Improved Side-Channel Collision Attacks on AES

Andrey Bogdanov

Chair for Communication Security
Ruhr-University Bochum, Germany
abogdanov@crypto.rub.de

Selected Areas in Cryptography, Ottawa, 2007

Table of Contents

Motivation

Framework

- DPA often requires several hundred measurements:
  - The new attack to require a lower number of measurements
- SPA seems unrealistic for most symmetric ciphers:
  - The new attack to be more realistic

Standard collision attacks

- Require a lower number of measurements (about 40)
- Are much more realistic than SPA
- **Improve the standard collisions attacks!**

Basic Collision Attack (Schramm et al): Outline

Attack Outline

- Generate random plaintexts of a special form
- Perform N measurements and detect simple collisions
- 16 simple collisions needed
  (construct 16 nonlinear equations)
- Solve the equations using pre-computed tables and test key candidates using a plaintext-ciphertext pair

Basic Attack: Notation

$B = \text{MixColumn}(A), A = \text{ShiftRows}(\text{SubBytes}(P \oplus K))$

$$\begin{pmatrix} b_{0j} \\ b_{1j} \\ b_{2j} \\ b_{3j} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \times \begin{pmatrix} a_{0j} \\ a_{1j} \\ a_{2j} \\ a_{3j} \end{pmatrix}$$

b_{00}

If $P = (p_{ij})$ is plaintext and $K = (k_{ij})$ is subkey, then

$$\begin{aligned} b_{00} &= 02 \cdot a_{00} \oplus 03 \cdot a_{10} \oplus 01 \cdot a_{20} \oplus 01 \cdot a_{30} = \\ &= 02 \cdot S(p_{00} \oplus k_{00}) \oplus 03 \cdot S(p_{11} \oplus k_{11}) \\ &\quad \oplus 01 \cdot S(p_{22} \oplus k_{22}) \oplus 01 \cdot S(p_{33} \oplus k_{33}). \end{aligned}$$

Basic Attack: Simple Collisions

$b_{00} = b'_{00}$

Second round:
$S(b_{00} \oplus k_{00}) = S(b'_{00} \oplus k_{00})$ detected $\Rightarrow$
$b_{00} \oplus k_{00} = b'_{00} \oplus k_{00} \Rightarrow$
$b_{00} = b'_{00}$

Collision equation

For two plaintexts P and P' with $p_{00} = p_{11} = p_{22} = p_{33} = \delta$ and $p'_{00} = p'_{11} = p'_{22} = p'_{33} = \epsilon$, $\delta \neq \epsilon$, one obtains the following, provided $b_{00} = b'_{00}$:

$$02 \cdot S(k_{00} \oplus \delta) \oplus 03 \cdot S(k_{11} \oplus \delta) \oplus 01 \cdot S(k_{22} \oplus \delta) \oplus 01 \cdot S(k_{33} \oplus \delta)$$
$$= 02 \cdot S(k_{00} \oplus \epsilon) \oplus 03 \cdot S(k_{11} \oplus \epsilon) \oplus 01 \cdot S(k_{22} \oplus \epsilon) \oplus 01 \cdot S(k_{33} \oplus \epsilon)$$

Basic Attack: Attack Complexity

Collision probability

The probability that after N executions at least one collision $b_{00} = b'_{00}$ occurs in a single byte is:

$$p_N = 1 - \prod_{l=0}^{N-1}(1 - l/2^8)$$

Complexity

- The attacker needs at least 16 collisions, 4 for each column of B, so $p_N^{16} \geq 1/2$ and $N \approx 40$
- About 540 MByte pre-computed tables
- Chosen-plaintext possibility needed

Improved Attack: Two Simple Mathematical Objects

Systems of binomial linear equations

$$S_m: \quad \begin{cases} k_{i_1,\,j_1} \oplus k_{i_2,\,j_2} = \Delta_{(i_1,\,j_1),\,(i_2,\,j_2)} \\ \dots \\ k_{i_{2m-1},\,j_{2m-1}} \oplus k_{i_{2m},\,j_{2m}} = \Delta_{(i_{2m-1},\,j_{2m-1}),(i_{2m},\,j_{2m})} \end{cases}$$

Definition (associated graphs)

A random graph $G_m = \langle V, E \rangle$ is associated with the random system S_m of linear equations, where $V = \{k_{0,0}, k_{0,1}, \dots, k_{3,3}\}$ is the set of 16 vertices of G_m and the edge $(k_{i_1,\,j_1}, k_{i_2,\,j_2})$ belongs to the edge set E iff the binomial equation

$$k_{i_1,\,j_1} \oplus k_{i_2,\,j_2} = \Delta_{(i_1,\,j_1),(i_2,\,j_2)}$$

belongs to the system S_m, $|E| = m$.

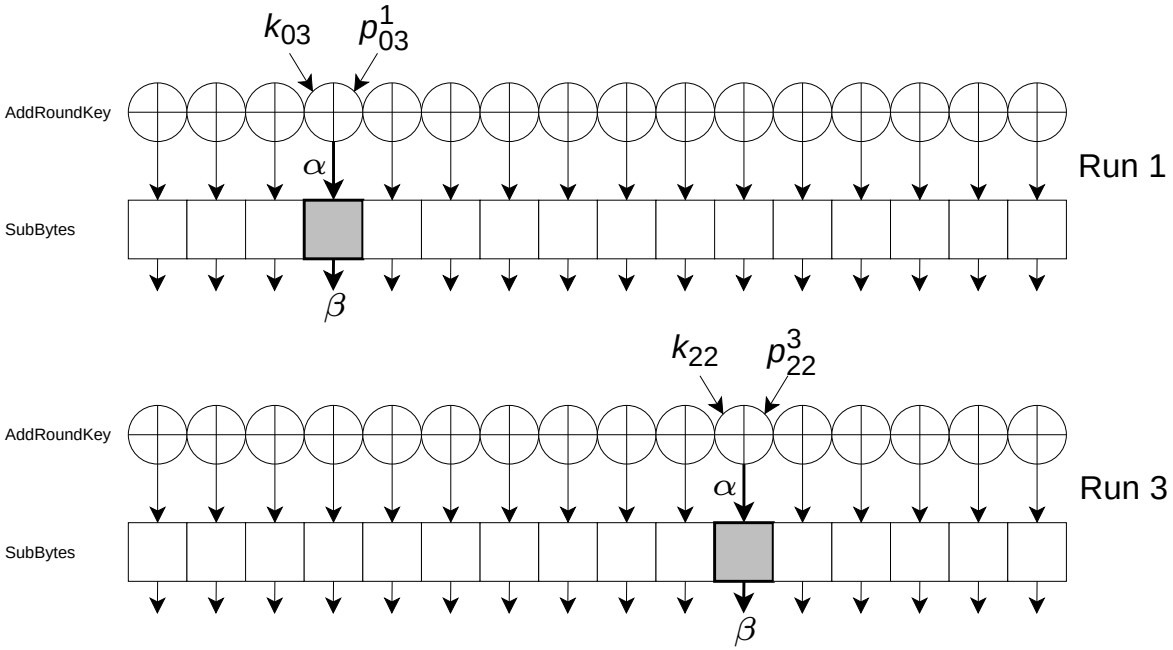
Improved Attack: Outline

Attack Outline

- Input random plaintexts $\Rightarrow$ known-plaintext attack
- Detect *generalized collisions* in t executions
- Construct m linear binomial equations S_m from the collisions
- Construct the graph G_m associated with S_m
  (16 vertices and m edges)
- Find q connected components in G_m
- Recover 16 key bytes by trying 2^{8q} key candidates

Attack Outline: 1) Generalized Collisions $\Rightarrow$ Linear Equations

t measurements $\Rightarrow$ generalized collisions



$$\Downarrow$$

$$k_{03} \oplus k_{22} = p^1_{03} \oplus p^3_{22} = \Delta_{03,22}$$

$\Rightarrow$

13 equations (S_m):

$$\begin{cases}
k_{00} \oplus k_{02} = \Delta_{00,02} \\
k_{00} \oplus k_{13} = \Delta_{00,13} \\
k_{01} \oplus k_{03} = \Delta_{01,03} \\
k_{01} \oplus k_{23} = \Delta_{01,23} \\
k_{02} \oplus k_{23} = \Delta_{02,23} \\
k_{03} \oplus k_{20} = \Delta_{03,20} \\
k_{10} \oplus k_{12} = \Delta_{10,12} \\
k_{10} \oplus k_{30} = \Delta_{10,30} \\
k_{10} \oplus k_{22} = \Delta_{10,22} \\
k_{11} \oplus k_{21} = \Delta_{11,21} \\
k_{12} \oplus k_{22} = \Delta_{12,22} \\
k_{32} \oplus k_{22} = \Delta_{32,22} \\
k_{32} \oplus k_{22} = \Delta_{32,22} \\
k_{32} \oplus k_{31} = \Delta_{32,31}
\end{cases}$$

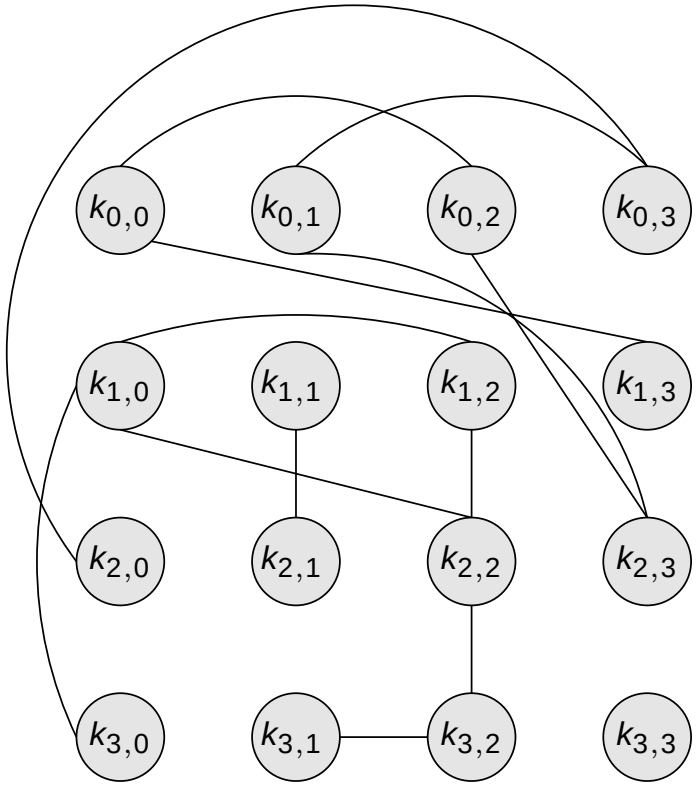
Attack Outline: 2) Linear Equations $\Rightarrow$ Associated Graph

$m = 13$ linear equations (S_m):

$$\begin{cases} k_{00} \oplus k_{02} = \Delta_{00,02} \\ k_{00} \oplus k_{13} = \Delta_{00,13} \\ k_{01} \oplus k_{03} = \Delta_{01,03} \\ k_{01} \oplus k_{23} = \Delta_{01,23} \\ k_{02} \oplus k_{23} = \Delta_{02,23} \\ k_{03} \oplus k_{20} = \Delta_{03,20} \\ k_{10} \oplus k_{12} = \Delta_{10,12} \\ k_{10} \oplus k_{30} = \Delta_{10,30} \\ k_{10} \oplus k_{22} = \Delta_{10,22} \\ k_{11} \oplus k_{21} = \Delta_{11,21} \\ k_{12} \oplus k_{22} = \Delta_{12,22} \\ k_{32} \oplus k_{22} = \Delta_{32,22} \\ k_{32} \oplus k_{22} = \Delta_{32,22} \\ k_{32} \oplus k_{31} = \Delta_{32,31} \end{cases}$$

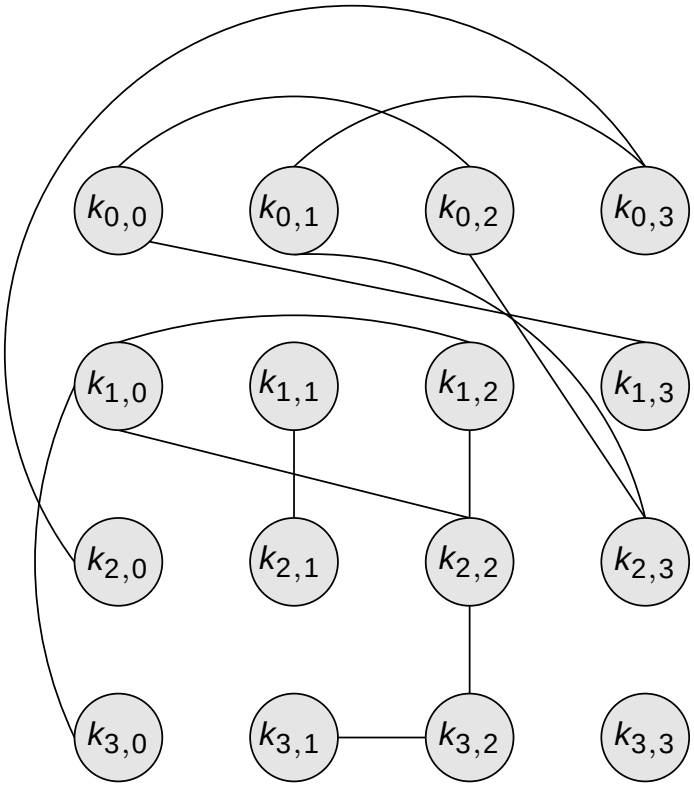
$\Rightarrow$

Construct associated graph G_m:



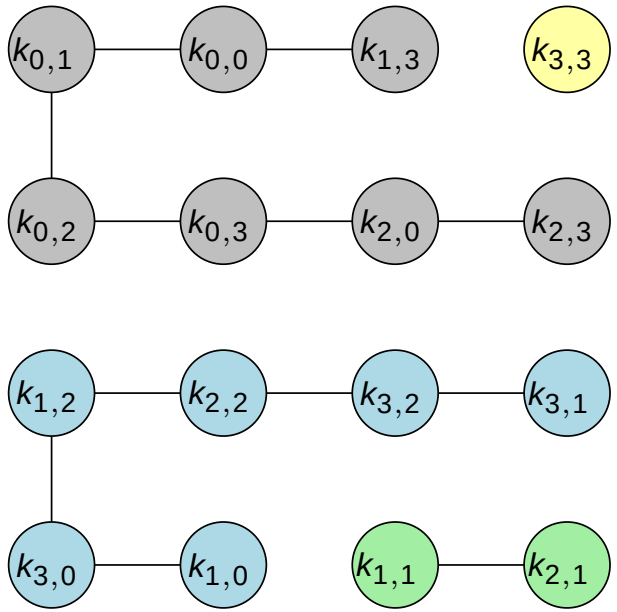
Attack Outline: 3) Associated Graph $\Rightarrow$ Connected Components

Associated graph G_m:



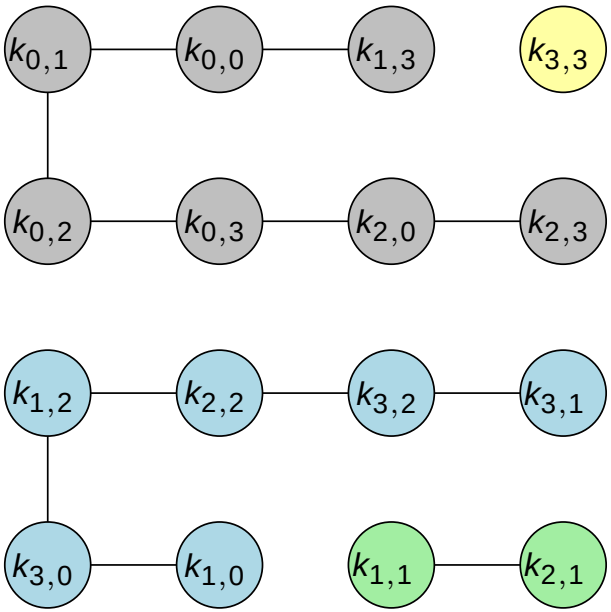
$\Rightarrow$

Find connected components in G_m:



Attack Outline: 4) Connected Components $\Rightarrow$ Key Bytes

Connected components in G_m:



$\Rightarrow$

Key recovery:

- $q = 4$ independent subsystems ($q = 4$ connected components) :
  - $\{\mathbf{k_{0,0}}, k_{2,3}, k_{0,1}, k_{0,2}, k_{0,3}, k_{1,3}, k_{2,0}\}$,
  - $\{\mathbf{k_{2,2}}, k_{3,0}, k_{3,1}, k_{3,2}, k_{1,0}, k_{1,2}\}$,
  - $\{\mathbf{k_{1,1}}, k_{2,1}\}$,
  - $\{\mathbf{k_{3,3}}\}$
- 4 bytes have to be tried
- Max. 2^{32} offline operations to recover the full encryption key

Attack Parameters: m, t and q

Questions

- How many edges (m) does one obtain after t measurements?
- How many connected components (q) does one get after t executions?
- How many measurements (t) are needed on average to make the offline stage feasible?
- What is the success probability of the attack?

Basic Properties of Systems and Graphs

Proposition 1

The maximal rank of S_m is 15, $rank(S_m) \leq 15$.

Proposition 2

The system S_m is of the maximal rank 15 iff its associated graph G_m is connected.

Proposition 3

Let $G = \langle V, E \rangle$ be a non-directed graph with n vertices, $|V| = n$. If $|E| > \binom{n-1}{2}$, the graph G is connected.

Number of Random Equations

Proposition 4

If generalized byte collision in AES are always detectable, the expected number $E(m)$ of edges in G_m (equivalently, the expected number of binomial equations in S_m) for the first round of AES after $t \geq 1$ measurements is

$$E(m) = 120 \cdot \left(1 - \left(\frac{119}{120}\right)^{16t - 256 + 256 \cdot \exp\left\{16t \cdot \ln \frac{255}{256}\right\}}\right).$$

Measurements, t	4	5	6	7	8	11	29
1R collisions, N_{1R}	7.27	11.18	15.82	21.14	28.12	48.55	249.64
Edges, $E(m)$	7.09	10.72	14.88	19.46	24.36	40.07	105.14

Number of Connected Components and Results

Measurements, t	5	6	7	8
Number of edges in G_m, m	10.72	14.88	19.46	24.36
Connected components of G_m, q	5.88	3.74	2.20	1.43
Offline complexity $\leq$ 40 bit	37.34	37.15	34.74	30.32
Success probability $\leq$ 40 bit	0.372	0.854	0.991	0.999
Offline complexity $\leq$ 48 bit	45.50	44.30	41.14	30.32
Success probability $\leq$ 48 bit	0.548	0.927	0.997	0.999

Possible Optimization

Optimization ideas

- Detect collisions in the key schedule S-box applications
- Detect collisions between the first and second rounds
  - Diagonals in the 1st round correspond to columns in the 2nd one
  - If a 1st round diagonal is covered by a connected component, inputs to the corresponding column of the 2nd round are known
- Together with the key schedule relations, this can result in new linear equations on $\{k_{ij}\}$

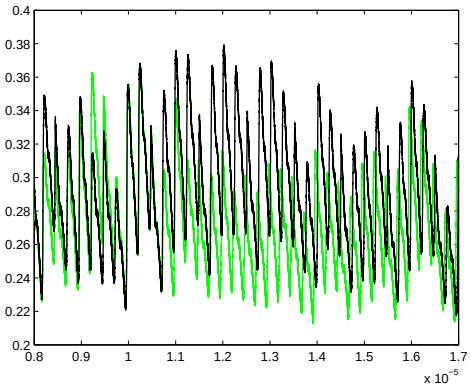
Practicability: Preconditions and Methods

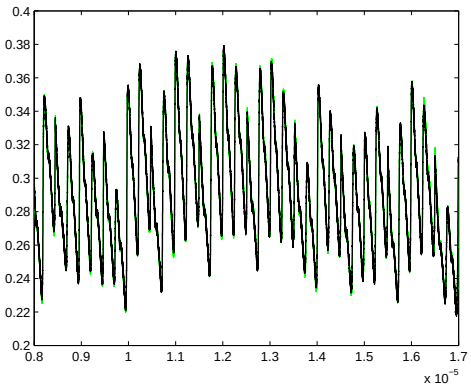
- All instances of the AES S-box have to be implemented *in a similar way*, e.g.:
  - The S-box is a separate routine
  - Low-end real-world embedded systems such as 8-bit controllers, where it is automatically fulfilled
- The attacker has to know *when* the S-boxes leak
- *High-precision* measurement setup required
  - Probably a 12-bit samples instead of traditional 8-bit ones
  - Averaging techniques may be needed to increase precision

Practicability: Example of measurements

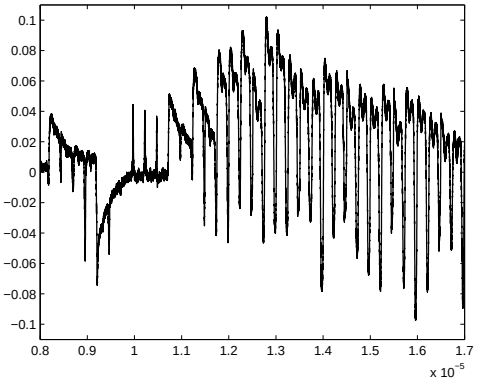
Kasper, Biryukov, Bogdanov and Khovratovich, CHES 2007

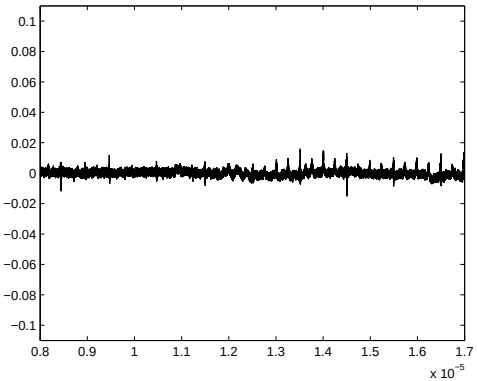
Power curves





Differences





Conclusions and Outlook

- Several improved collision attacks proposed
- These are known-plaintext attacks
- 7 measurements, $2^{34.74}$ offline operations, success probability 0.99
- 6 measurements, $2^{37.15}$ offline operations, success probability 0.854
- 5 measurements with
  - an offline complexity of $2^{45.5}$ and a probability of 0.548 or
  - an offline complexity of $2^{37.34}$ and a probability of 0.372
- Further improvements may be possible:
  - Consider nonlinear collisions over ≥ 2 rounds
  - Solve the resulting nonlinear equation systems