BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY
Excel@FIT 2026

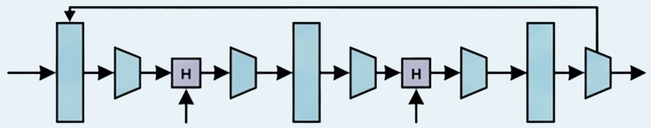
EFFICIENT HASHING ALGORITHMS FOR HIGH-SPEED FPGA APPLICATIONS

AUTHOR: ONDŘEJ SCHWARZ

Scan for VHDL Source Code

GENERAL APPROACH & CHARACTERISTICS

CONFIGURABILITY



VARIABLE PIPELINING WITH SUPPORT FOR DEEP PIPELINING

HIGH FREQUENCIES (UP TO 1 GHZ)

SPOOKYHASH (Short Version)

FAST NON-CRYPTOGRAPHIC, LOW RESOURCES, 128-BIT HASH

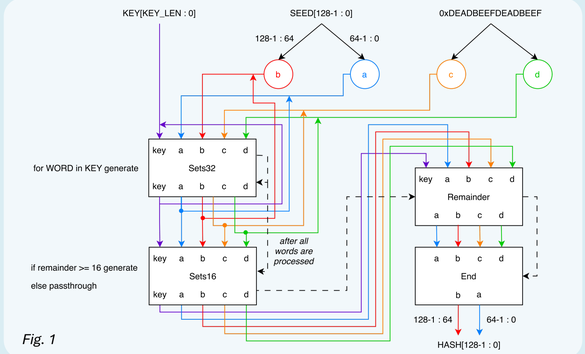


Fig. 1

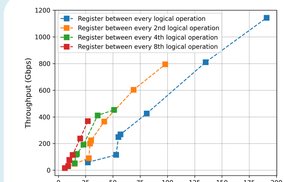


Fig. 2

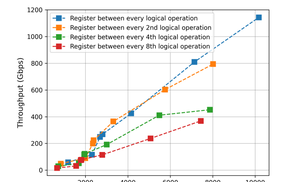


Fig. 3

STATISTICAL RESULTS

Collision resistance

31548 (opt. 31250)

Information entropy

3.611497 (opt. 4.0)

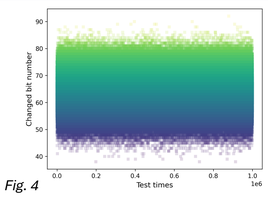


Fig. 4

SIPHASH (4 variants)

CRYPTOGRAPHIC, ARX NETWORK, 32-BIT, 64-BIT AND 128-BIT VARIANTS

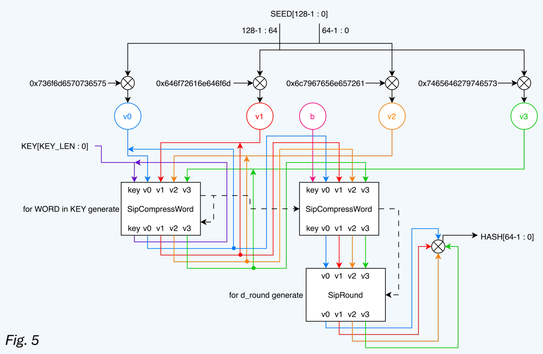


Fig. 5

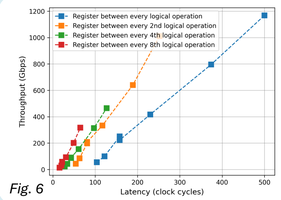


Fig. 6

Fig. 7

STATISTICAL RESULTS*

Collision resistance

31599 (opt. 31250)

Information entropy

3.611493 (opt. 4.0)

*Results for Siphash-4-8-128

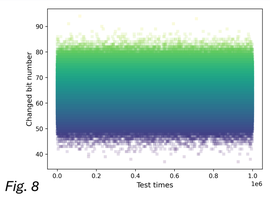


Fig. 8

CHASKEY

LIGHTWEIGTH CRYPTOGRAPHIC MAC, 32-BIT ARX NETWORK, 128-BIT HASH

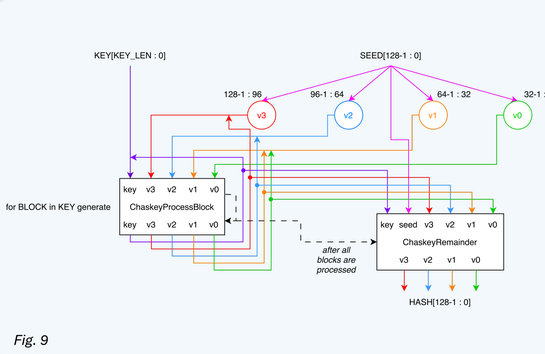


Fig. 9

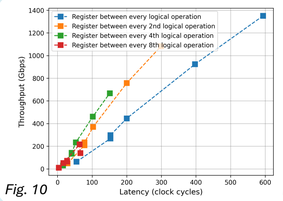


Fig. 10

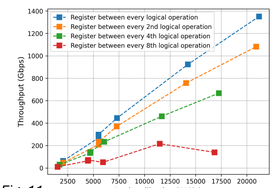


Fig. 11

STATISTICAL RESULTS*

Collision resistance

30978 (opt. 31250)

Information entropy

3.611528 (opt. 4.0)

*Results for Chaskey LTS

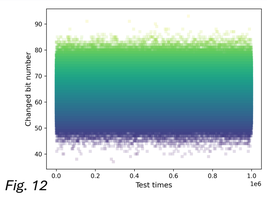


Fig. 12

PCARX

PARALLEL HASH TREE, CELLULAR AUTOMATA & ARX COMPRESSION

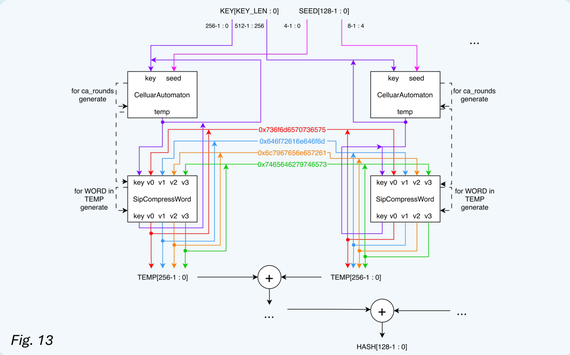


Fig. 13

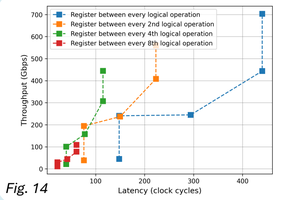


Fig. 14

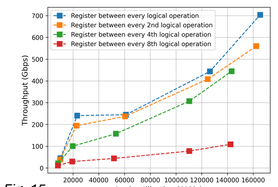


Fig. 15

STATISTICAL RESULTS*

Collision resistance

31294 (opt. 31250)

Information entropy

3.611641 (opt. 4.0)

*Results for PCARX-8-8

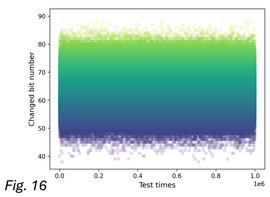


Fig. 16