An Overview of Cryptanalysis Research for the Advanced Encryption Standard

Alan Kaminsky, Rochester Institute of Technology
Michael Kurdziel, Harris Corporation
Stanisław Radziszowski, Rochester Institute of Technology

November 2, 2010

Agenda

- Background
  - History
  - Theoretical vs. practical attacks
  - Block cipher usage
- AES attacks
  - Brute force attacks
  - Linear and differential attacks
  - Algebraic attacks
  - SAT solver attacks
  - Related-key attacks
  - Side channel attacks
- Prognosis and recommendations

Background

History

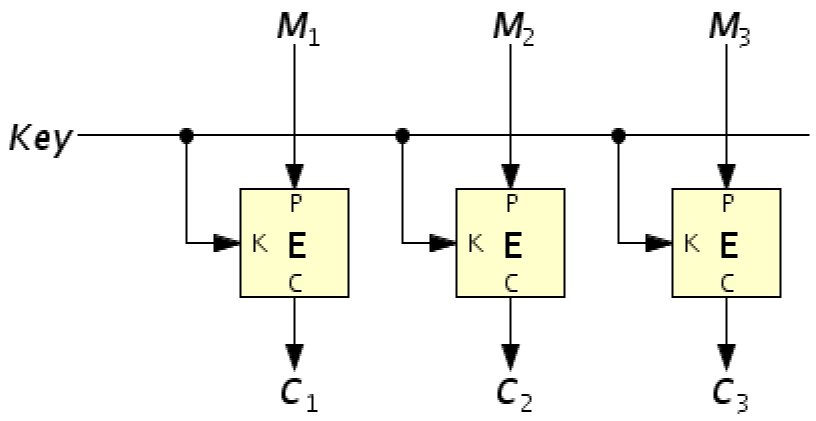
- 1976 — DES block cipher published
- 1991 — Differential cryptanalysis of DES published
- 1993 — Linear cryptanalysis of DES published
- 1997 — AES Competition commences
- 1998 — AES Competition Round 1 ends; 15 candidates chosen
- 1998 — EFF's Deep Crack breaks DES (56 hours, $250,000)
- 1998 — Triple-DES block cipher published
- 1999 — AES Competition Round 2 ends; 5 candidates chosen
- 2000 — AES Competition Round 3 ends; Rijndael wins
- 2001 — AES block cipher published
- 2003 — NSA approves AES for Type 1 Suite B encryption

- ???? — AES broken

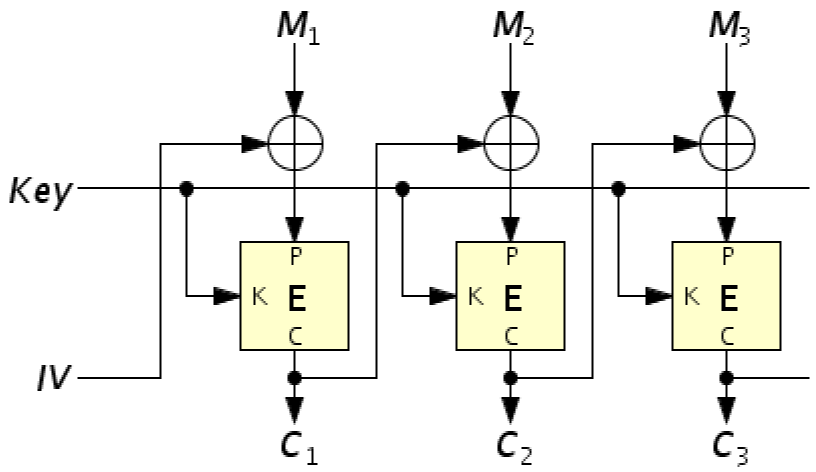
Theoretical vs. Practical Attacks

- Block cipher "break" = find the secret encryption key
- A block cipher can always be broken
  - Brute force search
  - 2^n operations, n = number of key bits
- Secure against attack X
  - Attack X needs more than 2^n operations
- Theoretical break
  - Attack X needs fewer than 2^n operations
  - But the time required is too long to be useful
- Practical break
  - Attack X needs fewer than 2^n operations
  - And the time required is short enough to be useful
- How short is short enough?
  - Military secrets: 50 years

Block Cipher Usage: Encryption

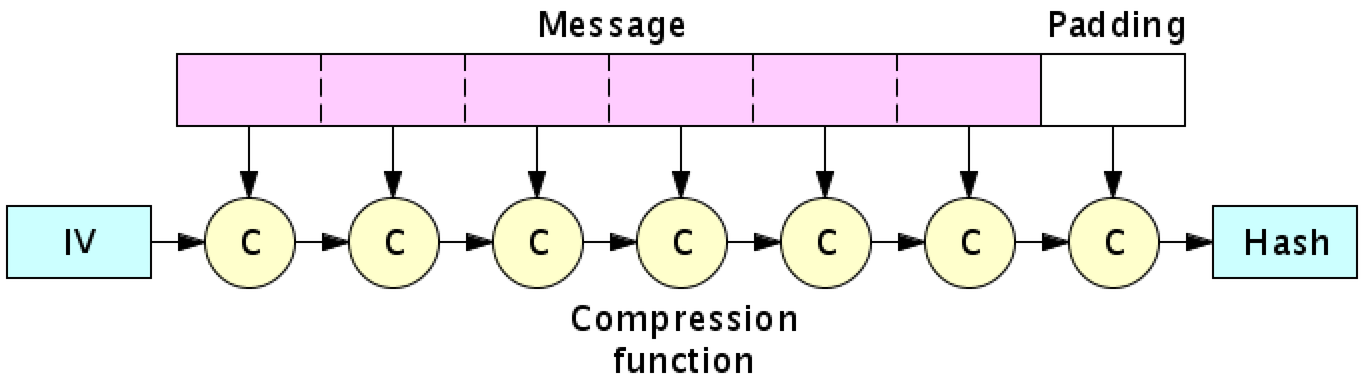


Electronic codebook (ECB) mode

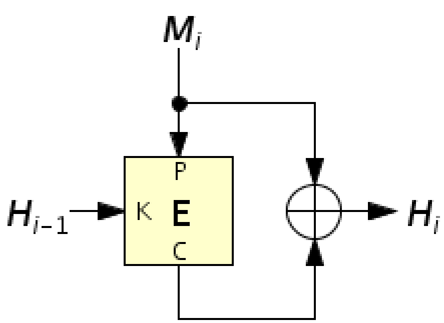


Cipher block chaining (CBC) mode

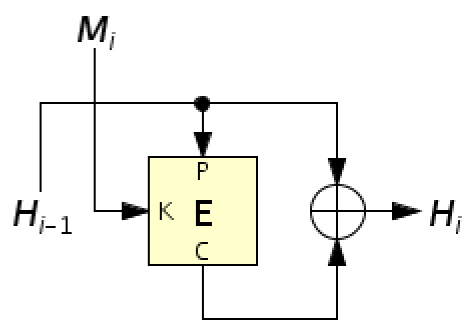
Block Cipher Usage: Hashing



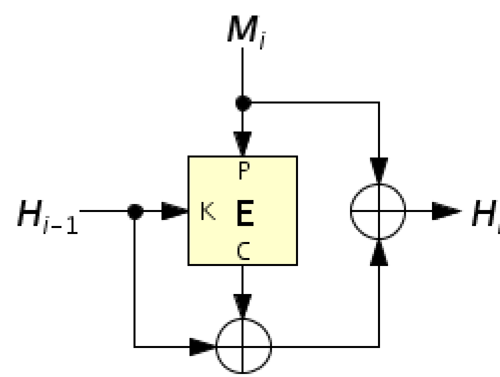
Merkle-Damgård construction



Matyas-Meyer-Oseas



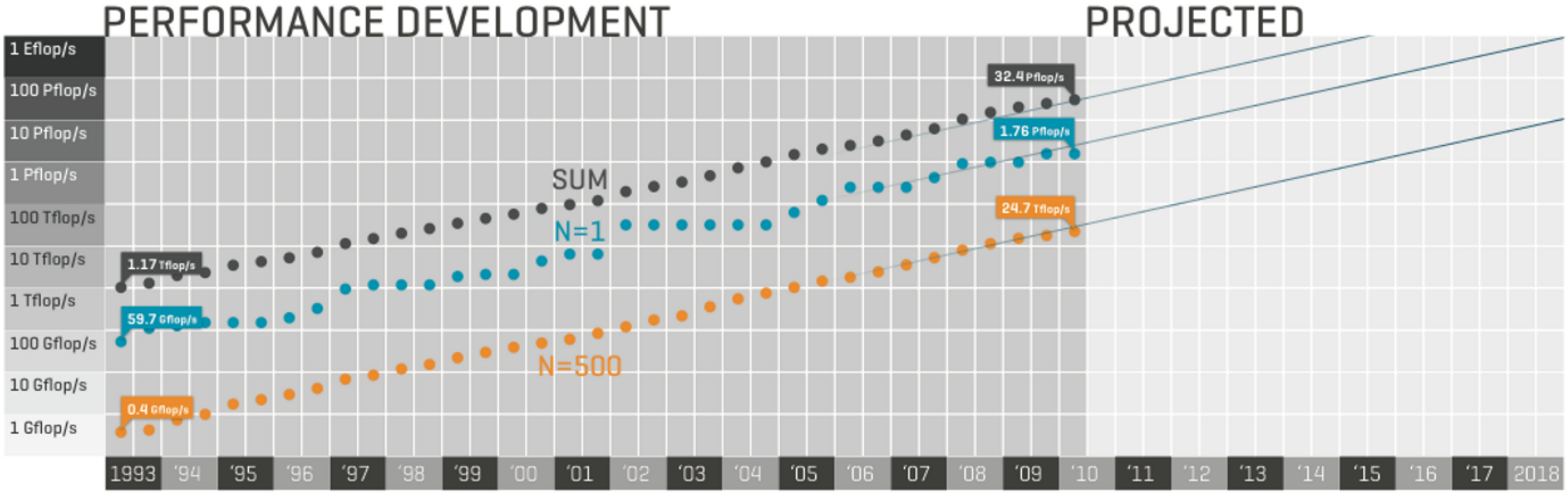
Davies-Meyer



Miyaguchi-Preneel

AES Attacks

Brute Force Attacks



- **June 2010 TOP500 List (www.top500.org)**
- **World's fastest supercomputer: ORNL's Jaguar**
  - **224,162 cores (2.6 GHz six-core Opteron chips)**
  - **1.759 petaflops Linpack performance (1,759,000 gigaflops)**
- **1,000-fold performance improvement per decade**

Brute Force Attacks

- Assume
  - 1 AES encryption = 200 floating point operations
- Top supercomputer brute force attack today
  - 2^n encryptions × 200 flop/encryption ÷ 1.76×10^{15} flop/sec
  - AES-128: 3.87×10^{25} sec = 1.23×10^{18} years
  - AES-192: 7.13×10^{44} sec = 2.26×10^{37} years
  - AES-256: 1.32×10^{64} sec = 4.17×10^{56} years
- Top supercomputer brute force attack in 2060
  - 2^n encryptions × 200 flop/encryption ÷ 1.76×10^{30} flop/sec
  - AES-128: 3.87×10^{10} sec = 1.23×10^{3} years
  - AES-192: 7.13×10^{29} sec = 2.26×10^{22} years
  - AES-256: 1.32×10^{49} sec = 4.17×10^{41} years
- AES prognosis: Safe

Linear and Differential Attacks

- Cryptanalytic attacks known before AES was invented
  - Linear attack
  - Differential attack
  - Boomerang attack
  - Truncated differential attack
  - Square attack
  - Interpolation attack
- AES was designed to be secure against all these attacks
  - Differential attack breaks AES reduced to 8 rounds
  - AES-128 was therefore designed with 10 rounds
  - Security margin: 20%
- AES prognosis: Safe, but . . .
  - Small security margin is troubling

Algebraic Attacks

- AES can be expressed as a system of quadratic equations
  - Variables are the plaintext, ciphertext, key, and internal state bits
- Such a system can be solved by linearization
  - Define new variables that are products of existing variables
  - Express original system as linear equations in the new variables
  - Add more equations so the new system has enough linearly independent equations to be solvable
  - Solve the now-linear system using, e.g., Gaussian elimination
- XL: eXtended Linearization attack (Courtois *et al.,* 2000)
- XSL: eXtended Sparse Linearization attack (Courtois & Pieprzyk, 2002)
- Problem
  - The AES linear system is too large to solve in a practical time
- AES prognosis: Safe, but . . .
  - No one has proven there isn't an efficient way to solve the AES linear system

Algebraic Attacks

- Any cipher can be expressed as a set of polynomial functions
  – Ciphertext bit $i = F_i$ (Plaintext, Key)
- Cube attack (Dinur & Shamir, 2009)
  – Requires $2^{d-1}n + n^2$ operations
  – n = number of key bits, d = degree of polynomials F_i
  – Succeeds in a practical time if degree is small enough
  – Requires only black-box access to the cipher
- Breaks reduced-round version of stream cipher Trivium
  – Trivium has a low-degree polynomial representation
- Problem
  – AES almost certainly has a too-high-degree polynomial representation
- AES prognosis: Safe

SAT Solver Attacks

- Any cipher can be represented as a Boolean expression
  - Variables are the plaintext, ciphertext, key, and internal state bits
  - Boolean expression is true if ciphertext = encrypt (plaintext, key)
- SAT solver
  - Given a Boolean expression, finds variable values that satisfy the expression (make the expression true)
  - Modern SAT solvers use sophisticated heuristics to avoid a brute force search
- Problem
  - AES Boolean expression is too large to solve in a practical time
- AES prognosis: Safe, but . . .
  - SAT solvers are getting better all the time
  - Hybrid SAT solver + algebraic attacks might reduce the problem size enough to become practical
  - Little research in this area heretofore

Related-Key Attacks

- Methodology
  - Given plaintext/ciphertext pairs encrypted with two secret keys
  - The keys have a known relationship, e.g., they differ in one bit
  - Find the two keys
- Theoretical breaks of full AES
  - AES-192 in 2^{176} operations; AES-256, 2^{119} (Biryukov *et al.,* 2009)
  - AES-256 in 2^{131} operations (Biryukov *et al.,* 2009)
- Practical breaks of reduced-round AES
  - AES-128, 8 (of 10) rounds, in 2^{48} operations (Gilbert & Peyrin, 2009)
  - AES-256, 9 (of 14) rounds, in 2^{39} operations; 10 rounds, 2^{45} (Biryukov *et al.,* 2010)
- AES prognosis: Theoretically broken, but . . .
  - This is mostly of concern for AES-based hashing, not encryption
  - A practical related-key attack on the full AES is not far off — we're 80% there for AES-128

Side Channel Attacks

- Attack the AES implementation, not the AES algorithm
  - Timing analysis attacks
  - Power analysis attacks
  - Fault injection attacks
- Many AES implementations are highly susceptible
  - Especially those using table lookups
  - Secret keys can be recovered with negligible effort
- Countermeasures
  - Don’t use table lookups
  - Use constant time operations (e.g., Intel’s AES opcodes)
  - Algorithm masking
- AES prognosis: Broken (if poorly implemented)

Prognosis and Recommendations

Prognosis

- DES lasted 22 years before falling to a brute force attack
- AES (Rijndael) has lasted 11 years so far without falling
  - AES will not fall to a brute force attack
  - AES will not fall to traditional attacks (linear, differential)
  - Cracks in the AES edifice are starting to appear from new, nontraditional attacks
- In 10 more years, by 2020:
  - AES will not have fallen, but . . .
  - Enough cryptanalysis will have been published to seriously weaken AES
  - NIST will start a new competition to design the AES-2 block cipher

Recommendations

- When implementing AES, incorporate side channel attack countermeasures
- Do not use any hash function based on AES
- Do not rely on AES to keep military grade secrets secure for more than the next 50 years
- Plan to replace AES with AES-2 in about 10 years