Do you care about

Fast Software Encryption
(and Decryption)?

Rumpsession FSE 2007
SPEED – Software Performance Enhancement for Encryption and Decryption
June 11. & 12. 2007
Amsterdam
An ECRYPT/VAMPIRE workshop on software speeds for symmetric key cryptography and public key cryptography

http://www.hyperelliptic.org/SPEED

Rumpsession FSE 2007
Topics

• software implementation of public key systems
• software implementation of hash functions and symmetric key systems
• algorithmic speed-ups of symmetric and public key systems
• CPU specific speed-ups
• benchmarking of symmetric and public key systems
• security/comparison of BATs submitted to eBATS
• compilers to automate producing efficient code and executables
• compilers to introduce cryptographic security into code
• cryptographic software engineering tools
Deadlines

- April 06, 2007: Submission (5-20 pages)
- May 11, 2007: Notification
- May 25, 2007: Revised versions due
- June 11-12, 2007: SPEED workshop

http://www.hyperelliptic.org/SPEED