Update on the 15.000 Euro PRINCE cipher-breaking challenge

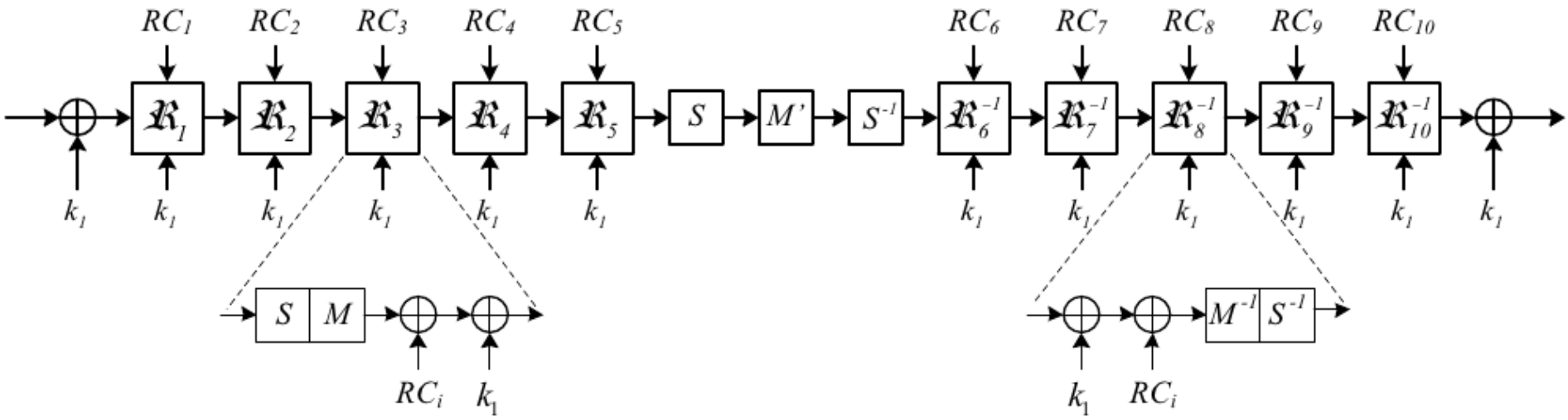
Gregor Leander (RUB)
Ventzi Nikov (NXP)
Christian Rechberger (DTU)
Vincent Rijmen (KU Leuven)

PRINCE

Cooperation between DTU, NXP and RUB

Published at Asiacrypt 2012

64-bit block size, 64+64=128-bit key



Reduced version: chop off outer rounds

Input from Industry

- Care about cryptanalysis
- Care about practical attacks
- Was usually not very concrete

This competition makes it more concrete

The PRINCE Challenge

Setting 1: Given 2^{20} chosen plaintexts/ciphertexts

- How fast can you break 4 rounds?
- How fast can you break 6 rounds?
- How fast can you break 8 rounds?
- How fast can you break 10 rounds?
- How fast can you break 12 rounds?

The PRINCE Challenge

Setting 2: Given 2^{30} known plaintexts

- How fast can you break 4 rounds?
- How fast can you break 6 rounds?
- How fast can you break 8 rounds?
- How fast can you break 10 rounds?
- How fast can you break 12 rounds?

Winners of Round 1

Patrick Derbez

SnT, University of Luxembourg

Léo Perrin

SnT, University of Luxembourg

Paweł Morawiecki

Polish Academy of Sciences, Computer Science Institute, and Kielce University of Commerce, Poland

The PRINCE Challenge

Setting 1: Given 2^{20} chosen plaintexts/ciphertexts

- How fast can you break 4 rounds?
  - Winner: Pawel, 2^7 CP, time 2^{11}
- How fast can you break 6 rounds?
  - Winners: Patrick, 2^{16}CP, time $2^{33.7}$ and Léo 2^{15}CP, time 90min
- How fast can you break 8 rounds?
  - Winner: Patrick: 2^{16}CP, time 2^{50}-2^{67}
- How fast can you break 10 rounds?
- How fast can you break 12 rounds?

The PRINCE Challenge

Setting 2: Given 2^{30} known plaintexts

- How fast can you break 4 rounds?
  - Patrick: 2^5 KP, time 2^{43}
- How fast can you break 6 rounds?
  - Patrick: 2^6 KP, time 2^{101}
- How fast can you break 8 rounds?
- How fast can you break 10 rounds?
- How fast can you break 12 rounds?

Prizes

- Best result for …
  - 4-round challenges: Chocolate/Beer
  - 6-round challenges: Chocolate/Beer
  - 8-round challenges: Chocolate/Beer
  - 10-round challenges: Chocolate/Beer
  - 12-round challenges: more Chocolate/Beer

- First attack with less than 2^{64} time, 2^{45} bytes memory on…
  - **8-rounds: 1.000 Euros**
  - **10-round: 4.000 Euros**
  - **12-round: 10.000 Euros**

Extension of Round-2 Schedule

submit convincing technical report to

prince-challenge@compute.dtu.dk

- Deadline: End of April 2015, before Eurocrypt

- Committee:
  - Gregor Leander (RUB)
  - Ventzi Nikov (NXP)
  - Christian Rechberger (DTU)
  - Vincent Rijmen (KUL)

Details

- Bonus points for even lower data complexities
- Bonus points for running code
- Bonus points for early submission
- Bonus points for clarity of description
- Bonus points for interesting observations used in the attack

- More details:

  https://www.emsec.rub.de/research/research_startseite/prince-challenge/

Update on the 15.000 Euro PRINCE cipher-breaking challenge

Gregor Leander (RUB)
Ventzi Nikov (NXP)
Christian Rechberger (DTU)
Vincent Rijmen (KU Leuven)