GOSTbusting Reloaded

Florian Mendel, Norbert Pramstaller, Christian Rechberger,
Marcin Kontak, and Janusz Szmidt

Institute for Applied Information Processing and Communications (IAIK) - Krypto Group

Faculty of Computer Science
Graz University of Technology

Motivation

- Russian Digital Signature Algorithm
  (GOST-R-34.10-94 and GOST R 34.10-2001)
- Proposed at the same time as SHA-1, but larger output size (256 instead of 160 bits)
- Based on conservative block cipher
  (32 round Feistel network)

First Collision Search Attack:

2^{105} instead of 2^{128}

Attacks on GOST

First Collision Search Attack:

2^{105} instead of 2^{128}

New Preimage and Second Preimage Attack:

2^{192} instead of 2^{256}

Attacks on GOST

First Collision Search Attack:

2^{105} instead of 2^{128}

New Preimage and Second Preimage Attack:

2^{192} instead of 2^{256}

New Insight:

exploit „**Doppelgänger“ property** of the block cipher

GOSTbusting Reloaded

Gostbuster Florian Mendel, Gostbuster Norbert Pramstaller, Gostbuster Christian Rechberger, Gostbuster Marcin Kontak, and Gostbuster Janusz Szmidt

Institute for Applied Information Processing and Communications (IAIK) - Krypto Group

Faculty of Computer Science
Graz University of Technology