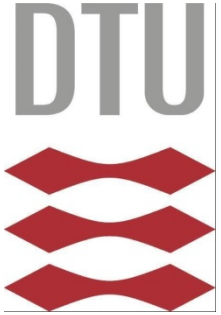
The PRINCE Challenge



Input from Industry

- Care about cryptanalysis
- Care about practical attacks
- Usually not very concrete

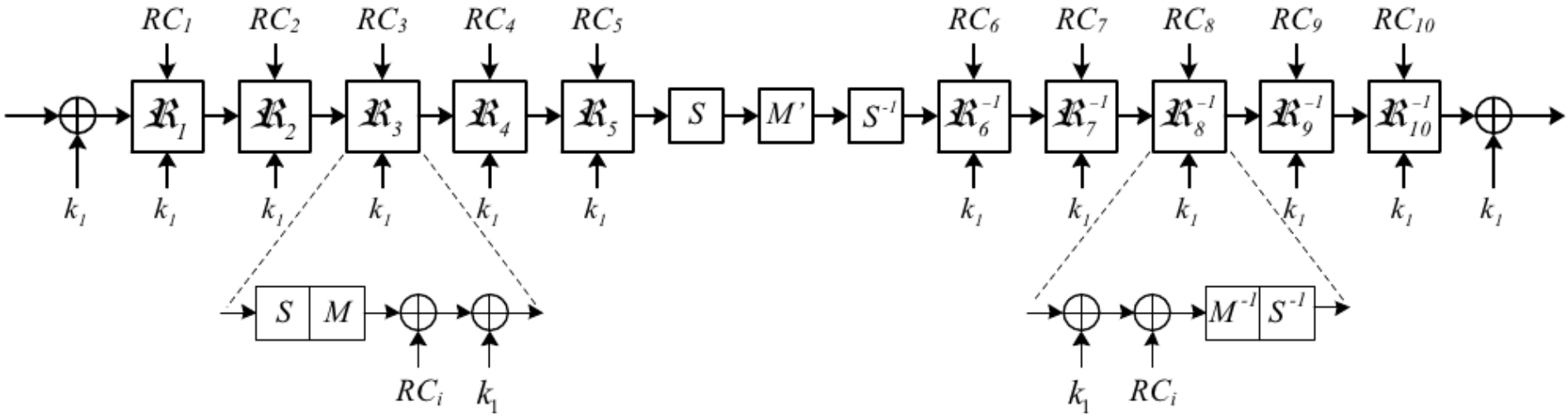
We will make it more concrete

PRINCE

Cooperation between DTU, NXP and RUB

Published at Asiacrypt 2012

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



Reduced version: chop off outer rounds

Existing cryptanalysis

- Published at Asiacrypt 2012
- Lots of existing cryptanalysis, no practical attacks, even on round-reduced versions

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?

Incentive Prizes

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

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

Cash Prizes

- Let's make it a bit more interesting…
- First attack with less than 2^{64} time, 2^{45} bytes memory on…
  - 8-round challenges: 1000 Euros
  - 10-round challenges : 4000 Euros
  - 12-round challenges : 10 000 Euros

Look at website for details

Schedule & Details

submit convincing technical report to
prince-challenge@compute.dtu.dk

- 1st round: before Crypto 2014
- Final round: before FSE 2015

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

- More details, and download of challenges:
  https://www.emsec.rub.de/research/research_startseite/prince-challenge/