Revisiting Related-Key Boomerang attacks on AES using computer-aided tool

Patrick Derbez, Marie Euler, Pierre-Alain Fouque, **Hoa Nguyen**

Univ Rennes, CNRS, IRISA

December, 2022

Updated results on AES-192

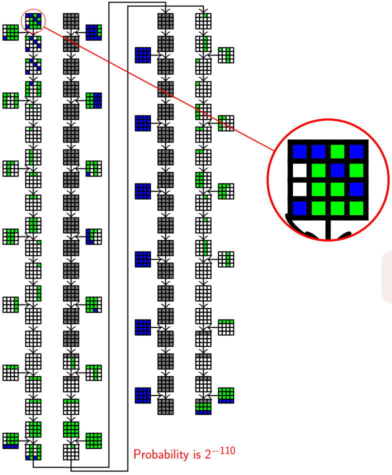
Key Size	Rounds	Time	Data	Memory	Type	Ref
192 bits	8/12	2^{172}	2^{107}	2^{96}	MITM	[Derbez et al., 2013]
	9/12	$2^{182.5}$	2^{117}	$2^{165.5}$		[Li et al., 2014]
	10/12	2^{183}	2^{124}	N/A	Related-key Rectangle	[Kim et al., 2007]
		2^{156}	2^{156}	2^{65}	Related-key Differential	[Gérault et al., 2018]
	12/12	$2^{190.16}$	2^{80}	2^{8}	Biclique	[Bogdanov et al., 2011]
		$2^{190.83}$	2	2^{60}		[Bogdanov et al., 2014]
		$2^{189.76}$	2^{48}	2^{60}		[Tao and Wu, 2015]
		2^{176}	2^{123}	2^{152}	Related-key Boomerang	[Biryukov and Khovratovich, 2009]

Updated results on AES-192

Key Size	Rounds	Time	Data	Memory	Type	Ref
192 bits	8/12	2^{172}	2^{107}	2^{96}	MITM	[Derbez et al., 2013]
	9/12	$2^{182.5}$	2^{117}	$2^{165.5}$		[Li et al., 2014]
	10/12	2^{183}	2^{124}	N/A	Related-key Rectangle	[Kim et al., 2007]
		2^{156}	2^{156}	2^{65}	Related-key Differential	[Gérault et al., 2018]
	12/12	$2^{190.16}$	2^{80}	2^{8}	Biclique	[Bogdanov et al., 2011]
		$2^{190.83}$	2	2^{60}		[Bogdanov et al., 2014]
		$2^{189.76}$	2^{48}	2^{60}		[Tao and Wu, 2015]
		2^{176}	2^{123}	2^{152}	Related-key Boomerang	[Biryukov and Khovratovich, 2009]
		2^{124}	2^{124}	$2^{79.8}$	Related-key Boomerang	This work

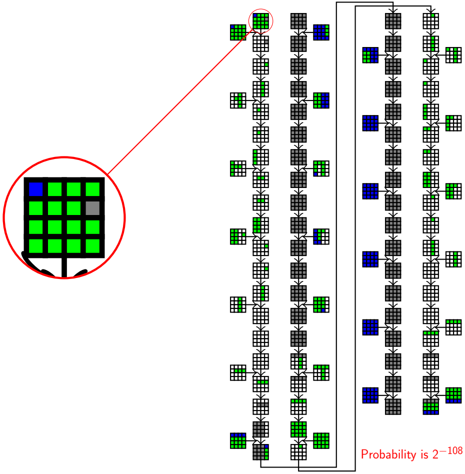
Its time complexity is 2^{52} times lower than the best-known attack!

The best-known attack (A) vs Our attack (B)



(A)

$$\sum \square_A < \sum \square_B$$



(B)

$\square$ = A known difference; $\square$ = Zero difference; $\blacksquare$ = A fixed difference

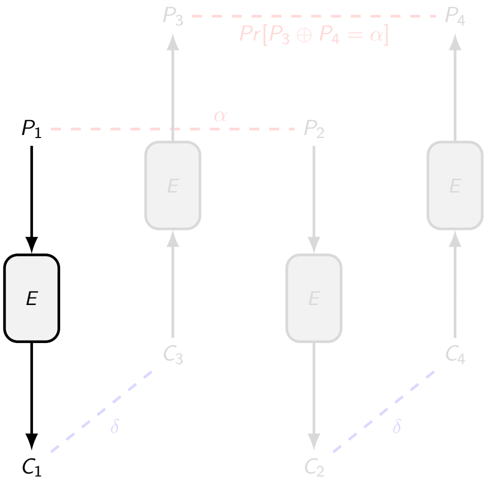
Overview

1. The boomerang attack
2. Previous works
3. Application to AES
4. Results

Boomerang Distinguisher 101

- The Boomerang attack [Wagner, 1999]
  - *When you send it properly,*
    it always comes back to you

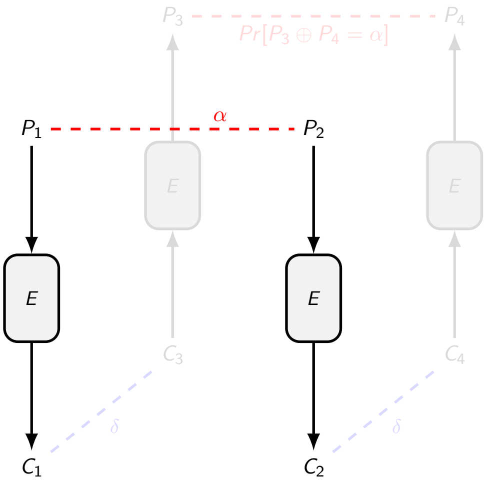
Boomerang Distinguisher 101



1. Pick P_1, ask for $C_1 = E(P_1)$
2. $P_2 = P_1 \oplus \alpha$, ask for C_2
3. $C_3 = C_1 \oplus \delta$, $C_4 = C_2 \oplus \delta$
4. Ask for $P_3 = E^{-1}(C_3)$, $P_4 = E^{-1}(C_4)$
5. Check if $P_3 \oplus P_4 = \alpha$

A distinguisher if α comes back
more often than a *random permutation*!

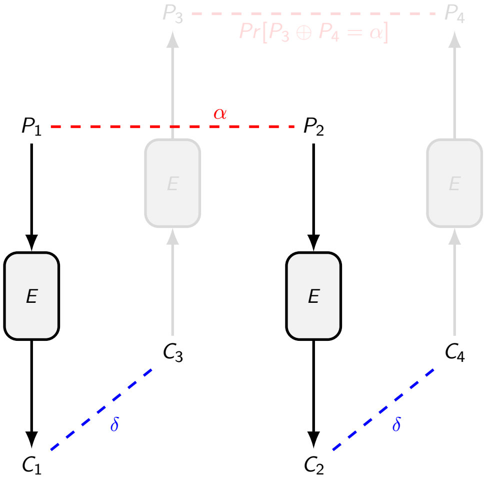
Boomerang Distinguisher 101



1. Pick P_1, ask for $C_1 = E(P_1)$
2. $P_2 = P_1 \oplus \alpha$, ask for C_2
3. $C_3 = C_1 \oplus \delta$, $C_4 = C_2 \oplus \delta$
4. Ask for $P_3 = E^{-1}(C_3)$, $P_4 = E^{-1}(C_4)$
5. Check if $P_3 \oplus P_4 = \alpha$

A distinguisher if α comes back more often than a *random permutation*!

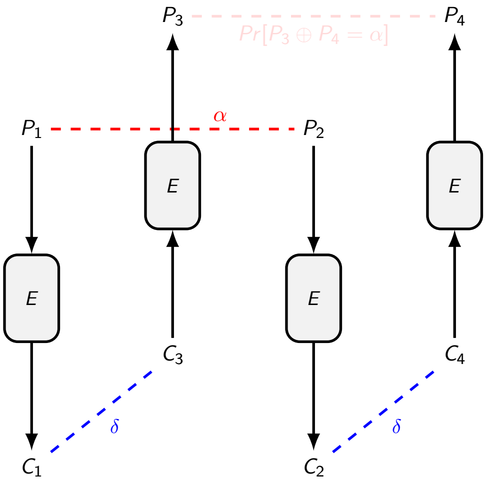
Boomerang Distinguisher 101



1. Pick P_1, ask for $C_1 = E(P_1)$
2. $P_2 = P_1 \oplus \alpha$, ask for C_2
3. $C_3 = C_1 \oplus \delta$, $C_4 = C_2 \oplus \delta$
4. Ask for $P_3 = E^{-1}(C_3)$, $P_4 = E^{-1}(C_4)$
5. Check if $P_3 \oplus P_4 = \alpha$

A distinguisher if α comes back more often than a *random permutation*!

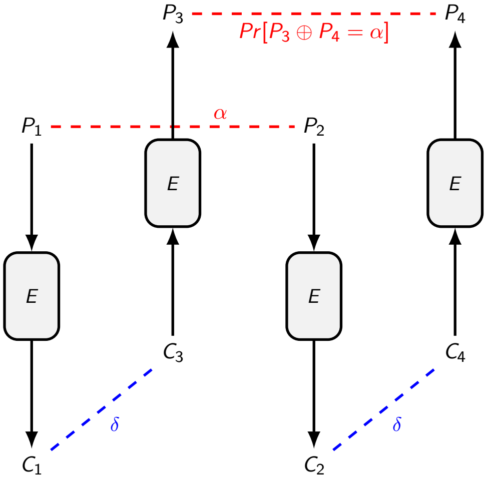
Boomerang Distinguisher 101



1. Pick P_1, ask for $C_1 = E(P_1)$
2. $P_2 = P_1 \oplus \alpha$, ask for C_2
3. $C_3 = C_1 \oplus \delta$, $C_4 = C_2 \oplus \delta$
4. Ask for $P_3 = E^{-1}(C_3)$, $P_4 = E^{-1}(C_4)$
5. Check if $P_3 \oplus P_4 = \alpha$

A distinguisher if α comes back
more often than a *random permutation*!

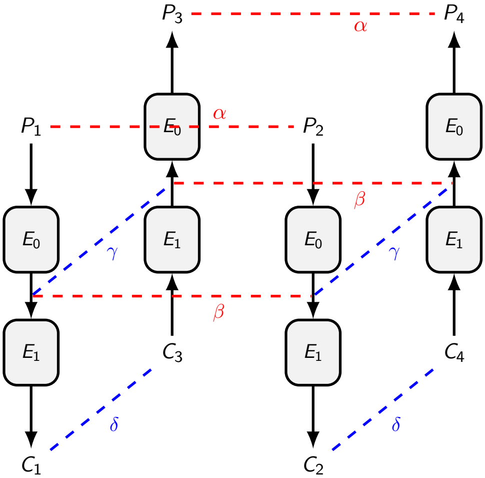
Boomerang Distinguisher 101



1. Pick P_1, ask for $C_1 = E(P_1)$
2. $P_2 = P_1 \oplus \alpha$, ask for C_2
3. $C_3 = C_1 \oplus \delta$, $C_4 = C_2 \oplus \delta$
4. Ask for $P_3 = E^{-1}(C_3)$, $P_4 = E^{-1}(C_4)$
5. Check if $P_3 \oplus P_4 = \alpha$

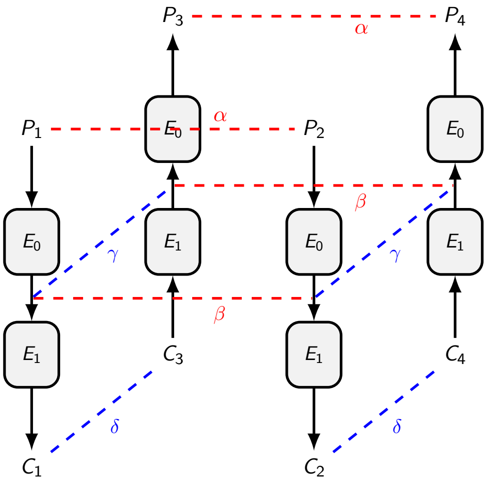
A distinguisher if α comes back
more often than a *random permutation*!

Boomerang Distinguisher 101



- Rewrite $E = E_1 \circ E_0$
  - $E_0 : Pr[\alpha \rightarrow \beta] = p$
  - $E_1 : Pr[\gamma \rightarrow \delta] = q$
- Expected probability: $p^2 q^2$
- Assumed two trails are independent

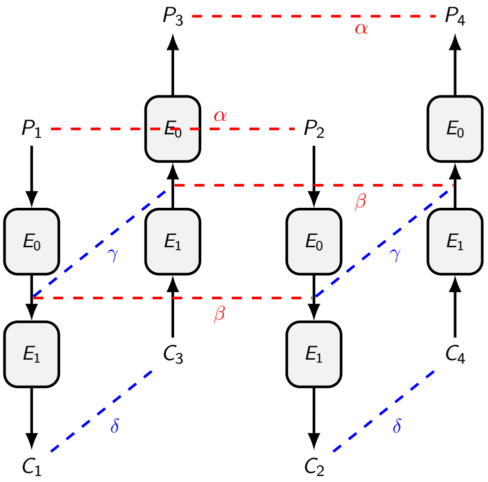
Boomerang Distinguisher 101



- Rewrite $E = E_1 \circ E_0$
  - $E_0 : Pr[\alpha \to \beta] = p$
  - $E_1 : Pr[\gamma \to \delta] = q$
- Expected probability: $p^2 q^2$
- Assumed two trails are independent

Assumption does NOT hold in practice!

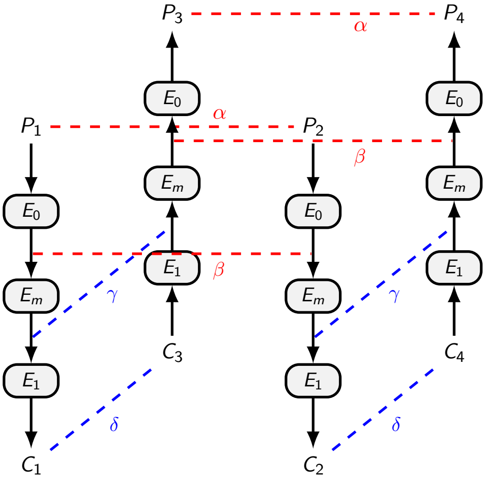
Boomerang Distinguisher 101



- Several examples of non-returning boomerangs [Murphy, 2011]
- At the junction of the two trails, dependency may exist
- Some attempts to refine the probability: sandwich, ladder switch, . . .

Assumption does NOT hold in practice!

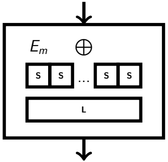
Boomerang Distinguisher 101



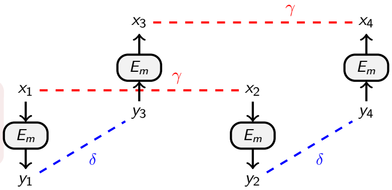
Sandwich attack [Dunkelman et al., 2010]

- Decompose $E = E_1 \circ E_m \circ E_0$
- E_m handles the dependency, with probability r
- Expected probability: $\tilde{p}^2 \tilde{q}^2 r$

Boomerang Distinguisher 101

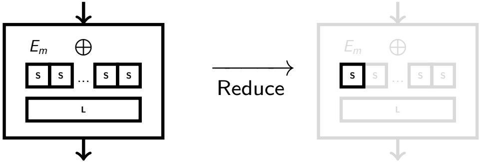


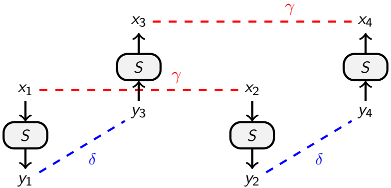
How to compute
the probability r of E_m?



$$\mathbb{P}(E_m^{-1}(E_m(X) \oplus \delta) \oplus E_m^{-1}(E_m(X \oplus \gamma) \oplus \delta) = \gamma)$$

Boomerang Distinguisher 101

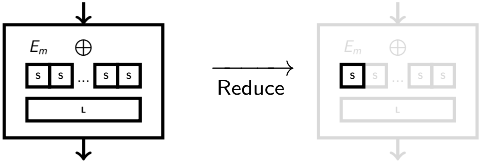


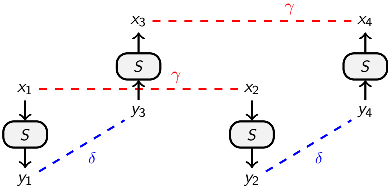


Boomerang Connectivity Table [Cid et al., 2018]

$$\mathrm{BCT}(\gamma, \delta) = \#\{x \in \mathbb{F}_2^n \mid S^{-1}(S(x) \oplus \delta) \oplus S^{-1}(S(x \oplus \gamma) \oplus \delta) = \gamma\}$$

Boomerang Distinguisher 101





Boomerang Connectivity Table [Cid et al., 2018]

$$\mathrm{BCT}(\gamma,\delta) = \#\{x \in \mathbb{F}_2^n \mid S^{-1}(S(x)\oplus\delta)\oplus S^{-1}(S(x\oplus\gamma)\oplus\delta) = \gamma\}$$

BCT Framework [Song et al., 2019]

- Determined the boundaries of E_m
- Calculated r of E_m in the sandwich attack

Boomerang Distinguisher 101

Automatic Search Boomerangs [Cid et al., 2017]

- Used a MILP model to study the ladder switch
- Improved attacks on `Deoxys` and `Deoxys-BC`

Automated Related-Key Boomerang [Liu and Sasaki, 2019]

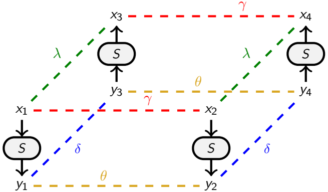
- MILP model to directly search for the best boomerang distinguisher on `GIFT`
- E_m is restricted to one single round

Catching the Fastest Boomerangs [Delaune et al., 2020]

- Introduced a set of tables to calculate the probability
- New MILP/CP/ad-hoc approach to search for boomerang distinguishers on `SKINNY`
- Automatically handle the middle round

Differential Tables [Delaune et al., 2020]

BCT is only a particular case



- $\mathrm{UBCT}(\gamma, \theta, \delta) = \#\left\{ x \in \mathbb{F}_2^n \;\middle|\; \begin{array}{l} S(x) \oplus S(x \oplus \gamma) = \theta \\ S^{-1}(S(x) \oplus \delta) \oplus S^{-1}(S(x \oplus \gamma) \oplus \delta) = \gamma \end{array} \right\}$
- $\mathrm{LBCT}(\gamma, \lambda, \delta) = \#\left\{ x \in \mathbb{F}_2^n \;\middle|\; \begin{array}{l} S(x) \oplus S(x \oplus \lambda) = \delta \\ S^{-1}(S(x) \oplus \delta) \oplus S^{-1}(S(x \oplus \gamma) \oplus \delta) = \gamma \end{array} \right\}$
- $\mathrm{EBCT}(\gamma, \theta, \lambda, \delta) = \#\left\{ x \in \mathbb{F}_2^n \;\middle|\; \begin{array}{l} S(x) \oplus S(x \oplus \gamma) = \theta \\ S(x) \oplus S(x \oplus \lambda) = \delta \\ S^{-1}(S(x) \oplus \delta) \oplus S^{-1}(S(x \oplus \gamma) \oplus \delta) = \gamma \end{array} \right\}$

Computing Probabilities [Delaune et al., 2020]

Given a boomerang characteristic, how to compute the probability for the boomerang to return?

Computing Probabilities [Delaune et al., 2020]

Given a boomerang characteristic, how to compute the probability for the boomerang to return?

Multiply the probability of transition for each Sbox separately!

Computing Probabilities [Delaune et al., 2020]

Given a boomerang characteristic, how to compute the probability for the boomerang to return?

How to compute the probability of transition for one particular Sbox?

Multiply the probability of transition for each Sbox separately!

Computing Probabilities [Delaune et al., 2020]

Given a boomerang characteristic, how to compute the probability for the boomerang to return?

Multiply the probability of transition for each Sbox separately!

How to compute the probability of transition for one particular Sbox?

The differential tables are used!

Computing Probabilities [Delaune et al., 2020]

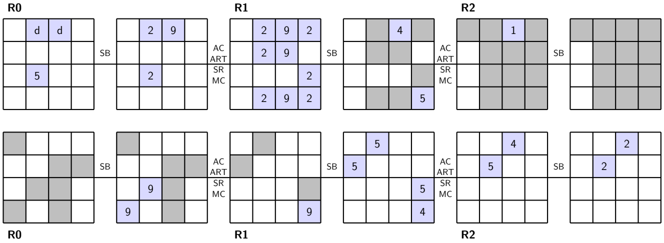


Figure: An example of **boomerang characteristic** on 3 rounds with
$\Delta_e = [0, d, d, 0, 0, 0, 0, 0, 0, 5, 0, 0, 0, 0, 0, 0]$ and
$\nabla_e = [0, 0, 2, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]$

Upper In	Upper Out	Lower In	Lower Out	Proba
*	*			$\mathbb{P}_{DDT}$
		*	*	
*	*			$\mathbb{P}_{DDT}(\cdot,\cdot)^2$
		*	*	
*			*	$\mathbb{P}_{BCT}$
*	*		*	$\mathbb{P}_{UBCT}$
*		*	*	$\mathbb{P}_{LBCT}$
*	*	*	*	$\mathbb{P}_{EBCT}$

Table: Summary of the used tables to compute probability

$$\mathbb{P}\left(\Delta_e \overset{E}{\rightleftarrows} \nabla_e\right) = \begin{array}{l} \mathbb{P}_{\mathrm{DDT}}(\mathrm{d},2)\cdot\mathbb{P}_{\mathrm{DDT}}(\mathrm{d},9)\cdot\mathbb{P}_{\mathrm{UBCT}}(5,2,9)\cdot\mathbb{P}_{\mathrm{DDT}}(9,4)\cdot \\ \mathbb{P}_{\mathrm{BCT}}(2,5)^2\cdot\mathbb{P}_{\mathrm{EBCT}}(2,5,9,4)\cdot\mathbb{P}_{\mathrm{LBCT}}(1,4,2)\cdot\mathbb{P}_{\mathrm{DDT}}(5,2)^2 \end{array}$$

□ = Zero; ■ = Free; □ = Specified

Computing Probabilities [Delaune et al., 2020]

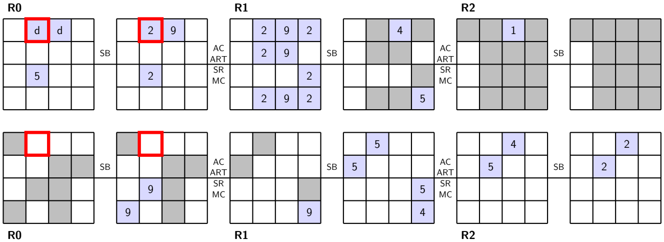


Figure: An example of **boomerang characteristic** on 3 rounds with $\Delta_e = [0, d, d, 0, 0, 0, 0, 0, 0, 5, 0, 0, 0, 0, 0, 0]$ and $\nabla_e = [0, 0, 2, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]$

Upper		Lower		Proba
In	Out	In	Out	
*	*			$\mathbb{P}_{DDT}$
		*	*	
*	*			$\mathbb{P}_{DDT}(\cdot,\cdot)^2$
		*	*	
*			*	$\mathbb{P}_{BCT}$
*	*		*	$\mathbb{P}_{UBCT}$
*		*	*	$\mathbb{P}_{LBCT}$
*	*	*	*	$\mathbb{P}_{EBCT}$

Table: Summary of the used tables to compute probability

$$\mathbb{P}\left(\Delta_e \overset{E}{\rightleftarrows} \nabla_e\right) = \mathbb{P}_{\mathrm{DDT}}(\mathrm{d}, 2) \cdot \mathbb{P}_{\mathrm{DDT}}(\mathrm{d}, 9) \cdot \mathbb{P}_{\mathrm{UBCT}}(5, 2, 9) \cdot \mathbb{P}_{\mathrm{DDT}}(9, 4) \cdot \mathbb{P}_{\mathrm{BCT}}(2, 5)^2 \cdot \mathbb{P}_{\mathrm{EBCT}}(2, 5, 9, 4) \cdot \mathbb{P}_{\mathrm{LBCT}}(1, 4, 2) \cdot \mathbb{P}_{\mathrm{DDT}}(5, 2)^2$$

□ = Zero; ■ = Free; □ = Specified

Computing Probabilities [Delaune et al., 2020]

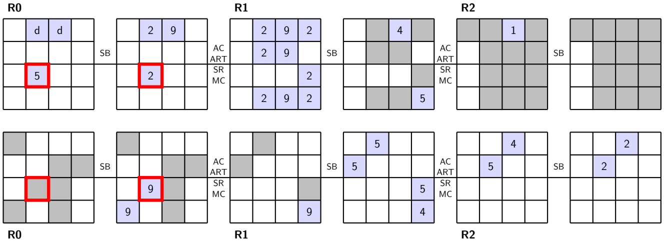


Figure: An example of **boomerang characteristic** on 3 rounds with $\Delta_e = [0, d, d, 0, 0, 0, 0, 0, 0, 5, 0, 0, 0, 0, 0, 0]$ and $\nabla_e = [0, 0, 2, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]$

Upper In	Upper Out	Lower In	Lower Out	Proba
*	*			$\mathbb{P}_{DDT}$
		*	*	
*	*			$\mathbb{P}_{DDT}(\cdot,\cdot)^2$
		*	*	
*			*	$\mathbb{P}_{BCT}$
*	*		*	$\mathbb{P}_{UBCT}$
*		*	*	$\mathbb{P}_{LBCT}$
*	*	*	*	$\mathbb{P}_{EBCT}$

Table: Summary of the used tables to compute probability

$$\mathbb{P}\left(\Delta_e \overset{E}{\rightleftarrows} \nabla_e\right) = \mathbb{P}_{\mathrm{DDT}}(\mathrm{d},2)\cdot\mathbb{P}_{\mathrm{DDT}}(\mathrm{d},9)\cdot\mathbb{P}_{\mathrm{UBCT}}(5,2,9)\cdot\mathbb{P}_{\mathrm{DDT}}(9,4)\cdot \mathbb{P}_{\mathrm{BCT}}(2,5)^2\cdot\mathbb{P}_{\mathrm{EBCT}}(2,5,9,4)\cdot\mathbb{P}_{\mathrm{LBCT}}(1,4,2)\cdot\mathbb{P}_{\mathrm{DDT}}(5,2)^2$$

□ = Zero; ■ = Free; □ = Specified

Truncated Boomerang Characteristics

Idea: convert a MILP model to search for truncated differential characteristics into a MILP model to search for truncated boomerang characteristics

MILP model

- Write twice the MILP model for truncated differential, once for the upper characteristic and once for the lower one
- Each difference can be either active (non-zero) or inactive (zero)
- Each difference can be either controlled (known) or free (unknown)
- **Objective:** an upper bound on the probability (somehow similar to *the number of active Sboxes*)

MILP model [Delaune et al., 2020]

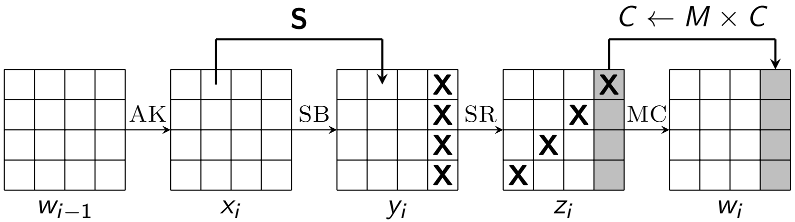
New constraints

- Constraints related to controlled/free variables
  - e.g. propagation of free variables
- Constraints related to controlled/free and active/inactive variables
  - e.g. if x is inactive then x is controlled
- Constraints related to tables
  - for each Sbox we need to know which table is involved (e.g. DDT, BCT, EBCT, ...)

- **Objective:** weighted sum over all the Sboxes and over all the tables
  - weighted by the maximum probability exponent

No "middle round" defined in the model!

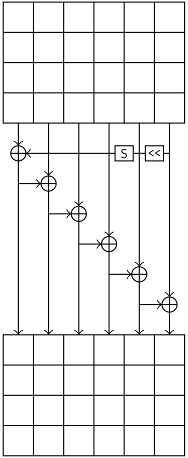
Applications to AES

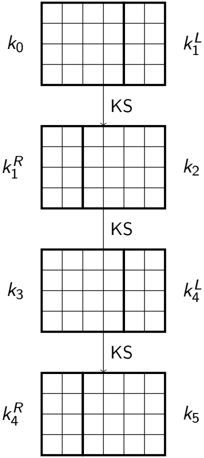


Advanced Encryption Standard (AES)

- Standardized in 2001
- Block size: 4×4 bytes (128 bits)
- $r_i = \mathrm{MC} \circ \mathrm{SR} \circ \mathrm{SB} \circ \mathrm{AK}$ (except the last round)
- AES-128 ($r = 10$), AES-192 ($r = 12$), AES-256 ($r = 14$)

AES-192 Key-schedule





AES-192 Key schedule round

$$
\begin{aligned}
K_{i,0} &\longleftarrow S(K_{i+1,5}) \oplus K_{i,0} \oplus C_r, && 0 \leq i \leq 3 \\
K_{i,j} &\longleftarrow S(K_{i,j-1}) \oplus K_{i,j}, && 0 \leq i \leq 3, 1 \leq j \leq 5
\end{aligned}
$$

Expand the master key K into $r+1$ round keys

The key schedule is
non linear,
the difference may be
unpredictable.

$\Longrightarrow$

Need
a new model!

New MILP Model

- Boomerang on the Related-Keys
  - Handle the non-linear key schedule
- Directly search for attacks, not only for distinguishers
  - Best distinguishers do not always lead to the best attacks!

Boomerang on the Related-Keys

Related-key: All keys $K_1, \ldots, K_4$ are secret, but relation $\Delta_{i,j} = K_i \oplus K_j$ are known.

- Control differences at both the input and output of an Sbox $\rightarrow$ zero difference
  - Or consider weak-keys distinguishers
- Keys generated by a boomerang with probability 1!

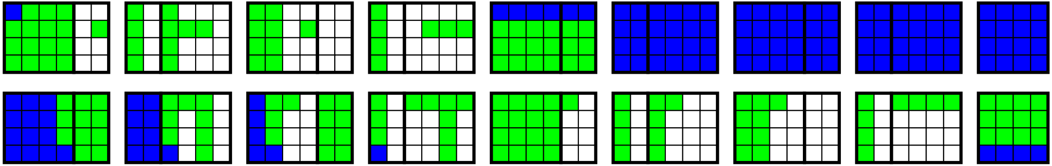


Figure: Key schedule for this attack. The subkeys for the upper trail are represented above the ones of the lower trail

= A known difference; = Zero difference; = fixed but unknown difference

Searching for Attacks

New variables

- $a^d = 1$: if the variable belongs to the distinguisher
- $a^z = 1$: if the difference is *zero*
- $a^k = 1$: if the difference is known
- $a^s = 1$: if the difference is set to a specific value

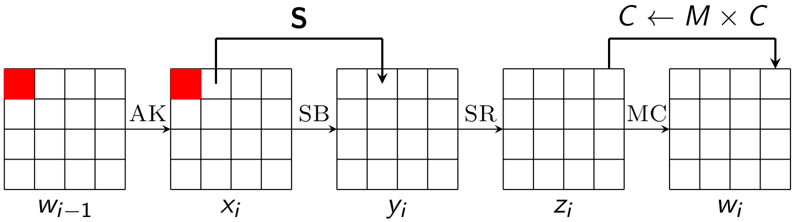
New propagation rules:

- Specific rules for both d and s
- Each equation $\bigoplus \alpha_i x_i = \beta$ implies the constraints

$$x_1^u + \ldots + x_n^u \neq n - 1$$

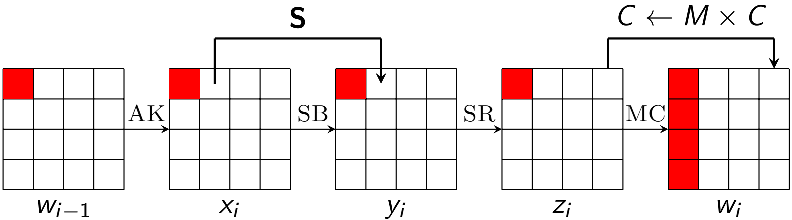
- Use callback and lazy constraints to ensure validity of solutions

Rules (Upper Trail)



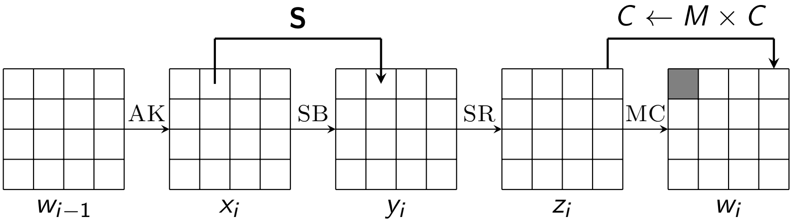
- $d = 1$: in the distinguisher

Rules (Upper Trail)



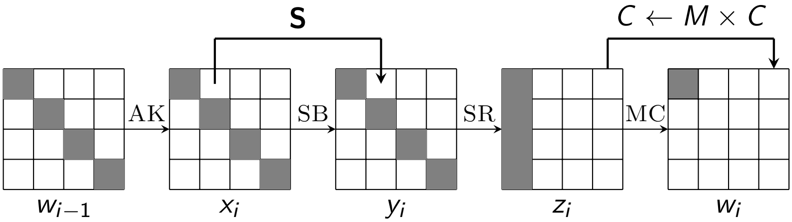
- $d = 1$: in the distinguisher

Rules (Upper Trail)



- $d = 0$: not in the distinguisher

Rules (Upper Trail)



- $d = 0$: not in the distinguisher

Computing Probabilities

Proba

$a^{z,up}$, $a^{k,up}$, $a^{s,up}$, $b^{z,up}$, $b^{k,up}$, $b^{s,up}$, $a^{z,low}$, $a^{k,low}$, $a^{s,low}$, $b^{z,low}$, $b^{k,low}$, $b^{s,low}$

$\Longrightarrow$ 59 possible cases in practice $\xrightarrow[\text{the associated proba}]{\textit{compute}}$

11 possibles values: 2^{0}, $2^{-5.4}$, 2^{-6}, 2^{-8}, 2^{-12}, $2^{-13.4}$, 2^{-14}, 2^{-16}, 2^{-20}, $2^{-21.4}$, 2^{-24}

Extra constraints

- Require 5 extra binary variables and 33 inequalities per S-box
- The probability of the distinguisher is greater than 2^{-127}

Note that: $\mathrm{b} = \mathrm{S}(\mathrm{a})$

Objective Function

- **Ideally:** optimize on the complexity of the attack ...
- ... but quite hard to compute (depends on the dimension of several vector spaces)

Idea: Use an approximation

- The smaller the vector spaces of plaintexts and ciphertexts, the better the attack
- The higher the probability of the distinguisher, the better the attack

Objective function

$$\texttt{Maximize}\left(2\times\left(\sum_{i=0}^{15} p[i]^{k,up}+c[i]^{k,lo}\right)+6\times\left(\sum_{i=0}^{15} p[i]^{s,up}+c[i]^{s,lo}\right)-p_{dist}\right)$$

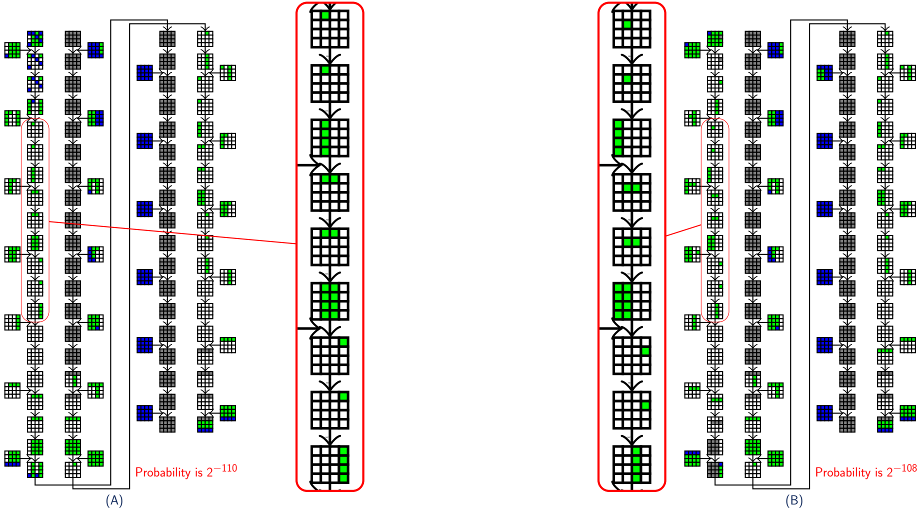
Note that: p_{dist} is the $-\log_2$ of the probability

Results

- Model is very slow $\rightarrow$ impossible to search for the best attacks
- Run the model on a restricted subspace
- Retrieved the attack against AES-256
- Found a better attack on AES-192

Key Size	Rounds	Time	Data	Memory	Type	Ref
192 bits	8/12	2^{172}	2^{107}	2^{96}	MITM	[Derbez et al., 2013]
	9/12	$2^{182.5}$	2^{117}	$2^{165.5}$		[Li et al., 2014]
	10/12	2^{183}	2^{124}	N/A	Related-key Rectangle	[Kim et al., 2007]
		2^{156}	2^{156}	2^{65}	Related-key Differential	[Gérault et al., 2018]
	12/12	$2^{190.16}$	2^{80}	2^{8}	Biclique	[Bogdanov et al., 2011]
		$2^{190.83}$	2	2^{60}		[Bogdanov et al., 2014]
		$2^{189.76}$	2^{48}	2^{60}		[Tao and Wu, 2015]
		2^{176}	2^{123}	2^{152}	Related-key Boomerang	[Biryukov and Khovratovich, 2009]
		2^{124}	2^{124}	$2^{79.8}$	Related-key Boomerang	This work

The best-known attack (A) vs Our attack (B)



■ = A known difference; □ = Zero difference; ■ = A fixed difference

Conclusion

Summary

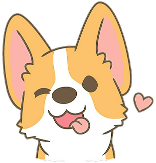
- Proposed a **new** MILP model to deal with **non-linear** key schedule
- Found a **new** related-keys attack against full `AES-192`
  - 2^{52} times lower complexity than the [Biryukov and Khovratovich, 2009] attack
- Recovered the attack on `AES-256` by [Biryukov and Khovratovich, 2009]

Note

- For more details: ia.cr/2022/725
- Code available at: `https://gitlab.inria.fr/pderbez/asia-2022-aes.git`

SCAN ME

Thanks for your attention!
Any questions?



References I

Biryukov, A. and Khovratovich, D. (2009).
Related-key cryptanalysis of the full AES-192 and AES-256.
In Matsui, M., editor, *Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings*, volume 5912 of *Lecture Notes in Computer Science*, pages 1–18. Springer.

Bogdanov, A., Chang, D., Ghosh, M., and Sanadhya, S. K. (2014).
Bicliques with minimal data and time complexity for AES.
In Lee, J. and Kim, J., editors, *Information Security and Cryptology - ICISC 2014 - 17th International Conference, Seoul, Korea, December 3-5, 2014, Revised Selected Papers*, volume 8949 of *Lecture Notes in Computer Science*, pages 160–174. Springer.

Bogdanov, A., Khovratovich, D., and Rechberger, C. (2011).
Biclique cryptanalysis of the full AES.
In Lee, D. H. and Wang, X., editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 344–371. Springer.

Cid, C., Huang, T., Peyrin, T., Sasaki, Y., and Song, L. (2017).
A security analysis of deoxys and its internal tweakable block ciphers.
IACR Trans. Symmetric Cryptol., 2017(3):73–107.

Cid, C., Huang, T., Peyrin, T., Sasaki, Y., and Song, L. (2018).
Boomerang connectivity table: A new cryptanalysis tool.
In Nielsen, J. B. and Rijmen, V., editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II*, volume 10821 of *Lecture Notes in Computer Science*, pages 683–714. Springer.

References II

Delaune, S., Derbez, P., and Vavrille, M. (2020).
Catching the fastest boomerangs application to SKINNY.
IACR Trans. Symmetric Cryptol., 2020(4):104–129.

Derbez, P., Fouque, P., and Jean, J. (2013).
Improved key recovery attacks on reduced-round AES in the single-key setting.
In *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 7881 of *Lecture Notes in Computer Science*, pages 371–387. Springer.

Dunkelman, O., Keller, N., and Shamir, A. (2010).
A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3g telephony.
In Rabin, T., editor, *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings*, volume 6223 of *Lecture Notes in Computer Science*, pages 393–410. Springer.

Gérault, D., Lafourcade, P., Minier, M., and Solnon, C. (2018).
Revisiting AES related-key differential attacks with constraint programming.
Inf. Process. Lett., 139:24–29.

Kim, J., Hong, S., and Preneel, B. (2007).
Related-key rectangle attacks on reduced AES-192 and AES-256.
In Biryukov, A., editor, *Fast Software Encryption, 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers*, volume 4593 of *Lecture Notes in Computer Science*, pages 225–241. Springer.

References III

Li, L., Jia, K., and Wang, X. (2014).
Improved single-key attacks on 9-round AES-192/256.
In Cid, C. and Rechberger, C., editors, *Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers*, volume 8540 of *Lecture Notes in Computer Science*, pages 127–146. Springer.

Liu, Y. and Sasaki, Y. (2019).
Related-key boomerang attacks on GIFT with automated trail search including BCT effect.
In Jang-Jaccard, J. and Guo, F., editors, *Information Security and Privacy - 24th Australasian Conference, ACISP 2019, Christchurch, New Zealand, July 3-5, 2019, Proceedings*, volume 11547 of *Lecture Notes in Computer Science*, pages 555–572. Springer.

Murphy, S. (2011).
The return of the cryptographic boomerang.
IEEE Trans. Inf. Theory, 57(4):2517–2521.

Song, L., Qin, X., and Hu, L. (2019).
Boomerang connectivity table revisited. application to SKINNY and AES.
IACR Trans. Symmetric Cryptol., 2019(1):118–141.

Tao, B. and Wu, H. (2015).
Improving the biclique cryptanalysis of AES.
In Foo, E. and Stebila, D., editors, *Information Security and Privacy - 20th Australasian Conference, ACISP 2015, Brisbane, QLD, Australia, June 29 - July 1, 2015, Proceedings*, volume 9144 of *Lecture Notes in Computer Science*, pages 39–56. Springer.

References IV

Wagner, D. A. (1999).
The boomerang attack.
In Knudsen, L. R., editor, *Fast Software Encryption, 6th International Workshop, FSE '99, Rome, Italy, March 24-26, 1999, Proceedings*, volume 1636 of *Lecture Notes in Computer Science*, pages 156–170. Springer.