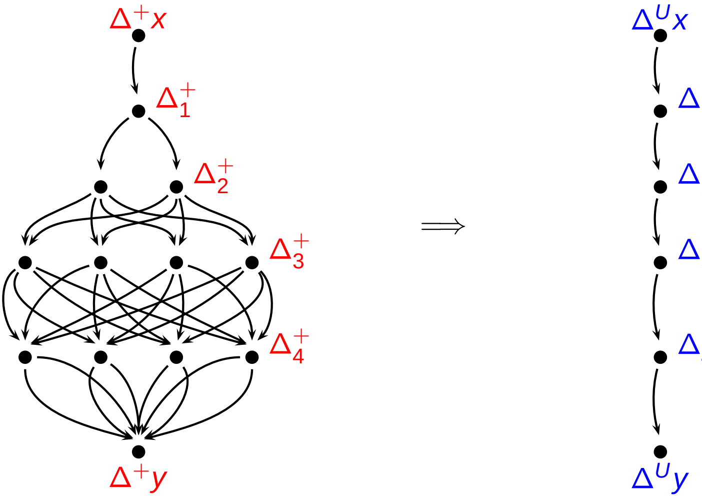
UNAF: A Special Set of Additive Differences with Application to the Differential Analysis of ARX

V. Velichkov N. Mouha C. De Cannière B. Preneel

COSIC, KU Leuven; IBBT

FSE 2012, March 19-21, Washington DC, USA

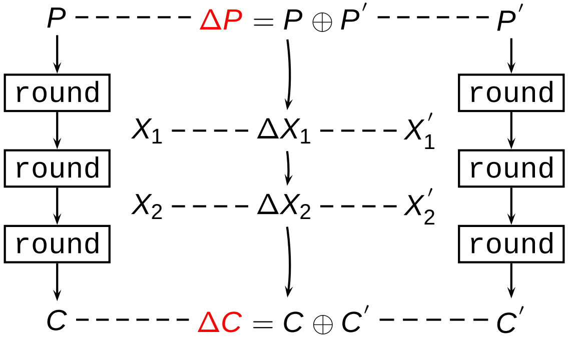
UNAF Differences Cluster Multiple Characteristics



Applications of UNAF Differences

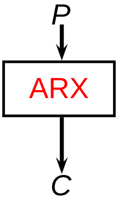
- Improved estimations of probabilities of differentials through ARX.
- New (better?) attacks.

Differential Cryptanalysis [Biham and Shamir,1991]

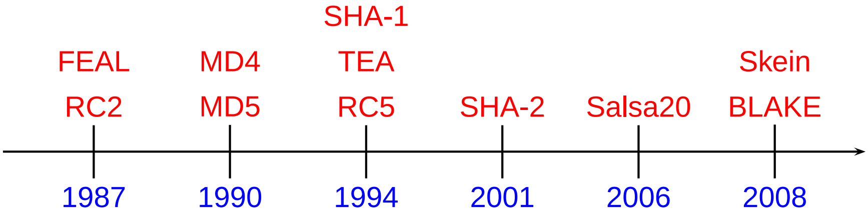


$$\Pr(\Delta P \rightarrow \Delta C) = ?$$

Addition, Rotation, XOR (ARX)



- Addition ($\boxplus$) : **confusion**
- Rotation ($\lll$) : **diffusion** within a word
- XOR ($\oplus$): **diffusion** between words



Types of Differences

- Additive difference Δ^+

Definition

$$\Delta^+ X = X' - X \quad .$$

Example

$$\begin{array}{rrl} & 1000_2 & = X' \\ - & 0101_2 & = X \\ \hline & 0011_2 & = \Delta^+ X \end{array}$$

Types of Differences

- XOR difference $\Delta^{\oplus}$

Definition

$$\Delta^{\oplus} X = X' \oplus X \ .$$

Example

$$\begin{array}{rrl} & 1000_2 & = X' \\ \oplus & 0101_2 & = X \\ \hline & 1101_2 & = \Delta^{\oplus} X \end{array}$$

Types of Differences

- BSD (Binary-Signed Digit) Difference $\Delta^{\pm}$

Definition

$$\Delta^{\pm}X : \Delta^{\pm}X[i] = (X'[i] - X[i]) \in \{\bar{1}, 0, 1\}, \quad 0 \leq i < n \ .$$

Example

$$\begin{array}{rrl} & 1000_2 & = X' \\ - & 0101_2 & = X \\ \hline & 1\bar{1}0\bar{1}_2 & = \Delta^{\pm}X \end{array}$$

Types of Differences

- NAF (Non-Adjacent Form) Difference Δ^N

Definition

A NAF is a special BSD diff. s.t. no two consecutive bits are non-zero:

$$\nexists i : \quad (\Delta^N X[i] \neq 0) \wedge (\Delta^N X[i+1] \neq 0), \quad 0 \leq i < n-1 \ .$$

Example

$$\Delta^+ X = 3 = \begin{cases} +1 \cdot 2^3 - 1 \cdot 2^2 - 1 \cdot 2^0 = 1\bar{1}0\bar{1}_2 = \Delta^{\pm} X \ , \\ +1 \cdot 2^2 - 1 \cdot 2^0 = 010\bar{1}_2 = \Delta^N X \ . \end{cases}$$

UNAF (Unsigned NAF) Difference

Definition

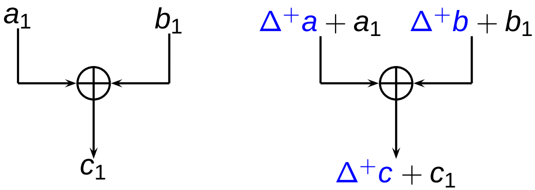
$$\Delta^U X = \{\Delta^+ a : |\Delta^N a| = |\Delta^N X|\} \ .$$

Example

$$\Delta^U X = 5 \implies \Delta^U X = \{3, 13, 5, 11\} \ .$$

$$\Delta^U X = 5 = \begin{cases} 3 = +1 \cdot 2^2 - 1 \cdot 2^0 \pmod{2^4} & = 010\bar{1} \\ 13 = -1 \cdot 2^2 + 1 \cdot 2^0 \pmod{2^4} & = 0\bar{1}01 \\ 5 = +1 \cdot 2^2 + 1 \cdot 2^0 \pmod{2^4} & = 0101 \\ 11 = -1 \cdot 2^2 - 1 \cdot 2^0 \pmod{2^4} & = 0\bar{1}0\bar{1} \end{cases} = 0101 \ .$$

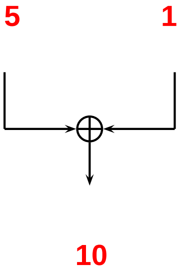
The Additive Differential Probability of XOR ($\mathrm{adp}^{\oplus}$)



$$((\Delta^{+}a + a_1) \oplus (\Delta^{+}b + b_1)) - (a_1 \oplus b_1) = \Delta^{+}c \quad .$$

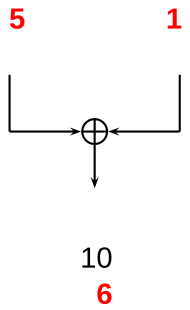
UNAF: Clustering of Differentials

$$\mathrm{adp}^{\oplus}(5, 1 \rightarrow 10) = 0.15625$$



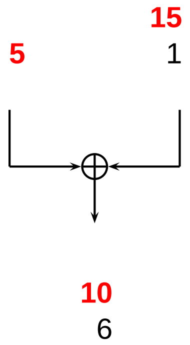
UNAF: Clustering of Differentials

$$\mathrm{adp}^{\oplus}(5, 1 \rightarrow 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 1 \rightarrow 6) = 0.15625$$

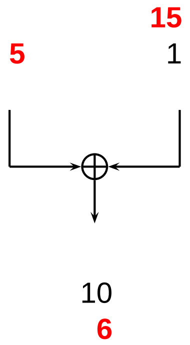


UNAF: Clustering of Differentials

$$\mathrm{adp}^{\oplus}(\ 5,\ \ 1 \to 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(\ 5,\ \ 1 \to \ \ 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(\ 5, 15 \to 10) = 0.15625$$

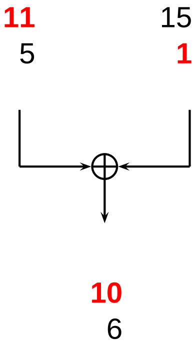


UNAF: Clustering of Differentials



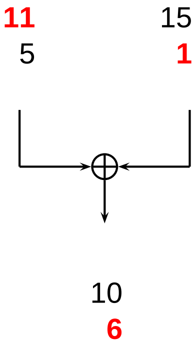
$$\mathrm{adp}^{\oplus}(\ 5,\ \ 1 \rightarrow 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(\ 5,\ \ 1 \rightarrow \ \ 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(\ 5, 15 \rightarrow 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(\ 5, 15 \rightarrow \ \ 6) = 0.15625$$

UNAF: Clustering of Differentials



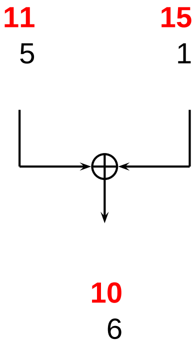
$$\mathrm{adp}^{\oplus}(5, 1 \rightarrow 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 1 \rightarrow 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 15 \rightarrow 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 15 \rightarrow 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 1 \rightarrow 10) = 0.15625$$

UNAF: Clustering of Differentials



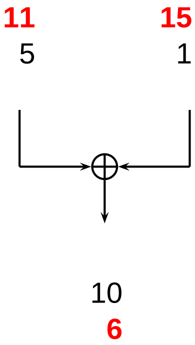
$$\mathrm{adp}^{\oplus}(5, 1 \to 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 1 \to 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 15 \to 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 15 \to 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 1 \to 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 1 \to 6) = 0.15625$$

UNAF: Clustering of Differentials



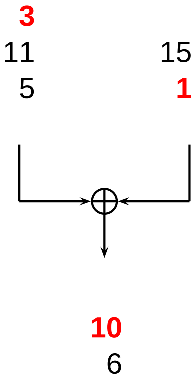
$$\mathrm{adp}^{\oplus}(5, 1 \to 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 1 \to 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 15 \to 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 15 \to 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 1 \to 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 1 \to 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 15 \to 10) = 0.15625$$

UNAF: Clustering of Differentials



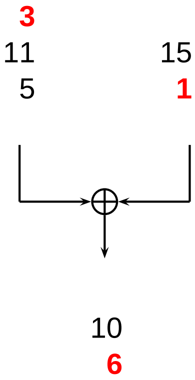
$$\mathrm{adp}^{\oplus}(5, 1 \to 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 1 \to 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 15 \to 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 15 \to 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 1 \to 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 1 \to 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 15 \to 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 15 \to 6) = 0.15625$$

UNAF: Clustering of Differentials



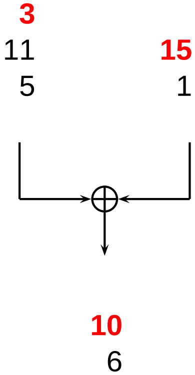
$$\mathrm{adp}^{\oplus}(5, 1 \to 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 1 \to 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 15 \to 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 15 \to 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 1 \to 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 1 \to 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 15 \to 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 15 \to 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(3, 1 \to 10) = 0.09375$$

UNAF: Clustering of Differentials



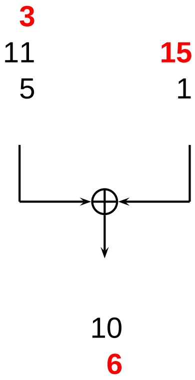
$$\mathrm{adp}^{\oplus}(5, 1 \to 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 1 \to 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 15 \to 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 15 \to 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 1 \to 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 1 \to 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 15 \to 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 15 \to 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(3, 1 \to 10) = 0.09375$$
$$\mathrm{adp}^{\oplus}(3, 1 \to 6) = 0.09375$$

UNAF: Clustering of Differentials



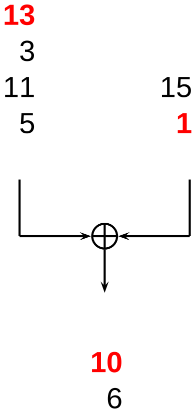
$$
\begin{aligned}
\mathrm{adp}^{\oplus}(5, 1 \rightarrow 10) &= 0.15625\\
\mathrm{adp}^{\oplus}(5, 1 \rightarrow 6) &= 0.15625\\
\mathrm{adp}^{\oplus}(5, 15 \rightarrow 10) &= 0.15625\\
\mathrm{adp}^{\oplus}(5, 15 \rightarrow 6) &= 0.15625\\
\mathrm{adp}^{\oplus}(11, 1 \rightarrow 10) &= 0.15625\\
\mathrm{adp}^{\oplus}(11, 1 \rightarrow 6) &= 0.15625\\
\mathrm{adp}^{\oplus}(11, 15 \rightarrow 10) &= 0.15625\\
\mathrm{adp}^{\oplus}(11, 15 \rightarrow 6) &= 0.15625\\
\mathrm{adp}^{\oplus}(3, 1 \rightarrow 10) &= 0.09375\\
\mathrm{adp}^{\oplus}(3, 1 \rightarrow 6) &= 0.09375\\
\mathrm{adp}^{\oplus}(3, 15 \rightarrow 10) &= 0.09375
\end{aligned}
$$

UNAF: Clustering of Differentials



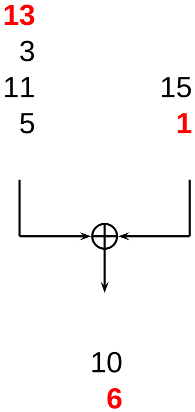
$$
\begin{aligned}
\mathrm{adp}^{\oplus}(5, 1 \rightarrow 10) &= 0.15625\\
\mathrm{adp}^{\oplus}(5, 1 \rightarrow 6) &= 0.15625\\
\mathrm{adp}^{\oplus}(5, 15 \rightarrow 10) &= 0.15625\\
\mathrm{adp}^{\oplus}(5, 15 \rightarrow 6) &= 0.15625\\
\mathrm{adp}^{\oplus}(11, 1 \rightarrow 10) &= 0.15625\\
\mathrm{adp}^{\oplus}(11, 1 \rightarrow 6) &= 0.15625\\
\mathrm{adp}^{\oplus}(11, 15 \rightarrow 10) &= 0.15625\\
\mathrm{adp}^{\oplus}(11, 15 \rightarrow 6) &= 0.15625\\
\mathrm{adp}^{\oplus}(3, 1 \rightarrow 10) &= 0.09375\\
\mathrm{adp}^{\oplus}(3, 1 \rightarrow 6) &= 0.09375\\
\mathrm{adp}^{\oplus}(3, 15 \rightarrow 10) &= 0.09375\\
\mathrm{adp}^{\oplus}(3, 15 \rightarrow 6) &= 0.09375
\end{aligned}
$$

UNAF: Clustering of Differentials



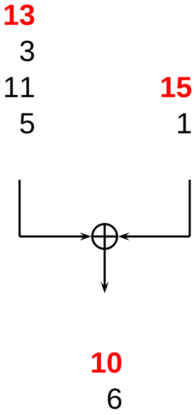
$$\mathrm{adp}^{\oplus}(5, 1 \to 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 1 \to 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 15 \to 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 15 \to 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 1 \to 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 1 \to 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 15 \to 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 15 \to 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(3, 1 \to 10) = 0.09375$$
$$\mathrm{adp}^{\oplus}(3, 1 \to 6) = 0.09375$$
$$\mathrm{adp}^{\oplus}(3, 15 \to 10) = 0.09375$$
$$\mathrm{adp}^{\oplus}(3, 15 \to 6) = 0.09375$$
$$\mathrm{adp}^{\oplus}(13, 1 \to 10) = 0.09375$$

UNAF: Clustering of Differentials



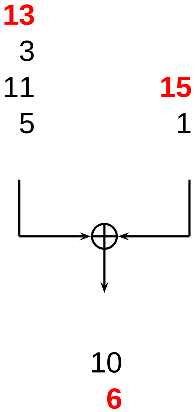
$$\mathrm{adp}^{\oplus}(5, 1 \to 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 1 \to 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 15 \to 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 15 \to 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 1 \to 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 1 \to 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 15 \to 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 15 \to 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(3, 1 \to 10) = 0.09375$$
$$\mathrm{adp}^{\oplus}(3, 1 \to 6) = 0.09375$$
$$\mathrm{adp}^{\oplus}(3, 15 \to 10) = 0.09375$$
$$\mathrm{adp}^{\oplus}(3, 15 \to 6) = 0.09375$$
$$\mathrm{adp}^{\oplus}(13, 1 \to 10) = 0.09375$$
$$\mathrm{adp}^{\oplus}(13, 1 \to 6) = 0.09375$$

UNAF: Clustering of Differentials



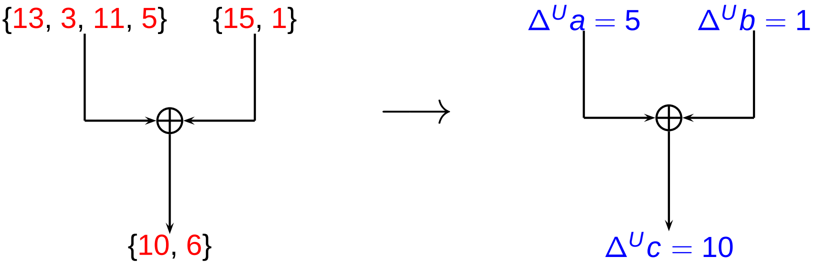
$$\mathrm{adp}^{\oplus}(5, 1 \rightarrow 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 1 \rightarrow 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 15 \rightarrow 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(5, 15 \rightarrow 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 1 \rightarrow 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 1 \rightarrow 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 15 \rightarrow 10) = 0.15625$$
$$\mathrm{adp}^{\oplus}(11, 15 \rightarrow 6) = 0.15625$$
$$\mathrm{adp}^{\oplus}(3, 1 \rightarrow 10) = 0.09375$$
$$\mathrm{adp}^{\oplus}(3, 1 \rightarrow 6) = 0.09375$$
$$\mathrm{adp}^{\oplus}(3, 15 \rightarrow 10) = 0.09375$$
$$\mathrm{adp}^{\oplus}(3, 15 \rightarrow 6) = 0.09375$$
$$\mathrm{adp}^{\oplus}(13, 1 \rightarrow 10) = 0.09375$$
$$\mathrm{adp}^{\oplus}(13, 1 \rightarrow 6) = 0.09375$$
$$\mathrm{adp}^{\oplus}(13, 15 \rightarrow 10) = 0.09375$$

UNAF: Clustering of Differentials



$$
\begin{aligned}
\mathrm{adp}^{\oplus}(5, 1 \to 10) &= 0.15625\\
\mathrm{adp}^{\oplus}(5, 1 \to 6) &= 0.15625\\
\mathrm{adp}^{\oplus}(5, 15 \to 10) &= 0.15625\\
\mathrm{adp}^{\oplus}(5, 15 \to 6) &= 0.15625\\
\mathrm{adp}^{\oplus}(11, 1 \to 10) &= 0.15625\\
\mathrm{adp}^{\oplus}(11, 1 \to 6) &= 0.15625\\
\mathrm{adp}^{\oplus}(11, 15 \to 10) &= 0.15625\\
\mathrm{adp}^{\oplus}(11, 15 \to 6) &= 0.15625\\
\mathrm{adp}^{\oplus}(3, 1 \to 10) &= 0.09375\\
\mathrm{adp}^{\oplus}(3, 1 \to 6) &= 0.09375\\
\mathrm{adp}^{\oplus}(3, 15 \to 10) &= 0.09375\\
\mathrm{adp}^{\oplus}(3, 15 \to 6) &= 0.09375\\
\mathrm{adp}^{\oplus}(13, 1 \to 10) &= 0.09375\\
\mathrm{adp}^{\oplus}(13, 1 \to 6) &= 0.09375\\
\mathrm{adp}^{\oplus}(13, 15 \to 10) &= 0.09375\\
\mathrm{adp}^{\oplus}(13, 15 \to 6) &= 0.09375
\end{aligned}
$$

UNAF: Clustering of Differentials



$$\mathrm{adp}^{\oplus} > 0 \quad .$$

Main UNAF Theorem

Theorem

$$\mathrm{adp}^{\oplus}(\Delta^{+}a, \Delta^{+}b \to \Delta^{+}c) > 0 \implies \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) > 0 \ ,$$

$$\forall \alpha \in \Delta^{U}a, \ \forall \beta \in \Delta^{U}b, \ \forall \gamma \in \Delta^{U}c \ .$$

The UNAF Differential Probability of XOR

$$\mathrm{udp}^{\oplus}(\Delta^{U}a, \Delta^{U}b \rightarrow \Delta^{U}c) =$$

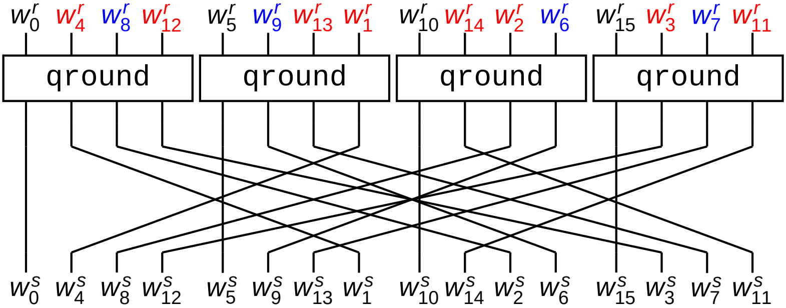
$$\frac{\#\{(a_1, b_1) : \Delta^{+}a \in \Delta^{U}a, \Delta^{+}b \in \Delta^{U}b, \Delta^{+}c \in \Delta^{U}c\}}{\#\{(a_1, b_1) : \Delta^{+}a \in \Delta^{U}a, \Delta^{+}b \in \Delta^{U}b\}} \ .$$

Salsa20 Input State

- 256-bit **key** $(k_0, k_1, \ldots, k_7)$
- 64-bit **nonce** (v_0, v_1)
- 64-bit **counter** (t_0, t_1)
- four 32-bit **constants** c_0, c_1, c_2, c_3

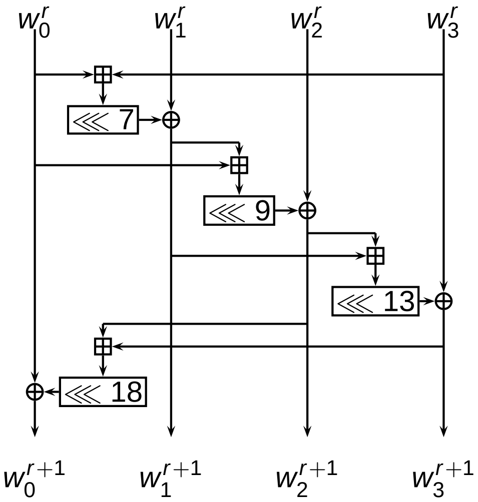
$$\begin{bmatrix} \boxed{c_0} & k_0 & k_1 & k_2 \\ k_3 & \boxed{c_1} & \boxed{v_0} & \boxed{v_1} \\ \boxed{t_0} & \boxed{t_1} & \boxed{c_2} & k_4 \\ k_5 & k_6 & k_7 & \boxed{c_3} \end{bmatrix} \rightarrow \begin{bmatrix} w_0^0 & w_1^0 & w_2^0 & w_3^0 \\ w_4^0 & w_5^0 & w_6^0 & w_7^0 \\ w_8^0 & w_9^0 & w_{10}^0 & w_{11}^0 \\ w_{12}^0 & w_{13}^0 & w_{14}^0 & w_{15}^0 \end{bmatrix} .$$

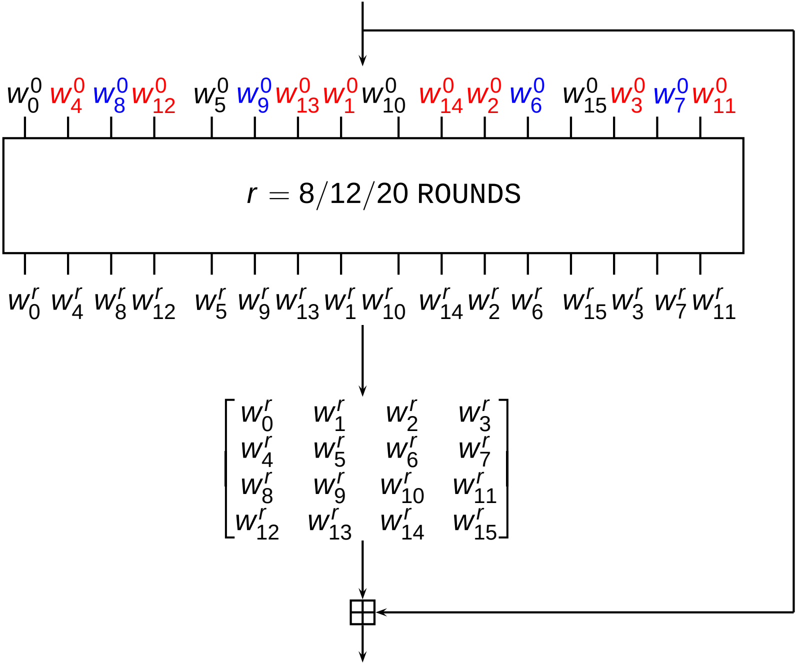
One Round



$$s = r + 1 \ .$$

One qround





w_0^0 w_4^0 w_8^0 w_{12}^0 w_5^0 w_9^0 w_{13}^0 w_1^0 w_{10}^0 w_{14}^0 w_2^0 w_6^0 w_{15}^0 w_3^0 w_7^0 w_{11}^0
$r = 8/12/20$ ROUNDS
w_0^r w_4^r w_8^r w_{12}^r w_5^r w_9^r w_{13}^r w_1^r w_{10}^r w_{14}^r w_2^r w_6^r w_{15}^r w_3^r w_7^r w_{11}^r
$\begin{bmatrix} w_0^r & w_1^r & w_2^r & w_3^r \\ w_4^r & w_5^r & w_6^r & w_7^r \\ w_8^r & w_9^r & w_{10}^r & w_{11}^r \\ w_{12}^r & w_{13}^r & w_{14}^r & w_{15}^r \end{bmatrix}$

Estimating Probability of Differentials using UNAF

Three estimations of the probabilities of the N-round differential:

$$\Delta^{+}{}_{\mathrm{in}} \xrightarrow{N} \Delta^{+}{}_{\mathrm{out}} \quad .$$

1. Based on experiments:

$$p_{\mathrm{exper}} \quad .$$

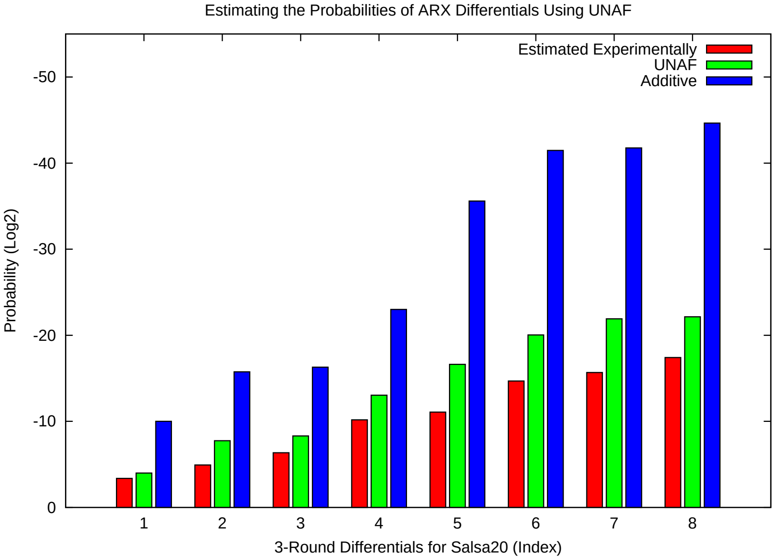
2. Using single additive differences:

$$\hat{p}_{\mathrm{add}} = \prod \mathrm{adp}^{\mathsf{ARX}} \quad .$$

3. Using UNAF differences:

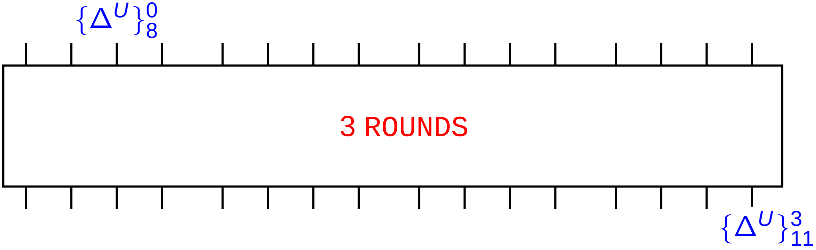
$$\hat{p}_{\mathrm{unaf}} = \prod \mathrm{udp}^{\mathsf{ARX}} \quad .$$

Improved Probability Estimations Using UNAF

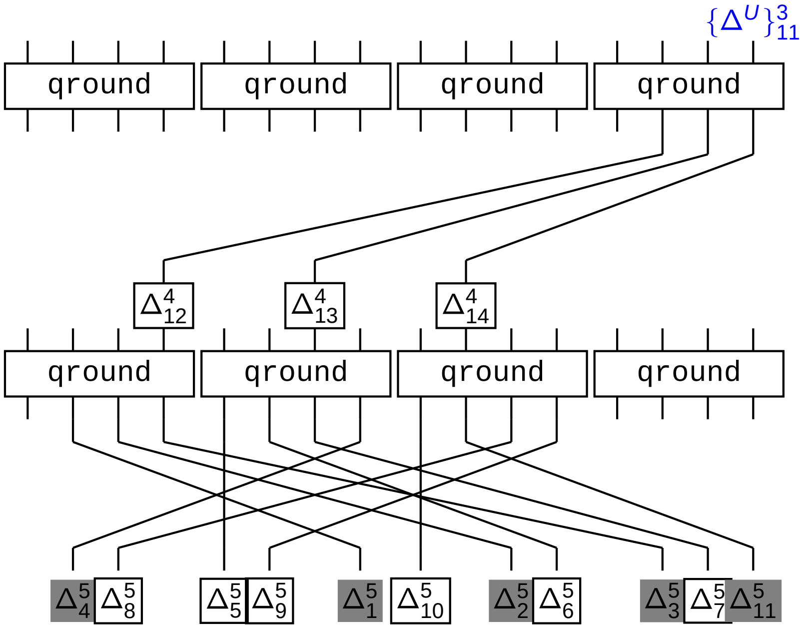


Key-recovery attack on Salsa20/5

$$\{\Delta^U\}_8^0 = \texttt{0x80000000} \rightarrow \{\Delta^U\}_{11}^3 = \texttt{0x01000024}$$



$P_\Delta = 2^{-3.38}$ $(P_{\text{rand}} = 2^{-29})$



$\{\Delta^U\}_{11}^3$
qround
qround
qround
qround
Δ_{12}^4
Δ_{13}^4
Δ_{14}^4
qround
qround
qround
qround
Δ_4^5 Δ_8^5
Δ_5^5 Δ_9^5
Δ_1^5 Δ_{10}^5
Δ_2^5 Δ_6^5
Δ_3^5 Δ_7^5 Δ_{11}^5

Attack Complexity

Rounds	Reference	Time	Data	Type of Differences
Salsa20/5	Our result*	$\mathbf{2^{167}}$	$\mathbf{2^{7}}$	Additive
Salsa20/5	Crowley	2^{165}	2^{6}	XOR
Salsa20/6	Fischer et al.	2^{177}	2^{16}	XOR
Salsa20/7	Aumasson et al.	2^{151}	2^{26}	XOR
Salsa20/8	Aumasson et al.	2^{251}	2^{31}	XOR

* Room for improval.

Contributions and Future Work

- Summary of Contributions:
  - Proposed new type of difference: UNAF.
  - UNAF improves estimation of probabilities of differentials.
  - Demonstrated practical application of UNAF to stream cipher Salsa20.
- Future Work:
  - Why are the probabilities of differentials from the same UNAF set very close? (More rigorous analysis is needed.)
  - Do UNAF differences lead to better attacks?
  - Apply UNAF to other algorithms: Skein, BLAKE, TEA, ...

Thank you for your attention!

Computation of $\mathrm{adp}^{\oplus}$

Computing the probability $\mathrm{adp}^{\oplus}$ is equivalent to the matrix multiplication:

$$\mathrm{adp}^{\oplus}(\Delta^{+}a, \Delta^{+}b \rightarrow \Delta^{+}c) = L A_{w[n-1]} \cdots A_{w[1]} A_{w[0]} C \ ,$$

where

$$w[i] = \Delta^{+}a[i] \parallel \Delta^{+}b[i] \parallel \Delta^{+}c[i], \ \ 0 \leq i < n \ ,$$

$$L = [\ 1 \ \ 1 \ \ 1 \ \ 1 \ \ 1 \ \ 1 \ \ 1 \ \ 1\ ] \ ,$$

$$C = [\ 0 \ \ 0 \ \ 0 \ \ 0 \ \ 1 \ \ 0 \ \ 0 \ \ 0\ ]^{T} \ .$$

Best-first Search Strategy Based on A*