Fast Serious Encryption

Tom

Nigel

Raphael*

Orr

Dan

Foundations of Software Engineering (FSE 2007)

Recent results…

- Serious technical work
- Journal of **********
  - Name withheld by Kerckhoffs' principle
  - Trade secret following requests by No Such Agency
- Impact factor = 128 bits
- Last check: 5-year back log of submissions
  - Editors have no time to do anything else
- Serious discussions with main publishers e.g. Fall-er, CRC32 ...

Past work…

- Pseudorandom topic generator
- H numbers
- Keyboard attacks
- Rap, Blues

Work in progress…

- At Eurocrypt:
- Side-channel attacks
- Hitch-hikers' guide
- Da *** code
- Fast pencil-and-paper encryption

Open problems…

- Random papers in the standard model
- Scheming IDs based on pairings
- Collisions at family functions
- Authenticating random strings with ransom oracles

This is not a conference announcement!

- There's more to life than just crypto…
- Double submissions are **not** discouraged
- Take a break, send us an email