

Gröbner Bases + Slow Iterative Approach to the Level of a Random Boolean Function = Weaknesses in Cryptographic Hash Function ?!



Danilo Gligoroski¹, Smile Markovski² and Svein J. Knapskog¹

[1] Centre for Quantifiable Quality of Service in Communication Systems, Norwegian University of Science and Technology, NORWAY

E-mail: danilog@q2s.ntnu.no, Svein.J.Knapskog@q2s.ntnu.no

[2] Institute of Informatics, Faculty of Natural Sciences and Mathematics, Ss Cyril and Methodius University, MACEDONIA

E-mail: smile@ii.edu.mk

Normalized Average Number of Terms (NANT)

Let $F : \{0,1\}^n \rightarrow \{0,1\}^r$ be a vector valued Boolean function. The Normalized Average Number of Terms (NANT) in its Algebraic Normal Form is denoted by \overline{L}_F and is defined as:

$$\overline{L}_F = \overline{L}_F(r, k) = \frac{1}{r} \frac{1}{2^{k-1}} \lim_{S \rightarrow \infty} \frac{1}{S} \sum_{j=1}^S L_{F_{\sigma_j}}$$

Properties of NANT: 1. NANT is a measure of the algebraic complexity of a Boolean function, i.e. how much it differs from a random Boolean function.

2. $0 \leq \overline{L}_F \leq 2$, 3. $EX(\overline{L}_F) = 1$.

Hypothesis: Let $C : \{0,1\}^n \rightarrow \{0,1\}^r$

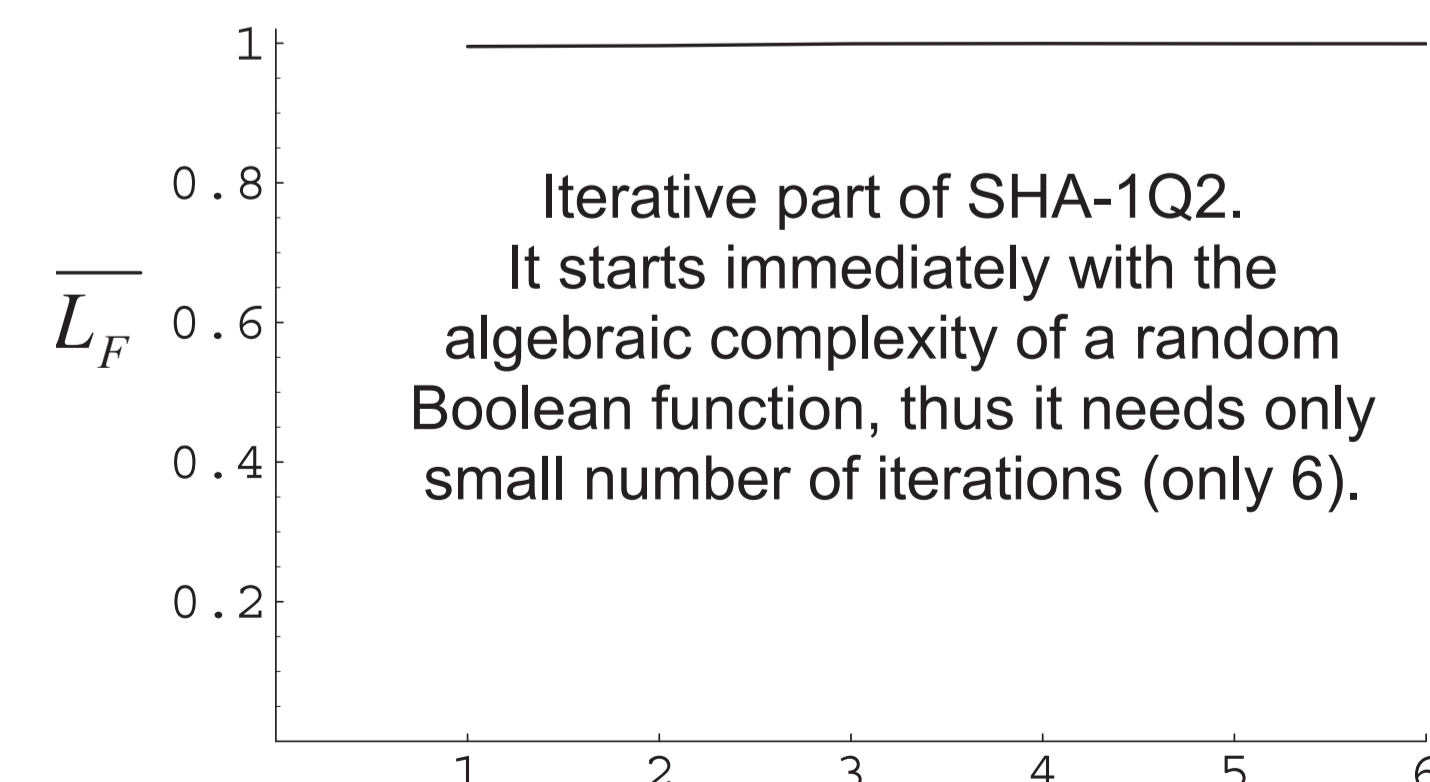
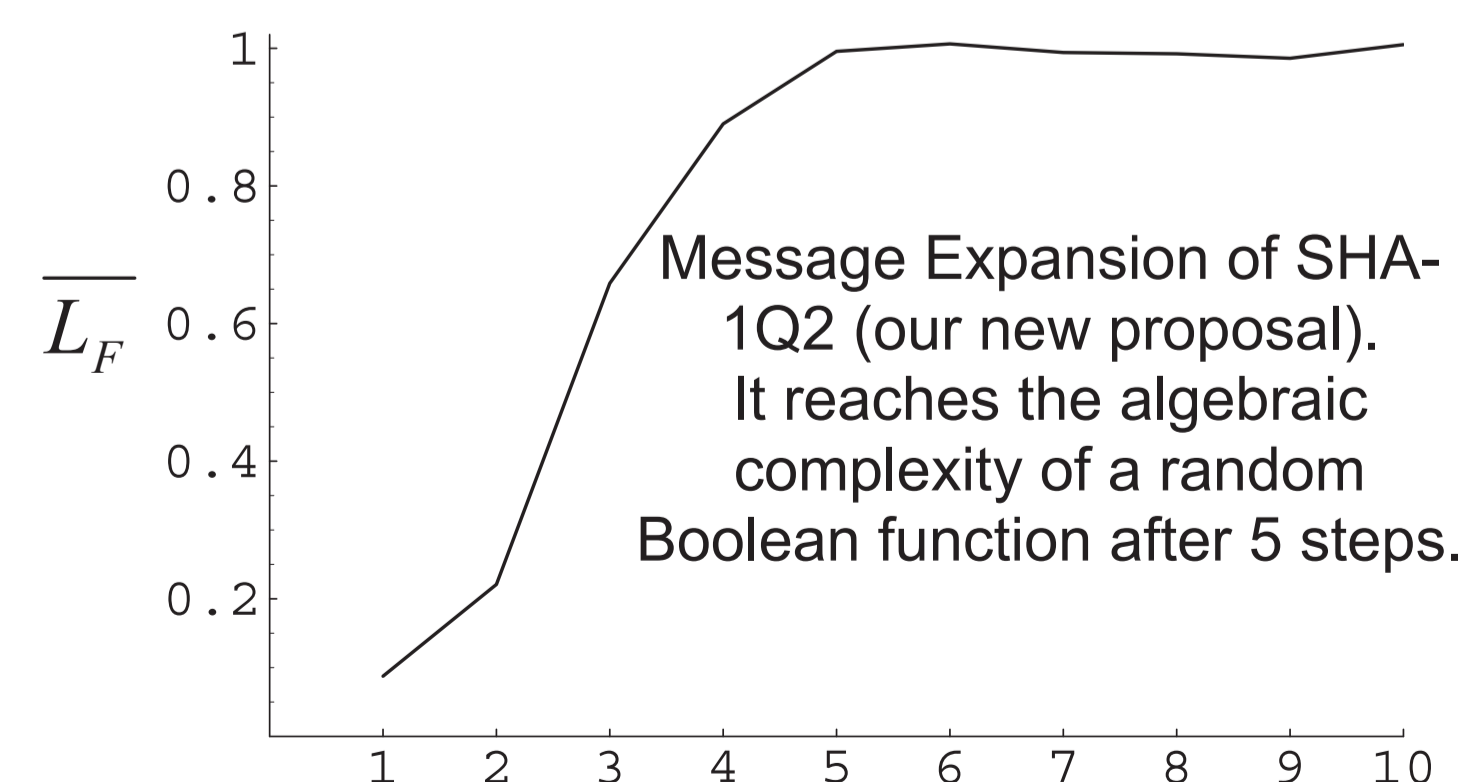
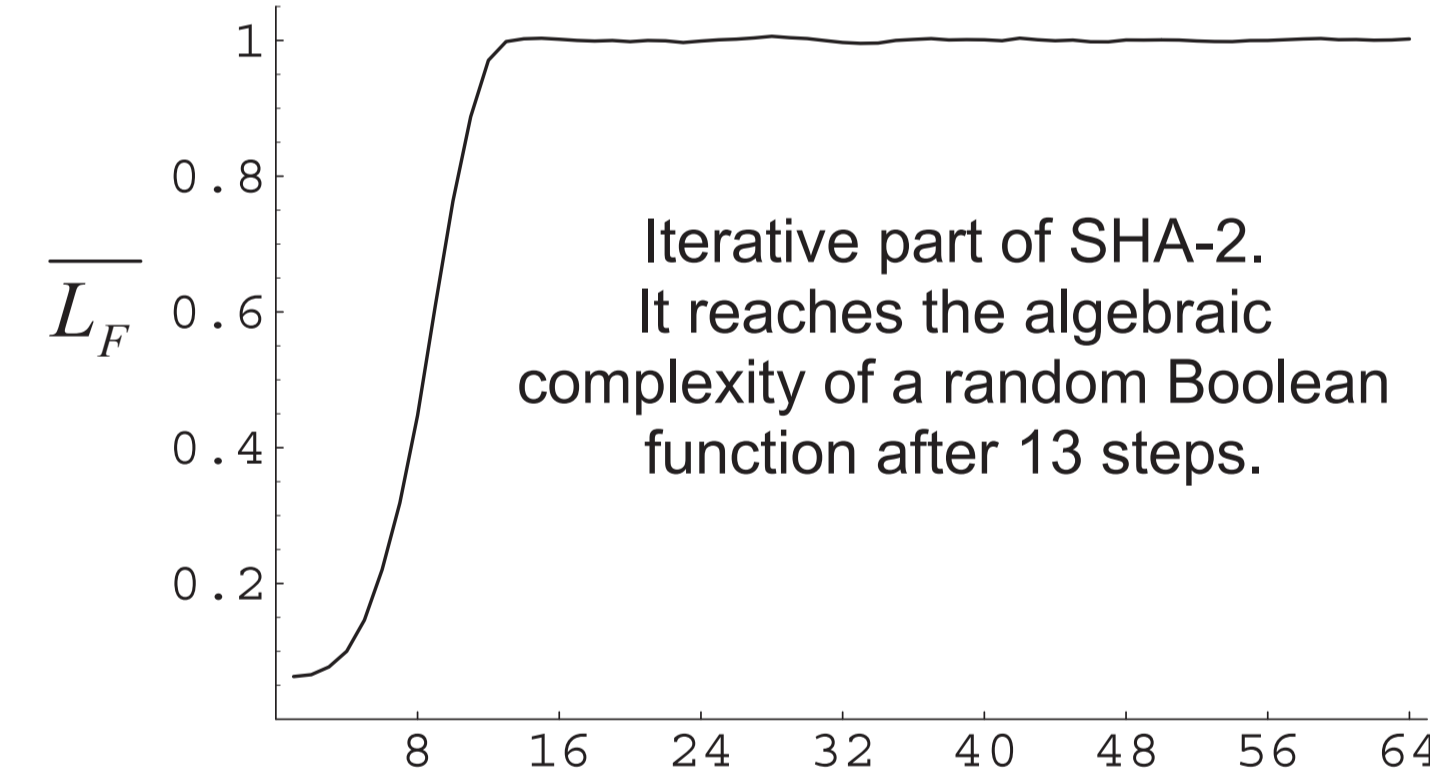
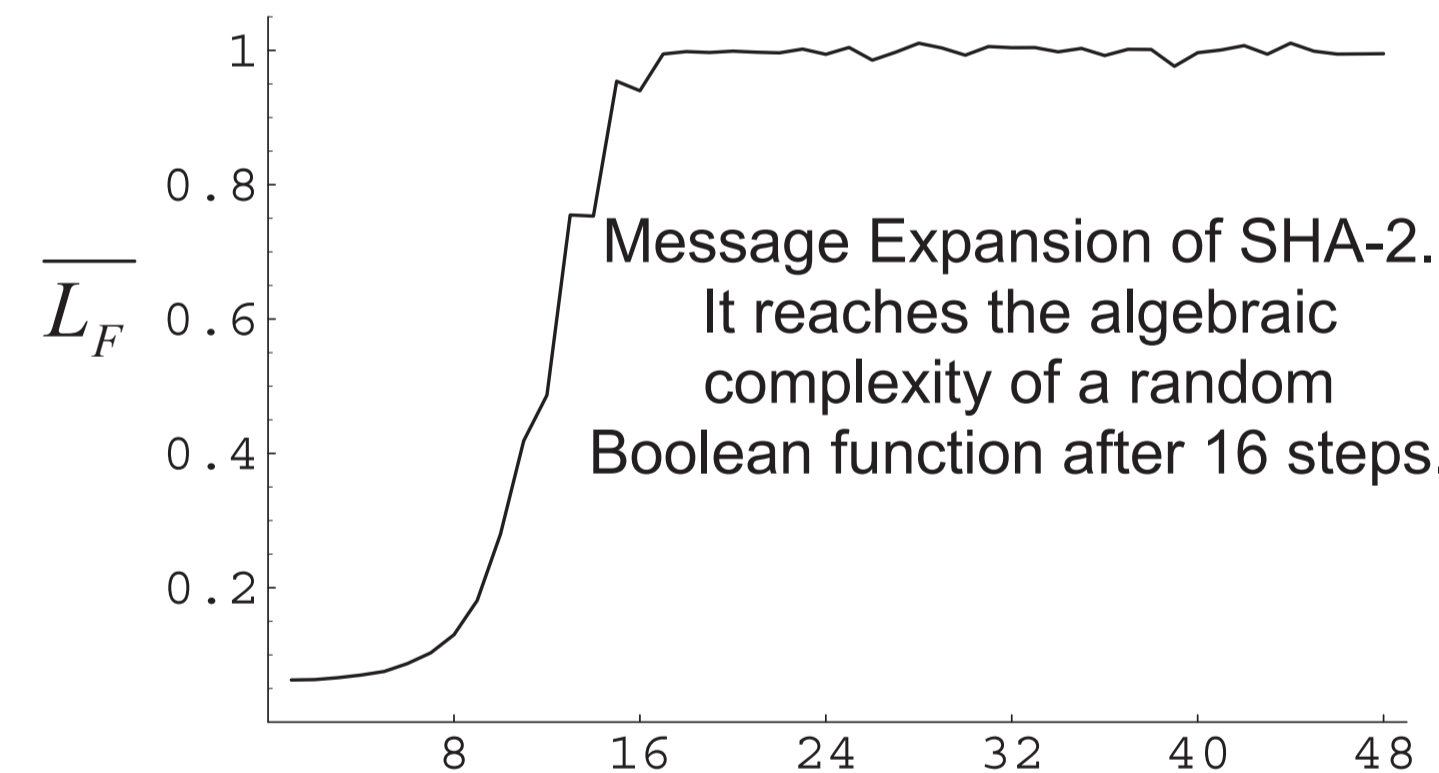
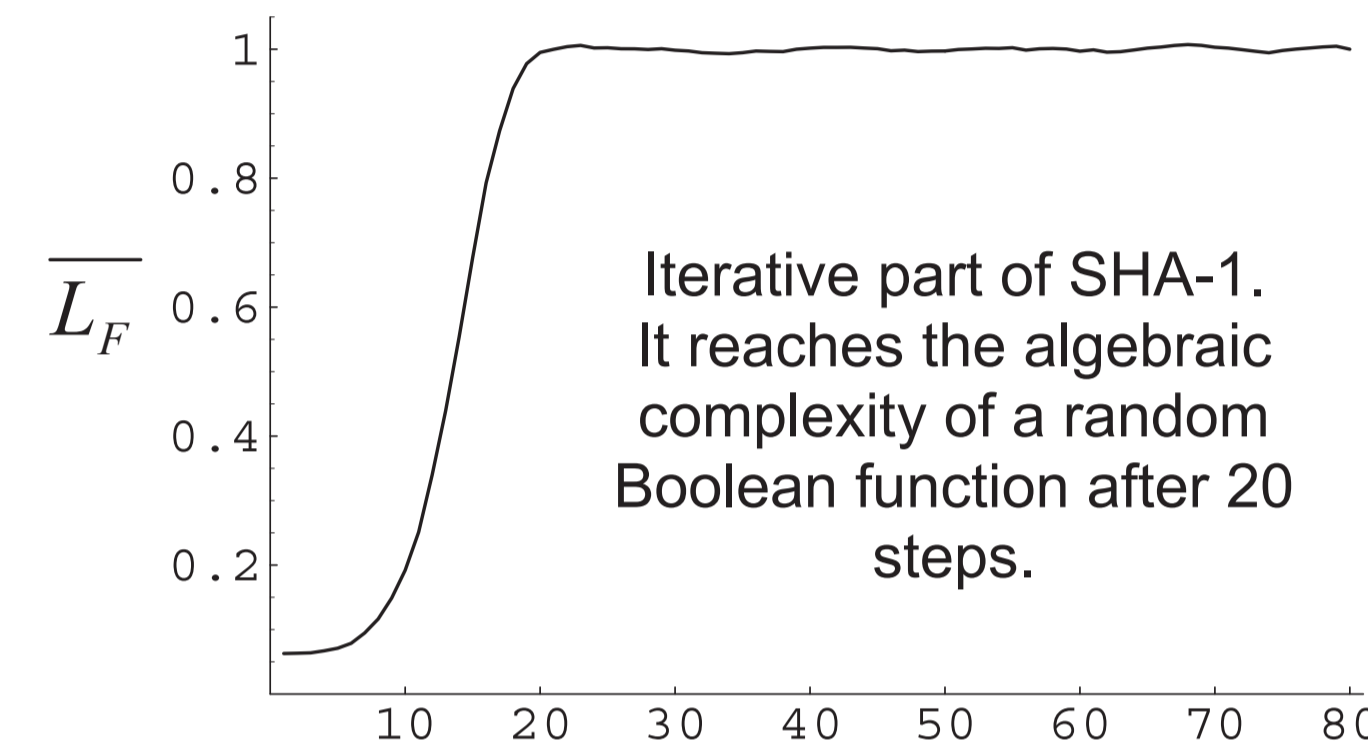
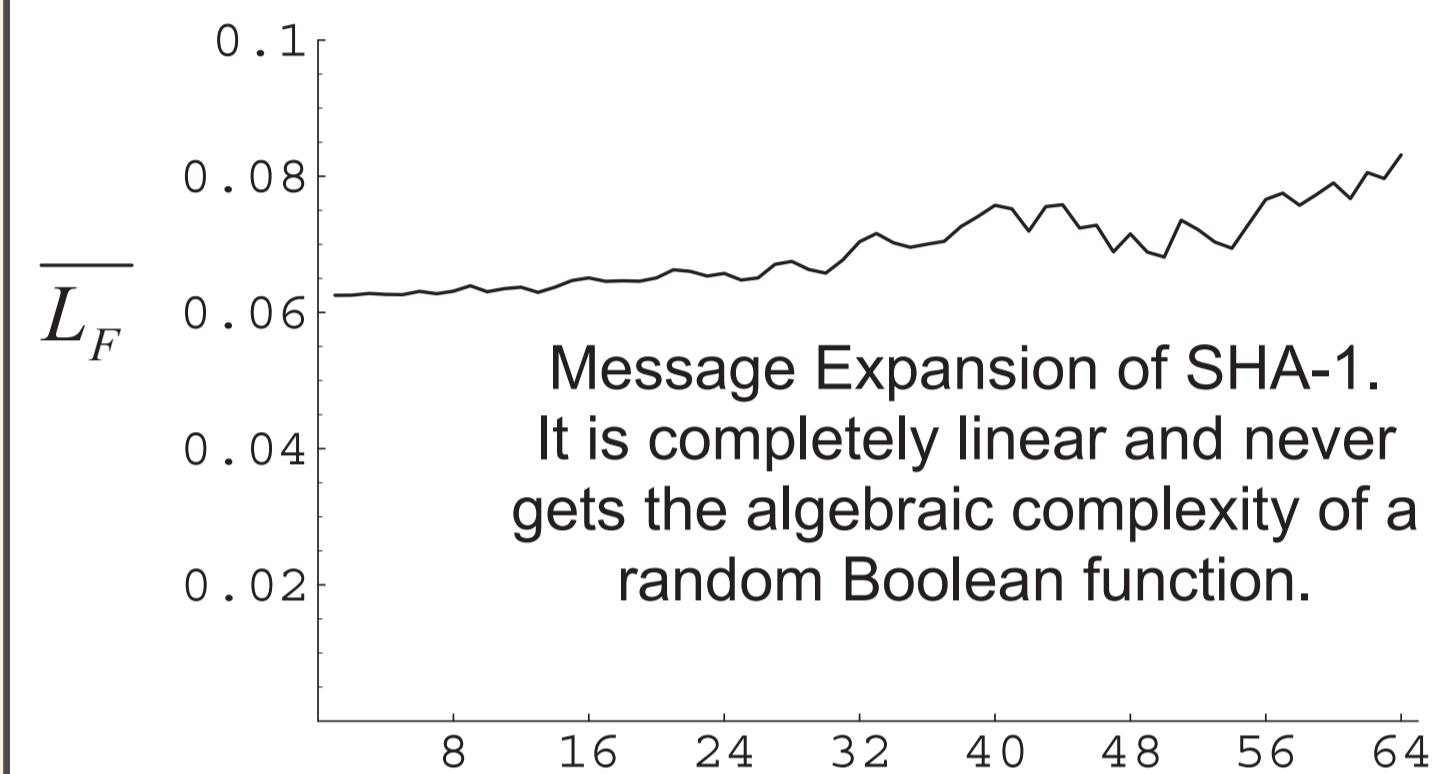
is the compression function of a one-way hash function that is iteratively defined in N steps and let

$C_j, j \in \{1, \dots, N\}$ be the reduced compression function on first j steps.

If $EX(\overline{L}_{C_j}) \approx 0$, then by using

Gröbner Bases and representing the function C_j in $GF(2)^r$ the collisions

for C_j can be found in effective way.



Linearity of SHA-1 message expansion part in combination with the linear and invertible operations applied in iteration part, are the essential reasons for the successes of finding collisions of reduced SHA-1 function up to 58 steps.

SHA-2 is much better designed, but still the design can be improved in security and speed.

Our new proposal SHA-1Q2 uses nonlinear technique "Quasigroup Folding" and introduces a new design principle: **computations in the iterative part of the compression function are performed only on variables produced in the message expansion part that have complexity level of a random Boolean function.**

References:

[1] D. Gligoroski, S. Markovski and S. J. Knapskog, "A Fix of the MD4 Family of Hash Functions - Quasigroup Fold", NIST Cryptographic Hash Workshop, 2005.

[2] D. Gligoroski, S. Markovski and S. J. Knapskog, "SHA-1Q2 secure hash algorithm with only 6 folded SHA-1 steps", submitted to CRYPTO06.