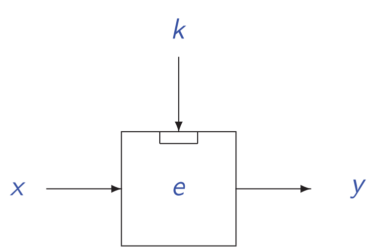
Hash Functions Based on Block Ciphers

Lars R. Knudsen

May 5, 2009

Block cipher - family of permutations

- $e : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$, $\quad m = \kappa + n > n$
- each κ-bit key specifies bijective mapping on n bits
- **must** hold for all x and k that $e_k^{-1}(e_k(x)) = x$.
- one-way function: given x and $e_k(x)$, hard to find k.



DES & AES

DES = Data Encryption Standard
AES = Advanced Encryption Standard

system	year	block size	key size
DES	1977	64	56
AES	2001	128	128, 192 or 256

DES & AES: History

DES:

- Developed in early 70's by IBM together with NSA
- 1977: publication of FIPS 46 (DES)

AES:

- Winner of open (world-wide) competition 1997-2001
- Designed by Daemen, Rijmen from Belgium

2009: most realistic key-recovery attack for both is an exhaustive search

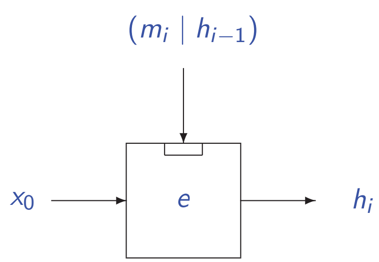
In the beginning there was ...

Diffie and Hellman, 1976. New directions in cryptography.

- Digital signatures .... for efficiency:
- "Let g be a one-way mapping from binary N-space to binary n-space...". "Take the N bit message m and operate on it with g to obtain the n bit vector m'."
- "It must be hard even given m to find a different inverse image of m'"
- "Finding such functions appears to offer little trouble"

Diffie-Hellman, $\kappa > n$

$e : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$



- x_0 fixed block
- 2nd preimages hard if e secure against known-plaintext attack

Hash function using a block cipher

Why build on a block cipher?

- it's natural !
- use existing technology
- transfer security (trust?!) to hash construction
- schemes "slow" (partly due to key-schedules)
- weaknesses of block cipher not relevant for encryption

Hash rate

- Given hash function built from block cipher

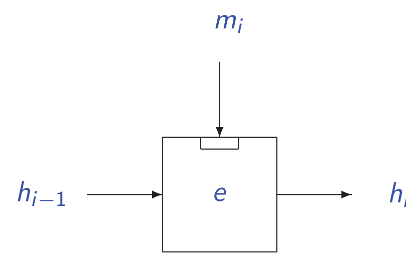
$$e : \{0,1\}^\kappa \times \{0,1\}^n \rightarrow \{0,1\}^n$$

- Hash rate defined as

$$\frac{\#\ n\text{-bit blocks hashed}}{\#\ \text{invocations of } e + \#\ \text{key-schedules}}$$

Rabin, 1978

$e : \{0,1\}^\kappa \times \{0,1\}^n \rightarrow \{0,1\}^n$



- rate $= (\kappa/n)/(1+1)$
- Yuval: collisions based on birthday paradox (79) (Merkle 79)
- Pre-images in approximately same time

Single block hash

- $e : \{0,1\}^\kappa \times \{0,1\}^n \rightarrow \{0,1\}^n$
- 12 secure ones (Preneel 93, Black et al 02), here three

$$h_i = e_{m_i}(h_{i-1}) \oplus h_{i-1} \quad \text{Davies-Meyer}$$
$$h_i = e_{h_{i-1}}(m_i) \oplus m_i \quad \text{Matyas-Meyer-Oseas}$$
$$h_i = e_{h_{i-1}}(m_i) \oplus m_i \oplus h_{i-1} \quad \text{Preneel-Miyaguchi}$$

- Hash rates. About 1/(1+1) (1/2 for DES and AES)
- Collisions (birthday attack) in $2^{n/2}$ operations

MD4-family

- MD4, Rivest 1990
- MD5, Rivest 1991
- SHA-0, 1993
- SHA-1, 1994
- all hash functions of Davies-Meyer form
- "block ciphers" with feed-forward
- hash rates for Davies-Meyer can be (arbitrarily) high

Double block hash - based on block ciphers

- Based on $e : \{0,1\}^\kappa \times \{0,1\}^n \rightarrow \{0,1\}^n$
- Length of hash, $2n$ bits
- Aim: 2^n security level for collisions
  - Merkle, 1989
  - MDC-2, Brachtl, Coppersmith et al 1988/1990
  - PBGV, QG, LOKI-DBH, ..., 1990s
  - Hirose, Nandi, 2005

Ideal cipher model

- Let $B_{n,k}$ be all block ciphers with a k-bit key and n-bit blocks,

$$\{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$$

- There are $2^n! \approx 2^{n2^n}$ bijections on n bits
- It holds that

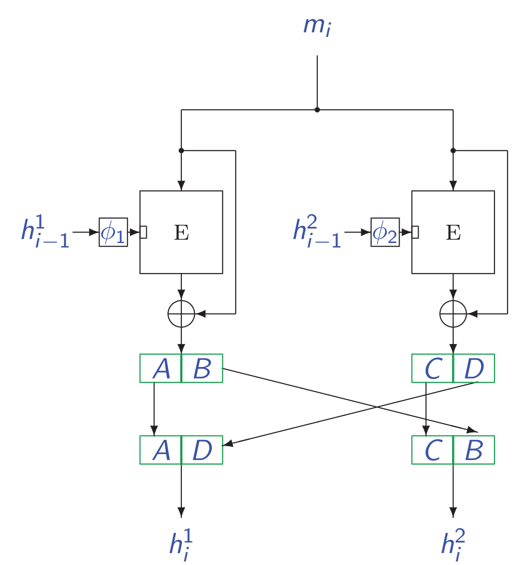
$$|B_{n,k}| = \binom{2^n!}{2^k}$$

- An ideal cipher is randomly selected from $B_{n,k}$

Merkle's double block schemes with DES (1989)

- "DES can be used to build a one-way hash function which is secure"
- if DES fails "it seems almost certain that some block cipher exist with the desirable properties"
- 128-bit hash function with proof of security in ideal cipher model
- collisions $\approx 2^{55}$, inconvenient block sizes, low hash rates
- "recent proposal from IBM looks very hopeful", but no proof..

MDC-2, IBM 1987



MDC-2

- Coppersmith, Meyer, Schilling et al, IBM, patent filed 1987
- designed for DES but can be used with any block cipher
- mapping from text to key: $\phi_1(\cdot), \phi_2(\cdot) : \{0,1\}^{64} \to \{0,1\}^{56}$
- hash rate 1/(2+2) (1/4 for DES and AES)
- MDC-4: variant using four encryptions per block

MDC-2 used with DES and AES

Best known attacks, Eurocrypt last week
(Knudsen, Mendel, Rechberger, Thomsen)

	DES	AES
Hash size	128	256
Preimage attack	2^{55}	2^{129}
2nd preimage attack	2^{55}	2^{129}
Collision attack	$2^{51.5}$	$2^{124.5}$
Hash rate	1/4	1/4

- For use with AES, "proof" that collision requries $> 2^{75}$ operations (Steinberger 2007)

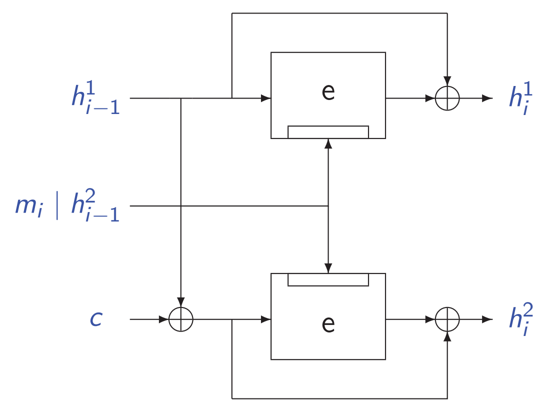
Hirose's double block mode 2006

Based on work by Nandi, 2005
$e : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$, $\kappa > n$, c nonzero constant

$$h_i^1 = e_{h_{i-1}^2 \mid m_i}(h_{i-1}^1) \oplus h_{i-1}^1$$
$$h_i^2 = e_{h_{i-1}^2 \mid m_i}(h_{i-1}^1 \oplus c) \oplus h_{i-1}^1 \oplus c$$

- Collision requires 2^n operations assuming $e(\cdot,\cdot)$ is ideal cipher
- AES-256, hash rate 1/3, security level 2^{128} for collisions

Hirose's double block mode, figure



Ideal cipher model ?

- proofs in model give protection against generic attacks
- no real-life cipher is an ideal cipher; "nearly ideal" cipher can be strong for encryption but very weak when used for hashing
- attacker in control of key can invest time in finding key(s) with certain properties

Hash based on fixed permutations

- Preneel, 1992
- Knudsen, 2005. SMASH: $h_i = p(m_i \oplus h_{i-1}) \oplus \theta m_i \oplus h_{i-1}$
- Pramstaller et al, 2005. SMASH broken
- Shrimpton-Stamm, 2007, construction with three bijections. Collision in time $\approx 2^{n/2}$ but same for preimages..
- Rogaway-Steinberger, 2008, construction with three bijections. Collision in time $\approx 2^{n/2}$, preimage in time $\approx 2^{2n/3}$