Curve25519 Cryptanalysis

J. Scheerder*
jeroenscheerder@on2it.eu

November 7, 2008

1 Introduction

In the recent past fundamental design flaws in the DNS protocol have been exposed. DNSCurve[1] is a proposal to improve upon the current situation.

Essential to DNSCurve is Curve25519, which is claimed to be a high-speed, high-security elliptic-curve-Diffie-Hellman function[2].

Now consider the following definition of the so-called *safety factor*:

> Let n be the number of rounds of the full cipher, and b be the largest number of rounds that has been broken. The safety factor σ is defined as $\sigma := n/b$.[3]

2 Goal

Analyze the Curve25519 algorithm to assess its security claims. Describe the best attacks against it, as currently known, and determine its safety factor.

3 Task

Perform a crypto-analysis of the Curve25519 design and implementation. Formulate and implement attack strategies and specific attacks.

*ON2IT b.v., Waardenburg, The Netherlands.

[1] See http://dnscurve.org/.

[2] "Curve25519: new Diffie-Hellman speed records", Daniel J. Bernstein, 2006 – http://cr.yp.to/ecdh/curve25519-20060209.pdf.

[3] Taken from "The Twofish Team's Final Comments on AES Selection", Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson, Tadayoshi Kohno, and Mike Stay, 2000.