Multiset analysis of ARX with application to 3fish (WIP)

Jean-Philippe Aumasson, Willi Meier, Raphael C.-W. Phan

NAGRAVISION KUDELSKI GROUP

n|w University of Applied Sciences Northwestern Switzerland

Loughborough University

Multiset analysis

Multiset = set of elements with multiplicities
e.g. $\{\alpha, \alpha, \beta, \gamma, \gamma, \gamma\} = \{(\alpha, 2), (\beta, 1), (\gamma, 3)\}$

Dates back to the Biryukov-Shamir attacks on SASAS…

- *C*: constant (multiplicity 2^w for w-bit multiset)
- *P*: permutation (all multiplicities 1)
- *E*: even (all multiplicities even)
- *B*: XOR sum of all multiset elements = zero
- *A*: ADD sum of all multiset elements = zero
- *D*: dual (either *P* or *E*)

Multiset analysis refinements

Subwords msets (Nakahara Jr et al. '05):

- *nw*-bit msets comprise (smaller) *w*-bit msets
- e.g. 32-bit *P* mset comprises four 8-bit *E* msets

Bitslicing (Z'aba et al. '08):

- *w*-bit msets split into *w* slices of bit multisets
- bit multiset a_i: alternating running sequence of 0 and 1, each of length 2^i

Multisets vs (64-bit) ARX

ROT:

- $\forall X \in \{C, P, E, B, D\}, X \lll n = X$

XOR:

- $\forall X, C \oplus X = X$
- $P \oplus P = B$, $P \oplus E = B$, $E \oplus E = B$, $B \oplus B = B$
- $P \oplus P =^\star C$, $P \oplus P =^\star E$, $P \oplus E =^\star E$

ADD:

- $\forall X, C + X = X$
- $P + P = A$
- $P + P =^\star C$, $P + P =^\star E$, $P + E =^\star E$

Etc.

*: when some conditions are satisfied

Multisets vs 3fish's **MIX**

$\mathbf{MIX}(x, y) = (x + y, (x + y) \oplus (y \lll n))$

Through **MIX**:

- $\langle P, C\rangle \mapsto \langle P + C, (P + C) \oplus C\rangle = \langle P, P\rangle$
- $\langle C, P\rangle \mapsto \langle C + P, (C + P) \oplus P\rangle = \langle P, B\rangle$
- If P's have "opposed" ordering wrt +:
  $\langle P, P\rangle \mapsto \langle P + P, (P + P) \oplus P\rangle = \langle C, P\rangle$

Can experiment with 8-bit shrinked versions, results essentially independent of the word size

Multisets vs 3fish's rounds

Key constants $\Rightarrow$ keying preserves C, P, E

Properties tracked through 7 rounds of 3fish1024:

$$\langle C, C, P, P, C, C, C, C, C, C, C, C, C, C, C, C\rangle$$
$$\langle C, C, C, C, C, C, C, C, C, C, C, P, C, C, C, C\rangle$$
$$\langle C, C, C, C, C, C, C, C, P, C, C, C, C, C, C, C\rangle$$
$$\langle C, P, C, C, C, C, C, C, C, C, C, C, C, C, P, C\rangle$$
$$\langle P, C, C, C, C, C, C, P, C, C, C, C, P, C, C, B\rangle$$
$$\langle P, C, C, P, P, C, C, X, C, X, P, C, X, C, C, P\rangle$$
$$\langle P, X, P, X, X, P, P, B, P, X, X, B, P, P, X, P\rangle$$
$$\langle X, X, X, X, X, X, X, X, X, X, E, X, X, X, X, X\rangle$$

Still some structure in X

Multisets through ARX revisited

$P + P' \mapsto ?$

- if P, P' same a_i sequence, e.g. both $a_2 a_1 a_0$, then $P + P' \mapsto E$
- if P, P' different a_i sequence, e.g. $P = a_2 a_1 a_0$, $P' = a_1 a_0 a_2$, then more involved, consider higher order

Higher-order analysis:

- Consider all 2^3 $P_x = a_2 a_1 a_0$ and $P_y = P_x \lll 1 = a_1 a_0 a_2)$
- Count #unique elements in each $P_x \oplus P_y$

More refinements (todo)

Inside-out approach (à la 0Σ)

Track other properties than *ABCPE*

Careful choice of *P*'s ordering and bitslices structure

Differential approach

Apply results from additive combinatorics re sumsets (see Chap. 2 of Tao/Vu 2006)

Optimize automated program. . .

Application to other ARX's (BLAKE. . .)

More. . .