} \oplus m_i) \oplus h_{i-1} \oplus \theta m_i \qquad \theta \notin \{0,1\}$$

Forward prediction:
Let $\alpha = h_{i-1} \oplus h'_{i-1}$, choose m_i, then compute $m'_i = m_i \oplus \alpha$.

$$h_i \oplus h'_i \;=\; (\theta + 1)\alpha$$

Inversion: Given h_i, choose a, compute $b = f^{-1}(h_i \oplus a) = h_{i-1} \oplus m_i$, then solve for h_{i-1} and m_i.

$$(a \quad b) \;=\; (h_{i-1} \quad m_i) \begin{pmatrix} 1 & 1 \\ \theta & 1 \end{pmatrix}$$

©Lars R. Knudsen 2007

Proposal: SMASH (2005)

$f : \{0,1\}^n \rightarrow \{0,1\}^n$

Compression function

$$\begin{aligned} h_0 &= f(iv) \oplus iv \\ h_i &= f(h_{i-1} \oplus m_i) \oplus h_{i-1} \oplus \theta m_i \qquad \text{for } i = 1, \ldots, t \\ h_{t+1} &= f(h_t) \oplus h_t \end{aligned}$$

Drawback: 2nd preimage attack of complexity $2^{n/2}$

2005: Kelsey-Schneier generic attack: $k2^{n/2} + 2^{n-k}$ with 2^k blocks

Two real-life constructions: SMASH-256, SMASH-512

©Lars R. Knudsen 2007

SMASH properties

Underlying field in SMASH-256 (256-bit blocks) is defined by irreducible polynomial

$$q(\theta) = \theta^{256} \oplus \theta^{16} \oplus \theta^3 \oplus \theta \oplus 1$$

over $GF(2)$

Forward prediction: given difference α after 1 round, choose messages s.t. difference in outputs of 2nd round is $(\theta \oplus 1)\alpha$.

Iterate to i blocks, yield predictable "difference" $(\theta \oplus 1)^i\alpha$.

Difference can be made "larger" by factor $(\theta \oplus 1)$ per round

©Lars R. Knudsen 2007

SMASHed

- Pramstaller, Rechberger, Rijmen, 2005
- 1st observation: rewrite polynomial

$$\begin{aligned} q(\theta) &= \theta^{256} \oplus \theta^{16} \oplus \theta^3 \oplus \theta \oplus 1 \\ &= 1 \oplus (\theta \oplus 1)^2 \oplus (\theta \oplus 1)^3 \oplus (\theta \oplus 1)^{16} \oplus (\theta \oplus 1)^{256} \end{aligned}$$

©Lars R. Knudsen 2007

SMASHed - Pramstaller, Rechberger, Rijmen, 2005

- Choose two different messages in 1st round, difference α
- Forward prediction

  round $i-1$: β
  round i : $(\theta \oplus 1)\beta$
- "Differential" property, make inputs to f equal to 1st round inputs

  round $i-1$: β
  round i : $(\theta \oplus 1)\beta \oplus \alpha$
- Ex.: sequence of differences $\alpha,\ (\theta \oplus 1)\alpha,\ (\theta \oplus 1)^2\alpha \oplus \alpha,$
- Iterate to 256 blocks, compute "difference" $q(\theta)\alpha$
- $q(\theta)\alpha = (1 \oplus (\theta \oplus 1)^2 \oplus (\theta \oplus 1)^3 \oplus (\theta \oplus 1)^{16} \oplus (\theta \oplus 1)^{256})\alpha$

The end