GRAZ UNIVERSITY OF TECHNOLOGY

AES: state of the art

Vincent Rijmen

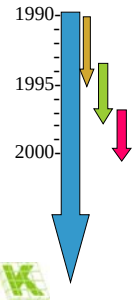
Institute for Applied Information Processing and Communications (IAIK) - Krypto Group

Faculty of Computer Science
Graz University of Technology

Overview

- Design history
- Design philosophy
- AES overview
- AES cryptanalysis
- AES usage

Design history



- PhD Daemen
- PhD Rijmen
- AES process

- 1996: Shark
- 1997: Square
- 1998: BKSQ, Rijndael

General design philosophy

1. Keep it simple
   - Maximize symmetry
     - Over rounds
     - Within round transformation
   - All operations in 1 algebra
     - Finite field GF(256)
   - Small number of building blocks
     - Only add when necessity demonstrated

General design philosophy

2. Performance is important
   - On variety of platforms
   - One security margin is enough
3. Don't reinvent the wheel
   - Coding theory
   - Existing S-boxes

Early feedback

- Square attack [Knudsen]
  - Increase number of rounds
- BKSQ evaluations [Knudsen], [Borst,Preneel]: related key concerns
  - Use more complicated key schedule

Benefits

- Algorithm easy to understand
- Easy to implement
- Provable resistance against specific attacks
  - Proofs are elegant and easy
- Minimize design effort
  - 2-person project (1.5 FTE)

Disadvantages

- Cryptanalysis
  - Simplicity as a design rule is contested
    - Resistance against unknown attacks
    - Risk for catastrophic failure
    - `Surprising' properties
  - Confusion between ease of analysis and ease of cryptanalysis
- Usage
  - Simplicity depends on your point of view
    - Finite fields not supported (yet) by popular scripting languages
    - S-box is bottleneck in hardware
    - Encryption different from decryption (?)

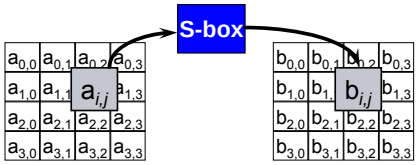
The AES at a glance

- Block cipher:
  - Input blocks of 128 bits
  - Output blocks of 128 bits
  - Key of 128/192/256 bits
- All represented by byte arrays:

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

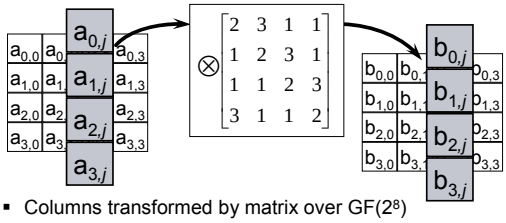
$k_{0,0}$	$k_{0,1}$	$k_{0,2}$	$k_{0,3}$	$k_{0,4}$	$k_{0,5}$	$k_{0,6}$	$k_{0,7}$
$k_{1,0}$	$k_{1,1}$	$k_{1,2}$	$k_{1,3}$	$k_{1,4}$	$k_{1,5}$	$k_{1,6}$	$k_{1,7}$
$k_{2,0}$	$k_{2,1}$	$k_{2,2}$	$k_{2,3}$	$k_{2,4}$	$k_{2,5}$	$k_{2,6}$	$k_{2,7}$
$k_{3,0}$	$k_{3,1}$	$k_{3,2}$	$k_{3,3}$	$k_{3,4}$	$k_{3,5}$	$k_{3,6}$	$k_{3,7}$

Round step 1: SubBytes



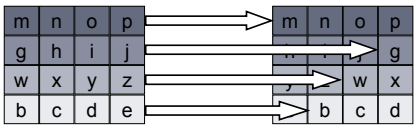
- Bytes are transformed by invertible S-box.
- One S-box (lookup table) for complete cipher

Round step 3: MixColumns



- Columns transformed by matrix over GF(2^8)
- High intra-column diffusion based on theory of error-correcting (MDS) codes

Round step 2: ShiftRows



- Rows are shifted over 4 different offsets
- High diffusion over multiple rounds:
  - Interaction with MixColumns

Round step 4: AddRoundKey

$$\begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix} + \begin{bmatrix} k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3} \\ k_{1,0} & k_{1,1} & k_{1,2} & k_{1,3} \\ k_{2,0} & k_{2,1} & k_{2,2} & k_{2,3} \\ k_{3,0} & k_{3,1} & k_{3,2} & k_{3,3} \end{bmatrix} = \begin{bmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3} \\ b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3} \\ b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3} \end{bmatrix}$$

- Makes round function key-dependent

State of the cryptanalysis

Known attacks

- Linear, differential cryptanalysis: covered by the wide trail design strategy
  - And all known variants
- Square attack: covered
  - Breaks reduced-round versions up to 6/7 rounds (out of 10/12 rounds)

Unknown attacks

- (Very) simple description [Murphy & Robshaw, '00]
- BES (Embedding in larger map) [Murphy & Robshaw, '02]
- Rewriting of equations
- No impact on security demonstrated (yet)

Unknown attacks

- Symmetry in the S-box [Fuller & Millan '02]
- Description with continued fractions [Ferguson, Schroeppel & Whiting, '01]

$$x = K + \sum \cfrac{C_1}{K^* + \sum \cfrac{C_2}{K^* + \sum \cfrac{C_3}{K^* + \sum \cfrac{C_4}{K^* + \sum \cfrac{C_5}{K + p^*}}}}}$$

- No impact on security demonstrated

Unknown attacks

Algebraic attacks (XSL)

1. Write out equations, round by round
   - Many intermediate variables
   - Equations of low degree (2, 3)
2. Solve for the unknown key
   - Some estimates predict breakthrough

Algebraic attack: problems

- No successful application known (block cipher)
- No consensus on the exact attack algorithm
- Several variants demonstrated to be impossible or impractical
  - [Diem 04] (XL)
  - [Ars et al. 04] (XL)
  - [Cid et al. 05] (XSL)

Strange bias

- [Filiol 03]
- Uses repetition codes to select chosen plaintexts
- Reports large bias in generated ciphertexts
- Devastating attack (2^{32} chosen plaintexts)

- Results not reproducible
- Seems to have gone away

Cache-timing attacks

- [Bernstein]

- Cache miss causes variations in execution time
  - Can be used to recover the secret key

- Implementation issue
  - "All fast implementations of AES are vulnerable"

- Intel? ;-)
- Needs to be investigated: impact and countermeasures

State of the usage

- AES is a block cipher
  - Primary use: encryption
  - Secondary use: MAC, PRNG

- Key lengths of 128, 192, 256 bits

- Block length of 128 bit
  - In most applications: not an easy drop-in for DES

State of the usage

- USA administration
  - Original scope: sensitive data
  - CNSS June 2003: Classified data
    - Up to level SECRET
    - Up to TOP SECRET with key 192, 256
- RFCs
  - S/MIME, TLS, MAC, key wrap, pseudo-random function, …

- IEEE 802.11i (wep)
- ISO 18033-3: block ciphers

State of the usage

- Winzip and similar tools
- Some Internet banking software (Belgium)
- Backup software, …
- RfID tags

Reasons for reluctance

- Investment in deployed products
- Investment in designed algorithms

- Not always based on correct arguments
  - Myth of the attack/anomaly
  - Myth of the low performance

AES Performance in hardware

- Top-speed implementations

Mbit/s	MHz	gates
1820	100	173000
2600	224	21000
7500	32	256000

AES performance: real-world platform

- For smartcard environments (low area)
- Standard cell, 100 MHz.

Mbit/s	Gate equivalents
122	5711
164	9530
267	16275

Tiny AES (Tina)

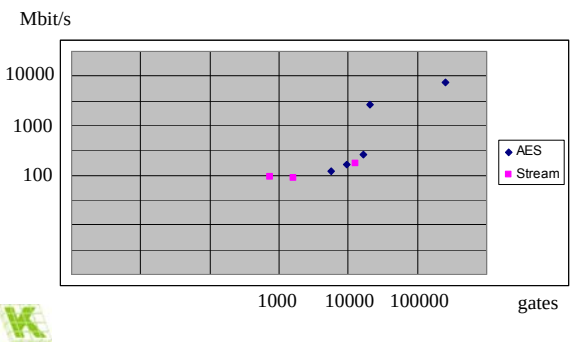
- Features:
  - Encryption and decryption, 128-bit key
  - Microcontroller interface
- Specs:
  - 0.27 mm^2 in 0.35 µm (4800 gate eq.)
  - 3 µA @ 100kHz, 1.5V
  - 100 encr./s (12.8 kbit/s)

Performance stream ciphers

- Gate counts [Batina et al., 2004]

E0	1637	90 Mbit/s
A5/1	752	93 Mbit/s
RC4	13000	171 Mbit/s

Overview



New developments

- Recent breakthrough in cryptanalysis of SHA-1 [Wang et al.]
- Replacement needed
  - SHA-256 or more different design?
- AES design philosophy is substantially different
  - Needs rate ½ hashing scheme (slow)

Conclusions

- A cryptanalytic attack seems further away than it seemed 2 years ago
  - We can never prove that an attack can never work
- Usage is still taking off
  - Replacement of DES rarely happens
  - Some good opportunities are arising