Rump Session 2016

Results of the Final Round of the 15.000 Euro PRINCE Cipher-Breaking Challenge

Gregor Leander; Ventzi Nikov; Christian Rechberger; Vincent Rijmen

RUB; NXP; TUG; KUL

Results of the final round of the 15.000 Euro PRINCE Cipher-Breaking Challenge

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

Input from Industry

- Need for new ciphers: PRINCE
- 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?

Prizes

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

- 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**

Timeline

Start in March 2014

Round 1 (August 2014)
Winners: Patrick Derbez, Léo Perrin, Paweł Morawiecki

Round 2 (April 2015)
Winners: Patrick Derbez,
Raluca Posteuca and Gabriel Negara.

Final Round 3 (May 2016)
Winners?

Final Results

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

- How fast can you break 4 rounds?
  - Round-1 winner: Pawel, 2^7 CP, time 2^{11}
- How fast can you break 6 rounds?
  - Round-2 winner: Raluca and Gabriel , $2^{14.6}$CP, time 2^{37}
- How fast can you break 8 rounds?
  - Round-2 winner: Patrick: 2^{16}CP, time $2^{66.4}$
- How fast can you break 10 rounds?
- How fast can you break 12 rounds?

Final Results

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

- How fast can you break 4 rounds?
  - Round-1 winner: Pawel, 2^7 CP, time 2^{11}
  - **Final-Round winner:**
    - **Integral attack Håvard Raddum and Shahram Rasoolzadeh, 2^6 texts, time: 9**
    - **Subspace trail attack by Lorenzo Grassi and Christian Rechberger: 17 texts, time: 2^{19}**
- How fast can you break 6 rounds?
  - Round-2 winner: Raluca and Gabriel , $2^{14.6}$CP, time 2^{37}
  - **Final-Round winner:**
    - **Integral attack Håvard Raddum and Shahram Rasoolzadeh, 2^{13} texts, time: $2^{24.5}$**
- How fast can you break 8 rounds?
  - Round-2 winner: Patrick: 2^{16}CP, time $2^{66.4}$
- 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?
  - Round-1 winner: Patrick: 2^5 KP, time 2^{43}
- How fast can you break 6 rounds?
  - Round-1 winner: 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?

The PRINCE Challenge

Setting 2: Given 2^{30} known plaintexts

- How fast can you break 4 rounds?
  - Round-1 winner: Patrick: 2^5 KP, time 2^{43}
- How fast can you break 6 rounds?
  - Round-1 winner: Patrick: 2^6 KP, time 2^{101}
  - **Final-Round winner:**
    - **MITM attack by Håvard Raddum and Shahram Rasoolzadeh, 2 texts, time: 2^{97}**
- How fast can you break 8 rounds?
  - **Final-Round winner:**
    - **MITM attack by Håvard Raddum and Shahram Rasoolzadeh, 2 texts, time: 2^{124}**

- How fast can you break 10 rounds?
- How fast can you break 12 rounds?

Results of final round of the 15.000 Euro PRINCE Cipher-Breaking Challenge

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