3rd Skinny Cryptanalysis Competition

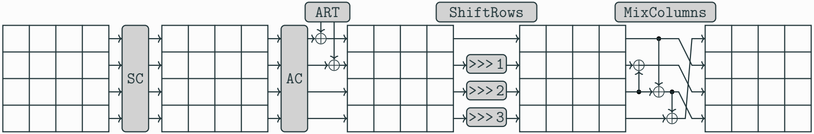
C. Beierle, J. Jean, S. Kölbl, G. Leander, A. Moradi,T. Peyrin, Y. Sasaki, P. Sasdrich and S.M. Sim

March 27th, 2019

Skinny Competition

Skinny

- Lightweight Tweakable Block Cipher
- Blocksize: 64- or 128-bit
- Tweakey: n, $2n$ or $3n$
- Received extensive cryptanalysis (20+ papers)



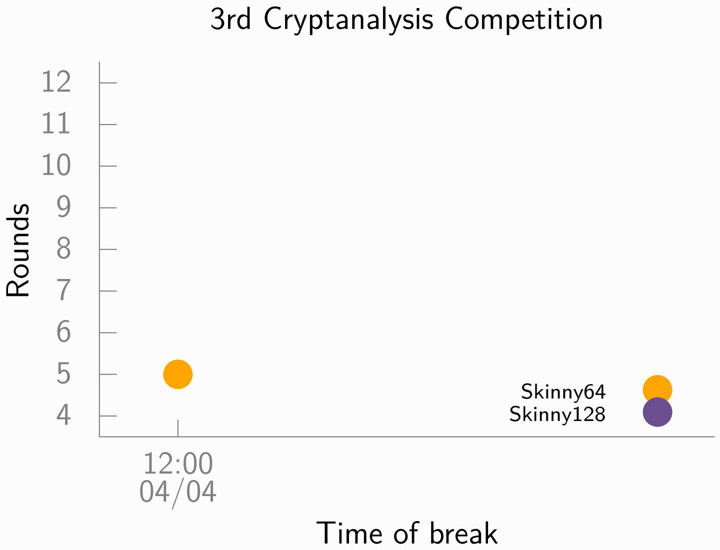
https://sites.google.com/site/skinnycipher/

Skinny Competition

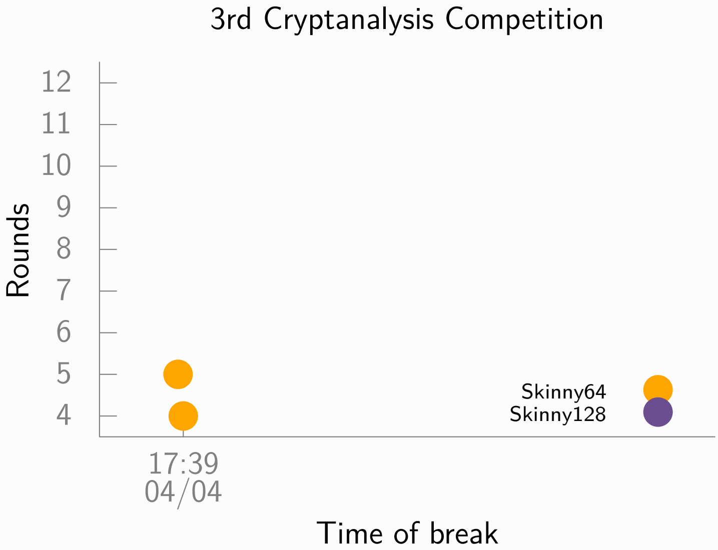
3rd Competition

- Targets: Skinny64 and Skinny128 (using 128-bit keys)
- 2^{20} plaintext/ciphertext pairs available
- Plaintexts are not random
- Goal: Recover the secret key

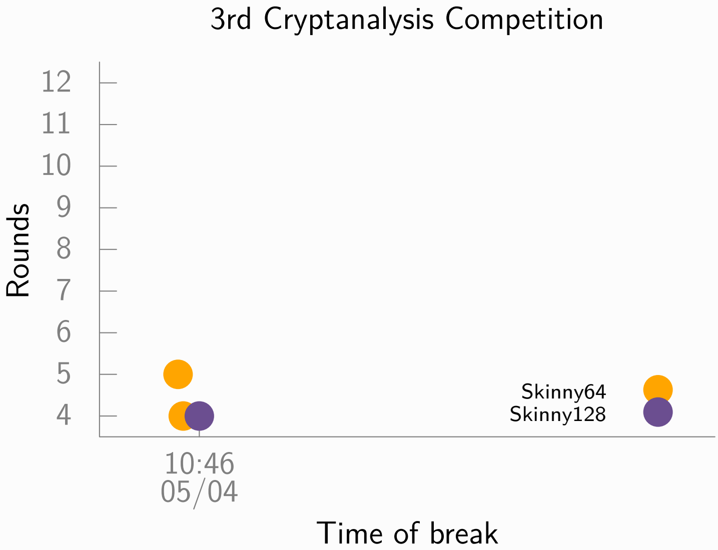
Skinny Competition



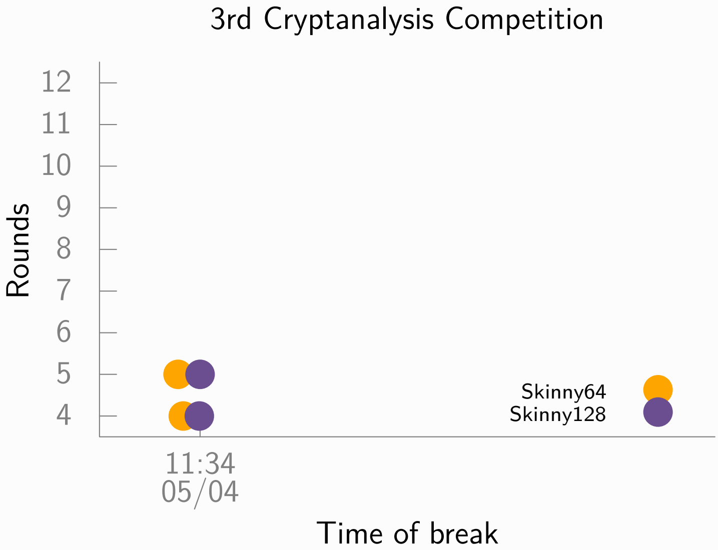
Skinny Competition



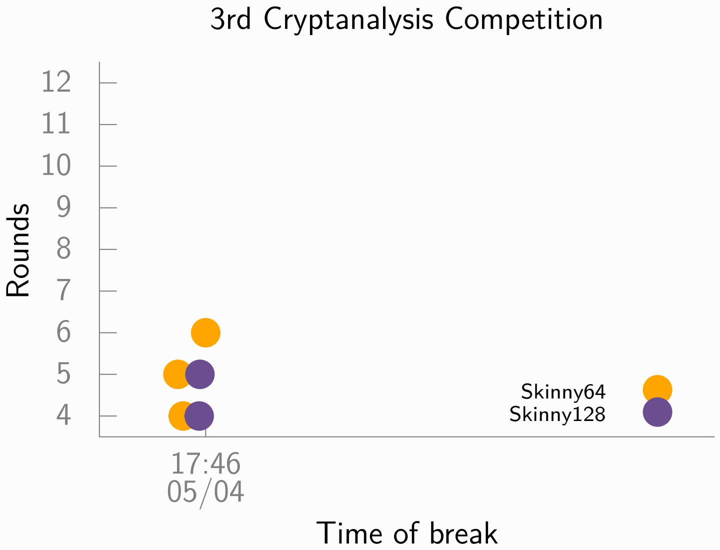
Skinny Competition



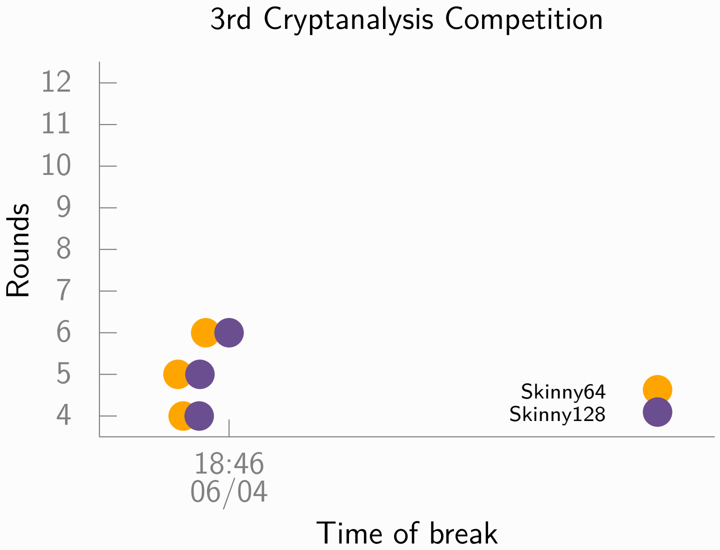
Skinny Competition



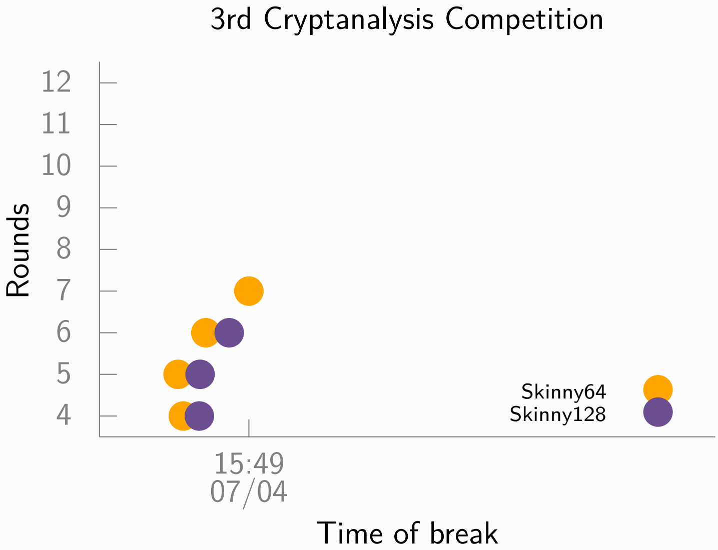
Skinny Competition



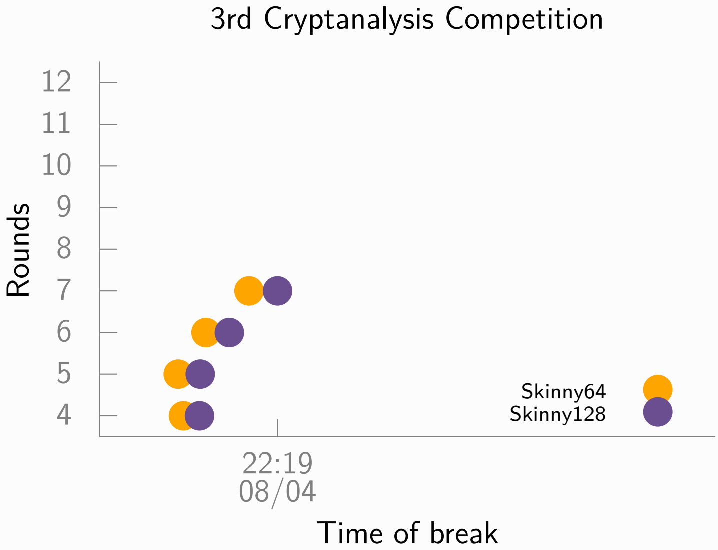
Skinny Competition



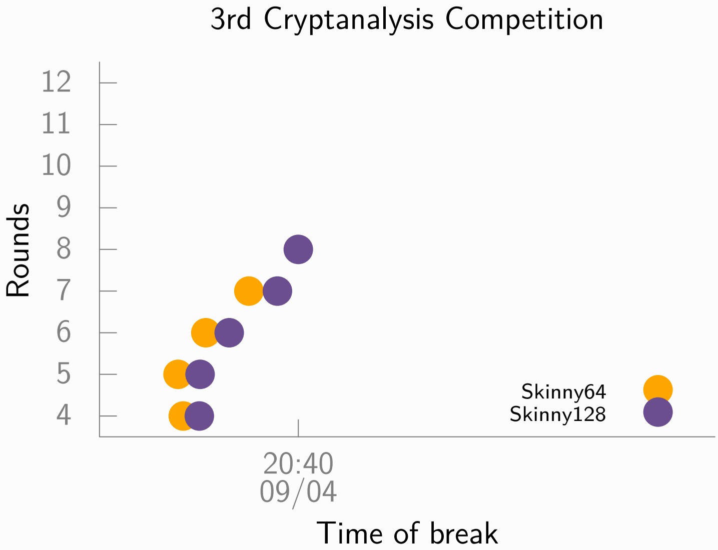
Skinny Competition



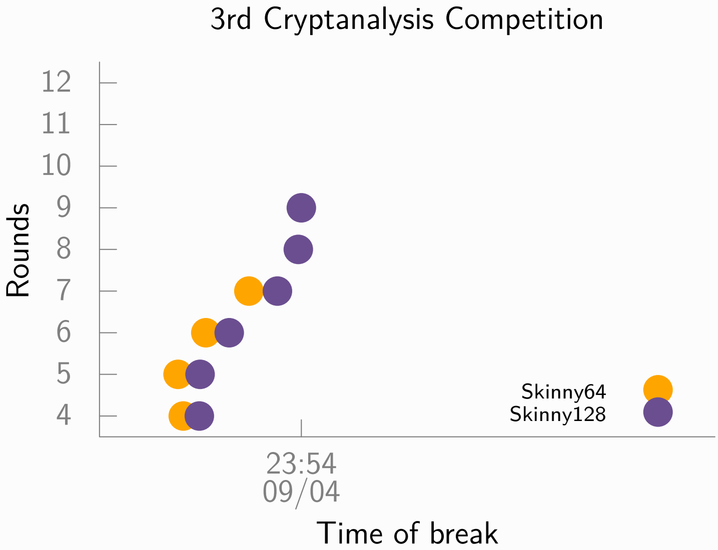
Skinny Competition



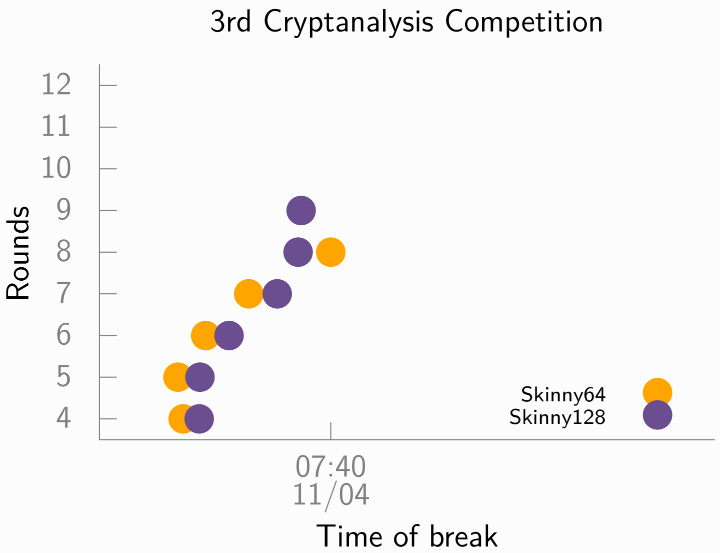
Skinny Competition



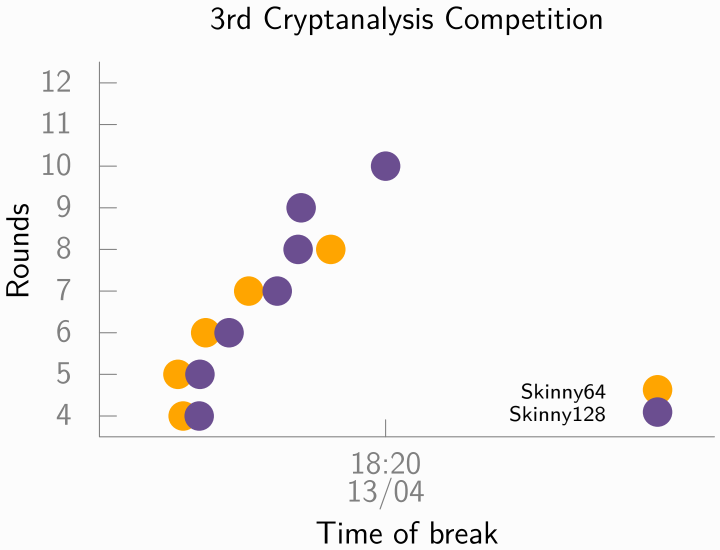
Skinny Competition



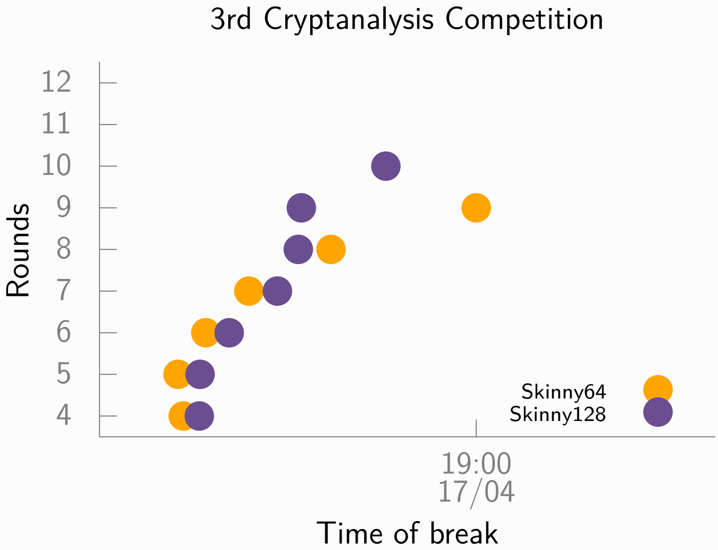
Skinny Competition



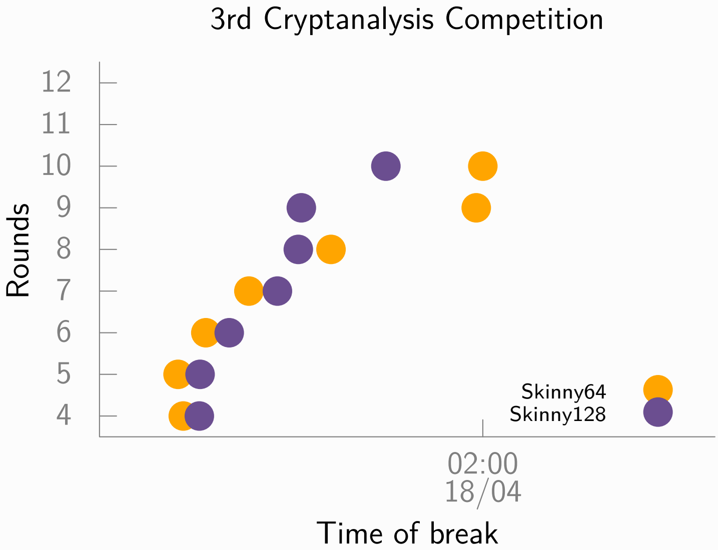
Skinny Competition



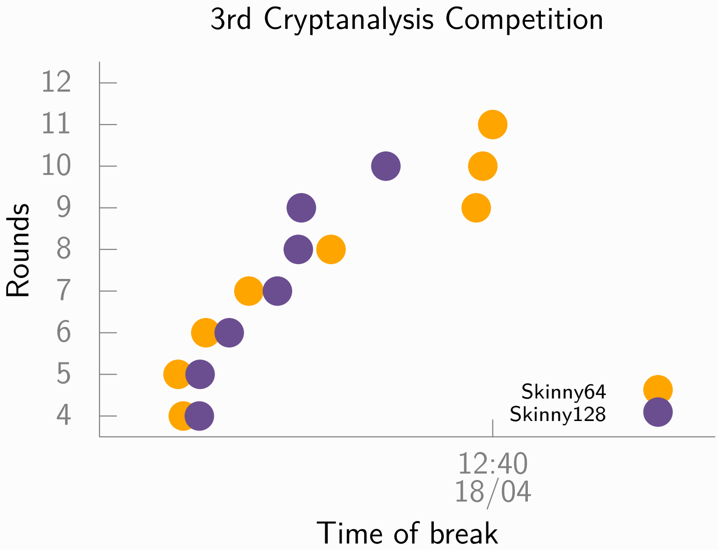
Skinny Competition



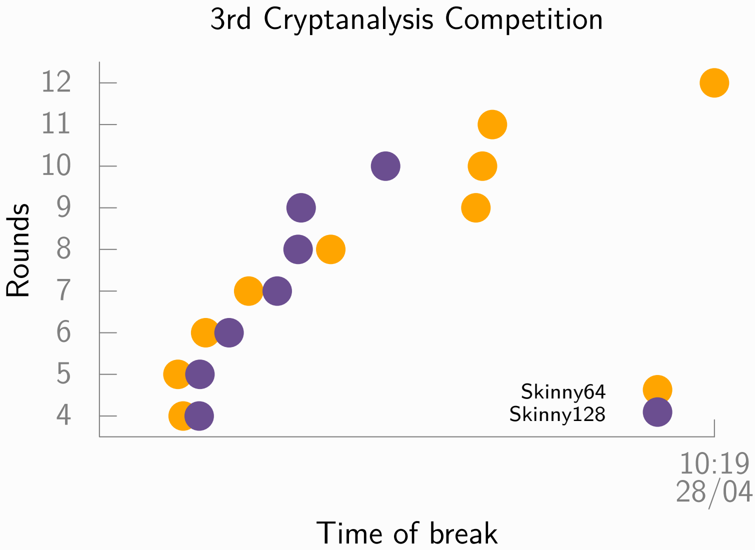
Skinny Competition



Skinny Competition



Skinny Competition



Skinny Competition

Winner Skinny 64

- Patrick Derbez and Virginie Lallemand
- 12 rounds

Skinny Competition

Winner Skinny 64

- Patrick Derbez and Virginie Lallemand
- 12 rounds

Winner Skinny 128

- Aleksei Udovenko
- 10 rounds

Skinny Competition

Most interesting cryptanalysis

- Patrick Derbez and Virginie Lallemand
- Breaking 12 rounds of Skinny64
- Truncated Differentials exploiting bias in data
- $\approx 2^{51.59}$ operations

Thank you to all the participants!

`https://sites.google.com/site/skinnycipher/`

Challenges are still available!