# Revisiting the Transferability of Chosen- to Known-plaintext Attacks and Applications to Round-reduced AES

SAC 2026

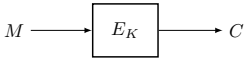
Xiaomeng Sun[1] Eik List[2] Wenying Zhang[1]

[1]School of Information Science and Engineering, Shandong Normal University, China
[2]School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore

24–28 Aug 2026

# Motivation

# Block-cipher Models




Block ciphers

- One of the cryptography's workhorses
- Their cryptanalysis impacts myriads of applications

Analysis often (have to) concentrates on chosen-data models

- Provide more freedom to adversaries
- Fully appropriate: in general, many block ciphers can be employed for use cases that support high degree of freedom

# RKP Model

- In many practical settings – randomized ciphers, MACs, or AE schemes – adversaries cannot freely choose the inputs to the underlying block cipher
- Known plaintexts (KP) allow adversaries to remain passive
- Random known plaintext (RKP) model poses the simplest assumptions on the input data: plaintexts are chosen randomly

# What Types of Attacks Apply in The RKP Model?

Cryptanalysis techniques in the RKP model:

- Linear cryptanalysis is well-known to work
- Algebraic methods and some MitM attacks can also work

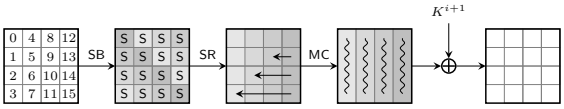
What about differential attacks?

- They usually need plaintext pairs with particular input differences
- They are often the more effective/efficient attacks

How large is the security gap between the models?

# The Advanced Encryption Standard

[Nat01]




- Probably the most widely deployed block cipher
- Versions: AES-128, -192, -256 with 10, 12, 14 rounds, respectively
- More than 25 years of cryptanalysis
- Much progress on new techniques in the past decade
- But heavy focus on chosen-data properties and attacks

# Best Known Results on the AES-128

**CP Model**

Key recovery: 7 rounds

- DS-MitM [DFJ13]
- Impossible differential [LP21]
- Related differential [BR22]

Distinguishers: 6 rounds

- Mixture differentials [BR19b]
- Truncated differentials [BGL20, CWSW22]

**ACP+ACC Model:** Distinguishers: 6 rounds

- Boomerang chains [YTXQ24]

**RKP Model**

Key recovery: 6 rounds

- MitM [BDF11]
  Best known attack for more than a decade

Distinguishers: 4 rounds

- Conditional linear [AT25]
- Zero-correlation linear [BR11]

# Motivation (cont'd)

## Related works

- Biham and Shamir [BS92]: Suggested the classical conversion of a CP differential attack requiring $2^r$ chosen pairs into an RKP attack using approximately $2^{(r+n+1)/2}$ data
- But it remained unapplied since
- Unclear whether other differential-based attacks, including impossible-differential, rectangle, mixture, and differential-based MitM attacks, can be effectively transferred to the RKP model
- If so, we could reduce the gap

How to generalize the transformation of attacks between the CP and RKP models?

# Key-recovery Attacks on Round-reduced AES

(a) Single-key attacks in the CP model.

| Version | Type | #Rds. | Time | Data | Memory | Reference |
|---|---|---|---|---|---|---|
| 128 | Integral | $7/10$ | $2^{128}-2^{119}$ | $2^{128}-2^{119}$ | n/a | [FKL+00] |
| | Imp. differential | $7/10$ | $2^{110.9}$ | $2^{104.9}$ | $2^{71.9}$ | [LP21, LP25] |
| | Zero difference | $7/10$ | $2^{110.2}$ | $2^{110.2}$ | $2^{110.2}$ | [BR22] |
| | DS-MitM | $7/10$ | $2^{99}+2^{100}$ | $2^{97}$ | $2^{98}$ | [DFJ13] |
| 192 | DS-MitM | $9/12$ | $2^{186.4}+2^{186.8}$ | $2^{121}$ | $2^{172.3}$ | [LZ24] |
| | DS-MitM | $9/12$ | $2^{182.8}+2^{182.8}$ | $2^{125.3}$ | $2^{173.2}$ | [DLW+24] |
| 256 | DS-MitM | $9/14$ | $2^{203}+2^{205}$ | $2^{120}$ | $2^{203}$ | [DFJ13] |
| | DS-MitM | $9/14$ | $2^{194.5}+2^{197.1}$ | $2^{127}$ | $2^{162.9}$ | [DLW+24] |

(b) Single-key attacks in the RKP model.

| Version | Attack type | #Rds. | Time | Data | Memory | Reference |
|---|---|---|---|---|---|---|
| 128 | MitM | $5/10$ | $2^{120}$ | $1$ | $2^{96}$ | [BDF11, Der13] |
| | MitM | $5/10$ | $2^{120}$ | $1$ | $2^{40}$ | [CGL+25] |
| | MitM | $6/10$ | $2^{120}$ | $2^{108.5}$ | $2^{109.5}$ | [BDD+12] |
| | **Rectangle** | $\mathbf{6/10}$ | $\mathbf{2^{105.8}}$ | $\mathbf{2^{99.1}}$ | $\mathbf{2^{103.2}}$ | **This work** |
| | **DS-MitM** | $\mathbf{7/10}$ | $\mathbf{2^{125.1}}$ | $\mathbf{2^{124}}$ | $\mathbf{2^{125}}$ | **This work** |
| | **Imp. differential** | $\mathbf{7/10}$ | $\mathbf{2^{118.1}}$ | $\mathbf{2^{116.5}}$ | $\mathbf{2^{117.5}}$ | **This work** |
| 192 | Zero correlation | $6/12$ | $2^{188.4}$ | $2^{128}$ | $2^{128}$ | [BR14] |
| | MitM | $7/12$ | $2^{184}$ | $1$ | $2^{72}$ | [CGL+25] |
| | **Imp. differential** | $\mathbf{7/12}$ | $\mathbf{2^{126}}$ | $\mathbf{2^{117.5}}$ | $\mathbf{2^{118.5}}$ | **Full version** |
| | **DS-MitM** | $\mathbf{8/12}$ | $\mathbf{2^{179}}$ | $\mathbf{2^{124}}$ | $\mathbf{2^{128.6}}$ | **Full version** |
| 256 | Zero correlation | $6/14$ | $2^{188.4}$ | $2^{128}$ | $2^{128}$ | [BR14] |
| | MitM | $8/14$ | $2^{248}$ | $1$ | $2^{72}$ | [CGL+25] |
| | Imp. differential$^{(*)}$ | $8/14$ | $2^{220}$ | $2^{118}$ | $2^{145}$ | [Kar25] |
| | **Imp. differential** | $\mathbf{8/14}$ | $\mathbf{2^{228.5}}$ | $\mathbf{2^{116.8}}$ | $\mathbf{2^{217}}$ | **Full version** |
| | **DS-MitM** | $\mathbf{9/14}$ | $\mathbf{2^{247.7}}$ | $\mathbf{2^{124}}$ | $\mathbf{2^{194.1}}$ | **Full version** |

#Rds. = #rounds, memory in #AES states, n/a = not available. $^{(*)}$ = we argue in the full version that the data does not suffice.

# Distinguishers on Round-reduced AES

(a) Single secret-key distinguishers under chosen data.

| Attack type | | #Rds. | Time | Data | Memory | Reference |
|---|---|---|---|---|---|---|
| Truncated differential | CP | 6 | $2^{96.5}$ | $2^{89.4}$ | $2^{89.4}$ | [BGL20] |
| Mixture differential | CP | 6 | $2^{88.2}$ | $2^{88.2}$ | $2^{88.2}$ | [BR19b] |
| Boomerang | CP+ACC | 6 | $2^{87}$ | $2^{87}$ | n/a | [BL23] |
| Mixture differential | CP+ACC | 6 | $2^{84}$ | $2^{83}$ | n/a | [BR19a] |
| Boomerang | CP+ACC | 6 | $2^{76.6}$ | $2^{76.6}$ | n/a | [YTXQ24] |

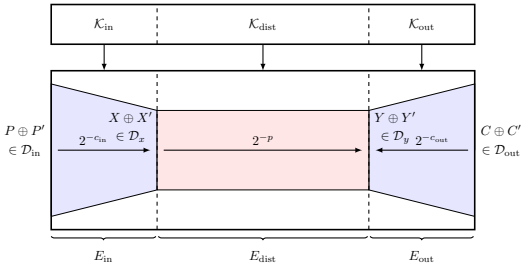
(b) Single secret-key distinguishers in the RKP model.

| Attack type | #Rds. | Time | Data | Memory | Reference |
|---|---|---|---|---|---|
| Zero correlation | 4 | $2^{128}$ | $2^{128}$ | negl. | [BR11] |
| Conditional linear | 4 | $2^{125.6}$ | $2^{125.6}$ | negl. | [AT23, AT25] |
| **Mixture differential** | **6** | $\mathbf{2^{118.1}}$ | $\mathbf{2^{115.5}}$ | $\mathbf{2^{117.5}}$ | **This work** |
| **Rectangle** | **6** | $\mathbf{2^{117.7}}$ | $\mathbf{2^{113.5}}$ | $\mathbf{2^{115.5}}$ | **Full version** |
| **Truncated differential** | **6** | $\mathbf{2^{111.9}}$ | $\mathbf{2^{106.8}}$ | $\mathbf{2^{108.4}}$ | **This work** |

#Rds. = #rounds, memory in #AES states, n/a = not available.

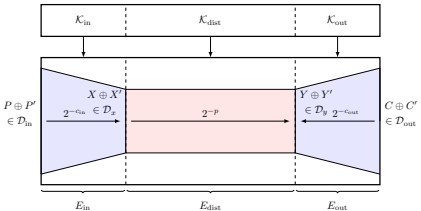
# Conversion of Classical Differential Attacks

# Classical Differential Attacks



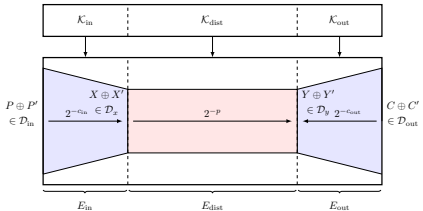

- Split $E = E_{\text{out}} \circ E_{\text{dist}} \circ E_{\text{in}}$
- Define a nontrivial differential $\Delta X \xrightarrow{E_{\text{dist}}} \Delta Y$ through $E_{\text{dist}}$ with probability $2^{-p}$
- Define a possible plaintext-difference space $\mathcal{D}_{\text{in}}$ and ciphertext-difference space $\mathcal{D}_{\text{out}}$
- Define $2^{\delta_{\text{in}}} = |\mathcal{D}_{\text{in}}|$ and $2^{\delta_{\text{out}}} = |\mathcal{D}_{\text{out}}|$,
- Define spaces of desired input differences $X \oplus X' \in \mathcal{D}_x$ and output differences $Y \oplus Y' \in \mathcal{D}_y$

# Conversion of Classical Differential Attacks




- CP attacks can use plaintext structures (CC attacks can use ciphertext structures)
- $2^d$ data can produce $2^{d+\min(d,\delta_{\text{in}})-1}$ pairs
- All those pairs are in $\mathcal{D}_{\text{in}}$
- KP attacks can use all data to form $2^{2d-1}$ pairs
- But pairs are not automatically in $\mathcal{D}_{\text{in}}$

# Conversion of Classical Differential Attacks




- CP attacks can use plaintext structures (CC attacks can use ciphertext structures)
- $2^d$ data can produce $2^{d+\min(d,\delta_{\text{in}})-1}$ pairs
- All those pairs are in $\mathcal{D}_{\text{in}}$
- KP attacks can use all data to form $2^{2d-1}$ pairs
- But pairs are not automatically in $\mathcal{D}_{\text{in}}$

## CP Expected Surviving Pairs:

$$\mathbb{E}[\#\mathbf{SP}^{\mathbf{Diff}}_{\mathbf{CP}}] = N_{\mathbf{CP}} \cdot \left(\tfrac{|\mathcal{D}_{\mathbf{out}}|}{2^n-1} \cdot (1-2^{-p}) + 2^{-p}\right)$$

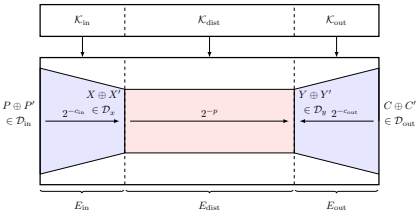
#Candidate pairs: $N_{\mathbf{CP}} \approx 2^{d+\min(d,\delta_{\text{in}})-1}$

## RKP Expected Surviving Pairs:

$$\mathbb{E}[\#\mathbf{SP}^{\mathbf{Diff}}_{\mathbf{RKP}}] = \tfrac{|\mathcal{D}_{\mathbf{in}}|}{2^n-1} \cdot N_{\mathbf{RKP}} \cdot \left(\tfrac{|\mathcal{D}_{\mathbf{out}}|}{2^n-1} \cdot (1-2^{-p}) + 2^{-p}\right)$$

#Candidate pairs: $N_{\mathbf{RKP}} \approx 2^{2d-1} \cdot 2^{\delta_{\text{in}}-n}$

# Conversion of Classical Differential Attacks




- CP attacks can use plaintext structures (CC attacks can use ciphertext structures)
- $2^d$ data can produce $2^{d+\min(d,\delta_{\text{in}})-1}$ pairs
- All those pairs are in $\mathcal{D}_{\text{in}}$
- KP attacks can use all data to form $2^{2d-1}$ pairs
- But pairs are not automatically in $\mathcal{D}_{\text{in}}$

## CP Expected Surviving Pairs:

$$\mathbb{E}[\#\mathbf{SP}^{\mathbf{Diff}}_{\mathbf{CP}}] = N_{\mathbf{CP}} \cdot \left(\tfrac{|\mathcal{D}_{\mathbf{out}}|}{2^n-1} \cdot (1-2^{-p}) + 2^{-p}\right)$$

#Candidate pairs: $N_{\mathbf{CP}} \approx 2^{d+\min(d,\delta_{\text{in}})-1}$

## RKP Expected Surviving Pairs:

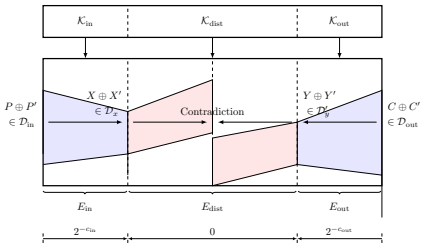
$$\mathbb{E}[\#\mathbf{SP}^{\mathbf{Diff}}_{\mathbf{RKP}}] = \tfrac{|\mathcal{D}_{\mathbf{in}}|}{2^n-1} \cdot N_{\mathbf{RKP}} \cdot \left(\tfrac{|\mathcal{D}_{\mathbf{out}}|}{2^n-1} \cdot (1-2^{-p}) + 2^{-p}\right)$$

#Candidate pairs: $N_{\mathbf{RKP}} \approx 2^{2d-1} \cdot 2^{\delta_{\text{in}}-n}$

## RKP data complexity must satisfy:

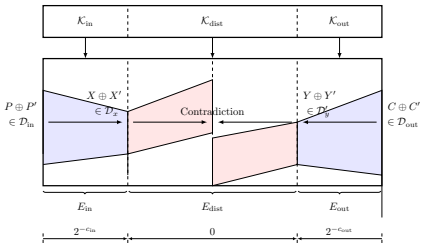
$$d^{\text{Diff}}_{\text{RKP}} \geq d^{\text{Diff}}_{\text{CP}} + \frac{n - \max(d^{\text{Diff}}_{\text{CP}}, \delta_{\text{in}})}{2}$$

# Conversion of Impossible-differential (ID) Attacks




- We can use a similar conversion for ID attacks
- Use a differential with probability $p = 0$
- CP attacks usually have plaintext structures
- Can use pairs whose ciphertext differences fall in $\mathcal{D}_{\text{out}}$
- Need to filter down $2^k$ keys
- A pair can filter a fraction of $2^{-(c_{\text{in}}+c_{\text{out}})}$ keys

# Conversion of Impossible-differential (ID) Attacks




- We can use a similar conversion for ID attacks
- Use a differential with probability $p = 0$
- CP attacks usually have plaintext structures
- Can use pairs whose ciphertext differences fall in $\mathcal{D}_{\text{out}}$
- Need to filter down $2^k$ keys
- A pair can filter a fraction of $2^{-(c_{\text{in}}+c_{\text{out}})}$ keys

## CP Expected Surviving Pairs:

$$\mathbb{E}[\#\mathbf{SP}^{\mathbf{ID}}_{\mathbf{CP}}] = N_{\mathbf{CP}} \cdot \frac{|\mathcal{D}_{\mathbf{out}}|}{2^n - 1}$$

#Candidate pairs: $N_{\text{CP}} \approx 2^{d+\min(d,\delta_{\text{in}})-1}$

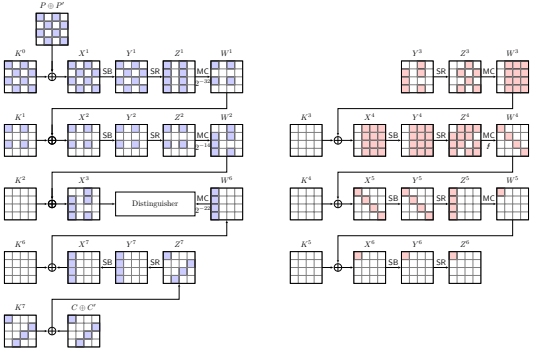
## RKP Expected Surviving Pairs:

$$\mathbb{E}[\#\mathbf{SP}^{\mathbf{ID}}_{\mathbf{RKP}}] = \frac{|\mathcal{D}_{\mathbf{in}}|}{2^n - 1} \cdot N_{\mathbf{RKP}} \cdot \frac{|\mathcal{D}_{\mathbf{out}}|}{2^n - 1}$$

#Candidate pairs: $N_{\text{RKP}} \approx 2^{2d+\delta_{\text{in}}-n-1}$

# Application

# 7-round Impossible-differential Attack on AES-128




- **Impossible-differential Trail.** 4-round impossible-differential distinguisher from [MDRM10], also used in the best attacks in [BLNS18, BNS14, LP21, LP25]
- **Key-guessing rounds.** 2 rounds before, 1 round after the distinguisher;

$$k = 112 \text{ key bits}$$

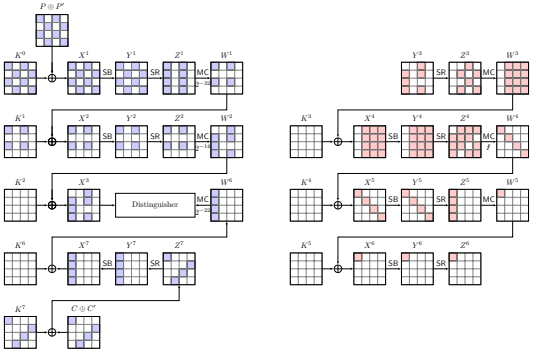
$$(c_{\text{in}}, c_{\text{out}}) \approx (46, 22) \text{ bit conditions}$$

- **Filter.** Every satisfying pair can filter out ca.

$$2^k \cdot 2^{-c_{\text{in}}-c_{\text{out}}} \approx 2^{112-46-22} = 2^{44} \text{ keys}$$

- **#Required pairs.** Needs approx. $2^4 \cdot 2^{112-44} = 2^{72}$ pairs that satisfy the differential

# 7-round Impossible-differential Attack on AES-128




- **Input-difference space.** Two fixed active plaintext diagonals, one fixed active ciphertext diagonal:

$$|\mathcal{D}_{\text{in}}| \approx 2^{64} \qquad |\mathcal{D}_{\text{out}}| \approx 2^{32}$$

- **Data complexity.** We also aim at $2^{72}$ surviving pairs. Thus, we require

$$2^{2d-1} \geq 2^{128-64} \cdot 2^{128-32} \cdot 2^{72}$$
$$d \geq \frac{72+1+64+96}{2} = 116.5$$

- Data collection dominates the time complexity

# Conversion of Mixture-differential Attacks

# Mixture-Differential Distinguishers

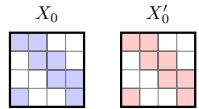
[Gra18]

- Start from one pair $(X_0, X_0')$ with $X_0 \oplus X_0' = \Delta X$
- Assume states are composed of $m$ $w$-bit words
- Exchange selected words between the two texts to generate related pairs. From an exchange vector

$$\alpha = (\alpha_0, \ldots, \alpha_{m-1}) \in \{0,1\}^m,$$

define

$$\big(\rho_\alpha(X_0, X_0')\big)[j] = \begin{cases} X_0[j], & \text{if } \alpha_j = 0, \\ X_0'[j], & \text{otherwise.} \end{cases}$$




- The related pair is

$$X_1 = \rho_\alpha(X_0, X_0'), \qquad X_1' = \rho_\alpha(X_0', X_0)$$

# Mixture-Differential Distinguishers (cont'd)

[Gra18]

- **Conditional Differential:** The exchange preserves the input difference:

$$X_1 \oplus X_1' = X_0 \oplus X_0' = \Delta X \in \mathcal{D}_x$$

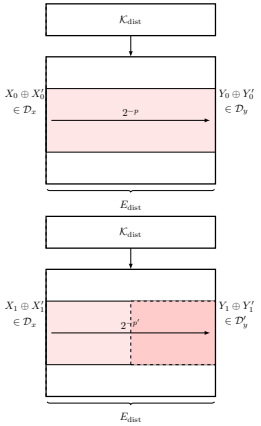
Let

$$E_x : E_{\text{dist}}(K, X_0) \oplus E_{\text{dist}}(K, X_0') \in \mathcal{D}_y \quad \text{and}$$
$$E_y : E_{\text{dist}}(K, X_1) \oplus E_{\text{dist}}(K, X_1') \in \mathcal{D}_y'.$$

A mixture differential exploits

$$\Pr[E_y \mid E_x] = 2^{-p'},$$

when this conditional probability differs from that of a random permutation.



# Conversion of Mixture-differential Attacks (cont'd)

**CP Expected Surviving Quartets.**
Starts from pairs of pairs in input-difference space

$$\mathbb{E}[\#\mathbf{SQ}^{\mathbf{Mix}}_{\mathbf{CP}}] = N_{\mathbf{CP}} \cdot \left( \frac{|\mathcal{D}_{\mathbf{out}}| \cdot |\mathcal{D}'_{\mathbf{out}}|}{(2^n-1)\cdot(2^n-3)} \cdot (1 - 2^{-(p+p')}) + 2^{-(p+p')} \right) \qquad N_{\mathbf{CP}} \approx 2^{d+\mathbf{min}(d,\delta_{\mathbf{in}})-3}$$

**RKP Expected Survivng Quartets.**
Starts from quartets that must lie in the spaces, form a pair, and a mixed pair

$$\mathbb{E}[\#\mathbf{SQ}^{\mathbf{Mix}}_{\mathbf{RKP}}] = \frac{|\mathcal{D}_{\mathbf{in}}| \cdot N_{\mathbf{RKP}}}{(2^n-1)_3} \cdot \left( \frac{|\mathcal{D}_{\mathbf{out}}| \cdot |\mathcal{D}'_{\mathbf{out}}|}{(2^n-1)\cdot(2^n-3)} \cdot \left(1 - 2^{-(p+p')}\right) + 2^{-(p+p')} \right) \qquad N_{\mathbf{RKP}} = 2 \cdot 3 \cdot \binom{2^d}{4} \approx 2^{4d-2}$$

# Conversion of Mixture-differential Attacks (cont'd)

**CP Expected Surviving Quartets.**
Starts from pairs of pairs in input-difference space

$$\mathbb{E}[\#\mathbf{SQ}_{\mathbf{CP}}^{\mathbf{Mix}}] = N_{\mathbf{CP}} \cdot \left( \frac{|\mathcal{D}_{\mathbf{out}}| \cdot |\mathcal{D}'_{\mathbf{out}}|}{(2^n-1)\cdot(2^n-3)} \cdot (1 - 2^{-(p+p')}) + 2^{-(p+p')} \right) \qquad N_{\mathbf{CP}} \approx 2^{d+\mathbf{min}(d,\delta_{\mathbf{in}})-3}$$

**RKP Expected Survivng Quartets.**
Starts from quartets that must lie in the spaces, form a pair, and a mixed pair

$$\mathbb{E}[\#\mathbf{SQ}_{\mathbf{RKP}}^{\mathbf{Mix}}] = \frac{|\mathcal{D}_{\mathbf{in}}| \cdot N_{\mathbf{RKP}}}{(2^n-1)_3} \cdot \left( \frac{|\mathcal{D}_{\mathbf{out}}| \cdot |\mathcal{D}'_{\mathbf{out}}|}{(2^n-1)\cdot(2^n-3)} \cdot \left(1 - 2^{-(p+p')}\right) + 2^{-(p+p')} \right) \qquad N_{\mathbf{RKP}} = 2 \cdot 3 \cdot \binom{2^d}{4} \approx 2^{4d-2}$$

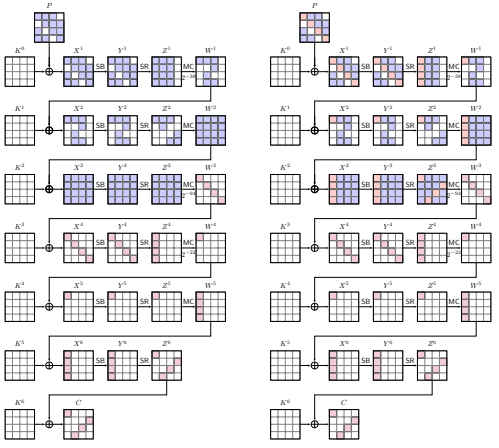
**RKP data complexity must satisfy:**

$$d_{\mathrm{RKP}}^{\mathrm{Mix}} \geq \frac{2d_{\mathrm{CP}}^{\mathrm{Mix}} + 3n - \max\left(d_{\mathrm{CP}}^{\mathrm{Mix}}, \delta_{\mathrm{in}}\right)}{4}$$

# Application

# Six-round Mixture Distinguisher in the CP Model

[BR19b]



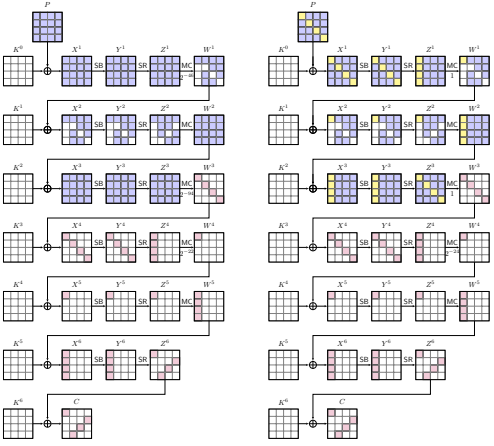

- **Plaintext differences.** Collects CPs with three active plaintext diagonals
- **Mixture Pairs.** The second pair is obtained by exchanging one plaintext diagonal. The probility of distinguisher:

$$p_{\text{real}} \approx 2^{-38} \cdot 2^{-94} \cdot 2^{-44} = 2^{-176}$$

$$p_{\text{ideal}} \approx 2^{-188}$$

- **Data complexity.** $2^{88.2}$ CPs yield one mixture quartet on average

# Six-round Mixture Distinguisher in the RKP Model



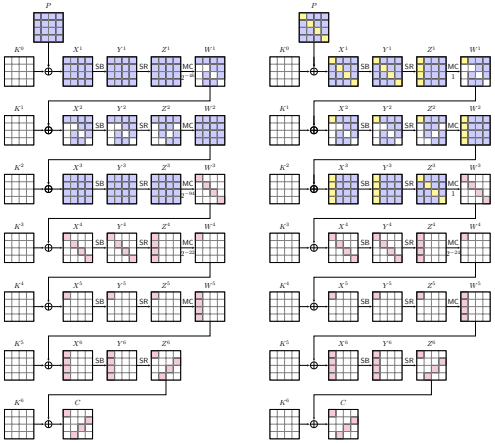
- **Plaintext differences.** Collects CPs with four active plaintext diagonals
- **Mixture trail.** The second pair is obtained by exchanging one plaintext diagonal. The probility of distinguisher:

$$p_{\text{real}} \approx 2^{-46} \cdot 2^{-94} \cdot 2^{-44} = 2^{-184}$$
$$p_{\text{ideal}} \approx 2^{-188}$$

- **Why not use the previous differentials?** The inactive plaintext diagonal would increase time and data complexities

$$2^{4d-2} \geq 2^{256} \cdot 2^{32} \cdot 2^{176}$$
$$\implies d \geq \frac{2 + 256 + 32 + 176}{4} = 116.5$$

# Six-round Mixture Distinguisher in the RKP Model (cont'd)

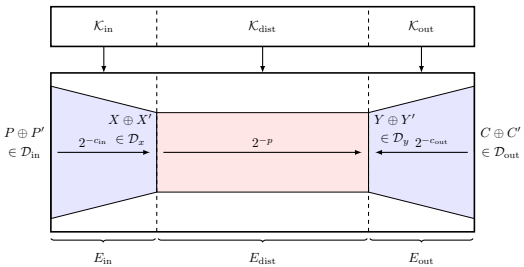


- **Consequence.** We have "only" a $94$-bit filter. Surviving #pairs would be the bottleneck of the time complexity
- **Trade-off.** Fix $20$ bits apriori in three unchanged diagonals of plaintexts where $P[i] = P'[i]$, such that $\overline{P}[i] = \overline{P'}[i]$ and use them as additional condition and filter
- **Data complexity.**

$$2^{4d-2} \geq 2^{256} \cdot 2^{20} \cdot 2^{184}$$
$$\implies d \geq \frac{2 + 256 + 20 + 184}{4} = 115.5$$

# Demirci-Selçuk Meet-in-the-Middle Attacks

# DS-MitM Attack with Differential Enumeration




- **Demirci-Selçuk (DS-)MitM attacks [DS08].** Trace a set of $m$ related texts through a distinguisher $E_{\text{dist}}$
- Compute all possible output sequences (or sets) through $E_{\text{dist}}$ in an offline step
- Exploit that the #output sequences is smaller for a real partial cipher than for a random permutation
- **Differential enumeration [DKS10].** Waits for a first pair that satisfies a differential to reduce the number of possibilities in the distinguisher

# DS-MitM Attack with Differential Enumeration

[DS08, DKS10]

- **In the CP model.** The attacker builds structures of many related texts, e.g. a $\delta$-set. The required related plaintexts are guaranteed to be available in the online phase. The surviving pairs:

$$\mathbb{E}[\#\mathbf{SP}^{\mathrm{DS}}_{\mathrm{CP}}] = \mathbb{E}[\#\mathbf{SP}^{\mathrm{Diff}}_{\mathrm{CP}}]$$

- **In the RKP model.** The number of pairs is similar as in a differential attack:

$$\mathbb{E}[\#\mathbf{SP}^{\mathrm{DS}}_{\mathrm{RKP}}] = \mathbb{E}[\#\mathbf{SP}^{\mathrm{Diff}}_{\mathrm{RKP}}]$$

But random data can not guarantee the availability of related texts. For $2^d$ known plaintexts, $m$ related texts are available with probability

$$\Pr[m \text{ related texts available}] \approx 2^{(d-n)m}$$

**How to avoid data complexity close to the full codebook in RKP model?**

# Conversion of DS-MitM Attacks with Diff. Enumeration

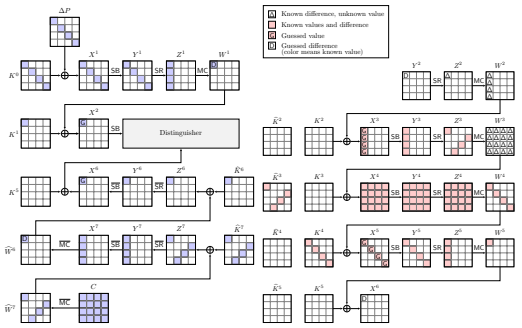
Let $m = \#$possible related texts, and $k = \#$required texts used for matching

- **$k$-out-of-$m$ strategy.**
- **Online phase.** Instead of requiring all related texts, only use the (lexicographically) first available $k$ out of $m$
- **Offline phase.** Compute $\binom{m}{k}$ index-set combinations
- **Matching.** Look up if $k$ out of $m$ texts are available; otherwise discard the current pair candidate
- Thus, the attack requires at least $k$ among $m$ related texts are available in the given data, whose probability is

$$q_{\text{succ}} \approx 1 - \left( \sum_{k=0}^{k-1} \binom{m}{k} (2^{d-n})^k (1 - 2^{d-n})^{m-k} \right)$$

# Application

# 7-round DS-MitM Attack on AES-128 in the CP Model



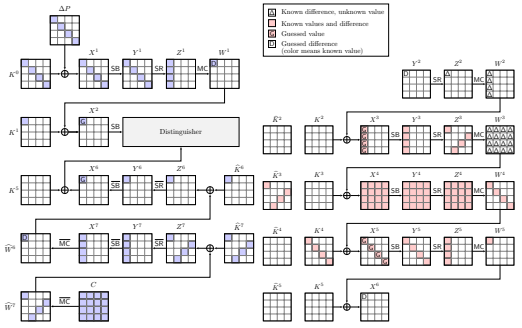

- **Differential-enumeration.** Using one of the 4-round trails from [DFJ13]
- **Offline complexity.** $2^{80}$ guesses per trail
- **Key-guessing rounds.** 1 rounds before, 2 round after the distinguisher
- **Probability.**

$$p \approx 2^{-24} \cdot 2^{-120} = 2^{-144}$$

A structure of $2^{32}$ CPs yields $2^{63}$ pairs. Thus, it needs $2^{144-63+32} = 2^{113}$ CPs

- **Complexity.** Dominated by encrypting $2^{113}$ CPs in the online phase

# 7-round DS-MitM attack on AES-128 in the RKP Model



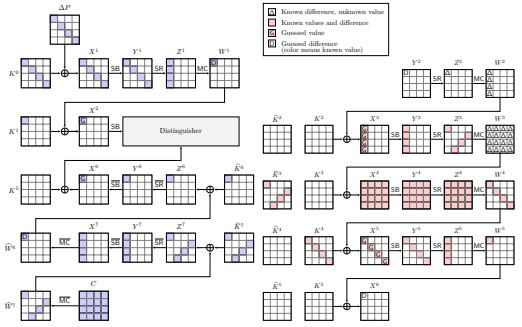

**Online Phase: Find candidate data**

- **Plain-ciphertexts Filter.** From $D = 2^d$ random known plaintexts, $2^{2d-1}$ pairs can be formed. The initial plaintext/ciphertext filter has probability

$$2^{-96} \cdot 2^{-96} = 2^{-192}.$$

- **Differential/Key Filter.** Guess the outer-round key information and restrict the difference at $\Delta Y^2[0]$ and $\Delta X^6[0]$.
- **Related-text availability.** For each surviving lead pair, derive the first $m$ related texts backwards to the plaintext side. Check whether they occur in the collected RKP data and store the sequences $(\Delta X^6, \Delta X^6_{i_1}, \ldots \Delta X^6_{i_k})$ into table $T_{\text{online}}$.

# 7-round DS-MitM attack on AES-128 in the RKP Model




**Offline Phase: DS-MitM Matching**

- Guess the required internal values/differences and trace the related texts through the distinguisher, obtaining the full sequence

$$(\Delta X^6, \Delta X_1^6, \ldots, \Delta X_m^6).$$

- Enumerate all

$$\binom{m}{k}$$

subsets $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, m\}$.

- For each subset, form

$$(\Delta X^6, \Delta X_{i_1}^6, \ldots, \Delta X_{i_k}^6; i_1, \ldots, i_k)$$

and look it up in $T_{\text{online}}$.

- For a match, use the remaining available related texts to further filter false candidates.

# 7-round DS-MitM attack on AES-128 in the RKP Model

- **Trade-off $d, m, k$.** A specific related plaintext is contained in the data with probability

$$p_{\text{av}} = 2^{d-128}.$$

Set $d = 124$, then $p_{\text{av}} = 2^{-4}$.
Among the first $m$ related texts, the expected number available is

$$\mathbb{E}[X] = m \cdot 2^{-4}.$$

Set $m = 144$, gives $\mathbb{E}[X] = 144/16 = 9$.
Therefore, set the threshold to

$$k = 9.$$

- **The number of right pairs remain.** For $d = 124$, the expected number of initial right pairs is

$$N_{\text{right}} = 2^{2d-128-192} = 2^{11}.$$

Extra restrict on $\Delta Y^2$ as $\alpha = 1$ out of approximately $2^8$ nonzero differences:

$$2^{11} \cdot 2^{-8} = \boxed{2^3 \text{ right pairs}}.$$

# Conclusion

# Conclusion

- **Generic CP-to-RKP conversions.** We develop generic conversions from the CP model to the RKP model for (truncated-)differential, impossible-differential, mixture, and rectangle attacks
- **Conversion of attacks with many related texts.** We show that DS-MitM attacks can also be mounted in the RKP model with a probabilistic $k$-out-of-$m$ technique and a time-data trade-off, without using almost the full codebook
- **New results on round-reduced AES.** The conversions yield improved RKP distinguishers and key-recovery attacks on all AES variants, extending previous results by at least one round
- **RKP may benefit from other trails than the CP model.**
  The conversion changes which properties are easy to obtain;
  thus, optimal trails can change
- **Security interpretation stays theoretical.** The complexities are far from threatening full AES.

**Thanks for your attention!**

Questions?

# Bibliography I



Tomer Ashur and Erik Takke.
A New Linear Distinguisher for Four-Round AES.
*IACR Cryptol. ePrint Arch.*, page 398, 2023.


Tomer Ashur and Erik Takke.
A New Linear Distinguisher for Four-Round AES.
*J. Cryptol.*, 38(4):30, 2025.


Charles Bouillaguet, Patrick Derbez, Orr Dunkelman, Pierre-Alain Fouque, Nathan Keller, and Vincent Rijmen.
Low-Data Complexity Attacks on AES.
*IEEE Trans. Inf. Theory*, 58(11):7002–7017, 2012.


Charles Bouillaguet, Patrick Derbez, and Pierre-Alain Fouque.
Automatic Search of Attacks on Round-Reduced AES and Applications.
In Phillip Rogaway, editor, *CRYPTO*, volume 6841 of *Lecture Notes in Computer Science*, pages 169–187. Springer, 2011.


Zhenzhen Bao, Jian Guo, and Eik List.
Extended Truncated-differential Distinguishers on Round-reduced AES.
*IACR Trans. Symmetric Cryptol.*, 2020(3):197–261, 2020.

# Bibliography II



Augustin Bariant and Gaëtan Leurent.
Truncated Boomerang Attacks and Application to AES-Based Ciphers.
In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT IV*, volume 14007 of *Lecture Notes in Computer Science*, pages 3–35. Springer, 2023.


Christina Boura, Virginie Lallemand, María Naya-Plasencia, and Valentin Suder.
Making the Impossible Possible.
*J. Cryptology*, 31(1):101–133, 2018.


Christina Boura, María Naya-Plasencia, and Valentin Suder.
Scrutinizing and Improving Impossible Differential Attacks: Applications to CLEFIA, Camellia, LBlock and Simon.
In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT I*, volume 8873 of *Lecture Notes in Computer Science*, pages 179–199. Springer, 2014.


Andrey Bogdanov and Vincent Rijmen.
Zero-Correlation Linear Cryptanalysis of Block Ciphers.
*IACR Cryptol. ePrint Arch.*, page 123, 2011.


Andrey Bogdanov and Vincent Rijmen.
Linear hulls with correlation zero and linear cryptanalysis of block ciphers.
*Des. Codes Cryptogr.*, 70(3):369–383, 2014.

# Bibliography III



Navid Ghaedi Bardeh and Sondre Rønjom.
Practical Attacks on Reduced-Round AES.
In Johannes Buchmann, Abderrahmane Nitaj, and Tajje-eddine Rachidi, editors, *Africacrypt*, volume 11627 of *Lecture Notes in Computer Science*, pages 297–310. Springer, 2019.


Navid Ghaedi Bardeh and Sondre Rønjom.
The Exchange Attack: How to Distinguish Six Rounds of AES with $2^{88.2}$ Chosen Plaintexts.
In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT III*, volume 11923 of *Lecture Notes in Computer Science*, pages 347–370. Springer, 2019.


Navid Ghaedi Bardeh and Vincent Rijmen.
New Key-Recovery Attack on Reduced-Round AES.
*IACR Trans. Symmetric Cryptol.*, 2022(2):43–62, 2022.


Eli Biham and Adi Shamir.
Differential Cryptanalysis of the Full 16-Round DES.
In Ernest F. Brickell, editor, *CRYPTO*, volume 740 of *Lecture Notes in Computer Science*, pages 487–496. Springer, 1992.


Shiyao Chen, Jian Guo, Eik List, Danping Shi, and Tianyu Zhang.
Scrutinizing the Security of AES-Based Hashing and One-Way Functions.
In Goichiro Hanaoka and Bo-Yin Yang, editors, *ASIACRYPT I*, volume 16245 of *Lecture Notes in Computer Science*, pages 157–188. Springer, 2025.

# Bibliography IV



Chengcheng Chang, Meiqin Wang, Ling Sun, and Wei Wang.
Improved Truncated Differential Distinguishers of AES with Concrete S-Box.
In Takanori Isobe and Santanu Sarkar, editors, *INDOCRYPT*, volume 13774 of *Lecture Notes in Computer Science*, pages 422–445. Springer, 2022.


Patrick Derbez.
*Attaques par Rencontre par le Milieu sur l'AES (Meet-in-the-Middle Attacks on AES)*.
PhD thesis, Ecole Normale Supérieure de Paris Paris, France, 2013.
https://theses.hal.science/tel-00918146.


Patrick Derbez, Pierre-Alain Fouque, and Jérémy Jean.
Improved Key Recovery Attacks on Reduced-Round AES in the Single-Key Setting.
In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT*, volume 7881 of *Lecture Notes in Computer Science*, pages 371–387. Springer, 2013.


Orr Dunkelman, Nathan Keller, and Adi Shamir.
Improved Single-Key Attacks on 8-Round AES-192 and AES-256.
In Masayuki Abe, editor, *ASIACRYPT*, volume 6477 of *Lecture Notes in Computer Science*, pages 158–176. Springer, 2010.


Xiaoli Dong, Jun Liu, Yongzhuang Wei, Wen Gao, and Jie Chen.
Meet-in-the-middle attacks on AES with value constraints.
*Des. Codes Cryptogr.*, 92(9):2423–2449, 2024.

# Bibliography V



Hüseyin Demirci and Ali Aydin Selçuk.
A Meet-in-the-Middle Attack on 8-Round AES.
In Kaisa Nyberg, editor, *FSE*, volume 5086 of *Lecture Notes in Computer Science*, pages 116–126. Springer, 2008.


Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Michael Stay, David A. Wagner, and Doug Whiting.
Improved Cryptanalysis of Rijndael.
In Bruce Schneier, editor, *FSE*, volume 1978 of *Lecture Notes in Computer Science*, pages 213–230. Springer, 2000.


Lorenzo Grassi.
Mixture Differential Cryptanalysis: a New Approach to Distinguishers and Attacks on round-reduced AES.
*IACR Transactions on Symmetric Cryptology*, 2018(2):133–160, 2018.


Orhun Kara.
Square impossible differential attack and security of AES in known plaintext scenario.
*Cryptologia*, 49(2):128–152, 2025.


Gaëtan Leurent and Clara Pernot.
New Representations of the AES Key Schedule.
In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT I*, volume 12696 of *Lecture Notes in Computer Science*, pages 54–84. Springer, 2021.

# Bibliography VI



Gaëtan Leurent and Clara Pernot.
New Representations of the AES Key Schedule.
*J. Cryptol.*, 38(1):2, 2025.


Jiqiang Lu and Wenchang Zhou.
Improved Meet-in-the-Middle Attacks on Nine Rounds of the AES-192 Block Cipher.
In Elisabeth Oswald, editor, *CT-RSA*, volume 14643 of *Lecture Notes in Computer Science*, pages 136–159. Springer, 2024.


Hamid Mala, Mohammad Dakhilalian, Vincent Rijmen, and Mahmoud Modarres-Hashemi.
Improved Impossible Differential Cryptanalysis of 7-Round AES-128.
In Guang Gong and Kishan Chand Gupta, editors, *INDOCRYPT*, volume 6498 of *Lecture Notes in Computer Science*, pages 282–291. Springer, 2010.


National Institute of Standards and Technology.
FIPS 197.
*National Institute of Standards and Technology, November*, pages 1–51, 2001.


Xueping Yan, Lin Tan, Hong Xu, and Wen-Feng Qi.
The Boomerang Chain Distinguishers: New Record for 6-Round AES.
In Kai-Min Chung and Yu Sasaki, editors, *ASIACRYPT VII*, volume 15490 of *Lecture Notes in Computer Science*, pages 301–329. Springer, 2024.