Non-commutative Algebra and its Applications in NIKE-Zero Knowledge Proofs

Tom Berson, Nigel Smart, Raphael C.-W. Phan,
Orr Dunkelman, Dan Page

18 August 2009

Ever Happened to You?

- Sat bored in the office?
- Had no motivation to work on your research?
- Wondered what happened to all the enthusiasm for crypto?

Ever Happened to You?

- Sat bored in the office?
- Had no motivation to work on your research?
- Wondered what happened to all the enthusiasm for crypto?

Is there a solution for researchia-dysfunction?

Hallelujah!

Journal of Craptology the Answer*

* — Please consult your physician in case you are reading other journals, or doing real research. Side effects may cause uncontrolled bursts of laughter, giggling and/or spasms. If these happen, please inform your closest colleague.

Journal of Craptology

- The journal of recreational cryptology.
- Started in 1998 (by our founding fathers, Lars, Keith, and Vincent).
- Revived in 2005 (by the current board).
- Latest volume — March 2009.

CFP

Contributions must adhere to the strict criteria:

- Craptologic research
- Funny and amusing
- Controversial
- Non-offending (unless...)

Submission Procedure

- Go to `http://www.anagram.com/~jcrap/cfp`
- Produce a paper (we accept all sorts of crap formats!)
- The use of IEEE/LNCS styles is **forbidden!**
- Pick an editor, send him an email with the paper.

Submission Procedure

- Go to `http://www.anagram.com/~jcrap/cfp`
- Produce a paper (we accept all sorts of crap formats!)
- The use of IEEE/LNCS styles is **forbidden!**
- Pick an editor, send him an email with the paper.
- Bribes are not compulsory, but are greatly appreciated and may even ensure review time of less than a year!

Decision Process

We read, we rank one out of four grades:

- Not funny
- Moderately funny
- Funny
- Hilarious

Acceptance level — funny or more.

Not Funny

- Real research
- Unethical submissions

Moderately Funny

- Using SMP in real life
- Any four letters (or more) before ZKP (e.g., CRSoL-ZKP)
- RSA with 128-bit key (or 32-bit entropy)
- Using single DES for encryption

Funny

- Trusting the government in privacy issues
- Digital Millennium Copyright Act (DMCA)
- WEP for protecting wireless communications
- Using random oracles in hashing

Hilarious

- Trusting the government
- NAC based on MAC address
- Airport security
- Claiming your driving ticket is faulty because the speed camera uses MD5

Summary

- Craptographers of the world — Unite!
- Short backlog and no page limit!
- Past issues, more information, and lot's of crap(tology):

http://www.anagram.com/~jcrap