Why Does Hardware API Matter?

Jens-Peter Kaps & Kris Gaj

William Diehl

George Mason University

CERG

Signatures Analysis Lab
Components of a Hardware API

1. Minimum Compliance Criteria

- Supported operations
- Permitted input sizes
- Decrypted plaintext release
- Permitted data port widths etc.

2. Interface

3. Communication Protocol

4. Timing Characteristics

https://cryptography.gmu.edu/athena  v1: October 2019
LWC Hardware API proposed by GMU, VT, & TUM

Figure 3.1: Top-level block diagram of the LWC core
API of the CryptoCore
(or equivalent)

~200-250 LUTs less
API of the CryptoCore Datapath (or equivalent)
API of the CryptoCore Datapath w/o Key Scheduling
Two-Pass FIFO

Key Sched + Padding

Enc/Dec FullB

CryptoCore Controller

Header FIFO

din
din_valid
din_ready
dout
dout_valid
dout_ready

Pre Processor

sdi_data
sdi_valid
sdi_ready

sw

pdi_data
pdi_valid
pdi_ready

w

Post Processor

bdo
bdo_valid
bdo_ready
bdo_type
bdo_valid_bytes
end_of_block

do_data
do_valid
do_ready
do_last

msg_auth
msg_auth_valid
msg_auth_ready

cmd

cmd_valid
cmd_ready

Key Sched + Padding

Enc/Dec FullB

Controller

sw

sdi_data
sdi_valid
sdi_ready

pdi_data
pdi_valid
pdi_ready

w

Figure 3.1: Top-level block diagram of the LWC core

API of the CryptoCore Datapath w/o Key Scheduling & w/o Padding
API of the CryptoCore Datapath
w/o Key Scheduling & w/o Padding, for short messages only

Two-Pass FIFO

Key Sched
+ Padding
+ Long msg support

Enc/Dec FullB 128B

CryptoCore Controller

Pre Processor

Post Processor

LWC

sdi_data
sdi_valid
sdi_ready

pdi_data
pdi_valid
pdi_ready

Key

Header FIFO
Hardware API does not leave any room for manipulation!
We should not compare apples with oranges!
Is it too late?
CAESAR Competition Timeline

- **2014.03.15**: Deadline for first-round submissions
- **2015.07.07**: Announcement of second-round candidates
- **2015.08.29**: Deadline for second-round tweaks
- **2015.09.15**: Deadline for second-round software
- **2016.05.16**: Hardware API officially approved by the CAESAR Committee
- **2016.06.17**: Hardware API posted on ePrint
- **2016.06.30**: Deadline for Verilog/VHDL
- **2016.08.15**: Announcement of third-round candidates
- **2016.10.15**: Deadline for third-round software
- **2016.11.24**: Addendum to the API approved by the CAESAR Committee
- **2017.07.15**: Deadline for third-round Verilog/VHDL
CAESAR Round 2 VHDL/Verilog Submissions

Algorithms with:

- **2 Compliant designs + 1 Non-Compliant Design**
  1: TriviA-ck

- **2 Compliant designs**
  3: Ascon, CLOC, Minalpher

- **1 Compliant Design + 1 Non-Compliant Design**
  8: Deoxys, ELmD, HS1-SIV, Joltik, NORX, Pi-Cipher, POET, SCREAM

- **1 Compliant Design**
  17: ACORN, AEGIS, AES-COPA, AES-JAMBU, AES-OTR, AEZ, ICEPOLE, Ketje, Keyak, MORUS, OCB, OMD, PAEQ, PRIMATEs-GIBBON, PRIMATEs-HANUMAN, SHELL, SILC, STRIBOB

- **No Designs**
  1: Tiaoxin
CAESAR Round 3 VHDL/Verilog Submissions

- 2 Compliant Submissions + 1 Non-Compliant Submission
  1: Deoxys-I

- 2 Compliant submissions
  4: AEGIS, CLOC-AES, COLM, SILC-AES

- 1 Compliant Submission + 1 Non-Compliant Submission
  2: Ascon, Ketje

- 1 Compliant Submission
  12: ACORN, AES-OTR x 2, AEZ, CLOC-TWINE, JAMBU-AES, JAMBU-SIMON, MORUS, NORX, OCB, SILC-LED/PRESENT, Tiaoxin

- 1 Partially Compliant Submission
  1: Keyak

- 1 Non-Compliant Submission
  1: Deoxys-II
CAESAR Round 3 VHDL/Verilog Submitters

1. CERG GMU - AEGIS, AEZ, Ascon, CLOC-AES, COLM, Deoxys-I, JAMBU-AES, NORX, OCB, SILC-AES, Tiaoxin (11)
2. CCRG NTU Singapore – ACORN, AEGIS, JAMBU-SIMON, MORUS (4)
3. CLOC-SILC Team, Japan – CLOC-AES, CLOC-TWINE, SILC-AES, SILC-LED/PRESENT (4)
4. Ketje-Keyak Team – Ketje x 2 & Keyak (3)
5. NEC Japan – AES-OTR x 2 (2)
6. IAIK TU Graz, Austria – Ascon x 2
7. CINVESTAV-IPN, Mexico – COLM
8. Axel Y. Poschmann and Marc Stöttinger – Deoxys-I & Deoxys-II
9. NTU Singapore – Deoxys-I

Total: 29 submissions
Possible Ways Forward
# LWC-compliant designs reported as completed or in progress

<table>
<thead>
<tr>
<th>Design Groups</th>
<th>Candidates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Submission Teams</td>
<td>17: ACE, ASCON, DryGASCON, ESTATE, ForkAE, GIFT-COFB, Gimli, ISAP, KNOT, LOTUS-LOCUS, Oribatida, Romulus, Spook, Subterranean 2.0, SUNDAE-GIFT, WAGE, Xoodyak</td>
</tr>
<tr>
<td>Virginia Tech</td>
<td>5: ASCON, COMET, GIFT-COFB, SPARKLE, SpoC</td>
</tr>
<tr>
<td>CINVESTAV-IPN</td>
<td>6: COMET, ESTATE*, LOTUS-LOCUS*, mixFeed, ORANGE, Oribatida*</td>
</tr>
<tr>
<td>Morgan State University</td>
<td>1: HyENA</td>
</tr>
<tr>
<td>George Mason University</td>
<td>8: Grain-128AEAD, Elephant, mixFeed, PHOTON-Beetle, Pyjamask, Saturnin, TinyJambu, Xoodyak</td>
</tr>
</tbody>
</table>

* Design by a member of a submission team
Our Proposal

- About 2 months (June-July 2020) devoted to converting all implementations to API-compliant implementations

- API-compliant implementations made open-source to date
  - Virginia Tech : 5

Proposed GMU Team responsibilities
- Completing and optimizing GMU designs : 8
- Assisting submission teams with conversion to the LWC Hardware API : 17
Our Recommendation

Requirement to make the following HDL implementations of Round 3 candidates open-source, or at least available for validation and benchmarking by the 3rd party:

- unprotected LWC cores - 3 months after the beginning of Round 3
- protected LWC cores – 3 months before the end of Round 3

All unprotected implementations compliant with the proposed LWC Hardware API

All protected implementations compliant with the extended LWC Hardware API (under development)
Why do benchmarking platforms matter?
Benchmarking
During the CAESAR Competition

Target FPGA Families:
- Xilinx Virtex-6
- Xilinx Virtex-7
- Altera Stratix IV
- Altera Stratix V

Benchmarking Team:
- CASEAR Committee delegated benchmarking to the CERG GMU Team

ATHENa Database of Results:
- https://cryptography.gmu.edu/athenadb/fpga_auth_cipher/rankings_view
- https://cryptography.gmu.edu/athenadb/fpga_auth_cipher/table_view
## LWC Benchmarking Platforms Reported to Date

<table>
<thead>
<tr>
<th>Submission</th>
<th>Design Team</th>
<th>FPGA families</th>
<th>ASIC libraries</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACE</td>
<td>ACE Team</td>
<td>Spartan-3, Spartan-6, Stratix IV</td>
<td>65 nm STMicroelectronics 65 nm TSMC</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>90 nm STMicroelectronics</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>130 nm IBM</td>
</tr>
<tr>
<td>Ascon</td>
<td>Ascon Team</td>
<td>Spartan-6, Artix-7, Virtex-6, <strong>Virtex-7</strong>, Cyclone IV, Cyclone V, Stratix IV, Stratix V</td>
<td>90 nm UMC 180 nm UMC</td>
</tr>
<tr>
<td>DryGASCON</td>
<td>Sebastien Riou</td>
<td>Zynq-7000, iCE40</td>
<td></td>
</tr>
<tr>
<td>ESTATE</td>
<td>ESTATE Team</td>
<td><strong>Virtex-7</strong></td>
<td></td>
</tr>
<tr>
<td>ForkAE</td>
<td>ForkAE Team</td>
<td></td>
<td>45 nm NanGate</td>
</tr>
<tr>
<td>GIFT-COFB</td>
<td>GIFT-COFB Team</td>
<td></td>
<td><strong>90 nm STMicroelectronics</strong></td>
</tr>
<tr>
<td>Gimli</td>
<td>Gimli Team</td>
<td>Spartan-6</td>
<td>28 nm FDSOI 180 nm UMC</td>
</tr>
<tr>
<td>Gimli</td>
<td>Intel Labs</td>
<td></td>
<td>10 nm Intel FinFET</td>
</tr>
<tr>
<td>Gimli</td>
<td>TUM</td>
<td>Artix-7</td>
<td></td>
</tr>
<tr>
<td>Grain-128AEAD</td>
<td>Grain Team</td>
<td></td>
<td>65 nm STMicroelectronics</td>
</tr>
<tr>
<td>Submission</td>
<td>Design Team</td>
<td>FPGA families</td>
<td>ASIC library</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>ISAP</td>
<td>ISAP Team</td>
<td></td>
<td>90 nm UMC, 130 nm UMC</td>
</tr>
<tr>
<td>KNOT</td>
<td>KNOT Team</td>
<td></td>
<td>45nm NanGate</td>
</tr>
<tr>
<td>LOTUS &amp; LOCUS</td>
<td>LOTUS &amp; LOCUS Team</td>
<td>Virtex-6, <strong>Virtex-7</strong></td>
<td></td>
</tr>
<tr>
<td>Oribatida</td>
<td>Oribatida Team</td>
<td>Virtex-7</td>
<td></td>
</tr>
<tr>
<td>Romulus</td>
<td>Romulus Team</td>
<td></td>
<td>65nm TSMC</td>
</tr>
<tr>
<td>SAEAES</td>
<td>SAEAES Team</td>
<td>Virtex-7, Cyclone V</td>
<td>45nm NanGate</td>
</tr>
<tr>
<td>SKINNY</td>
<td>SKINNY Team</td>
<td>Virtex-7</td>
<td>90 nm UMC, 130 nm IBM</td>
</tr>
<tr>
<td>Subterranean 2.0</td>
<td>Subterranean 2.0 Team</td>
<td>Zynq-7000</td>
<td>45nm FreePDK</td>
</tr>
<tr>
<td>SUNDAE-GIFT</td>
<td>SUNDAE Team</td>
<td></td>
<td>90 nm STMicroelectronics</td>
</tr>
<tr>
<td>TinyJambu</td>
<td>TinyJambu Team</td>
<td></td>
<td>90 nm UMC</td>
</tr>
<tr>
<td>WAGE</td>
<td>WAGE Team</td>
<td>Spartan-3, Spartan-6, Stratix IV</td>
<td>65 nm STMicroelectronics, 65 nm TSMC, <strong>90 nm STMicroelectronics</strong>, 130 nm IBM</td>
</tr>
</tbody>
</table>
Benchmarking Platforms Used by Other Teams

Only results obtained using the same FPGA family or the same ASIC library can be fairly compared with one another!

Not counting VT and GMU benchmarking efforts, at best 6 FPGA implementations and 4 ASIC implementations can be fairly compared with one another!
Possible Ways Forward
Our Recommendation

- NIST LWC Team delegates hardware benchmarking to several academic or industry labs, including the GMU LWC Team, and, if needed, serves as an intermediary during the submission of VHDL/Verilog Code.

- Half a month (August 1-16, 2020) devoted to comprehensive benchmarking by the GMU LWC Team.

- Publication of the comprehensive report (second half of August 2020).
Choice of Hardware Platforms and Tools

- Widely used low-cost, low-power, low-energy FPGA families
- Devices capable of holding SCA-protected designs (possibly using 3-4 times more resources than unprotected designs)
- Implementation using state-of-the-art industry tools
Proposed FPGA Families & Devices

Xilinx
- Artix-7 : xc7a12tcsg325-3
  - 8,000 LUTs – 16,000 FFs – 40 18Kbit BRAMs – 40 DSPs – 150 I/O
- Spartan-7 : xc7s15cpga196-2
  - 8,000 LUTs – 16,000 FFs – 20 18Kbit BRAMs – 20 DSPs – 150 I/O

Intel
- Cyclone 10 LP : 10CL016-YU256C6
  - 15,408 LEs – 15,408 FFs – 56 M9K blocks – 56 MULs – 162 I/O

Lattice Semiconductor
- ECP5 : LFE5U-25F-6BG381C
  - 24,000 LUTs – 24,000 FFs – 56 18Kbit blocks – 28 MULs – 197 I/O
RTL Benchmarking

HDL Code

Automated Optimization with Minerva or ATHENa

FPGA Tools

Optimal Options of Tools

Replication Script

Post Place & Route Results (Resource Utilization, Max. Clock Frequency)
ATHENa – Automated Tool for Hardware Evaluation

- Open-source
- Written in Perl
- Developed 2009-2012, SHA-3 Contest
- FPL Community Award 2010
- Automated search for optimal
  - Options of tools
  - Target frequency
  - Starting placement point
- Supporting Xilinx ISE, Altera Quartus

No support for Xilinx Vivado
Extension of ATHENa to Vivado: Minerva

- **Programming language:** Python
- **Target synthesis and implementation tool:** Xilinx Vivado Design Suite
- **Supported FPGA families:** All Xilinx 7 series and beyond
- **Optimization criteria:**
  1. Maximum frequency
  2. Frequency/#LUTs
  3. Frequency/#Slices

Released for use by other groups in December 2017
Q&A

Thank You!

Questions?  Comments?

Suggestions?

CERG: http://cryptography.gmu.edu
SAL: https://rijndael.ece.vt.edu/wdiehl