Gimli: NIST LWC Second-round Candidate Status Update

Daniel J. Bernstein Stefan Kölbl Stefan Lucks
Pedro Maat Costa Massolino Florian Mendel
Kashif Nawaz Tobias Schneider Peter Schwabe
François-Xavier Standaert Yosuke Todo Benoît Viguier

September 18, 2020

1 Introduction

This is a short update on Gimli.

Gimli is the simplest submission to the NIST Lightweight Cryptography Standardization Process. It naturally fits into very little code and very little hardware area, handles both hashing and AEAD with healthy security margins, and provides good speeds across a wide range of platforms.

Applications that communicate across different platforms are particularly favorable to Gimli, but Gimli is designed to do reasonably well in all applications. Gimli has already been demonstrated to outperform existing NIST standards on a variety of platforms. For example, the permutation takes 67 ns on a Xilinx Spartan 6 LX75 FPGA using just 221 slices (815 LUTs and 392 flip-flops), 20000 cycles on an AVR ATmega using just 778 bytes of code, and 419 cycles on an ARM Cortex-A8 using just 480 bytes of code, with many tradeoffs being possible. A recent Intel paper "Gimli encryption in 715.9 psec" [2] concludes that "Gimli stands out as a much faster encryption technique, when compared to other known algorithms including AES and PRINCE."

We do not plan to propose tweaks. Implementations have not encountered any performance problems. Third-party cryptanalysis (see Section 2) confirms the large security margin of both Gimli-Hash and Gimli-AEAD. A third-party library (`libhydrogen.org`) shows how easily Gimli can be integrated into software applications, and the Intel results show Gimli's suitability for integration into low-latency hardware applications.

Scheme	Attack	Rounds	Time	Memory	Data	Reference
Gimli-Hash	Collision	12	2^{96}	negl.		[3]
	Collision	6	$2^{91.4}$	negl.		[3]
	Collision	6	2^{113}	negl.		[7]
	Collision	6	2^{64}	2^{64}		[5]
	Preimages	5	2^{96}	$2^{65.6}$		[5]
Gimli-AEAD	State Recovery	9	2^{190}	2^{192}	4	[5]
	State Recovery	5	2^{128}	2^{126}	4	[5]

Table 1: Summary of attacks on Gimli-AEAD and Gimli-Hash. Gimli has 24 rounds.

2 Third-party cryptanalysis

This section briefly summarizes results published on the security of the Gimli permutation, Gimli-Hash, and Gimli-AEAD since the submission to NIST LWC.

The state-of-the-art attacks on reduced-round Gimli-AEAD and Gimli-Hash are summarized in Figure 1. The state-of-the-art permutation distinguisher is a generic distinguisher of the form "Is $P(0) = x$?" that succeeds against every permutation in time 1, when x is chosen appropriately, so the table omits discussion of slower distinguishers.

Specific results are as follows:

- In [4, 6, 5] the authors present various new results on Gimli. This includes distinguishers, collision and preimage attacks on reduced-round variants, and a new technique to find and verify differential characteristics for Gimli. It is shown that several previous differential attacks used invalid characteristics. Based on these results the authors propose several attacks on Gimli-Hash and Gimli-AEAD (see Table 1). The distinguishers are slower than the generic distinguisher described above.

- In [3] the authors provide several new distinguishers on the Gimli permutation and attacks on Gimli-Hash. The best attacks on Gimli-Hash are included in Table 1. The distinguishers are slower than the generic distinguisher described above.

- In [7] the authors present a 6-round collision attack on Gimli based on the differential properties of the Gimli permutation. See Table 1.

- In [1] the authors present distinguishers based on deep learning for 8 rounds of Gimli-Hash and Gimli-Cipher. These distinguishers are slower than the generic distinguisher described above; additionally, contrary to most classical attacks, it is not possible to extend their model to cover further rounds.

References

[1] Anubhab Baksi, Jakub Breier, Xiaoyang Dong, and Chen Yi. Machine learning assisted differential distinguishers for lightweight ciphers. Cryptology ePrint Archive, Report 2020/571, 2020. https://eprint.iacr.org/2020/571.

[2] Santosh Ghosh, Michael E. Kounavis, and Sergej Deutsch. Gimli encryption in 715.9 psec. Cryptology ePrint Archive, Report 2020/336, 2020. https://eprint.iacr.org/2020/336.

[3] Antonio Flórez Gutiérrez, Gaëtan Leurent, María Naya-Plasencia, Léo Perrin, André Schrottenloher, and Ferdinand Sibleyras. New results on Gimli: full-permutation distinguishers and improved collisions. Cryptology ePrint Archive, Report 2020/744, 2020. https://eprint.iacr.org/2020/744.

[4] Fukang Liu, Takanori Isobe, and Willi Meier. Preimages and collisions for up to 5-round Gimli-Hash using divide-and-conquer methods. Cryptology ePrint Archive, Report 2019/1080, 2019. https://eprint.iacr.org/2019/1080.

[5] Fukang Liu, Takanori Isobe, and Willi Meier. Automatic verification of differential characteristics: Application to reduced Gimli (full version). Cryptology ePrint Archive, Report 2020/591, 2020. https://eprint.iacr.org/2020/591.

[6] Fukang Liu, Takanori Isobe, and Willi Meier. Exploiting weak diffusion of Gimli: Improved distinguishers and preimage attacks. Cryptology ePrint Archive, Report 2020/561, 2020. https://eprint.iacr.org/2020/561.

[7] Rui Zong, Xiaoyang Dong, and Xiaoyun Wang. Collision attacks on round-reduced Gimli-Hash/Ascon-Xof/Ascon-Hash. Cryptology ePrint Archive, Report 2019/1115, 2019. https://eprint.iacr.org/2019/1115.