Pragmatism vs. Elegance

comparing two approaches to Simple Power Analysis on AES

Valentina Banciu Elisabeth Oswald

University of Bristol, Department of Computer Science
Merchant Venturers Building
Woodland Road, BS8 1UB, Bristol, UK
{valentina.banciu, elisabeth.oswald}@bristol.ac.uk

COSADE 2014

AES: Advanced Encryption Standard

- Symmetric-key block cipher
- Key size: **128**, 192, and 256 bits
- Block size: **128** bits

- Announced by the NIST as U.S. FIPS PUB 197 on 26.11.2001

Classic Simple Power Analysis (SPA) Attacks

- Classic SPA attacks can be compared to brute-force
- Side-channel information makes this approach feasible against modern-day ciphers
- Most common leakage models: **8-bit Hamming weight** and Hamming distance

Classic Simple Power Analysis (SPA) Attacks

- Classic SPA attacks can be compared to brute-force
- Side-channel information makes this approach feasible against modern-day ciphers
- Most common leakage models: **8-bit Hamming weight** and Hamming distance

- In practice, side-channel information cannot be measured perfectly (i.e., **noise**)
  - average over a few measurements
  - drop information with high error probability
  - encapsulate side-channel information as a set of (consecutive) possible values, **always containing the correct value**

Classic SPA Attacks on AES

Mangard's Attack

- Targets Key Schedule
- 5 consecutive round keys
- Side-channel information: **correct HW value** or **no information at all**

ASCA Attack

- Targets Encryption Rounds
- All encryption rounds
- Side-channel information: **sets of up to 3 possible HW values**

Classic SPA Attacks on AES

Mangard's Attack

- Targets Key Schedule
- 5 consecutive round keys
- Side-channel information: **correct HW value** or **no information at all**
- Result: Reduced keyspace

ASCA Attack

- Targets Encryption Rounds
- All encryption rounds
- Side-channel information: **sets of up to 3 possible HW values**
- Result: The correct key or nothing at all

Pragmatism vs. Elegance

Our goals:

- require less side-channel information
- tolerate a better error rate

Pragmatism vs. Elegance

Our goals:

- require less side-channel information
- tolerate a better error rate

Our approach:

- Combine information of Encryption Rounds *and* Key Schedule of a single round
- Side-channel information: sets of up to **5** possible values

The AES Encryption algorithm

Encryption Rounds

- Initial Round
  - AddRoundKey
- Intermediate Rounds
  - SubBytes
  - ShiftRows
  - MixColumns
  - AddRoundKey
- Final Round
  - SubBytes
  - ShiftRows
  - AddRoundKey.

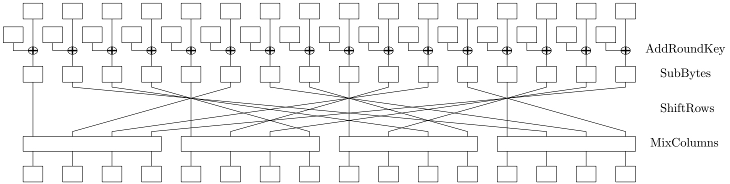
The AES Encryption algorithm

Encryption Rounds

- Initial Round
  - **AddRoundKey**
- Intermediate Rounds
  - **SubBytes**
  - **ShiftRows**
  - **MixColumns**
  - AddRoundKey
- Final Round
  - SubBytes
  - ShiftRows
  - AddRoundKey

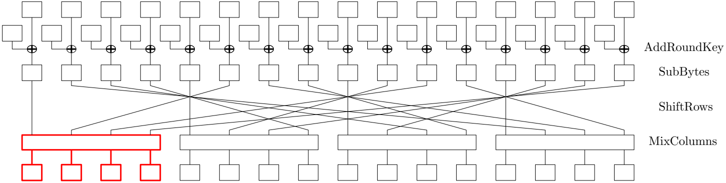
The AES Encryption algorithm

Attacking the Encryption Round Function



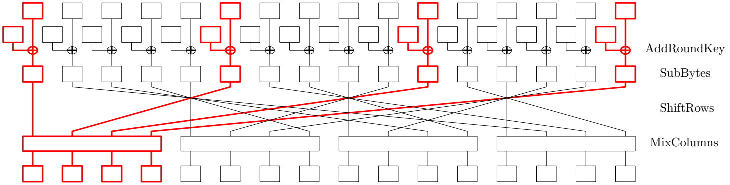
The AES Encryption algorithm

Attacking the Encryption Round Function



The AES Encryption algorithm

Attacking the Encryption Round Function



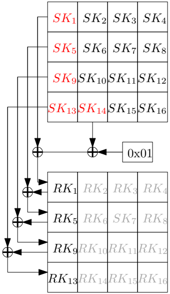
The AES Encryption algorithm

Key Schedule

- Represent the secret key as a set of 4-byte words
- Derive one new word at a time from two previous words
- Operations:
  - Circular shift of word bytes
  - S-box lookup
  - XOR-ing with a round constant
  - XOR-ing two words

The AES Encryption algorithm

Attacking the Key Expansion Function



The AES Encryption algorithm

Attacking the Key Expansion Function

SK_1	SK_2	SK_3	SK_4
SK_5	SK_6	SK_7	SK_8
SK_9	SK_{10}	SK_{11}	SK_{12}
SK_{13}	SK_{14}	SK_{15}	SK_{16}

The AES Encryption algorithm

Attacking the Key Expansion Function

SK_1	SK_2	SK_3	SK_4
SK_5	SK_6	SK_7	SK_8
SK_9	SK_{10}	SK_{11}	SK_{12}
SK_{13}	SK_{14}	SK_{15}	SK_{16}

The AES Encryption algorithm

Attacking the Key Expansion Function

SK_1	SK_2	SK_3	SK_4
SK_5	SK_6	SK_7	SK_8
SK_9	SK_{10}	SK_{11}	SK_{12}
SK_{13}	SK_{14}	SK_{15}	SK_{16}

The AES Encryption algorithm

Attacking the Key Expansion Function

SK_1	SK_2	SK_3	SK_4
SK_5	SK_6	SK_7	SK_8
SK_9	SK_{10}	SK_{11}	SK_{12}
SK_{13}	SK_{14}	SK_{15}	SK_{16}

Results

Previous results

Mangard's Attack (attacking 5 consecutive Round Keys, 1000 experiments)

HW used	**100%**	**95%**	**50%**
key space	11	16.5	$1.7 \cdot 10^{12}$
time	5m30s	5m	5h

ASCA Attack success rate (known PT and CT, 100 experiments)

# rounds	**2**	**4**	**6**
consecutive	0%	100%	100%
random	20%	60%	100%

Results

Previous results

Mangard's Attack (attacking 5 consecutive Round Keys, 1000 experiments)

HW used	100%	95%	50%
key space	11	16.5	$1.7 \cdot 10^{12}$
time	5m30s	5m	5h

ASCA Attack success rate (known PT and CT, 100 experiments)

# rounds	2	4	6
consecutive	0%	100%	100%
random	20%	60%	100%

Our results

(Using leaks from one encryption round and one round key. The PT is known. Averaged over 500 experiments)

	Encryption only		Key Schedule only		Combined	
Set size	**Key space**	**Execution time**	**Key space**	**Execution time**	**Key space**	**Execution time**
1	1	0.02 s	2^{58}	0.4 s	1	0.03 s
2	2^{20}	2.9 s	2^{74}	5 s	2^{12}	27 s
3	2^{48}	73.9 s	2^{95}	10 s	2^{13}	4 m
4	2^{64}	27 m	2^{106}	30 s	2^{52}	35 m
5	2^{116}	2.5 h	2^{115}	40 s	2^{60}	12 h

Results

Previous results

Mangard's Attack (attacking 5 consecutive Round Keys, 1000 experiments)

HW used	**100%**	**95%**	**50%**
key space	11	16.5	$1.7 \cdot 10^{12}$
time	5m30s	5m	5h

ASCA Attack success rate (known PT and CT, 100 experiments)

# rounds	**2**	**4**	**6**
consecutive	0%	100%	100%
random	20%	60%	100%

Our results

(Using leaks from one encryption round and one round key. The PT is known. Averaged over 500 experiments)

	Encryption only		**Key Schedule only**		**Combined**	
Set size	**Key space**	**Execution time**	**Key space**	**Execution time**	**Key space**	**Execution time**
1	1	0.02 s	2^{58}	0.4 s	1	0.03 s
2	2^{20}	2.9 s	2^{74}	5 s	2^{12}	27 s
3	2^{48}	73.9 s	2^{95}	10 s	2^{13}	4 m
4	2^{64}	27 m	2^{106}	30 s	2^{52}	35 m
5	2^{116}	2.5 h	2^{115}	40 s	2^{60}	12 h

Results

Previous results

Mangard's Attack (attacking 5 consecutive Round Keys, 1000 experiments)

HW used	100%	95%	50%
key space	11	16.5	$1.7 \cdot 10^{12}$
time	5m30s	5m	5h

ASCA Attack success rate (known PT and CT, 100 experiments)

# rounds	2	4	6
consecutive	0%	100%	100%
random	20%	60%	100%

Our results

(Using leaks from one encryption round and one round key. The PT is known. Averaged over 500 experiments)

	Encryption only		Key Schedule only		Combined	
Set size	**Key space**	**Execution time**	**Key space**	**Execution time**	**Key space**	**Execution time**
1	1	0.02 s	2^{58}	0.4 s	1	0.03 s
2	2^{20}	2.9 s	2^{74}	5 s	2^{12}	27 s
3	2^{48}	73.9 s	2^{95}	10 s	2^{13}	4 m
4	2^{64}	27 m	2^{106}	30 s	2^{52}	35 m
5	2^{116}	2.5 h	2^{115}	40 s	2^{60}	12 h

Results

Previous results

Mangard's Attack (attacking 5 consecutive Round Keys, 1000 experiments)

HW used	100%	95%	50%
key space	11	16.5	$1.7 \cdot 10^{12}$
time	5m30s	5m	5h

ASCA Attack success rate (known PT and CT, 100 experiments)

# rounds	2	4	6
consecutive	0%	100%	100%
random	20%	60%	100%

Our results

(Using leaks from one encryption round and one round key. The PT is known. Averaged over 500 experiments)

	Encryption only		Key Schedule only		Combined	
Set size	**Key space**	**Execution time**	**Key space**	**Execution time**	**Key space**	**Execution time**
1	1	0.02 s	2^{58}	0.4 s	1	0.03 s
2	2^{20}	2.9 s	2^{74}	5 s	2^{12}	27 s
3	2^{48}	73.9 s	2^{95}	10 s	2^{13}	4 m
4	2^{64}	27 m	2^{106}	30 s	2^{52}	35 m
5	2^{116}	2.5 h	2^{115}	40 s	2^{60}	12 h

Conclusion

By combining side-channel information from both encryption and key schedule, we are able to:

- use side-channel information from only one round
- tolerate better error rates

Conclusion

By combining side-channel information from both encryption and key schedule, we are able to:

- use side-channel information from only one round
- tolerate better error rates

Moreover, our attack gives a clear indication of the key space that needs to be brute-forced

Thank you for your attention