Universal Compostible Secure Broadcast based on Commutative Random Algebraic Partitions

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

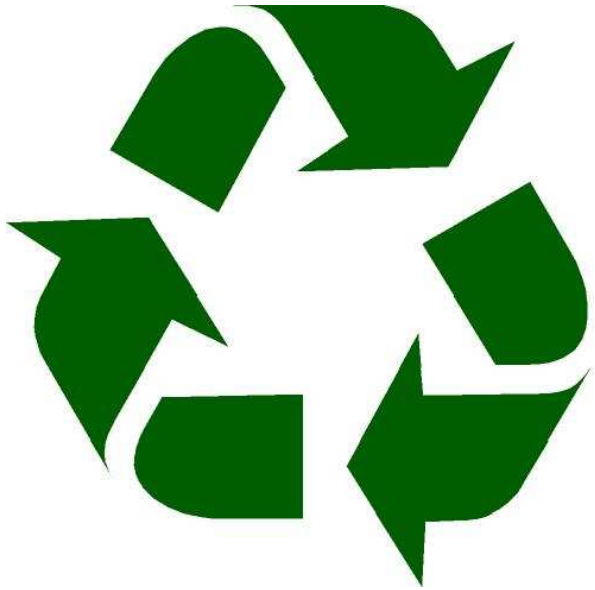
17 August 2010

Universal Composability

- Started by the seminal work of Canetti on running several MPC instances in parallel.
- Followed by many who helped to prove what you can do and cannot do in such settings.

Universal Composability

- Started by the seminal work of Canetti on running several MPC instances in parallel.
- Followed by many who helped to prove what you can do and cannot do in such settings.
- Allows recycling the same secret information in many parallel executions of the same protocol.



Universal Compostability for Secure Broadcast (UCSB)

- Combining composability with leakage — Compostability!

Universal Compostability for Secure Broadcast (UCSB)

- Combining composability with leakage — Compostability!

Commutative Random Algebraic Partitions (CRAP)

- 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 — February 2010.

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 — February 2010.

Call For Paper

Contributions must adhere to the strict criteria:

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

Why Bother?

Make an Impact!

Why Bother?

Make an Impact!

Why Bother? (cont.)

Since last CRYPTO, JoC papers were cited in various venues:

- "Comment — Practical Data Protection" by Das [D08] (citing Rawat and Saxena, "Practical Data Protection" Vol. 5).

Manik Lal Das
Comment — Practical Data Protection.
Arxiv preprint arXiv:0804.4628 —
http://arxiv.org/pdf/0804.4628

Why Bother? (cont.)

Since last CRYPTO, JoC papers were cited in various venues:

- "Weak Pseudorandom Functions in Minicrypt" by Pietrzak and Sjödin [PS10] (citing Dent, "Cryptography in a hitchhikers universe" Vol. 4).

Krzysztof Pietrzak and Johan Sjödin
Weak Pseudorandom Functions in Minicrypt.
Automata, Languages and Programming, 2010 (ICALP 2010).

Why Bother? (cont.)

Since last CRYPTO, JoC papers were cited in various venues:

- "New software speed records for cryptographic pairings" by Naehrig, Niederhagen, and Schwabe [NNS10], (citing Barreto , "A survey on craptological pairing algorithms" Vol. 7).

Michael Naehrig, Ruben Niederhagen, and Peter Schwabe
New software speed records for cryptographic pairings.
LatinCrypt 2010.

Why Bother? (cont.)

While working on the slides, I've found out that

Why Bother? (cont.)

While working on the slides, I've found out that this is not a new phenomena!

- "An algebraic framework for cipher embeddings" by Cid, Murphy, and Robshaw [CMR05] cited Knudsen's "New Directions in Cryptography (Volume II)" of volume 1 of the journal.
- Back in 2005!

Carlos Cid, Sean Murphy, and Matt J.B. Robshaw
An Algebraic Framework for Cipher Embeddings.
Cryptography and Coding, 10th IMA International Conference, 2005.

Why Bother? (cont.)

- **Open Access Journal** (unlike some competitors).

Why Bother? (cont.)

- **Open Access Journal** (unlike some competitors).
- Impact Factor (2009):

Why Bother? (cont.)

- **Open Access Journal** (unlike some competitors).
- Impact Factor (2009): **0**

Why Bother? (cont.)

- **Open Access Journal** (unlike some competitors).
- Impact Factor (2009): **0** (unlike some competitors).

Why Bother? (cont.)

- **Open Access Journal** (unlike some competitors).
- Impact Factor (2009): **0** (unlike some competitors).
- Invited papers and presentations.

New Directions in Craptology

- Design a key exchange protocol secure against the man in the middle, but insecure against the woman in the middle.

New Directions in Craptology

- Design a key exchange protocol secure against the man in the middle, but insecure against the woman in the middle.
- Define Zero Knowledge Protocols for Omniscient entities (or how Zeus can prove to Buddha that he knows the solution to his Sudoku).

New Directions in Craptology

- Design a key exchange protocol secure against the man in the middle, but insecure against the woman in the middle.
- Define Zero Knowledge Protocols for Omniscient entities (or how Zeus can prove to Buddha that he knows the solution to his Sudoku).
- How to teach your kids to flip coins for cryptography without having them addicted to online gambling.

New Directions in Craptology

- Design a key exchange protocol secure against the man in the middle, but insecure against the woman in the middle.
- Define Zero Knowledge Protocols for Omniscient entities (or how Zeus can prove to Buddha that he knows the solution to his Sudoku).
- How to teach your kids to flip coins for cryptography without having them addicted to online gambling.
- ...

Summary

Enjoy the short backlog and lack of page limit!

Past issues, more information, and lot's of crap(tology):

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