Aalto University
School of Science

Links Between Truncated Differential and Multidimensional Linear Properties of Block Ciphers and Underlying Attack Complexities

Céline Blondeau and Kaisa Nyberg

Monday 12 May 2014

EUROCRYPT, Copenhagen

Outline

Statistical Attacks
- Truncated Differential (TD) Cryptanalysis
- Multidimensional Linear (ML) Cryptanalysis

Link between ML and TD Attacks
- Mathematical Relation between ML and TD
- Complexity of TD and ML Distinguishing Attacks

Statistical Saturation Attack
- Definition
- Statistical Saturation Attack on PRESENT

Converting a ML Attack to a TD Attack
- Example on PRESENT
- Conclusion

Outline

Statistical Attacks
- Truncated Differential (TD) Cryptanalysis
- Multidimensional Linear (ML) Cryptanalysis

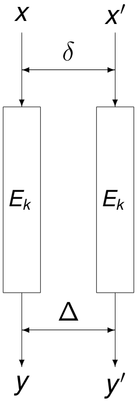
Link between ML and TD Attacks
- Mathematical Relation between ML and TD
- Complexity of TD and ML Distinguishing Attacks

Statistical Saturation Attack
- Definition
- Statistical Saturation Attack on PRESENT

Converting a ML Attack to a TD Attack
- Example on PRESENT
- Conclusion

Differential Cryptanalysis [Biham Shamir 90]

Difference between plaintext and ciphertext pairs



Input difference : δ
Output Difference : Δ

Differential Probability :

$$\mathbf{P}[\delta \to \Delta] = P_x[\, E_k(x) \oplus E_k(x \oplus \delta) = \Delta]$$

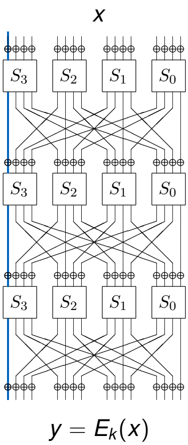
Truncated Differential (TD) [Knudsen 94] :

Set of input differences : $\delta \in A$
Set of output differences : $\Delta \in B$

$$\mathbf{P}[A \to B] = \frac{1}{|A|} \sum_{\delta \in A} \sum_{\Delta \in B} P[\delta \to \Delta]$$

Linear Cryptanalysis [Tardy Gilbert 91] [Matsui 93]

Linear relation involving plaintext, key and ciphertext bits



Input mask : u

Output mask : v

Correlation :

$$\mathbf{cor}_x(u, v) = 2 \cdot P_x \left[u \cdot x \oplus v \cdot E_k(x) = 0\right] - 1$$

Multidimensional Linear (ML) Approximation [Hermelin et al 08] :

Set of masks $(u, v) \in U \times V \setminus \{0, 0\}$

Capacity :

$$C = \sum_{u \in U \setminus \{0\}} \sum_{v \in V \setminus \{0\}} \mathbf{cor}_x^2(u, v)$$

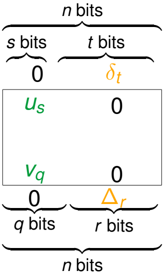
Outline

Link between Differential and Linear Cryptanalysis

[Chabaud Vaudenay 94] :

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$

$$\mathbf{P}[\delta \to \Delta] = 2^{-m} \sum_{u \in \mathbb{F}_2^n} \sum_{v \in \mathbb{F}_2^m} (-1)^{u \cdot \delta \oplus v \cdot \Delta} \mathbf{cor}_x^2(u, v)$$

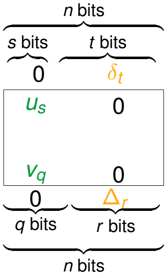


Link between Differential and Linear Cryptanalysis

[Chabaud Vaudenay 94] :

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$

$$\mathbf{P}[\delta \to \Delta] = 2^{-m} \sum_{u \in \mathbb{F}_2^n} \sum_{v \in \mathbb{F}_2^m} (-1)^{u \cdot \delta \oplus v \cdot \Delta} \mathbf{cor}_x^2(u, v)$$



Generalization :

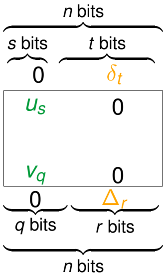
- ML : $[(u_s, 0), (v_q, 0)]_{u_s \in \mathbb{F}_2^s \setminus \{0\},\ v_q \in \mathbb{F}_2^q}$ with capacity C
- TD : $[(0, \delta_t), (0, \Delta_r)]_{\delta_t \in \mathbb{F}_2^t,\ \Delta_r \in \mathbb{F}_2^r}$ with probability p

Link between Differential and Linear Cryptanalysis

[Chabaud Vaudenay 94] :

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$

$$\mathbf{P}[\delta \to \Delta] = 2^{-m} \sum_{u \in \mathbb{F}_2^n} \sum_{v \in \mathbb{F}_2^m} (-1)^{u \cdot \delta \oplus v \cdot \Delta} \mathbf{cor}_x^2 (u, v)$$



Generalization :

- ML : $[(u_s, 0), (v_q, 0)]_{u_s \in \mathbb{F}_2^s \setminus \{0\},\ v_q \in \mathbb{F}_2^q}$ with capacity C
- TD : $[(0, \delta_t), (0, \Delta_r)]_{\delta_t \in \mathbb{F}_2^t,\ \Delta_r \in \mathbb{F}_2^r}$ with probability p

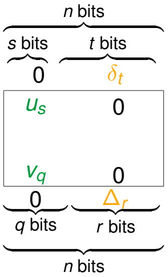
$$p = 2^{-q}(C + 1)$$

Link between Differential and Linear Cryptanalysis

[Chabaud Vaudenay 94] :

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$

$$\mathbf{P}[\delta \to \Delta] = 2^{-m} \sum_{u \in \mathbb{F}_2^n} \sum_{v \in \mathbb{F}_2^m} (-1)^{u \cdot \delta \oplus v \cdot \Delta} \mathbf{cor}_x^2(u, v)$$



Generalization :

- ML : $[(u_s, 0), (v_q, 0)]_{u_s \in \mathbb{F}_2^s \setminus \{0\},\ v_q \in \mathbb{F}_2^q}$ with capacity C
- TD : $[(0, \delta_t), (0, \Delta_r)]_{\delta_t \in \mathbb{F}_2^t,\ \Delta_r \in \mathbb{F}_2^r}$ with probability p

$$p = 2^{-q}(C + 1)$$

- TD is a chosen plaintext (CP) attack
- ML is a known plaintext (KP) attack

Data Complexity of a Distinguishing Attack

[Selçuk 07] $P_S = 50\%$ and $\varphi_a = \Phi^{-1}(1 - 2^{-a})$, with a the advantage

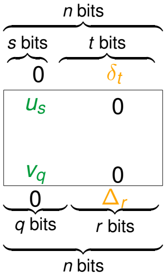
- Multidimensional Linear :

$$N^{ML} = \frac{2^{(s+q+1)/2}}{C} \cdot \varphi_a$$

- Truncated Differential :

$$N^{TD} = \frac{2^{-q+1}}{M \cdot (p - 2^{-q})^2} \cdot \varphi_a^2,$$

where M is the size of a structure (usually $M = 2^t$)



Data Complexity of a Distinguishing Attack

[Selçuk 07] $P_S = 50\%$ and $\varphi_a = \Phi^{-1}(1 - 2^{-a})$, with a the advantage

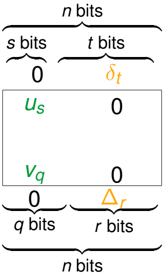
- Multidimensional Linear :

$$N^{ML} = \frac{2^{(s+q+1)/2}}{C} \cdot \varphi_a$$

- Truncated Differential :

$$N^{TD} = \frac{2^{-q+1}}{M \cdot (p - 2^{-q})^2} \cdot \varphi_a^2,$$

where M is the size of a structure (usually $M = 2^t$)



- For $p = 2^{-q}(C + 1)$:

$$N^{TD} = \frac{2^{q+1}}{2^t \cdot C^2} \cdot {\varphi_a}^2$$

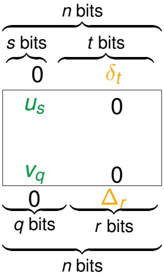
Data Complexity of a Distinguishing Attack

[Selçuk 07] $P_S = 50\%$ and $\varphi_a = \Phi^{-1}(1 - 2^{-a})$, with a the advantage

- $$N^{ML} = \frac{2^{(s+q+1)/2}}{C} \cdot \varphi_a$$

- For $p = 2^{-q}(C+1)$:

$$N^{TD} = \frac{2^{q+1}}{2^t \cdot C^2} \cdot {\varphi_a}^2$$



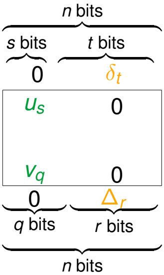
Data Complexity of a Distinguishing Attack

[Selçuk 07] $P_S = 50\%$ and $\varphi_a = \Phi^{-1}(1 - 2^{-a})$, with a the advantage

- $$N^{ML} = \frac{2^{(s+q+1)/2}}{C} \cdot \varphi_a$$

- For $p = 2^{-q}(C+1)$:

$$N^{TD} = \frac{2^{q+1}}{2^t \cdot C^2} \cdot {\varphi_a}^2$$



$$N^{TD} = \frac{1}{2^n} \cdot (N^{ML})^2$$

Data Complexity of a Distinguishing Attack

[Selçuk 07] $P_S = 50\%$ and $\varphi_a = \Phi^{-1}(1 - 2^{-a})$, with a the advantage

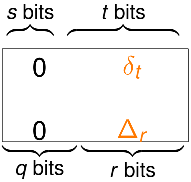
- $$N^{ML} = \frac{2^{(s+q+1)/2}}{C} \cdot \varphi_a$$
- For $p = 2^{-q}(C+1)$:
$$N^{TD} = \frac{2^{q+1}}{2^t \cdot C^2} \cdot {\varphi_a}^2$$

$$\begin{array}{|cc|} \multicolumn{2}{c}{\overbrace{\hspace{8em}}^{n \text{ bits}}} \\ \multicolumn{1}{c}{\overbrace{0}^{s \text{ bits}}} & \multicolumn{1}{c}{\overbrace{\delta_t}^{t \text{ bits}}} \\ \hline u_s & 0 \\ & \\ v_q & 0 \\ \hline \multicolumn{1}{c}{\underbrace{0}_{q \text{ bits}}} & \multicolumn{1}{c}{\underbrace{\Delta_r}_{r \text{ bits}}} \\ \multicolumn{2}{c}{\underbrace{\hspace{8em}}_{n \text{ bits}}} \end{array}$$

$$N^{TD} = \frac{1}{2^n} \cdot (N^{ML})^2$$

$N^{TD} \leq N^{ML}$ with equality when using the full codebook

Truncated Differential Distinguisher



$$x = (x_s, x_t)$$

$$y = (y_q, y_r)$$

M : size of a structure
S : number of structures

$$N^{TD} = S \cdot M$$

$D = 0$
for S values of $x_s \in \mathbb{F}_2^s$ **do**
  Create a table T of size M
  for M values of $x_t \in \mathbb{F}_2^t$ **do**
    $(y_q, y_r) = E((x_s, x_t))$
    $T[x_t] = y_q$
  for all pairs (x_t, x_t') **do**
    if $(T[x_t] \oplus T[x_t']) == 0$ **then**
      $D += 1$

For S structures

For all elements in a structure

Store the partial ciphertexts

Count the number of pairs which have no difference on the q bits

Truncated Differential Distinguisher

Time Complexity : Verifying all pairs

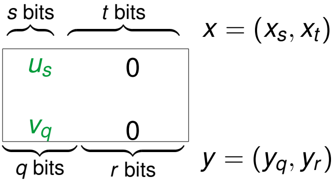
$$Time \approx S \cdot M^2/2$$

Memory Complexity : Storing all ciphertexts inside a structure

$$Memory \approx M$$

$D = 0$	
for S values of $x_s \in \mathbb{F}_2^s$ **do**	For S structures
Create a table T of size M	
for M values of $x_t \in \mathbb{F}_2^t$ **do**	For all elements in a structure
$(y_q, y_r) = E((x_s, x_t))$	Store the partial ciphertexts
$T[x_t] = y_q$	
for all pairs (x_t, x'_t) **do**	Count the number of pairs which have no difference on the q bits
if $(T[x_t] \oplus T[x'_t]) == 0$ **then**	
$D += 1$	

Multidimensional Linear Distinguisher



Set a counter D to 0
Create a table T of size 2^{q+s}
for N^{ML} plaintexts **do**
    $(y_q, y_r) = E((x_s, x_t))$
    $T[(x_s, y_q)] += 1$
for all (x_s, y_q) **do**
    $D += (T[(x_s, y_q)] - N/2^{q+s})^2$

For N^{ML} plaintexts
  Count the number of occurrences of each pair (x_s, y_q)

Compute the statistic

Multidimensional Linear Distinguisher

Time Complexity : Reading all messages

$$Time \approx N^{ML}$$

Memory Complexity : Storing the number of occurrences of $(x_s^i, y_q^j)_{i,j}$

$$Memory \approx 2^{s+q}$$

Set a counter D to 0
Create a table T of size 2^{q+s}
for N^{ML} plaintexts **do**
    $(y_q, y_r) = E((x_s, x_t))$
    $T[(x_s, y_q)] += 1$
for all (x_s, y_q) **do**
    $D += (T[(x_s, y_q)] - N/2^{q+s})^2$

For N^{ML} plaintexts
  Count the number of occurrences of each pair (x_s, y_q)

Compute the statistic

Complexities of TD and ML Attacks

- ML distinguisher :

$$Data = N^{ML}$$

$$Time \approx N^{ML}$$

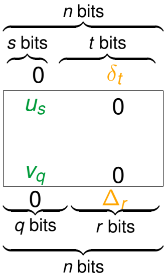
$$Memory \approx 2^{s+q}$$

- TD distinguisher :

$$Data = N^{TD} = S \cdot 2^{t} < N^{ML}$$

$$Time \approx N^{TD} \cdot 2^{t-1}$$

$$Memory \approx 2^{t}$$



Question : Can we decrease the time complexity of a TD attack?

TD with Less Time Complexity

- Dominant part: Verifying the output difference for each pair of ciphertexts

Example :

- 4 ciphertexts : (y_1, b_1) (y_2, b_2) (y_1, b_3) (y_3, b_4)
  1 pair with equal y_i
- Previous algorithm : 6 comparisons

TD with Less Time Complexity

- Dominant part: Verifying the output difference for each pair of ciphertexts

Example :

- 4 ciphertexts : (y_1, b_1) (y_2, b_2) (y_1, b_3) (y_3, b_4)
  1 pair with equal y_i
- Previous algorithm : 6 comparisons

Improved Version :

- Count the occurrences of each y_i :

	y_1	y_2	y_3
$T[y_i]$	2	1	1

and compute $D = \sum_i T[y_i](T[y_i] - 1)/2 = 1$

TD with Less Time Complexity

$D = 0$
for S values of $x_s \in \mathbb{F}_2^s$ **do**
  Create a table T of size 2^q
  for M values of $x_t \in \mathbb{F}_2^t$ **do**
    $(y_q, y_r) = E((x_s, x_t))$
    $T[y_q] += 1$
  for all $y_q \in \mathbb{F}_2^q$ **do**
    $D += T[y_q](T[y_q] - 1)/2$

For S structures

For all elements in a structure

Count the number of occurrences of the partial ciphertexts

Compute the statistic

$$Data = N^{TD} = S \cdot M < N^{ML}$$

$$Time \approx max(N^{TD}, S \cdot 2^q)$$

$$Memory \approx 2^q$$

TD with Less Time Complexity

$D = 0$
for S values of $x_s \in \mathbb{F}_2^s$ **do**
    Create a table T of size 2^q
    for M values of $x_t \in \mathbb{F}_2^t$ **do**
        $(y_q, y_r) = E((x_s, x_t))$
        $T[y_q] += 1$
    for all $y_q \in \mathbb{F}_2^q$ **do**
        $D += T[y_q](T[y_q] - 1)/2$

For S structures

For all elements in a structure

Count the number of occurrences of the partial ciphertexts

Compute the statistic

Remark :

This distinguisher is the same as the statistical saturation (SS) distinguisher

Outline

Statistical Saturation (SS) Attack [Collard Standaert 09]

Idea :

- "Dual" of the saturation attack
- Takes advantage of several plaintexts with some fixed bits while the others vary randomly
- We observe the diffusion of the fixed bits during the encryption process

Application on PRESENT [Bogdanov et al 08] :

- Distinguisher on 20 / 21 rounds
- Key-recovery on 24 rounds

Link between SS, TD and ML distinguishers

Link [Leander 11] :
For a fixed $x_s \in \mathbb{F}_2^s$, we denote by $C(x_s)$ the capacity of the distribution of y_q :

$$C = 2^{-s} \sum_{x_s \in \mathbb{F}_2^s} C(x_s)$$

Link between SS, TD and ML distinguishers

Link [Leander 11] :
For a fixed $x_s \in \mathbb{F}_2^s$, we denote by $C(x_s)$ the capacity of the distribution of y_q :

$$C = 2^{-s} \sum_{x_s \in \mathbb{F}_2^s} C(x_s)$$

- SS attacks link mathematically with ML attacks

Link between SS, TD and ML distinguishers

Link [Leander 11] :
For a fixed $x_s \in \mathbb{F}_2^s$, we denote by $C(x_s)$ the capacity of the distribution of y_q :

$$C = 2^{-s} \sum_{x_s \in \mathbb{F}_2^s} C(x_s)$$

- SS attacks link mathematically with ML attacks

SS is a chosen plaintext (CP) attack
ML is a known plaintext (KP) attack

Link between SS, TD and ML distinguishers

Link [Leander 11] :
For a fixed $x_s \in \mathbb{F}_2^s$, we denote by $C(x_s)$ the capacity of the distribution of y_q :

$$C = 2^{-s} \sum_{x_s \in \mathbb{F}_2^s} C(x_s)$$

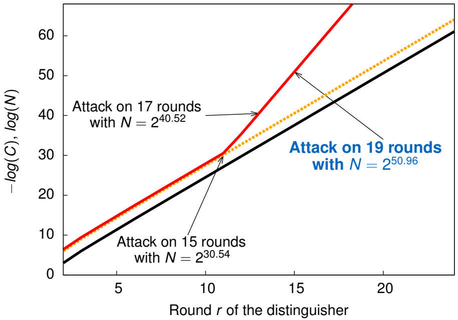
- SS attacks link mathematically with ML attacks

SS is a chosen plaintext (CP) attack
ML is a known plaintext (KP) attack

- SS attacks link algorithmically with TD attacks

On the SS Attack on PRESENT [Collard Standaert 09]

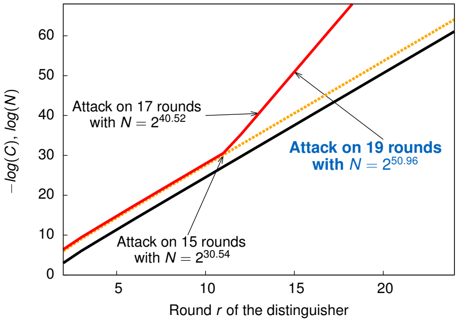
Attack on $r + 4$ rounds with $M = 2^{32}$



- [Collard Standaert 09]
  Data increases linearly
- [Leander 11]
  Estimate of the capacity C
- [Our work]
  Data is $N = \dfrac{2^{q+1}}{M \cdot C^2} \cdot \varphi_a^2$

On the SS Attack on PRESENT [Collard Standaert 09]

Attack on $r + 4$ rounds with $M = 2^{32}$



[Collard Standaert 09]
Data increases linearly

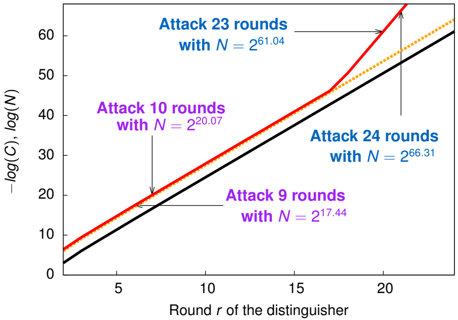
[Leander 11]
Estimate of the capacity C

[Our work]
Data is $N = \dfrac{2^{q+1}}{M \cdot C^2} \cdot \varphi_a^2$

- The attack has been verified experimentally [Kerckhof et al 11]
- Our estimate match with the experiments (N around 2^{51} for 19 rounds)

On the SS Attack on PRESENT [Collard Standaert 09]

Attack on $r + 3$ rounds with $M = 2^{48}$



- Estimate of the capacity C
- *Data* is proportional to $\frac{1}{C}$
- *Data* is $N = \frac{2^{q+1}}{M \cdot C^2} \cdot \varphi_a^2$

- In this model, one can only perform an attack 23 rounds

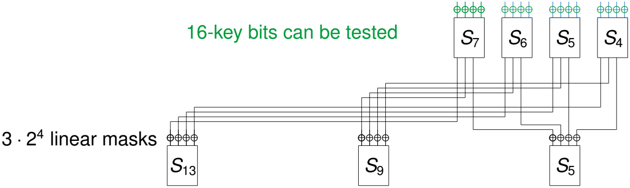
Outline

KP ML and CP TD Attacks : An Example on PRESENT

[Cho 10] :

- ML distinguisher on 24 rounds
- KP ML attack on 26 rounds (inversion of the first and last round)

First round : (In Cho's ML characteristic)



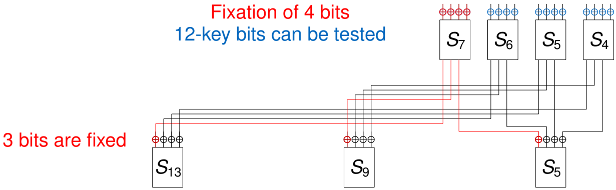
- KP ML $\Rightarrow$ Guess 16-key bits

KP ML and CP TD Attacks : An Example on PRESENT

[Cho 10] :

- ML distinguisher on 24 rounds
- KP ML attack on 26 rounds (inversion of the first and last round)

First round : (In Cho's ML characteristic)



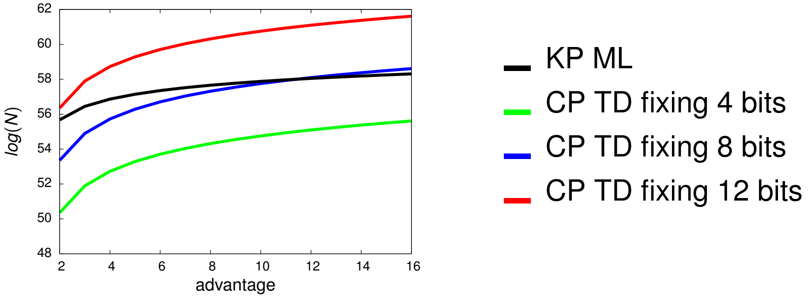
- KP ML $\Rightarrow$ Guess 16-key bits

Using the link between TD and ML

- CP TD $\Rightarrow$ Guess $4, 8, 12, 16$-key bits

Example of CP TD Attack on 24 Rounds of PRESENT

Data Complexity (*Data*) :



- The *Data* of a KP ML is proportional to $\varphi_a = \Phi^{-1}(1 - 2^{-a})$
- The *Data* of a CP TD is proportional to φ_a^2
- Depending of the size of the fixation, the data complexity of a CP ML attack can be smaller than for a KP ML attack

Example of CP TD Attack on 24 Rounds of PRESENT

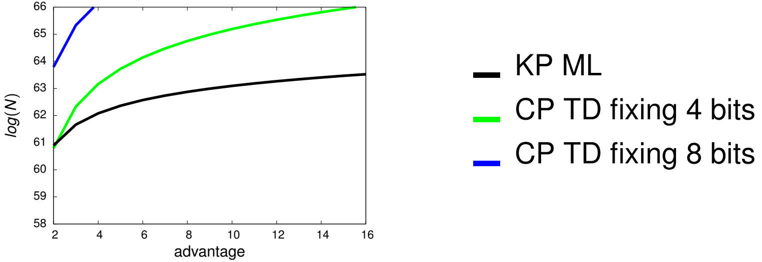
Fixing 4 bits :

Model	a	*Data*	*Memory*	$Time_1$	$Time_2$
CP TD	10	$2^{54.75}$	2^{29}	$2^{54.75}$	2^{70}
KP ML	5	$2^{57.14}$	2^{32}	$2^{57.14}$	2^{75}

$Time_1$: Complexity of the distillation phase
$Time_2$: Complexity of the search phase

- Data, time and memory complexities of the CP TD are smaller than those of a KP ML attack

Example of CP TD Attack on 26 Rounds of PRESENT



Model	a	*Data*	*Memory*	$Time_1$	$Time_2$
CP TD	4	$2^{63.16}$	2^{29}	$2^{63.16}$	2^{76}
KP ML	4	$2^{62.08}$	2^{32}	$2^{62.08}$	2^{76}

- A CP TD attack on 26 rounds of PRESENT with less memory than the KP ML attack
- The previous differential-type attack was on 19 rounds

Conclusion

In this work :

- We analyze the complexities of some statistical attacks and their relation
- We show that the SS attack is a TD attack
- We illustrate that a KP ML attack can be converted to a CP TD attack with smaller complexities

Thank You