# Cryptology ePrint Archive: Report 2011/558

**Improved Attacks on Full GOST**

*Itai Dinur and Orr Dunkelman and Adi Shamir*

**Abstract:** GOST is a well known block cipher which was developed in the Soviet Union during the 1970's as an alternative to the US-developed DES. In spite of considerable cryptanalytic effort, until very recently there were no published single key attacks against its full 32-round version which were faster than the $2^{256}$ time complexity of exhaustive search. In February 2011, Isobe used in a novel way the previously discovered reflection property in order to develop the first such attack, which requires $2^{32}$ data, $2^{64}$ memory and $2^{224}$ time. Shortly afterwards, Courtois and Misztal used a different technique to attack the full GOST using $2^{64}$ data, $2^{64}$ memory and $2^{226}$ time. In this paper we introduce a new fixed point property and a better way to attack 8-round GOST in order to find improved attacks on full GOST: Given $2^{32}$ data we can reduce the memory complexity from an impractical $2^{64}$ to a practical $2^{36}$ without changing the $2^{224}$ time complexity, and given $2^{64}$ data we can simultaneously reduce the time complexity to $2^{192}$ and the memory complexity to $2^{36}$.

**Category / Keywords:** secret-key cryptography / Block cipher, cryptanalysis, GOST, reflection property, fixed point property, 2D meet in the middle attack

**Date:** received 11 Oct 2011

**Contact author:** itaid at weizmann ac il