Observations on Blake

Dmitry Khovratovich, Gaëtan Leurent, María Naya-Plasencia

March 23, 2011

Main idea

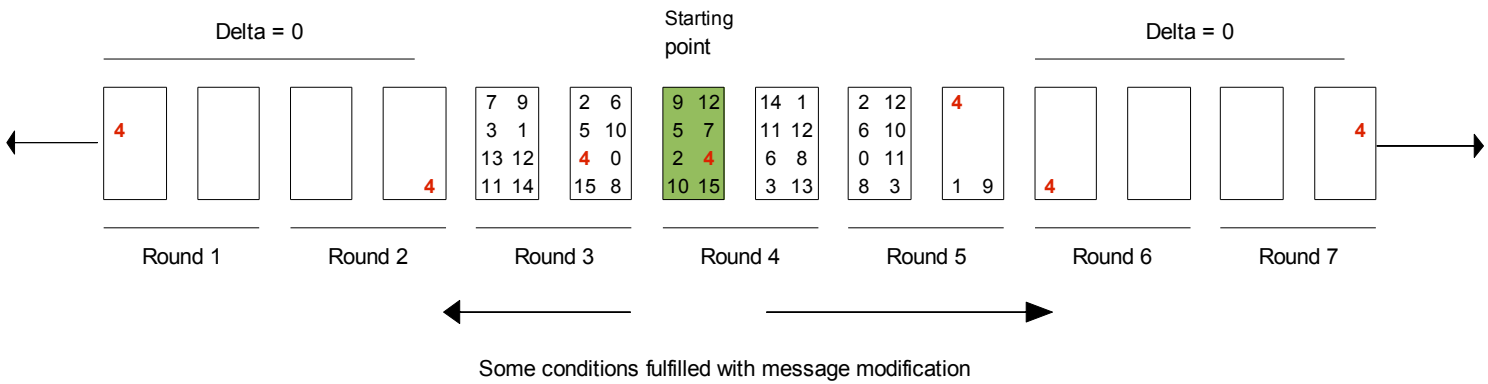
Rebound+Differential+Local collision

$\approx$ 10-round distinguisher for the permutation

Inbound

Inbound phase:

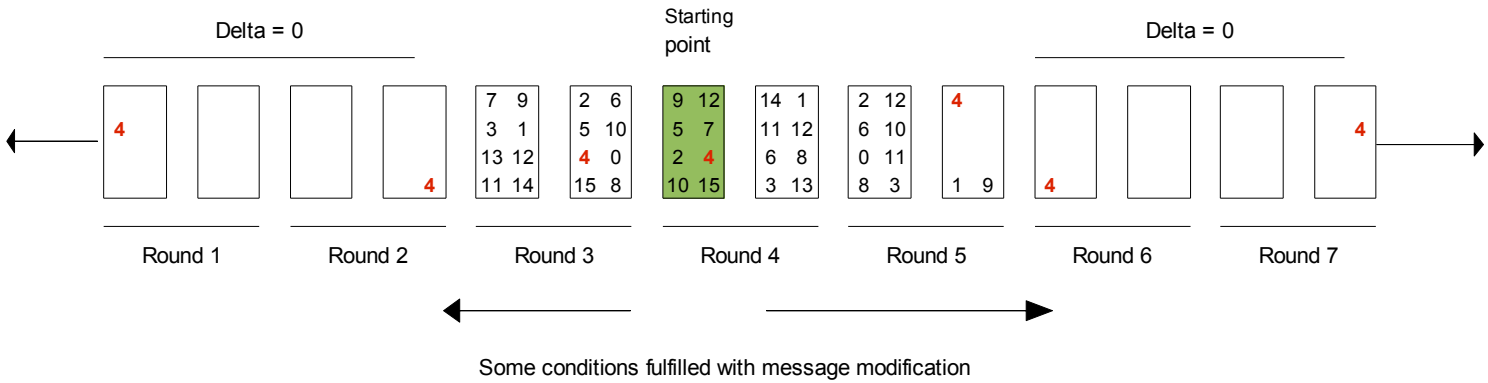
- Low-weight difference injection in a message (e.g., m_4 in rounds 2 and 6);
- ≈ 3.5 rounds of propagation towards each other in the linear fashion;
- Get input/output differences for the G-functions in a half-round in between;
- Resolve to values for each modular addition in G.



Outbound

Outbound phase:

- Message modification to conform the trail conditions in the middle rounds;
- About 3 rounds without difference in total;
- Probabilistic propagation in the ends.



Problems

Problems:

- Sparse differences do not resolve;
- High-weight trails are too expensive;
- Automated trail search is painful :)

Problems

Problems:

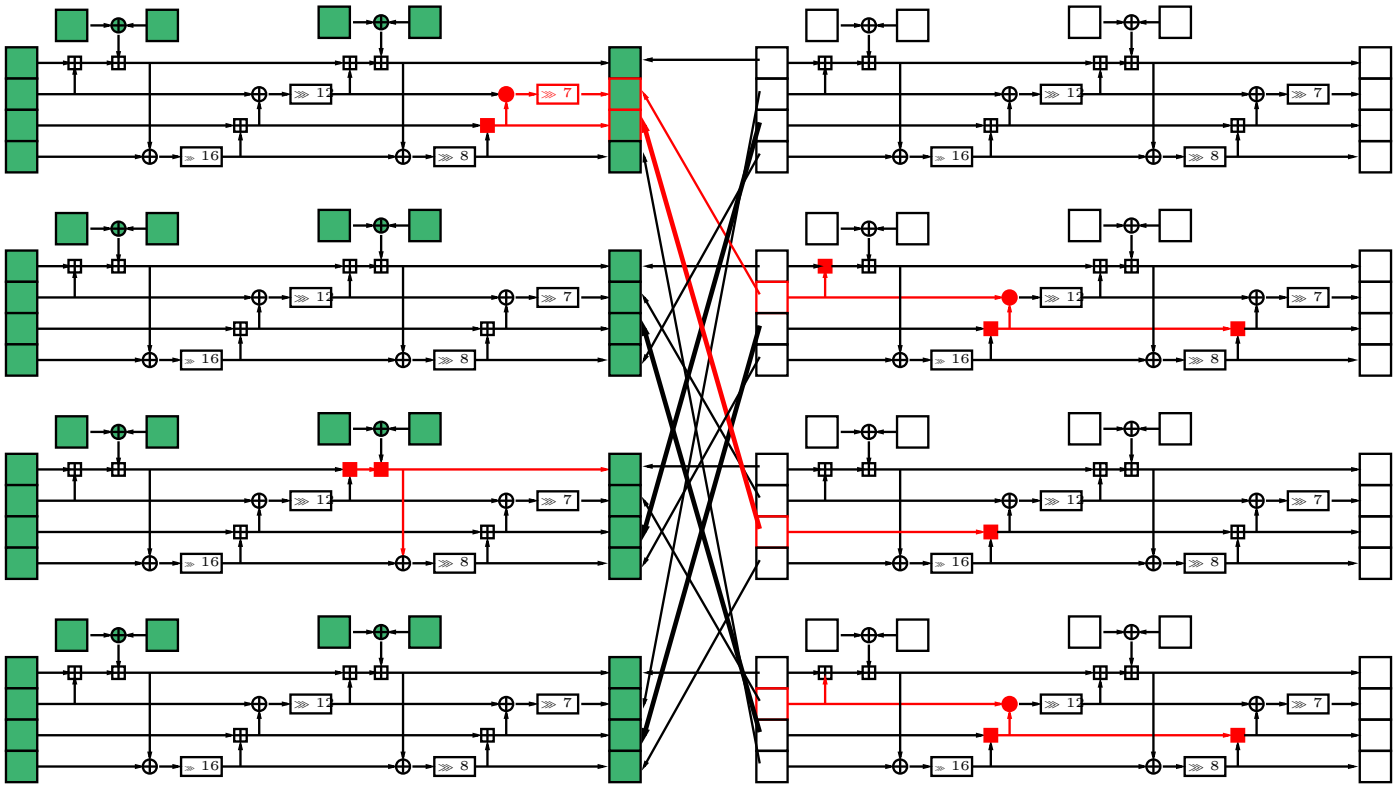
- Sparse differences do not resolve;
- High-weight trails are too expensive;
- Automated trail search is painful :)

Solutions?

- Adaptively introduce corrections to differential trails making them non-linear;
- Use more sophisticated message difference;
- Use multiple trails.

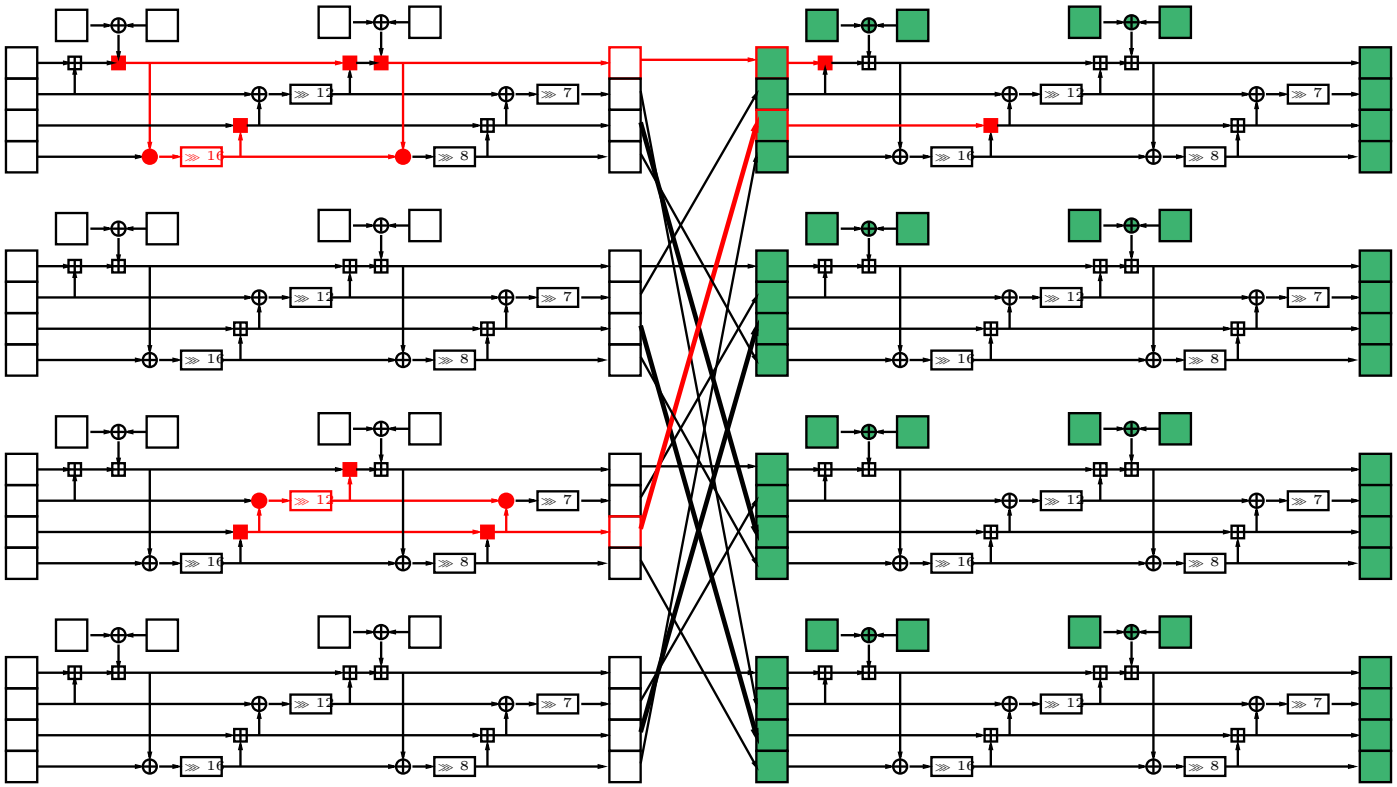
Corrections I

Corrections to the inbound phase trails: right side



Corrections II

Corrections to the inbound phase trails: left side



Future work

To be continued...