# Cube Testers and Key-Recovery Attacks on Reduced-Round MD6 and Trivium

Jean-Philippe Aumasson, Itai Dinur, Willi Meier, Adi Shamir

n|w University of Applied Sciences Northwestern Switzerland
School of Engineering

מכון ויצמן למדע
WEIZMANN INSTITUTE OF SCIENCE

# Cube attacks

# Timeline

**Aug 08**: Shamir presents cube attacks at CRYPTO

**Sep 08**: Dinur/Shamir paper on ePrint,
attack on 771-round Trivium

**Oct 08**: cube attacks reported on 14-round MD6

**Oct 08**: cube testers reported on 18-round MD6

**Dec 08**: Dinur/Shamir paper accepted to EUROCRYPT

**Jan 09**: cube testers reported on Shabal

# Cube attacks in a nutshell

Can attack any primitive with **secret and public variables**

- keyed hash functions
- stream ciphers
- block ciphers
- MACs

Target algorithms with **low-degree** components

- stream ciphers based on low-degree NFSR
- hash functions with only XORs and a few ANDs

# Cube attacks in a nutshell

Requirements of the attacker:

- only **black-box access** to the function
- negligible memory

Cube attacks work in 2 phases

- **precomputation**: chosen keys and chosen IVs
- **online**: fixed unknown key and chosen IVs

# Key observation 1

Any function

$$f : \{0,1\}^m \mapsto \{0,1\}^n$$

admits an **algebraic normal form** (ANF)

Example: $f : \{0,1\}^{10} \mapsto \{0,1\}^4$

$$\begin{aligned}
f_1(x) &= x_1x_2 + x_2x_8x_9 + x_3x_4x_5x_6x_7 \\
f_2(x) &= x_2x_4 + x_6x_8x_9 + x_5x_6x_7x_8x_9x_{10} \\
f_3(x) &= 1 \\
f_4(x) &= 1 + x_1 + x_3 + x_5
\end{aligned}$$

# Key observation 2

**Computation of the largest monomial's coefficient**

$$\begin{aligned} f(x_1, x_2, x_3, x_4) &= x_1 + x_3 + x_1x_2x_3 + x_1x_2x_4 \\ &= x_1 + x_3 + x_1x_2x_3 + x_1x_2x_4 + 0 \times x_1x_2x_3x_4 \end{aligned}$$

Sum over all values of $(x_1, x_2, x_3, x_4)$:

$$f(0,0,0,0) + f(0,0,0,1) + f(0,0,1,0) + \cdots + f(1,1,1,1) = 0$$

# Key observation 3

**Evaluation of factor polynomials**

$$\begin{aligned} f(x_1, x_2, x_3, x_4) &= x_1 + x_3 + x_1 x_2 x_3 + x_1 x_2 x_4 \\ &= x_1 + x_3 + x_1 x_2 (x_3 + x_4) \end{aligned}$$

Fix $x_3$ and $x_4$, sum over all values of $(x_1, x_2)$:

$$\begin{aligned} \sum_{(x_1, x_2) \in \{0,1\}^2} f(x_1, x_2, x_3, x_4) &= 4 \times x_1 + 4 \times x_3 + 1 \times (x_3 + x_4) \\ &= x_3 + x_4 \end{aligned}$$

# Key observation 3

**Evaluation of factor polynomials**

$$f(x_1, x_2, x_3, x_4) = \cdots + x_1 x_2 (x_3 + x_4)$$

Fix $x_3$ and $x_4$, sum over all values of $(x_1, x_2)$:

$$\sum_{(x_1, x_2) \in \{0,1\}^2} f(x_1, x_2, x_3, x_4) = x_3 + x_4$$

# Terminology

$$f(x_1, x_2, x_3, x_4) = x_1 + x_3 + x_1 x_2 (x_3 + x_4)$$

$(x_3 + x_4)$ is called the **superpoly** of the **cube** $x_1 x_2$

# Evaluation of a superpoly

$x_3$ and $x_4$ fixed and unknown

$f(\cdot, \cdot, x_3, x_4)$ queried as a **black box**

**ANF unknown**, except: $x_1 x_2$'s superpoly is $(x_3 + x_4)$

$$f(x_1, x_2, x_3, x_4) = \cdots + x_1 x_2 (x_3 + x_4) + \cdots$$

Query $f$ to evaluate the superpoly:

$$\sum_{(x_1, x_2) \in \{0,1\}^2} f(x_1, x_2, x_3, x_4) = x_3 + x_4$$

# Key-recovery attack

On a stream cipher with key $k$ and IV $v$

$$f : (k, v) \mapsto \text{first keystream bit}$$

**Offline**: find cubes with linear superpolys

$$\begin{aligned}
f(k, v) &= \cdots + v_1 v_3 v_5 v_7 (k_2 + k_3 + k_5) + \cdots \\
f(k, v) &= \cdots + v_1 v_2 v_6 v_8 v_{12} (k_1 + k_2) + \cdots \\
\cdots &= \cdots \\
f(k, v) &= \cdots + v_3 v_4 v_5 v_6 (k_3 + k_4 + k_5) + \cdots
\end{aligned}$$

(reconstruct the superpolys with linearity tests)

**Online**: evaluate the superpolys, solve the system

# Cube testers

# Cube testers in a nutshell

Like cube attacks:

- need only black-box access
- target primitives with secret and public variables and
- built on low-degree components

Unlike cube attacks:

- give **distinguishers** rather than key-recovery
- don't require low-degree functions
- need **no precomputation**

# Basic idea

Detect structure (nonrandomness) in the superpoly,

using **algebraic property testers**

A tester for property $\mathcal{P}$ on the function $f$:

- makes (adaptive) queries to $f$
- accepts when $f$ satisfies $\mathcal{P}$
- rejects with bounded probability otherwise

# Examples of efficiently testable properties

- balance
- linearity
- low-degree
- constantness
- presence of linear variables
- presence of neutral variables

General characterization by Kaufman/Sudan, *STOC' 08*

# Superpolys attackable by testing...

... **low-degree** (6)

$$\cdots + x_1 x_2 x_3 (x_2 x_3 + x_4 x_{21} + x_6 x_9 x_{20} x_{30} x_{40} x_{50}) + \cdots$$

... **neutral variables** ($x_6$)

$$\cdots + x_1 x_2 x_3 x_4 x_5 \cdot g(x_7, x_8, \ldots, x_{80}) + \cdots$$

... **linear variables** ($x_6$)

$$\cdots + x_1 x_2 x_3 x_4 x_5 \cdot (x_6 + g(x_7, x_8, \ldots, x_{80})) + \cdots$$

# Results

# MD6

Presented by Rivest at CRYPTO 2008

Submitted to the SHA-3 competition

- quadtree structure
- construction RO-indifferentiable
- low-degree compression function
- at least **80 rounds**
- best attack by the designers: 12 rounds

# MD6's compression function

$$\{0,1\}^{64\times 89} \mapsto \{0,1\}^{64\times 16}$$

Input: 64-bit words $A_0.A_1,\ldots,A_{88}$

Compute the $A_i$'s with the recursion

$$x \leftarrow S_i \oplus A_{i-17} \oplus A_{i-89} \oplus (A_{i-18} \wedge A_{i-21}) \oplus (A_{i-31} \wedge A_{i-67})$$
$$x \leftarrow x \oplus (x \gg r_i)$$
$$A_i \leftarrow x \oplus (x \ll \ell_i)$$

- round-dependent constant $S_i$
- quadratic step, at least 1280 steps

# Results on MD6

Cube attack (key recovery)

- on the **14-round** compression function
- recover any 128-bit key
- in time $\approx 2^{22}$

Cube testers (testing balance)

- detect nonrandomness on **18 rounds**
- detect nonrandomness on **66 rounds** when $S_i = 0$
- in time $\approx 2^{17}$, $2^{24}$, resp.

# Trivium

Stream cipher by De Cannière and Preneel, 2005

eSTREAM HW portfolio

- 80-bit key and IV
- 3 quadratic NFSRs
- 1152 initialization rounds
- best attack on 771 rounds (cube attack)

# Cube testers on Trivium

Test the presence of **neutral variables**

Distinguishers (only choose IVs)

- $2^{24}$: 772 rounds
- $2^{30}$: 790 rounds

Nonrandomness (assumes some control of the key)

- $2^{24}$: 842 rounds
- $2^{27}$: 885 rounds

Full version: 1152 rounds

# Conclusions

# Cube testers

+

- more general than classical cube attacks
- no precomputation
- "polymorphic"

–

- only gives distinguishers
- only finds feasible attacks
- relevant for a minority of functions (like cube attacks)

# Open issues

How to predict the existence of unexpected properties?

How to find the best cubes?

Attack on (reduced versions of) other algorithms:

Grain, ESSENCE, Keccak, Luffa, Shabal,…

# Cube Testers and Key-Recovery Attacks on Reduced-Round MD6 and Trivium

Jean-Philippe Aumasson, Itai Dinur, Willi Meier, Adi Shamir

n|w University of Applied Sciences Northwestern Switzerland
School of Engineering

מכון ויצמן למדע
WEIZMANN INSTITUTE OF SCIENCE