How to win duck-related prizes?

Saturnin$^{1,2,3}$

$^1$ Inria, France  $^2$ UCL Crypto Group, Belgium  $^3$ NCC Group, Canada
Who am I?
Saturnin: Who am I?

satyrnē
Saturnin: Who am I?

- Obviously, a lightweight duck
- A second-round NIST lightweight candidate:
  - The only candidate based on a block cipher with 256-bit blocks.
  - The only candidate claiming quantum security against superposition queries.
- You’ll hear more about me tomorrow.
What’s new?
Saturnin: What's new?

- In my update, we propose a new instance: Saturnin-QCB.
- It uses a new mode Q2-safe, efficient and parallelizable.
- We need related-key security for this: we use 16 rounds.
- The best RK attack for now: covers 10 rounds (new note in our page).
A new challenge!

https://project.inria.fr/saturnin/challenge

- Both classical and quantum (reduced-round) attacks welcome.
- Targets: Saturnin-QCB and related-key attacks on the block cipher.
- New improved results will be posted and awarded as they arrive.
- The winners will have a choice between several duck-related prizes: will be given in March 2021.
- Please contact us or visit our page for more information.
A new challenge!

Thank you!

No animals were harmed during the preparation of this presentation.