The ARX Challenge

Ralf-Philipp Weinmann

University of Luxembourg

Workshop on Fast Software Encryption 2009
Leuven, 2009-02-24

The Problem

- k-bit words (usually $k \in \{32, 64\}$)
- AXR: addition (mod 2^k), bitwise word rotations, XORs
- equation system composed of above operations
- solvable ?
- number of solutions ?
- detemine solutions
- problem is under-researched

uni.lu UNIVERSITÉ DU LUXEMBOURG

The Challenge

- Equation systems for reduced round versions of primitives
- Interested in practical attacks using equation systems
- Any tool may be used, to claim prize, authors must however submit (Linux or Win32 binary, x86 or AMD64) performing attack for verification

Selected Candidates

Reduced round versions of

- TEA
- SALSA20
- SKEIN
- SHA-256 (not ARX, can derive ARX equations however)

Duration & Prizes

- Challenge will start on 2009-03-09
- It will run until FSE 2010
- Prizes are not fixed yet, but we'll be offering bottles of *Vin de Glace* (Luxembourgish ice wine)

Where?

http://arxchallenge.org

http://cryptolux.uni.lu/ARX_Challenge

UNIVERSITÉ DU LUXEMBOURG