More on the Automatic Search for Differential Trails in NORX (Work in Progress)

V. Velichkov

University of Luxembourg, SnT

Directions in Authenticated Ciphers (DIAC) 2016
September 26, 2016, Nagoya, Japan
1 Motivation

2 NORX

3 Automatic Search for Trails

4 Results

5 Conclusions
1. Motivation

2. NORX

3. Automatic Search for Trails

4. Results

5. Conclusions
Resistance of NORX Against DC

- Designers give bounds against DC [AJN14]
- Use SAT-solver; memory is exhausted for more rounds
- Bounds based on best trails for up to $F^{2.0}$ rounds

<table>
<thead>
<tr>
<th>W</th>
<th>Scenarios</th>
<th>init$_N$</th>
<th>init$_{N,K}$</th>
<th>rate</th>
<th>full</th>
<th>init$_N$</th>
<th>init$_{N,K}$</th>
<th>rate</th>
<th>full</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$F^{0.5}$</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>$F^{1.0}$</td>
<td>(60)</td>
<td>22</td>
<td>10</td>
<td>2</td>
<td>(53)</td>
<td>22</td>
<td>12</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>$F^{1.5}$</td>
<td>(60)</td>
<td>(40)</td>
<td>(31)</td>
<td>12</td>
<td>(53)</td>
<td>(35)</td>
<td>(27)</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>$F^{2.0}$</td>
<td>(61)</td>
<td>(45)</td>
<td>(34)</td>
<td>(27)</td>
<td>(51)</td>
<td>(37)</td>
<td>(30)</td>
<td>(23)</td>
</tr>
</tbody>
</table>

Scenario: modify the nonce (init$_N$), nonce + key (init$_{N,K}$), rate words (rate), full state (full).
MOTIVATION

Research Goal

Provide tighter bounds than the ones reported by [AJN14]

Disclaimer: Work-in-progress; preliminary results.
Our Contributions

1. New algorithm for finding optimal trails – **Best Search (BS)**
2. Heuristic version of BS – **Heuristic Search (HS)**
3. New (sub-optimal) trails on up to $F^{2.0}$ rounds with HS

<table>
<thead>
<tr>
<th>Scenario</th>
<th>init$_N$</th>
<th>init$_{N,K}$</th>
<th>rate</th>
<th>full</th>
<th>init$_N$</th>
<th>init$_{N,K}$</th>
<th>rate</th>
<th>full</th>
</tr>
</thead>
<tbody>
<tr>
<td>$F^{0.5}$</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>$F^{1.0}$</td>
<td>84</td>
<td>22</td>
<td>10</td>
<td>2</td>
<td>88</td>
<td>22</td>
<td>12</td>
<td>2</td>
</tr>
<tr>
<td>$F^{1.5}$</td>
<td>319</td>
<td>210</td>
<td>205</td>
<td>12</td>
<td>413</td>
<td>263</td>
<td>245</td>
<td>12</td>
</tr>
<tr>
<td>$F^{2.0}$</td>
<td>606</td>
<td>476</td>
<td>493</td>
<td>354</td>
<td>809</td>
<td>656</td>
<td>645</td>
<td>561</td>
</tr>
<tr>
<td></td>
<td>OUTLINE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Motivation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>NORX</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Automatic Search for Trails</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Results</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Conclusions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(University of Luxembourg, SnT)
OVERVIEW OF NORX

- Word size: $W \in \{32, 64\}$ bits
- Rounds: $1 \leq R \leq 63$
- Parallelism: $0 \leq D \leq 255$
- Tag size: $|A| \leq 10W$

<table>
<thead>
<tr>
<th>NORXW-R-D</th>
<th>Nonce (2W)</th>
<th>Key (4W)</th>
<th>Tag (4W)</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>NORX64-4-1</td>
<td>128</td>
<td>256</td>
<td>256</td>
<td>Standard</td>
</tr>
<tr>
<td>NORX32-4-1</td>
<td>64</td>
<td>128</td>
<td>128</td>
<td>Standard</td>
</tr>
<tr>
<td>NORX64-6-1</td>
<td>128</td>
<td>256</td>
<td>256</td>
<td>High security</td>
</tr>
<tr>
<td>NORX32-6-1</td>
<td>64</td>
<td>128</td>
<td>128</td>
<td>High security</td>
</tr>
<tr>
<td>NORX64-4-4</td>
<td>128</td>
<td>256</td>
<td>256</td>
<td>High throughput</td>
</tr>
</tbody>
</table>

Credits: Philipp Jovanovic, ESORICS 2014.
NORX = NO(T A)RX

- Sponge structure based on the monkeyDuplex construction
- LRX permutation: $\oplus$, $\gg$, $\land$, $\ll 1$
- Non-linear component: $H(x, y) = (x \oplus y) \oplus ((x \land y) \ll 1)$
- No S-box; No modular addition

Credits: NORX Specification https://norx.io/
PERMUTATION $F$

$F$ is composed of $G$-circuit (next slide) applied in parallel first to each of the 4 columns of the state followed by an application to each of the 4 diagonals of the state: $F = F_{\text{dia}} \circ F_{\text{col}}$

Credits: NORX Specification https://norx.io/
**HALF-ROUND:** $F^{0.5} = F_{\text{col}}$

4 parallel app. of the G-circuit, where $H(x, y) = (x \oplus y) \oplus ((x \land y) \ll 1)$.

Note: Initialization = $F^8$; Data processing = $F^4$. 
Matsui’s Algorithm

Input: best $p$ for $n - 1$ rounds:
$B_1, B_2, \ldots, B_{n-1}; \bar{B}_n$

Output: best $p$ for $n$ rounds:
$B_n$

if $P_1P_2\ldots P_iB_{n-i} \geq \bar{B}_n$ : $i \leftarrow i + 1$

if $i = n$: $B_n \leftarrow \bar{B}_n$
Matsui’s Algorithm for ARX [BVLC16]

\[
\begin{align*}
\alpha &
\quad \beta \\
\gamma &
\quad xdp^+ \\
\quad &
\quad 2^{-\text{hw}(-\text{eq} (\alpha, \beta, \gamma) \land \text{mask}_{n-1})} \quad [LM01]
\end{align*}
\]

Proposition (Monotonicity of \( xdp^+ \))

\( xdp^+ \) is monotonously decreasing with the word size \( w \) of \( \alpha, \beta, \gamma \):

\[
\tilde{p}_1 \geq \tilde{p}_2 \geq \ldots \geq \tilde{p}_{w-1} \geq \tilde{p}_w = xdp^+ (\alpha, \beta \rightarrow \gamma),
\]

where \( \tilde{p}_i = xdp^+ (\alpha[i-1:0], \beta[i-1:0] \rightarrow \gamma[i-1:0]) : w \geq i \geq 1 \), is the probability of the partial differential composed of the \( i \) LS bits of \( \alpha, \beta, \gamma \).
**MONOTONICITY OF \( xdp^H \)**

\[
\begin{align*}
\alpha & \rightarrow H \\
\downarrow & \\
\gamma & \leftarrow H \rightarrow xdp^H \beta
\end{align*}
\]

\[
H(x, y) = (x \oplus y) \oplus ((x \land y) \ll 1)
\]

---

**The Differential Probability of \( H \) [AJN14]**

\[
xdp^H(\alpha, \beta \rightarrow \gamma) = \begin{cases} 
2^{-hw((\alpha \lor \beta) \ll 1)} & \iff (\alpha \oplus \beta \oplus \gamma) \land (\neg((\alpha \lor \beta) \ll 1)) = 0 \\
0, \text{ otherwise} & 
\end{cases}
\]

---

**Proposition (Monotonicity of \( xdp^H \))**

\( xdp^H \) is monotonously decreasing with the word size of \( \alpha, \beta, \gamma \).
**Best Search (BS): Rounds $i$ and $i+1$**

\[
\tilde{P}_i = \tilde{p}^0[0]
\]

\[
\text{if } P_1 P_2 \ldots \tilde{P}_i B_{n-i} \geq \bar{B}_n \text{ assign next bit}
\]
**Best Search (BS): Rounds $i$ and $i+1$**

![Diagram showing the best search process in NORX]

If $P_1P_2\ldots \tilde{P}_i B_{n-i} \geq \bar{B}_n$ assign next bit
Best Search (BS): Rounds $i$ and $i+1$

$\tilde{P}_i = \tilde{p}^0[0:2]$

if $P_1 P_2 \ldots \tilde{P}_i B_{n-i} \geq \bar{B}_n$ assign next bit
**Best Search (BS): Rounds \( i \) and \( i + 1 \)**

\[
\tilde{P}_i = p^0
\]

\[
\text{if } P_1 P_2 \ldots \tilde{P}_i B_{n-i} \geq \tilde{B}_n \text{ assign next bit}
\]
Best Search (BS): Rounds $i$ and $i + 1$

\[
\tilde{P}_i = p_0p_1
\]

if \( P_1P_2\ldots \tilde{P}_iB_{n-i} \geq \bar{B}_n \) assign next bit
**Best Search (BS): Rounds $i$ and $i+1$**

$$
\tilde{P}_i = p^0 p^1 p^2
$$

if $P_1 P_2 \ldots \tilde{P}_i B_{n-i} \geq \bar{B}_n$ assign next bit
Best Search (BS): Rounds $i$ and $i + 1$

\[ P_i = p_0 p_1 p_2 p_3 \]

\[ H \]

\[ B_n \geq \bar{B}_n \] assign next bit
**Best Search (BS): Rounds \( i \) and \( i + 1 \)**

\[
\tilde{P}_{i+1} = \tilde{p}^0[0]
\]

if \( P_1P_2...P_i\tilde{P}_{i+1}B_{n-i-1} \geq \bar{B}_n \) assign next bit
**Best Search (BS): Rounds $i$ and $i + 1$**

If $P_1 P_2 \cdots P_i \tilde{P}_{i+1} B_{n-i-1} \geq \bar{B}_n$ assign next bit

$(University of Luxembourg, SnT)$ Automatic Search for Trails in NORX
Best Search (BS): Rounds $i$ and $i+1$

If $P_1 P_2 \ldots P_i \tilde{P}_{i+1} B_{n-i-1} \geq \tilde{B}_n$ assign next bit
Best Search (BS): Rounds $i$ and $i + 1$

\[ P_1 P_2 \ldots P_i \tilde{P}_{i+1} \bar{B}_{n-i-1} \geq \bar{B}_n \] assign next bit
**Best Search (BS): Rounds $i$ and $i+1$**

If $P_1 P_2 \ldots P_i \tilde{P}_{i+1} B_{n-i-1} \geq \tilde{B}_n$ assign next bit

\[ \tilde{P}_{i+1} = p^0 p^1 \]
**Best Search (BS): Rounds $i$ and $i + 1$**

\[
\tilde{P}_{i+1} = p^0 p^1 p^2
\]

if $P_1 P_2 \ldots P_i \tilde{P}_{i+1} B_{n-i-1} \geq \bar{B}_n$ assign next bit
**Best Search (BS): Rounds $i$ and $i+1$**

If $P_1 P_2 \ldots P_i P_{i+1} B_{n-i-1} \geq \bar{B}_n$ assign next bit

(University of Luxembourg, SnT)
**COMPLEXITY OF BS**

### Time and Memory Requirements

- Negligible memory (**good**)
- Time is proportional to num. of rounds and word size (**bad**)
- Feasible up to $F^{0.5} / F^{1.0}$ rounds (SAT-solver covers up to $F^{1.0} / F^{1.5}$)

### Time Measurements for NORX32 and NORX64

- **BS** $F^{0.5} / F^{1.0}$ $\approx$ 49 days; negl. RAM (3.4GHz PC)
- **SAT** $F^{1.0} / F^{1.5}$ $\approx$ 8 hours; 49 GB RAM [AJN14]
**Heuristic Search (HS)**

Heuristics to lower the time complexity of BS

1. **Time Limit (TL)**
   - How long to wait before the recursive call is terminated

2. **Maximum Number of Tries (MT)**
   - Number of times that we restart the search after the TL is exceeded.

3. **Branch Factor Percentage $x$ (BF)**
   - In $x$ out of 100 cases branch and explore both 0 and 1 for a given bit.
   - In the remaining cases set the bit to 0.
   - Intuition: due to $xdp^H(\alpha, \beta \rightarrow \gamma) = 2^{-\text{hw}((\alpha \lor \beta) \ll 1)}$

<table>
<thead>
<tr>
<th>TL, sec</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>30</th>
<th>60</th>
<th>60</th>
<th>600</th>
<th>3600</th>
</tr>
</thead>
<tbody>
<tr>
<td>MT</td>
<td>65535</td>
<td>1024</td>
<td>512</td>
<td>256</td>
<td>256</td>
<td>256</td>
<td>64</td>
<td>1</td>
</tr>
<tr>
<td>BF</td>
<td>30</td>
<td>50</td>
<td>75</td>
<td>50</td>
<td>50</td>
<td>50</td>
<td>75</td>
<td>100</td>
</tr>
</tbody>
</table>
NORX8: BS vs. HS, scenario: $\text{INIT}_N$
NORX8: BS vs. HS, scenario: FULL

Best Search vs. Heuristic Search $W = 8$

Round Number $R$: $F_R$

Probability, $|\log_2|$
NORX16: BS vs. HS, SCENARIO: INIT_N

Best Search vs. Heuristic Search W = 16

Probability, $|\log_2|$ vs. Round Number $R$: $F^R$

- HS init-N (red)
- BS init-N (green)

(Upon closer inspection, the table of results and other sections of the document are not included in this response.)
NORX16: BS vs. HS, Scenario: FULL
## Conclusions and Future Work

<table>
<thead>
<tr>
<th>Scenario</th>
<th>init&lt;sub&gt;N&lt;/sub&gt;</th>
<th>init&lt;sub&gt;N,K&lt;/sub&gt;</th>
<th>rate</th>
<th>full</th>
<th>init&lt;sub&gt;N&lt;/sub&gt;</th>
<th>init&lt;sub&gt;N,K&lt;/sub&gt;</th>
<th>rate</th>
<th>full</th>
</tr>
</thead>
<tbody>
<tr>
<td>F&lt;sup&gt;0.5&lt;/sup&gt;</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>F&lt;sup&gt;1.0&lt;/sup&gt;</td>
<td>84</td>
<td>22</td>
<td>10</td>
<td>2</td>
<td>88</td>
<td>22</td>
<td>12</td>
<td>2</td>
</tr>
<tr>
<td>F&lt;sup&gt;1.5&lt;/sup&gt;</td>
<td>319</td>
<td>210</td>
<td>205</td>
<td>12</td>
<td>413</td>
<td>263</td>
<td>245</td>
<td>12</td>
</tr>
<tr>
<td>F&lt;sup&gt;2.0&lt;/sup&gt;</td>
<td>606</td>
<td>476</td>
<td>493</td>
<td>354</td>
<td>809</td>
<td>656</td>
<td>645</td>
<td>561</td>
</tr>
</tbody>
</table>

- New heuristic algorithm for diff. search in NORX
- Matsui-like; Negligible memory; Manageable time
- Accuracy drastically degrades in the num. rounds and word size
CONCLUSIONS AND FUTURE WORK

<table>
<thead>
<tr>
<th>Scenario</th>
<th>init_N</th>
<th>init_N,K</th>
<th>rate</th>
<th>full</th>
<th>init_N</th>
<th>init_N,K</th>
<th>rate</th>
<th>full</th>
</tr>
</thead>
<tbody>
<tr>
<td>$F^{0.5}$</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>$F^{1.0}$</td>
<td>84</td>
<td>22</td>
<td>10</td>
<td>2</td>
<td>88</td>
<td>22</td>
<td>12</td>
<td>2</td>
</tr>
<tr>
<td>$F^{1.5}$</td>
<td>319</td>
<td>210</td>
<td>205</td>
<td>12</td>
<td>413</td>
<td>263</td>
<td>245</td>
<td>12</td>
</tr>
<tr>
<td>$F^{2.0}$</td>
<td>606</td>
<td>476</td>
<td>493</td>
<td>354</td>
<td>809</td>
<td>656</td>
<td>645</td>
<td>561</td>
</tr>
</tbody>
</table>

- New trails on up to $F^{2.0}$ rounds $\Rightarrow$ new diff. bounds
- Designers’ bounds are too pessimistic (designer’s PoV)
- Our bounds are too optimistic (designer’s PoV)
- Need better heuristics; new (algorithmic) optimizations; BS + SAT
CONCLUSIONS AND FUTURE WORK

<table>
<thead>
<tr>
<th>Scenario</th>
<th>$W$</th>
<th>32</th>
<th>64</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>init$_N$</td>
<td>init$_{N,K}$</td>
<td>rate</td>
</tr>
<tr>
<td>$F^{0.5}$</td>
<td>6</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>$F^{1.0}$</td>
<td>84</td>
<td>22</td>
<td>10</td>
</tr>
<tr>
<td>$F^{1.5}$</td>
<td>319</td>
<td>210</td>
<td>205</td>
</tr>
<tr>
<td>$F^{2.0}$</td>
<td>606</td>
<td>476</td>
<td>493</td>
</tr>
</tbody>
</table>

Main Message

NORX is a conservative design with large security margin against DC
CONCLUSIONS AND FUTURE WORK

<table>
<thead>
<tr>
<th>W</th>
<th>32</th>
<th></th>
<th>64</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scenario</td>
<td>init&lt;sub&gt;N&lt;/sub&gt;</td>
<td>init&lt;sub&gt;N,K&lt;/sub&gt;</td>
<td>rate</td>
</tr>
<tr>
<td>F&lt;sup&gt;0.5&lt;/sup&gt;</td>
<td>6</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>F&lt;sup&gt;1.0&lt;/sup&gt;</td>
<td>84</td>
<td>22</td>
<td>10</td>
</tr>
<tr>
<td>F&lt;sup&gt;1.5&lt;/sup&gt;</td>
<td>319</td>
<td>210</td>
<td>205</td>
</tr>
<tr>
<td>F&lt;sup&gt;2.0&lt;/sup&gt;</td>
<td>606</td>
<td>476</td>
<td>493</td>
</tr>
</tbody>
</table>

Main Message

NORX is a conservative design with large security margin against DC

Thank you for your attention!

Questions?