Cryptanalysis of Reduced-Round MARS

John Kelsey and Bruce Schneier
Counterpane Internet Securirty
{kelsey,schneier}@counterpane.com

Overview of Talk

- Introduction and Context of Research
- Reduced-Round MARS Variants
- Notation and Terminology
- Cryptanalysis of MARS 8-5-8
- Cryptanalysis of MARS 3-6-3
- Summary and Conclusions