Exact Formula for RX-Differential Probability Through Modular Addition for All Rotations

Alex Biryukov Baptiste Lambin Aleksei Udovenko

FSE 2025, March 18th

DCS and SnT, University of Luxembourg

Luxembourg's FNR and Germany's DFG joint project APLICA (C19/IS/13641232)

Outline

Rotational-XOR Cryptanalysis

Exact Probability Formula for all Rotations k

Modeling and Applications

- New best RX-trails for Alzette
- RX-backdoor from malicious constants - Malzette

Conclusions

Plan

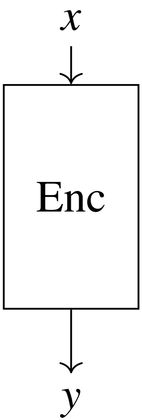
Rotational-XOR Cryptanalysis

Exact Probability Formula for all Rotations k

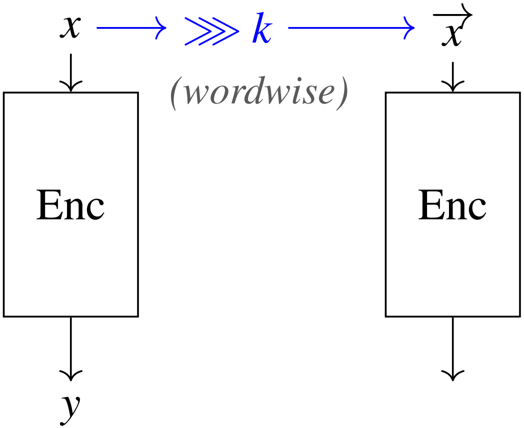
Modeling and Applications

Conclusions

Rotational Cryptanalysis [Khovratovich and Nikolic 2010 FSE]



Rotational Cryptanalysis [Khovratovich and Nikolic 2010 FSE]



Rotational Cryptanalysis [Khovratovich and Nikolic 2010 FSE]

$$
\begin{tikzcd}
x \arrow[r, "\ggg k"] \arrow[d] & \overrightarrow{x} \arrow[d] \\
\mathrm{Enc} \arrow[d] & \mathrm{Enc} \arrow[d] \\
y \arrow[r, "\ggg k"] & \overrightarrow{y}\,?
\end{tikzcd}
$$

Rotational Cryptanalysis [Khovratovich and Nikolic 2010 FSE]

Through XOR

$$
\begin{tikzcd}
\overrightarrow{x} \arrow[d] & \\
\oplus \arrow[d] & \overrightarrow{y} \arrow[l] \\
\overrightarrow{x \oplus y} &
\end{tikzcd}
$$

Rotational Cryptanalysis [Khovratovich and Nikolic 2010 FSE]

Through XOR

$$\begin{tikzcd} \overrightarrow{x} \arrow[d] & \\ \oplus \arrow[d] & \textcolor{red}{\overrightarrow{k}} \arrow[l] \\ \overrightarrow{x \oplus \textcolor{red}{k}} & \end{tikzcd}$$

Related-Key

Rotational Cryptanalysis [Khovratovich and Nikolic 2010 FSE]

Through XOR

$$\begin{tikzcd}
\overrightarrow{x} \arrow[d] & \\
\oplus \arrow[d] & \overrightarrow{k} \arrow[l] \\
\overrightarrow{x \oplus k} &
\end{tikzcd}$$

Related-Key

Through ADD

$$\begin{tikzcd}
\overrightarrow{x} \arrow[d] & \\
\boxplus \arrow[d, "\mathrm{Pr=p}"] & \overrightarrow{y} \arrow[l] \\
\overrightarrow{x \boxplus y} &
\end{tikzcd}$$

Rotational Cryptanalysis [Khovratovich and Nikolic 2010 FSE]

Through XOR

$$\begin{tikzcd} \overrightarrow{x} \arrow[d] & \\ \oplus \arrow[d] & \overrightarrow{k} \arrow[l] \\ \overrightarrow{x \oplus k} & \end{tikzcd}$$

Related-Key

Through ADD

$$\begin{tikzcd} \overrightarrow{x} \arrow[d] & \\ \boxplus \arrow[d, "\mathrm{Pr=p}"] & \overrightarrow{y} \arrow[l] \\ \overrightarrow{x \boxplus y} & \end{tikzcd}$$

$$\underset{(k=\frac{n}{2})}{\frac{2}{8}} \leq p \leq \underset{(k=1)}{\frac{3}{8}} + \epsilon$$

Rotational Cryptanalysis [Khovratovich and Nikolic 2010 FSE]

Through XOR

$$\begin{tikzcd}
\overrightarrow{x} \arrow[d] & \\
\oplus \arrow[d] & \overrightarrow{k} \arrow[l] \\
\overrightarrow{x \oplus k} &
\end{tikzcd}$$

Related-Key

Through ADD

$$\begin{tikzcd}
\overrightarrow{x} \arrow[d] & \\
\boxplus \arrow[d, "\mathrm{Pr=p}"] & \overrightarrow{y} \arrow[l] \\
\overrightarrow{x \boxplus y} &
\end{tikzcd}$$

$$\underset{(k=\frac{n}{2})}{\frac{2}{8}} \leq p \leq \underset{(k=1)}{\frac{3}{8}} + \epsilon$$

Through XOR-const

$$\begin{tikzcd}
\overrightarrow{x} \arrow[d] & \\
\oplus \arrow[d] & c \arrow[l] \\
\overrightarrow{x \oplus c}\ ? &
\end{tikzcd}$$

Rotational Cryptanalysis [Khovratovich and Nikolic 2010 FSE]

Through XOR

$$\begin{tikzcd}
\overrightarrow{x} \arrow[d] & \\
\oplus \arrow[d] & \overrightarrow{k} \arrow[l] \\
\overrightarrow{x \oplus k} &
\end{tikzcd}$$

Related-Key

Through ADD

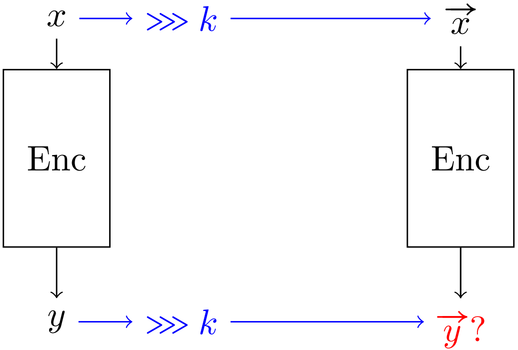
$$\begin{tikzcd}
\overrightarrow{x} \arrow[d] & \\
\boxplus \arrow[d, "\mathrm{Pr=p}"] & \overrightarrow{y} \arrow[l] \\
\overrightarrow{x \boxplus y} &
\end{tikzcd}$$

$$\underset{(k=\frac{n}{2})}{\frac{2}{8}} \leq p \leq \underset{(k=1)}{\frac{3}{8}} + \epsilon$$

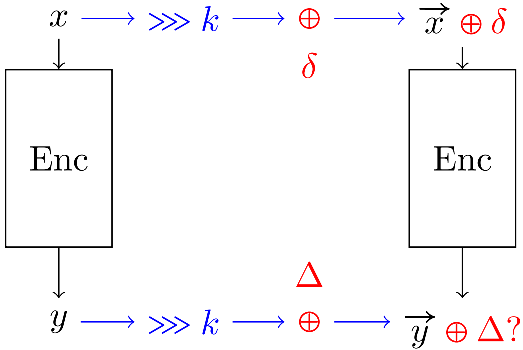
Through XOR-const

$$\begin{tikzcd}
\overrightarrow{x} \arrow[d] & \\
\oplus \arrow[d] & c \arrow[l] \\
\overrightarrow{x \oplus c} \oplus (c \oplus \overrightarrow{c}) &
\end{tikzcd}$$

Rotational-XOR (RX) Cryptanalysis [Ashur and Liu 2016 FSE]



Rotational-XOR (RX) Cryptanalysis [Ashur and Liu 2016 FSE]



Rotational-XOR (RX) Cryptanalysis [Ashur and Liu 2016 FSE]

$$
\begin{tikzcd}
\overleftarrow{x} \oplus \alpha \arrow[d] & \\
\boxplus \arrow[d, "\mathrm{Pr=p}"] & \overleftarrow{y} \oplus \beta \arrow[l] \\
\overleftarrow{x \boxplus y} \oplus \Delta &
\end{tikzcd}
$$

Rotational-XOR (RX) Cryptanalysis [Ashur and Liu 2016 FSE]

$$
\begin{tikzcd}
\overleftarrow{x} \oplus \alpha \arrow[d] & \\
\boxplus \arrow[d, "\mathrm{Pr=p}"] & \overleftarrow{y} \oplus \beta \arrow[l] \\
\overleftarrow{x \boxplus y} \oplus \Delta &
\end{tikzcd}
$$

Theorem ([AL16], $k = 1$)

$$
\begin{aligned}
p = {} & \mathbb{1}_{(I \oplus \mathrm{SHL})(\chi_L) \oplus 1 \preccurlyeq \mathrm{SHL}(\nu_L)} \cdot 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))} \cdot 2^{-3} \\
& + \mathbb{1}_{(I \oplus \mathrm{SHL})(\chi_L) \preccurlyeq \mathrm{SHL}(\nu_L)} \cdot 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))} \cdot 2^{-1.415}
\end{aligned}
$$

Rotational-XOR (RX) Cryptanalysis [Ashur and Liu 2016 FSE]

$$\begin{tikzcd}
\overleftarrow{x} \oplus \alpha \arrow[d] & \\
\boxplus \arrow[d, "\mathrm{Pr}=\mathrm{p}"] & \overleftarrow{y} \oplus \beta \arrow[l] \\
\overleftarrow{x \boxplus y} \oplus \Delta &
\end{tikzcd}$$

Theorem ([AL16], $k = 1$)

$$p = \mathbb{1}_{(I \oplus \mathsf{SHL})(\chi_L) \oplus 1 \preccurlyeq \mathsf{SHL}(\nu_L)} \cdot 2^{-\mathrm{wt}(\mathsf{SHL}(\nu_L))} \cdot 2^{-3}$$
$$+ \mathbb{1}_{(I \oplus \mathsf{SHL})(\chi_L) \preccurlyeq \mathsf{SHL}(\nu_L)} \cdot 2^{-\mathrm{wt}(\mathsf{SHL}(\nu_L))} \cdot 2^{-1.415}$$

where

$(\chi_L || \chi_0) = \alpha \oplus \beta \oplus \Delta$

$(\nu_L || \nu_0) = (\alpha \oplus \beta) \vee (\alpha \oplus \Delta)$ *(not-all-equal)*

SHL : shift left by 1 position (drop MSB)

$2^{-\mathrm{wt}(\mathsf{SHL}(\nu_L))}$ is a normal ARX differential prob. (excl. LSB)

Our contribution

Our contribution

Ours: probability, any k

$$p = T_{n-k}(\chi_L, \nu_L, \chi_0) \times T_k(\chi_R, \nu_R, \chi_k)$$

$$T_m(\boldsymbol{\chi}, \boldsymbol{\nu}, \hat{\chi}_i) = 2^{-\mathrm{wt}(\mathsf{SHL}(\boldsymbol{\nu}))-1} + \mathbb{1}_{\boldsymbol{\chi} \in \{0\ldots0,1\ldots1\}} \times (-1)^{\hat{\chi}_i} \times 2^{-m-1}$$

Our contribution

[AL16], $k = 1$

Not fully correct:

$\exists$ class of transitions with probability

2x lower or **1.5x** higher

Ours: probability, any k

$$p = T_{n-k}(\chi_L, \nu_L, \chi_0) \times T_k(\chi_R, \nu_R, \chi_k)$$

$$T_m(\boldsymbol{\chi}, \boldsymbol{\nu}, \hat{\chi}_i) = 2^{-\mathrm{wt}(\mathsf{SHL}(\boldsymbol{\nu}))-1} + \mathbb{1}_{\boldsymbol{\chi} \in \{0\ldots0,1\ldots1\}} \times (-1)^{\hat{\chi}_i} \times 2^{-m-1}$$

Our contribution

[AL16], $k = 1$

Not fully correct:

$\exists$ class of transitions with probability

2x lower or **1.5x** higher

[HXW22], any k

Incorrect:

large discrepancies with experiments,

imprecise validity condition

Ours: probability, any k

$$p = T_{n-k}(\chi_L, \nu_L, \chi_0) \times T_k(\chi_R, \nu_R, \chi_k)$$

$$T_m(\boldsymbol{\chi}, \boldsymbol{\nu}, \hat{\chi}_i) = 2^{-\mathrm{wt}(\mathsf{SHL}(\boldsymbol{\nu}))-1} + \mathbb{1}_{\boldsymbol{\chi} \in \{0\ldots0,1\ldots1\}} \times (-1)^{\hat{\chi}_i} \times 2^{-m-1}$$

Our contribution

[AL16], $k = 1$

Not fully correct:

$\exists$ class of transitions with probability

2x lower or **1.5x** higher

[HXW22], any k

Incorrect:

large discrepancies with experiments,

imprecise validity condition

Ours: probability, any k

$$p = T_{n-k}(\chi_L, \nu_L, \chi_0) \times T_k(\chi_R, \nu_R, \chi_k)$$

$$T_m(\boldsymbol{\chi}, \boldsymbol{\nu}, \hat{\chi}_i) = 2^{-\mathrm{wt}(\mathsf{SHL}(\boldsymbol{\nu}))-1} + \mathbb{1}_{\boldsymbol{\chi} \in \{0\ldots0,1\ldots1\}} \times (-1)^{\hat{\chi}_i} \times 2^{-m-1}$$

Ours: validity, any k

$p > 0$ if and only if $u_i \leq v_i \quad \forall i \neq 0, k$

$$u = (I \oplus \mathsf{SHL})(\alpha \oplus \beta \oplus \Delta)$$
$$v = \mathsf{SHL}((\alpha \oplus \Delta) \vee (\beta \oplus \Delta))$$

Our contribution

[AL16], $k = 1$

Not fully correct:

$\exists$ class of transitions with probability

2x lower or **1.5x** higher

[HXW22], any k

Incorrect:

large discrepancies with experiments,

imprecise validity condition

Ours: probability, any k

$$p = T_{n-k}(\chi_L, \nu_L, \chi_0) \times T_k(\chi_R, \nu_R, \chi_k)$$

$$T_m(\boldsymbol{\chi}, \boldsymbol{\nu}, \hat{\chi}_i) = 2^{-\mathrm{wt}(\mathrm{SHL}(\boldsymbol{\nu}))-1} + \mathbb{1}_{\boldsymbol{\chi} \in \{0\ldots0,1\ldots1\}} \times (-1)^{\hat{\chi}_i} \times 2^{-m-1}$$

Ours: validity, any k

$p > 0$ if and only if $u_i \leq v_i \quad \forall i \neq 0, k$

$$u = (I \oplus \mathrm{SHL})(\alpha \oplus \beta \oplus \Delta)$$
$$v = \mathrm{SHL}((\alpha \oplus \Delta) \vee (\beta \oplus \Delta))$$

Extensively verified by experiments!

Plan

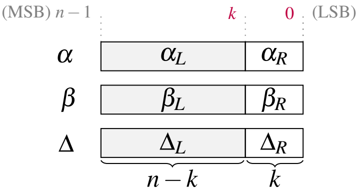
Rotational-XOR Cryptanalysis

Exact Probability Formula for all Rotations k

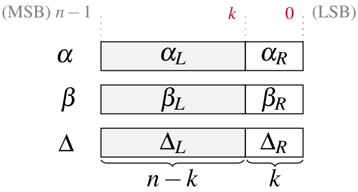
Modeling and Applications

Conclusions

Our result (probability, any k)

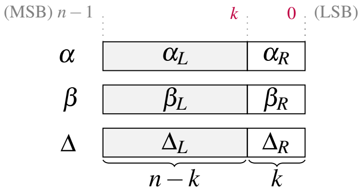


Our result (probability, any k)



Theorem (Main, if $p > 0$)

$$p = T_{n-k}(\alpha_L, \beta_L, \Delta_L, \alpha_0 \oplus \beta_0 \oplus \Delta_0) \ \times \ T_k(\alpha_R, \beta_R, \Delta_R, \alpha_k \oplus \beta_k \oplus \Delta_k)$$



Theorem (Main, if $p > 0$)

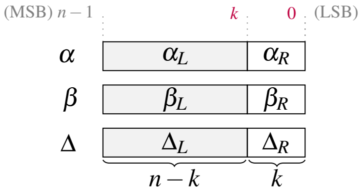
$$p = T_{n-k}(\alpha_L, \beta_L, \Delta_L, \alpha_0 \oplus \beta_0 \oplus \Delta_0) \;\times\; T_k(\alpha_R, \beta_R, \Delta_R, \alpha_k \oplus \beta_k \oplus \Delta_k)$$

where

$$T_m(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\Delta}, \mathsf{w}) = 2^{-d-1} + \mathbb{1}_{\boldsymbol{\alpha}\oplus\boldsymbol{\beta}\oplus\boldsymbol{\Delta}\in\{0\ldots0,1\ldots1\}} \times (-1)^{\mathsf{w}} \times 2^{-m-1}$$

$$d = \mathrm{wt}(\mathsf{SHL}(\boldsymbol{\nu})) = \mathrm{wt}(\mathsf{SHL}((\boldsymbol{\alpha} \oplus \boldsymbol{\beta}) \vee (\boldsymbol{\alpha} \oplus \boldsymbol{\Delta})))$$

Our result (probability, any k)



$$\chi = \alpha \oplus \beta \oplus \Delta$$

$$\nu = (\alpha \oplus \beta) \vee (\alpha \oplus \Delta)$$

Theorem (Main, if $p > 0$)

$$p = T_{n-k}(\chi_L, \nu_L, \chi_0) \; \times \; T_k(\chi_R, \nu_R, \chi_k)$$

where

$$T_m(\boldsymbol{\chi}, \boldsymbol{\nu}, \hat{\chi}_i) = 2^{-\mathrm{wt}(\mathsf{SHL}(\boldsymbol{\nu}))-1} + \mathbb{1}_{\boldsymbol{\chi} \in \{0\ldots0, 1\ldots1\}} \times (-1)^{\hat{\chi}_i} \times 2^{-m-1}$$

Our result (validity criterion, any k)

Theorem (RX-differential, $0 < k < n$)

$$p = \Pr\left[(\overleftarrow{x} \oplus \alpha) \boxplus (\overleftarrow{y} \oplus \beta) \;\oplus\; \overleftarrow{x \boxplus y} = \Delta\right] > 0$$

if and only if $u_i \leq v_i$ *for all* $i \neq 0, k,$ *where*

$$u = (I \oplus \mathrm{SHL})(\alpha \oplus \beta \oplus \Delta)$$
$$v = \mathrm{SHL}((\alpha \oplus \Delta) \vee (\beta \oplus \Delta))$$

Our result (validity criterion, any k)

Theorem (Normal differential ($k = 0$), Lipmaa and Moriai 2002)

$$p = \Pr\left[(x \oplus \alpha) \boxplus (y \oplus \beta) \ \oplus \ x \boxplus y = \Delta\right] > 0$$

if and only if $u_i \leq v_i$ *for all* i, *where*

$$u = (I \oplus \mathrm{SHL})(\alpha \oplus \beta \oplus \Delta)$$
$$v = \mathrm{SHL}((\alpha \oplus \Delta) \vee (\beta \oplus \Delta))$$

Impact of correction for $k = 1$

Theorem ([AL16], $k = 1$)

$$
\begin{aligned}
p = {} & \mathbb{1}_{(I \oplus \mathrm{SHL})(\chi_L) \oplus \mathbf{1} \preccurlyeq \mathrm{SHL}(\nu_L)} && \cdot 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))} \cdot 2^{-3} \\
& + \mathbb{1}_{(I \oplus \mathrm{SHL})(\chi_L) \preccurlyeq \mathrm{SHL}(\nu_L)} && \cdot 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))} \cdot 2^{-1.415}
\end{aligned}
$$

Impact of correction for $k = 1$

Theorem ([AL16], $k = 1$)

$$
\begin{aligned}
p = {} & \mathbb{1}_{(I \oplus \mathrm{SHL})(\chi_L) \oplus 1 \preccurlyeq \mathrm{SHL}(\nu_L)} && \cdot 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))} \cdot 2^{-3} \\
& + \mathbb{1}_{(I \oplus \mathrm{SHL})(\chi_L) \preccurlyeq \mathrm{SHL}(\nu_L)} && \cdot 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))} \cdot 2^{-1.415}
\end{aligned}
$$

Theorem (Ours)

Thm [AL16] holds exactly when $\chi_L \notin \{0\dots0, 1\dots1\}$, *where* $(\chi_L || \chi_0) = \alpha \oplus \beta \oplus \Delta$.

Impact of correction for $k = 1$

Theorem ([AL16], $k = 1$)

$$p = \mathbb{1}_{(I \oplus \mathrm{SHL})(\chi_L) \oplus 1 \preccurlyeq \mathrm{SHL}(\nu_L)} \cdot 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))} \cdot 2^{-3}$$
$$+ \mathbb{1}_{(I \oplus \mathrm{SHL})(\chi_L) \preccurlyeq \mathrm{SHL}(\nu_L)} \cdot 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))} \cdot 2^{-1.415}$$

Theorem (Ours)

Thm [AL16] holds exactly when $\chi_L \notin \{0 \ldots 0, 1 \ldots 1\}$, *where* $(\chi_L || \chi_0) = \alpha \oplus \beta \oplus \Delta$.

- Correction factor: 2x lower or 1.5x higher actual prob.

Impact of correction for $k = 1$

Theorem ([AL16], $k = 1$)

$$
\begin{aligned}
p = {} & \mathbb{1}_{(I \oplus \mathrm{SHL})(\chi_L) \oplus 1 \preccurlyeq \mathrm{SHL}(\nu_L)} && \cdot 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))} \cdot 2^{-3} \\
& + \mathbb{1}_{(I \oplus \mathrm{SHL})(\chi_L) \preccurlyeq \mathrm{SHL}(\nu_L)} && \cdot 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))} \cdot 2^{-1.415}
\end{aligned}
$$

Theorem (Ours)

Thm [AL16] holds exactly when $\chi_L \notin \{0 \ldots 0, 1 \ldots 1\}$, *where* $(\chi_L || \chi_0) = \alpha \oplus \beta \oplus \Delta$.

- Correction factor: 2x lower or 1.5x higher actual prob.
- High prob. trail: $\chi_L = 0 \ldots 0$ is likely to occur (sparse), but negl. correction

Impact of correction for $k = 1$

Theorem ([AL16], $k = 1$)

$$\begin{aligned} p = &\mathbb{1}_{(I \oplus \mathrm{SHL})(\chi_L) \oplus 1 \preccurlyeq \mathrm{SHL}(\nu_L)} && \cdot 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))} \cdot 2^{-3} \\ + &\mathbb{1}_{(I \oplus \mathrm{SHL})(\chi_L) \preccurlyeq \mathrm{SHL}(\nu_L)} && \cdot 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))} \cdot 2^{-1.415} \end{aligned}$$

Theorem (Ours)

Thm [AL16] holds exactly when $\chi_L \notin \{0 \dots 0, 1 \dots 1\}$, *where* $(\chi_L || \chi_0) = \alpha \oplus \beta \oplus \Delta$.

- Correction factor: 2x lower or 1.5x higher actual prob.
- High prob. trail: $\chi_L = 0 \dots 0$ is likely to occur (sparse), but negl. correction
- Low prob. trail: unlikely to occur (dense)

Impact of correction for $k = 1$

Theorem ([AL16], $k = 1$)

$$\begin{aligned} p = {} & \mathbb{1}_{(I \oplus \mathrm{SHL})(\chi_L) \oplus 1 \preccurlyeq \mathrm{SHL}(\nu_L)} & \cdot 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))} \cdot 2^{-3} \\ & + \mathbb{1}_{(I \oplus \mathrm{SHL})(\chi_L) \preccurlyeq \mathrm{SHL}(\nu_L)} & \cdot 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))} \cdot 2^{-1.415} \end{aligned}$$

Theorem (Ours)

Thm [AL16] holds exactly when $\chi_L \notin \{0\ldots0, 1\ldots1\}$, *where* $(\chi_L \| \chi_0) = \alpha \oplus \beta \oplus \Delta$.

- Correction factor: 2x lower or 1.5x higher actual prob.
- High prob. trail: $\chi_L = 0\ldots0$ is likely to occur (sparse), but negl. correction
- Low prob. trail: unlikely to occur (dense)

Conclusion: concrete trails are probably not affected, optimality claims do

Plan

Rotational-XOR Cryptanalysis

Exact Probability Formula for all Rotations k

Modeling and Applications

- New best RX-trails for Alzette
- RX-backdoor from malicious constants - Malzette

Conclusions

MILP Model

Model 1 - Heuristic (NEQ)

- Ignore the approximation factor: $p \approx 2^{-\operatorname{wt}\operatorname{SHL}\boldsymbol{\nu_L}-\operatorname{wt}\operatorname{SHL}\boldsymbol{\nu_R}-2}$
- A special case of the standard ARX model
- Bonus: model $[y = 1 \text{ if and only if } x_1 = \ldots = x_m]$ with 4 inequalities for any m

MILP Model

Model 1 - Heuristic (NEQ)

- Ignore the approximation factor: $p \approx 2^{-\operatorname{wt} \mathrm{SHL}\, \boldsymbol{\nu_L} - \operatorname{wt} \mathrm{SHL}\, \boldsymbol{\nu_R} - 2}$
- A special case of the standard ARX model
- Bonus: model $[y = 1 \text{ if and only if } x_1 = \ldots = x_m]$ with 4 inequalities for any m

Model 2 - Precise

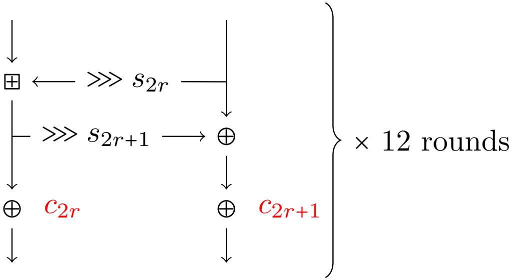
- Model the weight of the correction factor using logarithm tables (PieceWise-Linear constraints - PWL)
- "Flag" variables to determine if the correction is needed

Alzette (64-bit ARX-box, 4 32-bit modular additions)

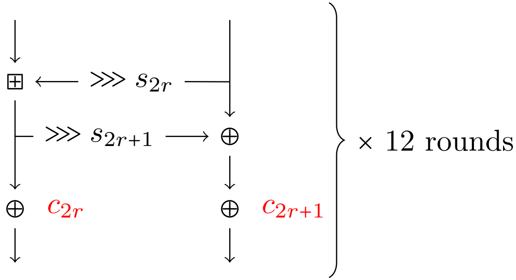
	CASCADA,[LWRA17] ($k = 1$)	This work ($k = 1$)	This work ($k > 1$)	[HXW22] ($k = 1$)	[HXW22] ($k > 1$)
c_i	wt	wt	wt	wt	wt
c_0	**33.66**	**33.66**	33.93	37.66	43.00
c_1	**31.66**	**31.66**	33.01	38.66	-
c_2	37.66	37.66	**34.00**	52.66	-
c_3	38.66	38.66	**32.75**	45.66	-
c_4	35.66	35.66	**33.00**	45.66	-
c_5	32.66	33.66	**30.89**	44.66	-
c_6	**30.66**	**30.66**	32.97	40.66	-
c_7	37.66	37.66	**32.45**	49.66	-

(all values are $-\log_2 p$*)*

Malzette

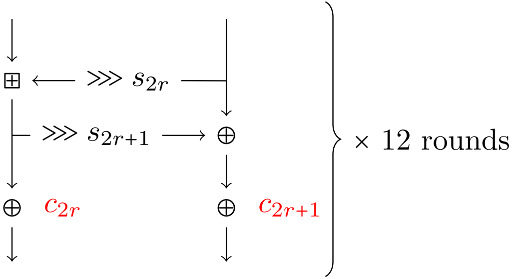


Malzette



Round	Constants	$\log_2$(prob)
1	`1c71c924:249cad47`	-2.83
2	`49249c71:1249871c`	-1.83
3	`6db6c71c:5b127ffe`	-3.19
4	`38e39249:152ad249`	-1.83
5	`638e36db:649cad55`	-2.83
6	`1c71c7ff:471c9492`	-1.83
7	`36db6d55:63f1c71d`	-2.83
8	`471c7249:36a4ff1c`	-2.19
9	`4924938e:5b6c8e47`	-3.19
10	`2aab6db6:71c736db`	-1.83
11	`6db638e3:55b9c71d`	-2.83
12	`fb3d2330:b6da4b61`	-2.19
Total		-29.41

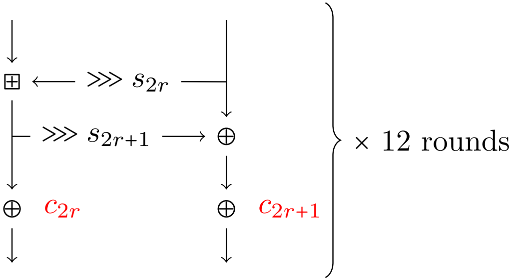
Malzette



- Diff./lin. lower bounds 2^{54} and 2^{38}
- RX-differential prob. $2^{-29.41}$ ($k = 3$)
- Verified experimentally

Round	Constants	$\log_2$(prob)
1	`1c71c924:249cad47`	-2.83
2	`49249c71:1249871c`	-1.83
3	`6db6c71c:5b127ffe`	-3.19
4	`38e39249:152ad249`	-1.83
5	`638e36db:649cad55`	-2.83
6	`1c71c7ff:471c9492`	-1.83
7	`36db6d55:63f1c71d`	-2.83
8	`471c7249:36a4ff1c`	-2.19
9	`4924938e:5b6c8e47`	-3.19
10	`2aab6db6:71c736db`	-1.83
11	`6db638e3:55b9c71d`	-2.83
12	`fb3d2330:b6da4b61`	-2.19
Total		-29.41

Malzette



- Diff./lin. lower bounds 2^{54} and 2^{38}
- RX-differential prob. $2^{-24.86}$ ($k = 3$)
- Verified experimentally

Round	Constants	$\log_2$(prob)
1	`00000000:4e381c1c`	-2.19
2	`2aaaaaaa:36dbe492`	-2.19
3	`7fffffff:1236db6c`	-1.83
4	`55555555:0763638e`	-1.83
5	`2aaaaaaa:1b6d4949`	-2.19
6	`55555555:638ef1c7`	-1.83
7	`00000000:47638e39`	-2.19
8	`2aaaaaaa:5236b6db`	-2.19
9	`55555555:4e381c1c`	-1.83
10	`7fffffff:638eb1c7`	-2.19
11	`7fffffff:47638e39`	-2.19
12	`3f2bb31e:b6c004cc`	-2.19
Total		-24.86

Plan

Rotational-XOR Cryptanalysis

Exact Probability Formula for all Rotations k

Modeling and Applications

Conclusions

Conclusions

Theory

- Compact exact probability for all rotations k
- Useful ARX theory
- RXDP with constant addition - state machine (Q: can be simplified?)

Conclusions

Theory

- Compact exact probability for all rotations k
- Useful ARX theory
- RXDP with constant addition - state machine (Q: can be simplified?)

Applications

- MILP model using PWL
- Applied to Alzette, Toy Speck, etc. (Q: improve performance, SMT?)
- Malzette - proof-of-concept RX-backdoor

Conclusions

Theory

- Compact exact probability for all rotations k
- Useful ARX theory
- RXDP with constant addition - state machine (Q: can be simplified?)

Applications

- MILP model using PWL
- Applied to Alzette, Toy Speck, etc. (Q: improve performance, SMT?)
- Malzette - proof-of-concept RX-backdoor

github.com/cryptolu/RX-Differentials-Probability

tosc.iacr.org/index.php/ToSC/article/view/12087

References i

- Ashur, Tomer and Yunwen Liu (2016). **"Rotational Cryptanalysis in the Presence of Constants".** In: *IACR Trans. Symm. Cryptol.* 2016.1, pp. 57–70. issn: 2519-173X. doi: 10.13154/tosc.v2016.i1.57-70. url: https://tosc.iacr.org/index.php/ToSC/article/view/535.
- Daum, Magnus (2005). **"Cryptanalysis of Hash functions of the MD4-family".** PhD thesis. Ruhr University Bochum. url: http://www-brs.ub.ruhr-uni-bochum.de/netahtml/HSS/Diss/DaumMagnus/.
- Huang, Mingjiang, Zhen Xu, and Liming Wang (2022). **"On the Probability and Automatic Search of Rotational-XOR Cryptanalysis on ARX Ciphers".** In: *Comput. J.* 65.12, pp. 3062–3080. doi: 10.1093/COMJNL/BXAB126.

- Khovratovich, Dmitry and Ivica Nikolic (Feb. 2010). **"Rotational Cryptanalysis of ARX".** In: *FSE 2010*. Ed. by Seokhie Hong and Tetsu Iwata. Vol. 6147. LNCS. Springer, Berlin, Heidelberg, pp. 333–346. doi: 10.1007/978-3-642-13858-4_19.
- Lipmaa, Helger and Shiho Moriai (Apr. 2002). **"Efficient Algorithms for Computing Differential Properties of Addition".** In: *FSE 2001*. Ed. by Mitsuru Matsui. Vol. 2355. LNCS. Springer, Berlin, Heidelberg, pp. 336–350. doi: 10.1007/3-540-45473-X_28.
- Liu, Yunwen, Glenn De Witte, Adrián Ranea, and Tomer Ashur (2017). **"Rotational-XOR Cryptanalysis of Reduced-round SPECK".** In: *IACR Trans. Symm. Cryptol.* 2017.3, pp. 24–36. issn: 2519-173X. doi: 10.13154/tosc.v2017.i3.24-36.

Ranea, Adrián and Vincent Rijmen (2022). **"Characteristic automated search of cryptographic algorithms for distinguishing attacks (CASCADA)".** In: *IET Inf. Secur.* 16.6, pp. 470–481. doi: 10.1049/ise2.12077.

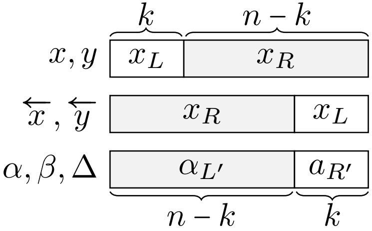
Proof ideas - Decomposition

$$x, y \quad \overbrace{\boxed{x_L}}^{k}\overbrace{\boxed{\qquad x_R \qquad}}^{n-k}$$

$$\overleftarrow{x}, \overleftarrow{y} \quad \boxed{\qquad x_R \qquad}\boxed{x_L}$$

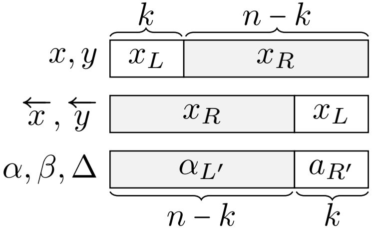
$$\alpha, \beta, \Delta \quad \underbrace{\boxed{\qquad \alpha_{L'} \qquad}}_{n-k}\underbrace{\boxed{a_{R'}}}_{k}$$

Proof ideas - Decomposition



$$\begin{cases} (x_R \oplus \alpha_{L'}) \boxplus (y_R \oplus \beta_{L'}) \boxplus c_L \;\oplus\; x_R \boxplus y_R = \Delta_{L'} \\ (x_L \oplus \alpha_{R'}) \boxplus (y_L \oplus \beta_{R'}) \;\oplus\; x_L \boxplus y_L \boxplus c_R = \Delta_{R'} \\ c_R = \mathbb{1}_{x_R + y_R \geq 2^{n-k}} \\ c_L = \mathbb{1}_{(x_L \oplus \alpha_{R'}) + (y_L \oplus \beta_{R'}) \geq 2^k} \end{cases}$$

Proof ideas - Decomposition



$$\begin{cases} (x_R \oplus \alpha_{L'}) \boxplus (y_R \oplus \beta_{L'}) \boxplus c_L \oplus x_R \boxplus y_R = \Delta_{L'} \\ (x_L \oplus \alpha_{R'}) \boxplus (y_L \oplus \beta_{R'}) \oplus x_L \boxplus y_L \boxplus c_R = \Delta_{R'} \\ c_R = \mathbb{1}_{x_R + y_R \geq 2^{n-k}} \\ c_L = \mathbb{1}_{(x_L \oplus \alpha_{R'}) + (y_L \oplus \beta_{R'}) \geq 2^k} \end{cases}$$

$$\boxed{\begin{cases} (x \oplus \boldsymbol{\alpha}) \boxplus (y \oplus \boldsymbol{\beta}) \boxplus (\boldsymbol{\alpha}_0 \oplus \boldsymbol{\beta}_0 \oplus \boldsymbol{\Delta}_0) \oplus x \boxplus y = \boldsymbol{\Delta} \\ \mathbb{1}_{x+y \geq 2^m} = \mathrm{w} \end{cases}}$$

Proposition (Carry-constrained Differential through $\boxplus$)

Let

$$XDS_n = \#\{(x, y) \mid x \boxplus y \quad \oplus \quad (x \oplus \alpha) \boxplus (y \oplus \beta) = \Delta\} \text{ (Lipmaa-Moriai)}$$

$$R_n(\alpha, \beta, \Delta) = \#\{(x, y) \in XDS_n(\alpha, \beta, \Delta) \mid x + y < 2^n\}$$

Then, for $\tilde{\alpha} = (\alpha'||\alpha), \tilde{\beta} = (\beta'||\beta), \tilde{\Delta} = (\Delta'||\Delta), \chi' = \alpha' \oplus \beta' \oplus \Delta'$ *we have*

$$R_{n+1}(\tilde{\alpha}, \tilde{\beta}, \tilde{\Delta}) = \begin{cases} 2R_n(\alpha, \beta, \Delta) \text{ if not } (\alpha_{n-1} = \beta_{n-1} = \Delta_{n-1}) \text{ and } \chi' = 0 \\ \#XDS_n(\alpha, \beta, \Delta) \text{ if not } (\alpha_{n-1} = \beta_{n-1} = \Delta_{n-1}) \text{ and } \chi' = 1 \\ \#XDS_n(\alpha, \beta, \Delta) + 2R_n(\alpha, \beta, \Delta) \text{ if } \alpha_{n-1} = \beta_{n-1} = \Delta_{n-1} = 0 \text{ and } \chi' = 0 \\ 2 \times \#XDS_n(\alpha, \beta, \Delta) \text{ if } \delta_{n-1} = \alpha_{n-1} = \beta_{n-1} = \Delta_{n-1} = 1 \text{ and } \chi' = 1 \end{cases}$$

Impact of correction for $k = 1$

Theorem ([AL16], $k = 1$)

$$p = \mathbb{1}_{(I \oplus \mathsf{SHL})(\chi_L) \oplus 1 \preccurlyeq \mathsf{SHL}(\nu_L)} \cdot 2^{-\operatorname{wt}(\mathsf{SHL}(\nu_L))} \cdot 2^{-3}$$
$$+ \mathbb{1}_{(I \oplus \mathsf{SHL})(\chi_L) \preccurlyeq \mathsf{SHL}(\nu_L)} \cdot 2^{-\operatorname{wt}(\mathsf{SHL}(\nu_L))} \cdot 2^{-1.415}$$

Impact of correction for $k = 1$

Theorem ([AL16], $k = 1$)

$$p = \mathbb{1}_{(I \oplus \mathrm{SHL})(\chi_L) \oplus \mathbf{1} \preccurlyeq \mathrm{SHL}(\nu_L)} \cdot 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))} \cdot 2^{-3}$$
$$+ \mathbb{1}_{(I \oplus \mathrm{SHL})(\chi_L) \preccurlyeq \mathrm{SHL}(\nu_L)} \cdot 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))} \cdot 2^{-1.415}$$

Theorem (Ours)

Thm [AL16] holds exactly when $\chi_L \notin \{0\ldots0, 1\ldots1\}$, *where* $(\chi_L || \chi_0) = \alpha \oplus \beta \oplus \Delta$.

Impact of correction for $k = 1$

Theorem ([AL16], $k = 1$)

$$
\begin{aligned}
p = \; & \mathbb{1}_{(I \oplus \mathrm{SHL})(\chi_L) \oplus 1 \preccurlyeq \mathrm{SHL}(\nu_L)} && \cdot 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))} \cdot 2^{-3} \\
+ \; & \mathbb{1}_{(I \oplus \mathrm{SHL})(\chi_L) \preccurlyeq \mathrm{SHL}(\nu_L)} && \cdot 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))} \cdot 2^{-1.415}
\end{aligned}
$$

Theorem (Ours)

Thm [AL16] holds exactly when $\chi_L \notin \{0\ldots0, 1\ldots1\}$, *where* $(\chi_L || \chi_0) = \alpha \oplus \beta \oplus \Delta$.

$$
\begin{aligned}
T_1(\chi_0, \nu_0, \chi_1) &= 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_0))-1} + \mathbb{1}_{\chi_0 \in \{0\ldots0, 1\ldots1\}} \times (-1)^{\chi_1} \times 2^{-2} \\
T_{n-1}(\chi_L, \nu_L, \chi_0) &= 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))-1} + \mathbb{1}_{\chi_L \in \{0\ldots0, 1\ldots1\}} \times (-1)^{\chi_0} \times 2^{-n}
\end{aligned}
$$

Impact of correction for $k = 1$

Theorem ([AL16], $k = 1$)

$$p = \mathbb{1}_{(I \oplus \mathrm{SHL})(\chi_L) \oplus 1 \preccurlyeq \mathrm{SHL}(\nu_L)} \cdot 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))} \cdot 2^{-3}$$
$$+ \mathbb{1}_{(I \oplus \mathrm{SHL})(\chi_L) \preccurlyeq \mathrm{SHL}(\nu_L)} \cdot 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))} \cdot 2^{-1.415}$$

Theorem (Ours)

Thm [AL16] holds exactly when $\chi_L \notin \{0 \ldots 0, 1 \ldots 1\}$, *where* $(\chi_L || \chi_0) = \alpha \oplus \beta \oplus \Delta$.

$$T_1(\chi_0, \nu_0, \chi_1) = 2^{-1} + (-1)^{\chi_1} \times 2^{-2} \quad \in \{2^{-2}, 2^{-0.415}\}$$
$$T_{n-1}(\chi_L, \nu_L, \chi_0) = 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))-1} + \mathbb{1}_{\chi_L \in \{0\ldots0, 1\ldots1\}} \times (-1)^{\chi_0} \times 2^{-n}$$

Impact of correction for $k = 1$

Theorem ([AL16], $k = 1$)

$$p = \mathbb{1}_{(I \oplus \mathrm{SHL})(\chi_L) \oplus 1 \preccurlyeq \mathrm{SHL}(\nu_L)} \cdot 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))} \cdot 2^{-3}$$
$$+ \mathbb{1}_{(I \oplus \mathrm{SHL})(\chi_L) \preccurlyeq \mathrm{SHL}(\nu_L)} \cdot 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))} \cdot 2^{-1.415}$$

Theorem (Ours)

Thm [AL16] holds exactly when $\chi_L \notin \{0\dots0, 1\dots1\}$, *where* $(\chi_L || \chi_0) = \alpha \oplus \beta \oplus \Delta$.

$$T_1(\chi_0, \nu_0, \chi_1) = 2^{-1} + (-1)^{\chi_1} \times 2^{-2} \qquad \in \{2^{-2}, 2^{-0.415}\}$$
$$T_{n-1}(\chi_L, \nu_L, \chi_0) = 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))-1} + \boxed{\mathbb{1}_{\chi_L \in \{0\dots0,1\dots1\}} \times (-1)^{\chi_0} \times 2^{-n}}$$

Impact of correction for $k = 1$

Theorem ([AL16], $k = 1$)

$$\begin{aligned} p = \ & \mathbb{1}_{(I \oplus \mathrm{SHL})(\chi_L) \oplus \mathbf{1} \preccurlyeq \mathrm{SHL}(\nu_L)} && \cdot 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))} \cdot 2^{-3} \\ + \ & \mathbb{1}_{(I \oplus \mathrm{SHL})(\chi_L) \preccurlyeq \mathrm{SHL}(\nu_L)} && \cdot 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))} \cdot 2^{-1.415} \end{aligned}$$

Theorem (Ours)

Thm [AL16] holds exactly when $\chi_L \notin \{0\ldots0, 1\ldots1\}$, where $(\chi_L || \chi_0) = \alpha \oplus \beta \oplus \Delta$.

- Correction factor: 2x lower or 1.5x higher actual prob.

Impact of correction for $k = 1$

Theorem ([AL16], $k = 1$)

$$
\begin{aligned}
p = {} & \mathbb{1}_{(I \oplus \mathrm{SHL})(\chi_L) \oplus 1 \preccurlyeq \mathrm{SHL}(\nu_L)} && \cdot 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))} \cdot 2^{-3} \\
& + \mathbb{1}_{(I \oplus \mathrm{SHL})(\chi_L) \preccurlyeq \mathrm{SHL}(\nu_L)} && \cdot 2^{-\mathrm{wt}(\mathrm{SHL}(\nu_L))} \cdot 2^{-1.415}
\end{aligned}
$$

Theorem (Ours)

Thm [AL16] holds exactly when $\chi_L \notin \{0 \dots 0, 1 \dots 1\}$, *where* $(\chi_L || \chi_0) = \alpha \oplus \beta \oplus \Delta$.

- Correction factor: 2x lower or 1.5x higher actual prob.
- High prob. trail: $\chi_L = 0 \dots 0$ is likely to occur (sparse), but negl. correction

Impact of correction for $k = 1$

Theorem ([AL16], $k = 1$)

$$\begin{aligned} p = {} & \mathbb{1}_{(I \oplus \mathsf{SHL})(\chi_L) \oplus 1 \preccurlyeq \mathsf{SHL}(\nu_L)} && \cdot 2^{-\operatorname{wt}(\mathsf{SHL}(\nu_L))} \cdot 2^{-3} \\ & + \mathbb{1}_{(I \oplus \mathsf{SHL})(\chi_L) \preccurlyeq \mathsf{SHL}(\nu_L)} && \cdot 2^{-\operatorname{wt}(\mathsf{SHL}(\nu_L))} \cdot 2^{-1.415} \end{aligned}$$

Theorem (Ours)

Thm [AL16] holds exactly when $\chi_L \notin \{0 \ldots 0, 1 \ldots 1\}$, *where* $(\chi_L || \chi_0) = \alpha \oplus \beta \oplus \Delta$.

- Correction factor: 2x lower or 1.5x higher actual prob.
- High prob. trail: $\chi_L = 0 \ldots 0$ is likely to occur (sparse), but negl. correction
- Low prob. trail: unlikely to occur (dense)

Impact of correction for $k = 1$

Theorem ([AL16], $k = 1$)

$$p = \mathbb{1}_{(I \oplus \mathsf{SHL})(\chi_L) \oplus 1 \preccurlyeq \mathsf{SHL}(\nu_L)} \cdot 2^{-\operatorname{wt}(\mathsf{SHL}(\nu_L))} \cdot 2^{-3}$$
$$+ \mathbb{1}_{(I \oplus \mathsf{SHL})(\chi_L) \preccurlyeq \mathsf{SHL}(\nu_L)} \cdot 2^{-\operatorname{wt}(\mathsf{SHL}(\nu_L))} \cdot 2^{-1.415}$$

Theorem (Ours)

Thm [AL16] holds exactly when $\chi_L \notin \{0\ldots0, 1\ldots1\}$, *where* $(\chi_L || \chi_0) = \alpha \oplus \beta \oplus \Delta$.

- Correction factor: 2x lower or 1.5x higher actual prob.
- High prob. trail: $\chi_L = 0\ldots0$ is likely to occur (sparse), but negl. correction
- Low prob. trail: unlikely to occur (dense)

Conclusion: concrete trails are probably not affected, optimality claims do