FSE 2010
Rump Session

Agenda - Announcements

- 16:03-16:10 Bart Preneel — The International Association for Cryptologic Research
- 16:10-16:12 Shoichi Hirose — CFP of IWSEC 2010
- 16:12-16:13 Shoichi Hirose — CFP of Pairings 2010
- 16:13-16:15 Riaal Domingues — Africacrypt 2010

Agenda – New Results

- 16:15-16:21 Bonwook Koo — Related-Key Boomerang Attack on Block Cipher SQUARE
- 16:21-16:26 Thomas Peyrin — Improved Cryptanalysis of ECHO and Grøstl
- 16:26-16:32 Gaëtan Leurent — Pseudo-preimage attack against SHAvite-3 compression function
- 16:32-16:34 Bo-Yin Yang — Solving Multivariate Polynomial Systems
- 16:34-16:41 Ming-Shing Chen — What price a provably secure stream cipher?
- 16:41-16:47 Orr Dunkelman — Low Data Complexity Attacks on AES

Housekeeping Announcements

- We have a limited time
- On the talk before yours, there is going to be a reminder for you to prepare yourself
- When you have 60 seconds left, I will raise a sign in your direction
- When you have 30 seconds left, I will raise a sign in your direction

Housekeeping Announcements

- When you reach the allocated time, I will raise a sign in the direction of the audience
- Which will then start rumbling...

Practice

בבקשה, השמיעו רעש ברמה נמוכה (אמרו "רמבל" אם אין לכם משהו אחר להגיד)

Please rumble (say rumble, if you do not know what to "rumble" about)

Faites du bruit, s'il vous plaît (dites "rumble", si vous ne savez pas quoi dire)

Housekeeping Announcements

- When you are way over time (more than 15 seconds), I will change the sign for the audience
- Who will start clapping...

Practice part II

בבקשה, מחאו כפיים

Please clap your hands

Applaudissez, s'il vous plaît

Final Comments

- We would like to put the rump session presentations online
- You will be contacted to give your permission to have the slides and the video online

Let the Rump Session Begin!