Why Does Hardware API Matter?

Jens-Peter Kaps
& Kris Gaj

William
Diehl

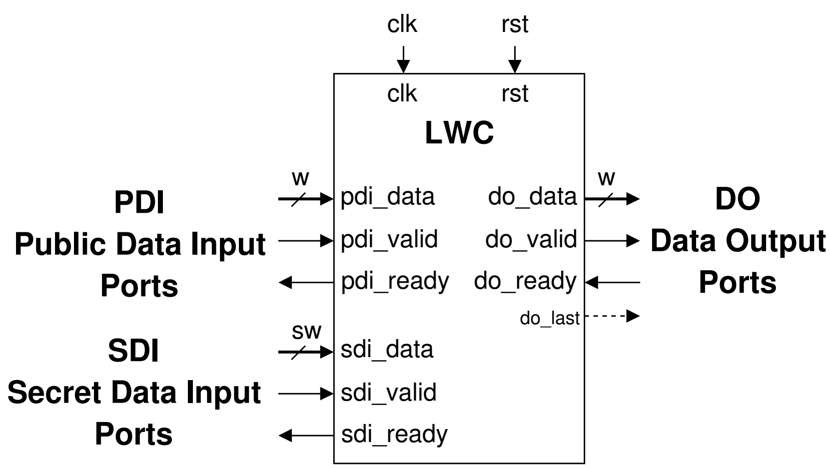
Components of a Hardware API

1. Minimum Compliance Criteria

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

etc.

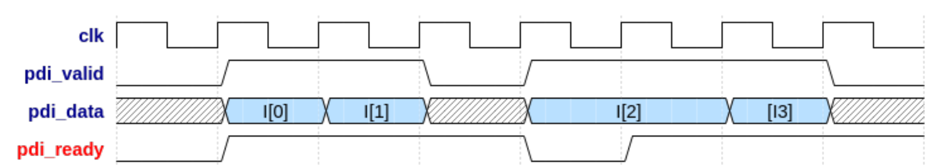
2. Interface



3. Communication Protocol

instruction = ACTKEY
instruction = ENC
seg_0_header
seg_0 = Npub
seg_1_header
seg_1 = AD
seg_2_header
seg_2 = Plaintext

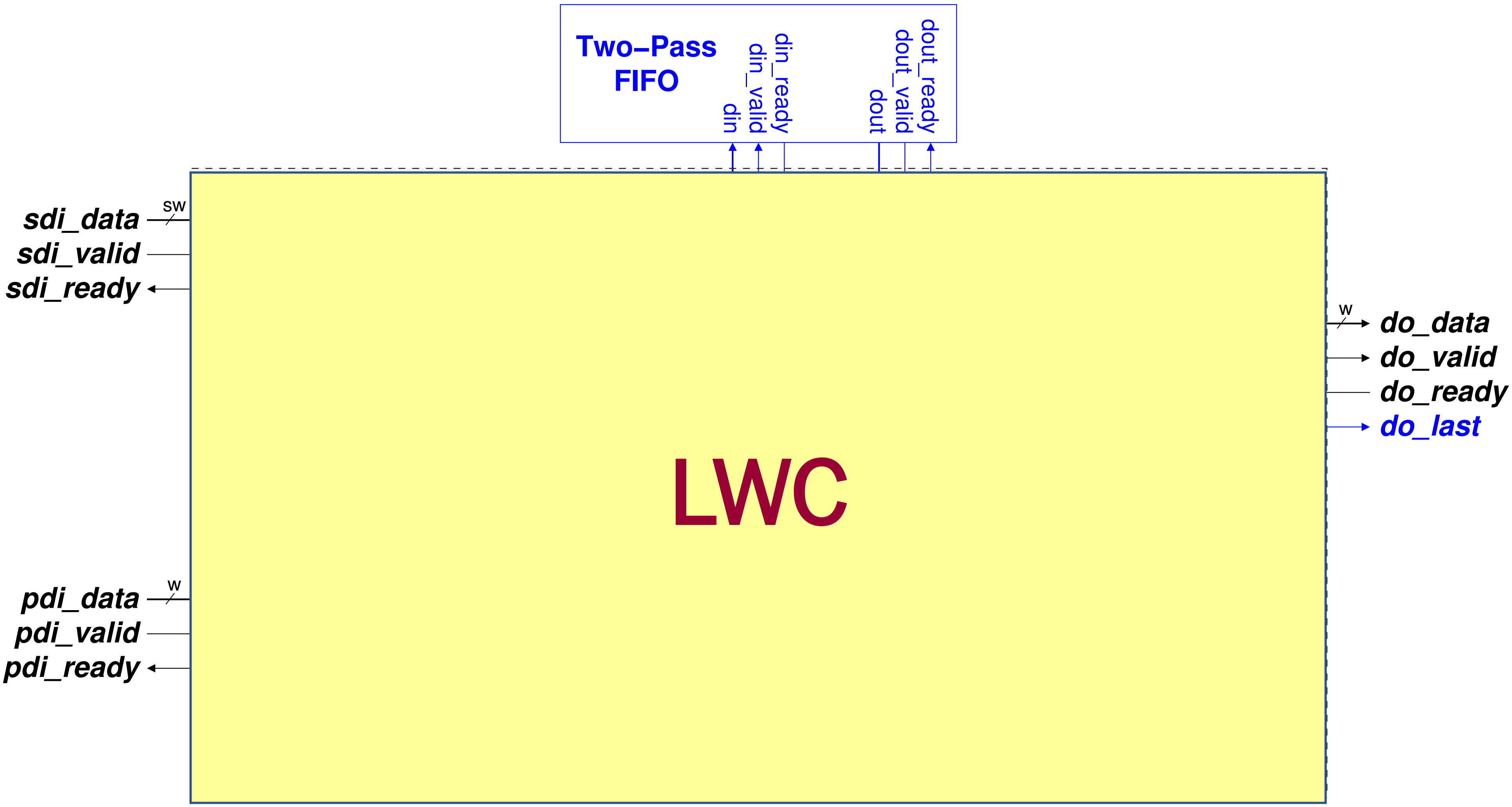
4. Timing Characteristics



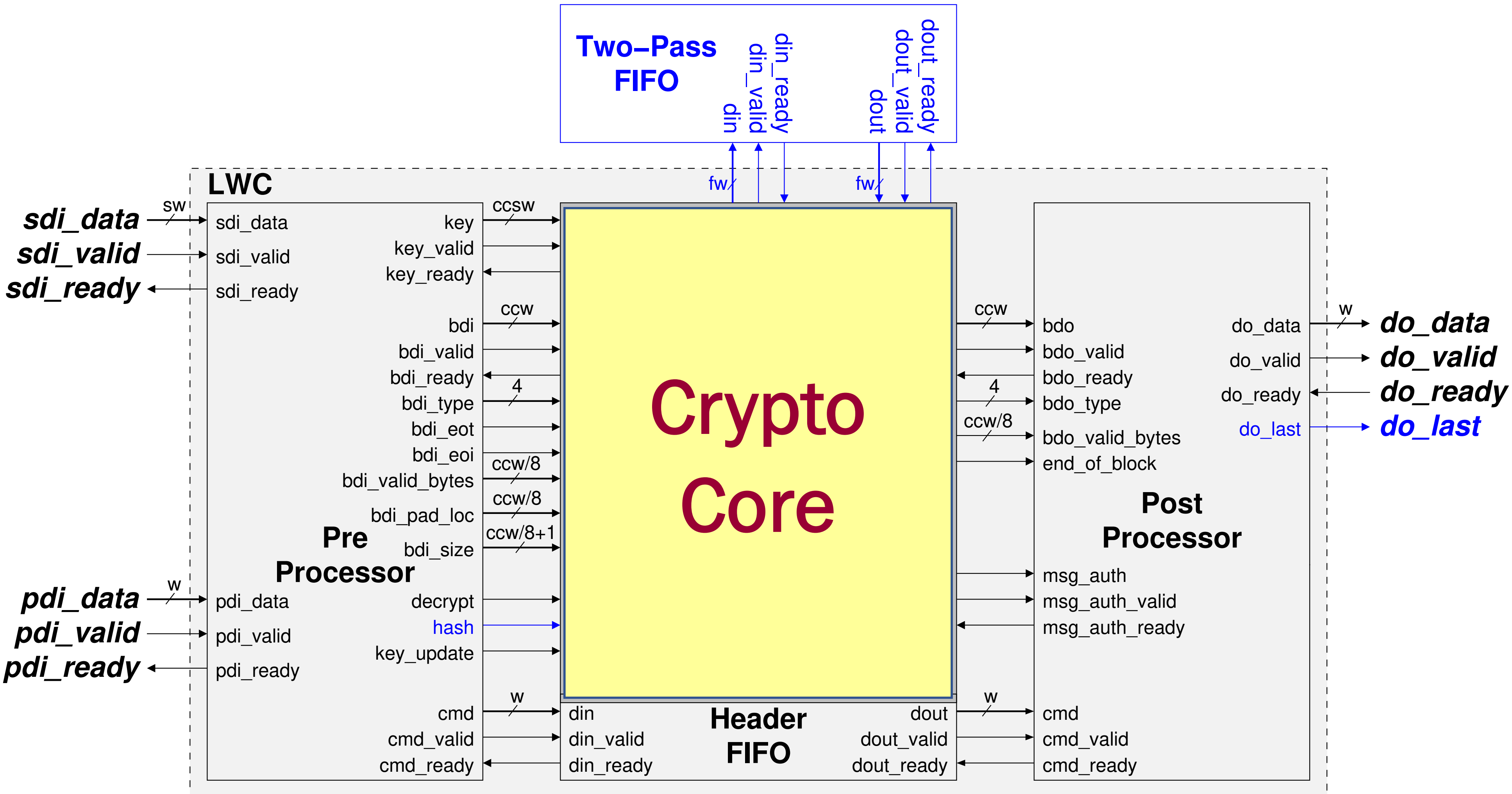
https://cryptography.gmu.edu/athena

v1: October 2019

LWC Hardware API proposed by GMU, VT, & TUM

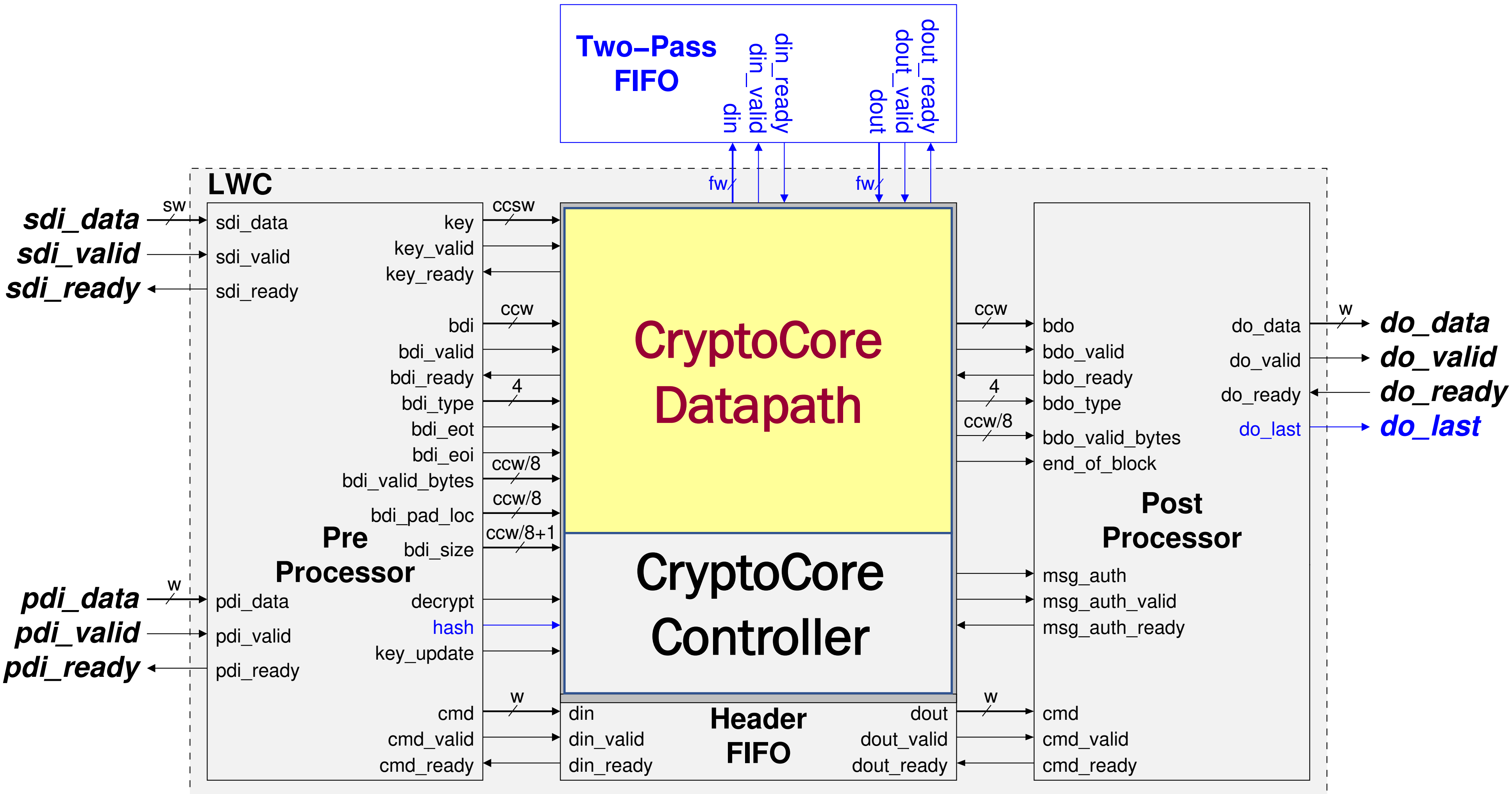


API of the CryptoCore (or equivalent)

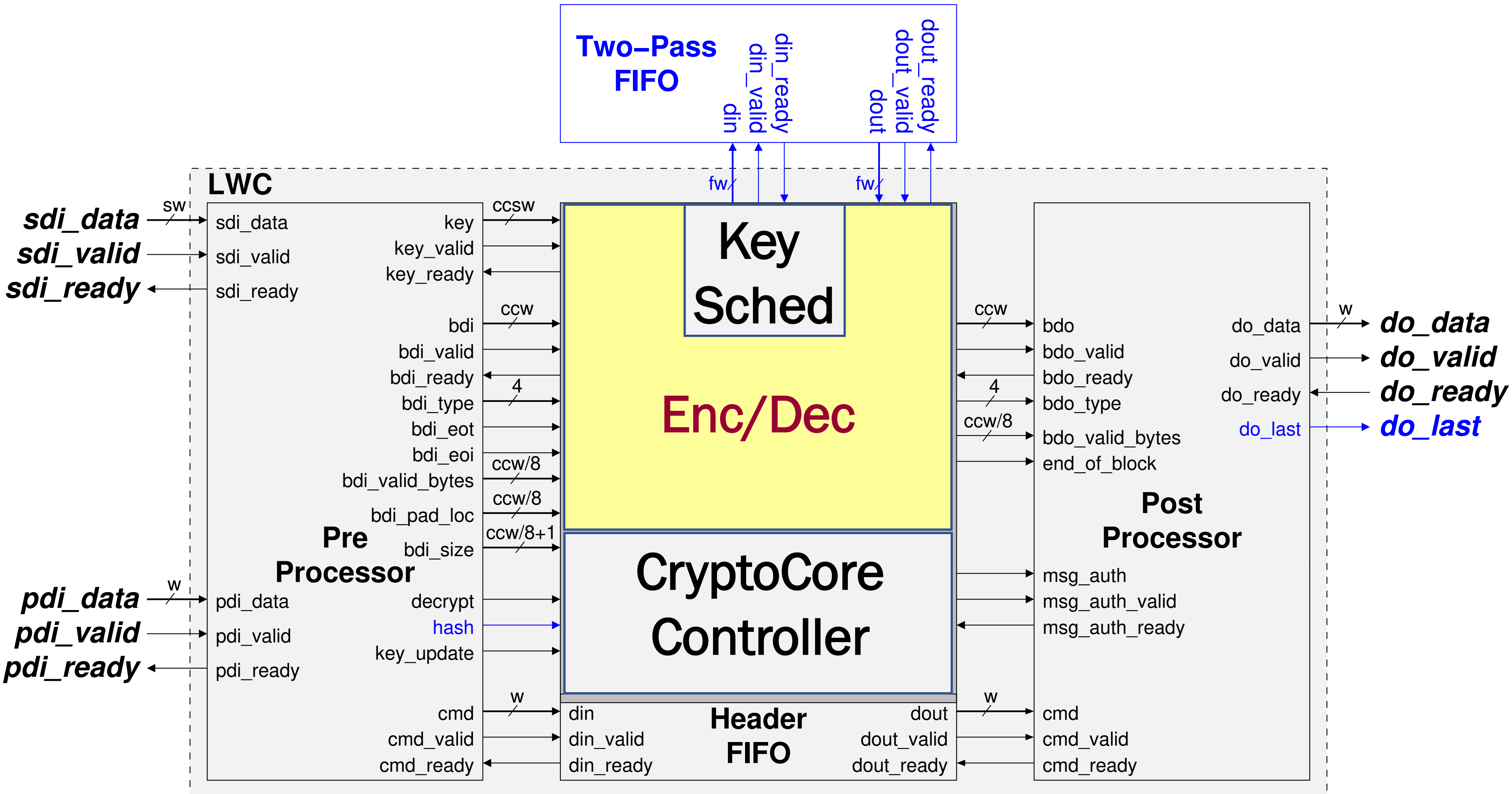


~200-250 LUTs less

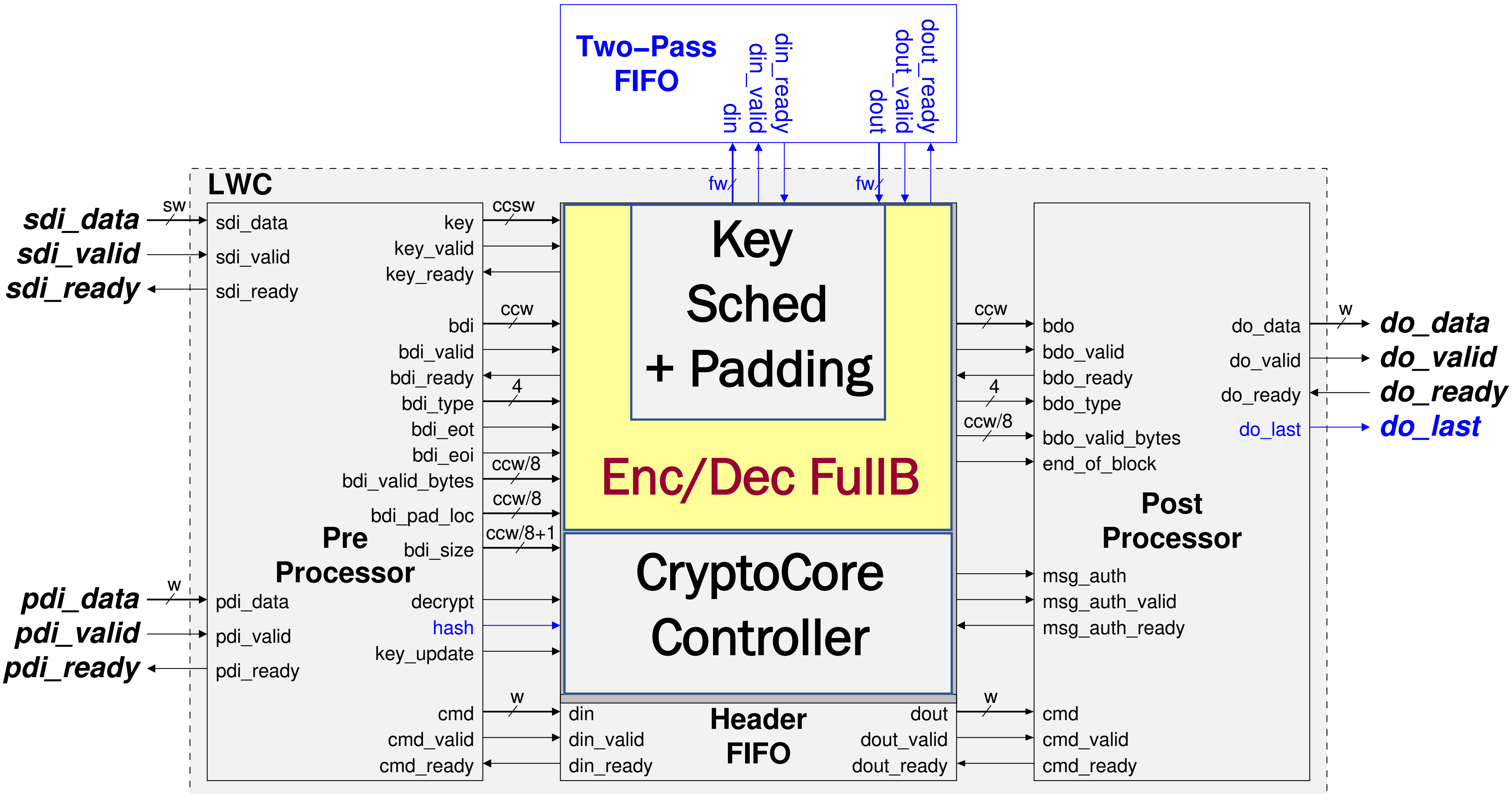
API of the CryptoCore Datapath (or equivalent)



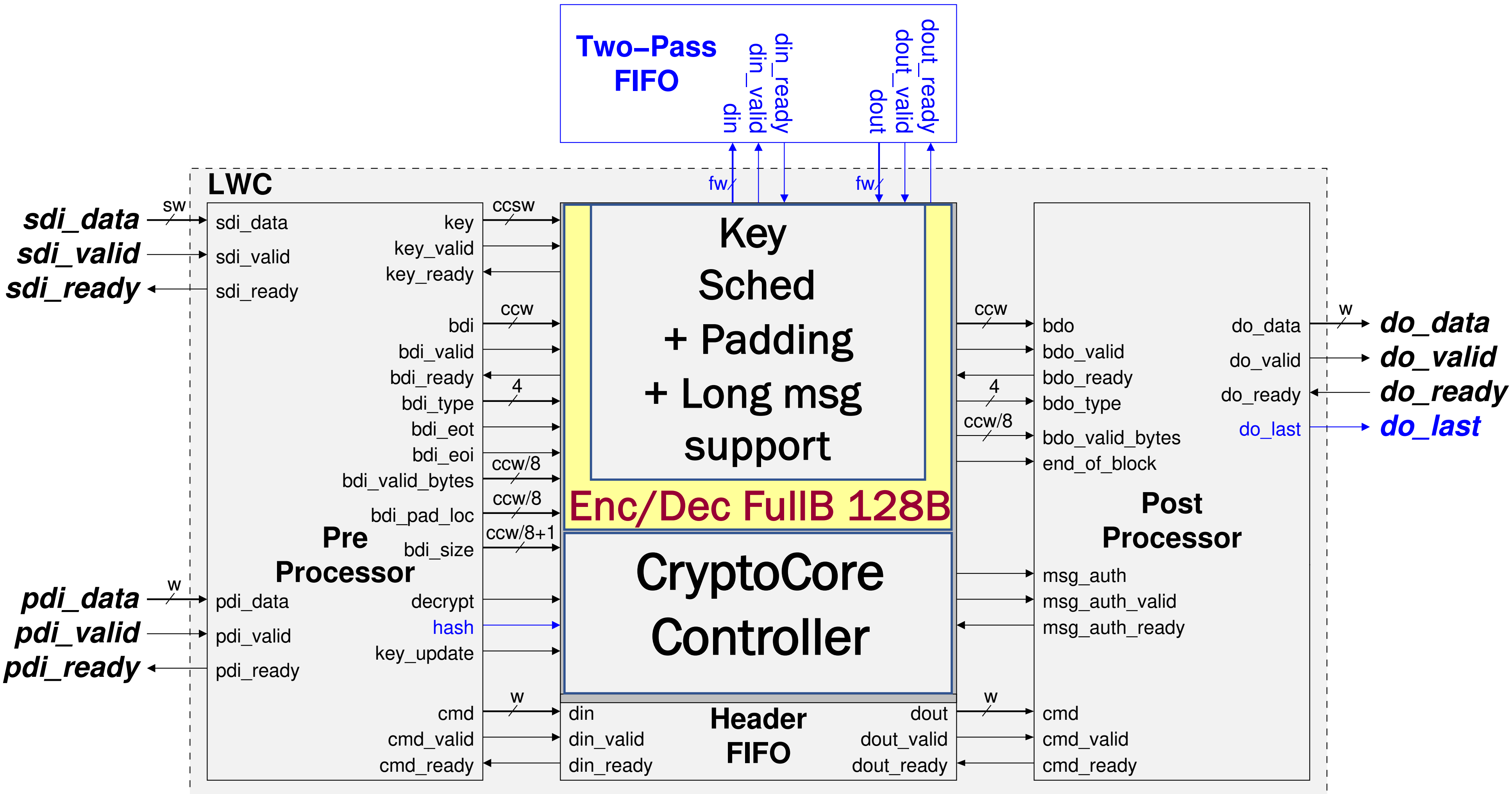
API of the CryptoCore Datapath w/o Key Scheduling



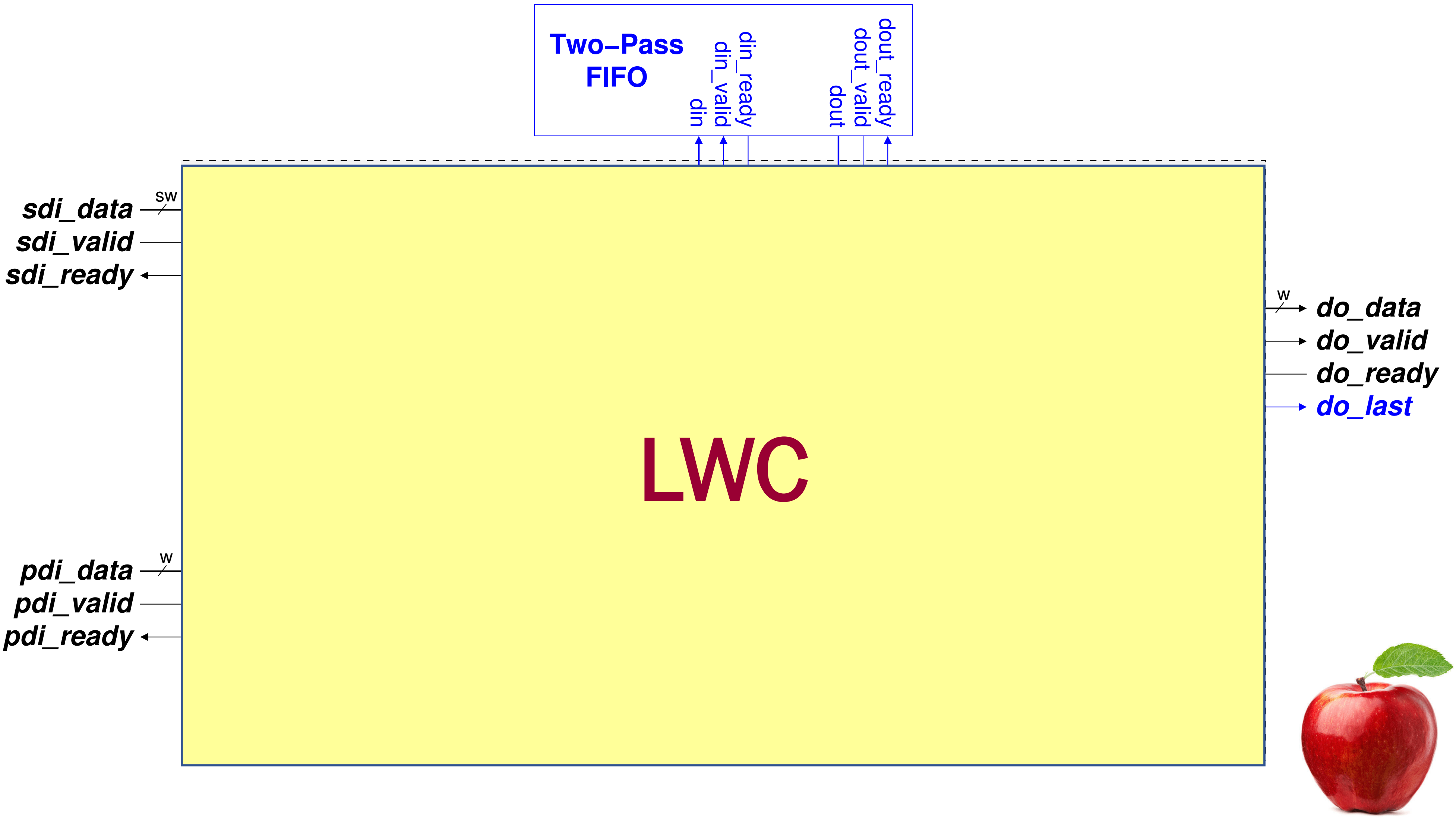
API of the CryptoCore Datapath w/o Key Scheduling & w/o Padding



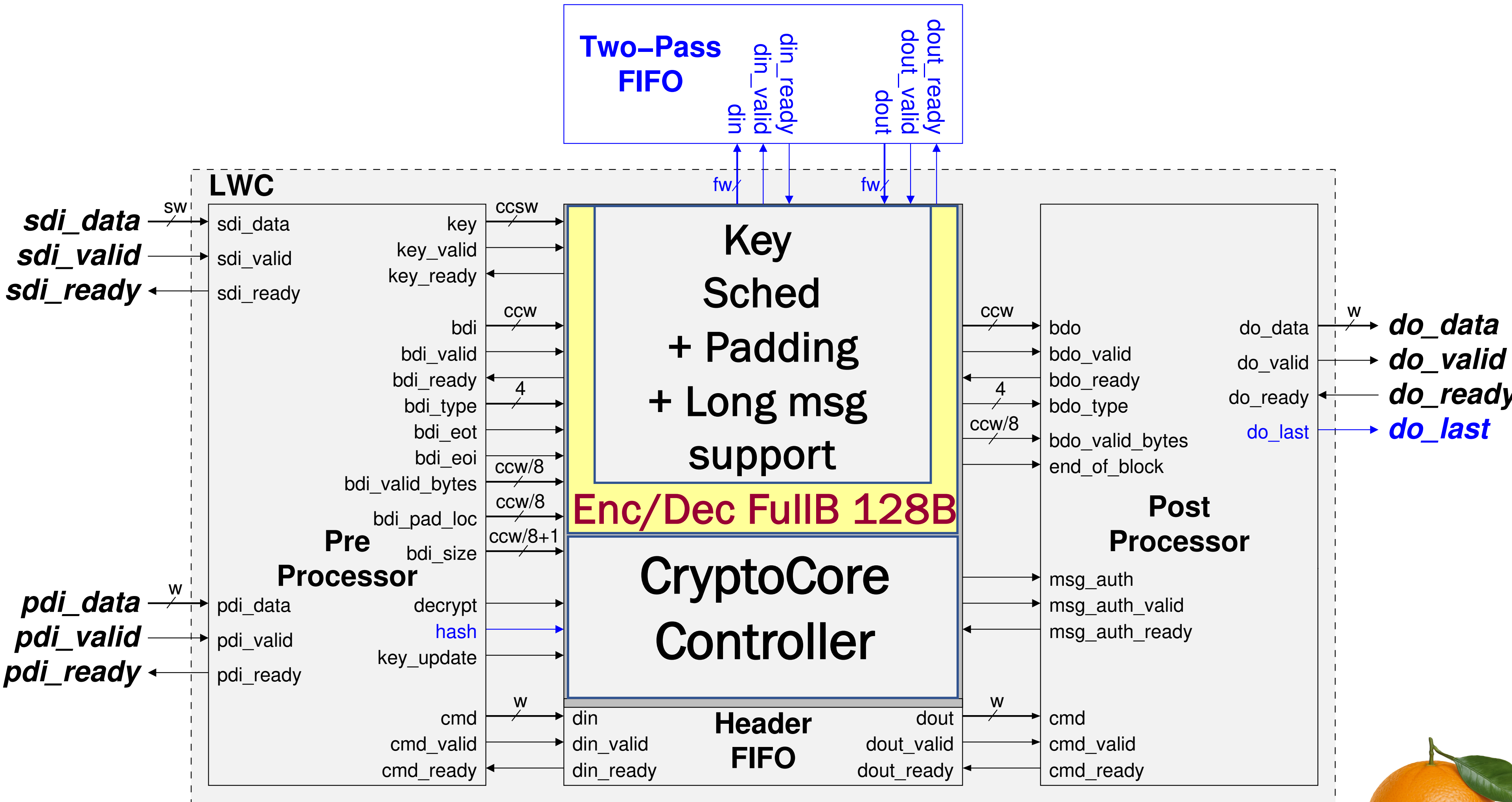
API of the CryptoCore Datapath w/o Key Scheduling & w/o Padding, for short messages only



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

R O U N D 2

- 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**

R O U N D 3

- 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)
5. Ketje-Keyak Team – Ketje x 2 & Keyak (3)
6. NEC Japan – AES-OTR x 2 (2)
7. IAIK TU Graz, Austria – Ascon x 2
8. CINVESTAV-IPN, Mexico – COLM
9. Axel Y. Poschmann and Marc Stöttinger – Deoxys-I & Deoxys-II
10. NTU Singapore – Deoxys-I

Total: 29 submissions

Possible Ways Forward

LWC-compliant designs
reported as completed or in progress

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

* 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

Submission	Design Team	FPGA families	ASIC libraries
ACE	ACE Team	Spartan-3, Spartan-6, Stratix IV	65 nm STMicroelectronics 65 nm TSMC 90 nm STMicroelectronics 130 nm IBM
Ascon	Ascon Team	Spartan-6, Artix-7, Virtex-6, Virtex-7, Cyclone IV, Cyclone V, Stratix IV, Stratix V	90 nm UMC 180 nm UMC
DryGASCON	Sebastien Riou	Zynq-7000, iCE40	
ESTATE	ESTATE Team	Virtex-7	
ForkAE	ForkAE Team		45 nm NanGate
GIFT-COFB	GIFT-COFB Team		90 nm STMicroelectronics
Gimli	Gimli Team	Spartan-6	28 nm FDSOI 180 nm UMC
Gimli	Intel Labs		10 nm Intel FinFET
Gimli	TUM	Artix-7	
Grain-128AEAD	Grain Team		65 nm STMicroelectronics

LWC Benchmarking Platforms Reported to Date

Submission	Design Team	FPGA families	ASIC library
ISAP	ISAP Team		90 nm UMC 130 nm UMC
KNOT	KNOT Team		45nm NanGate
LOTUS & LOCUS	LOTUS & LOCUS Team	Virtex-6, Virtex-7	
Oribatida	Oribatida Team	Virtex-7	
Romulus	Romulus Team		65nm TSMC
SAEAES	SAEAES Team	Virtex-7, Cyclone V	45nm NanGate
SKINNY	SKINNY Team	Virtex-7	90 nm UMC 130 nm IBM
Subterranean 2.0	Subterranean 2.0 Team	Zynq-7000	45nm FreePDK
SUNDAE-GIFT	SUNDAE Team		90 nm STMicroelectronics
TinyJambu	TinyJambu Team		90 nm UMC
WAGE	WAGE Team	Spartan-3, Spartan-6, Stratix IV	65 nm STMicroelectronics 65 nm TSMC 90 nm STMicroelectronics 130 nm IBM

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

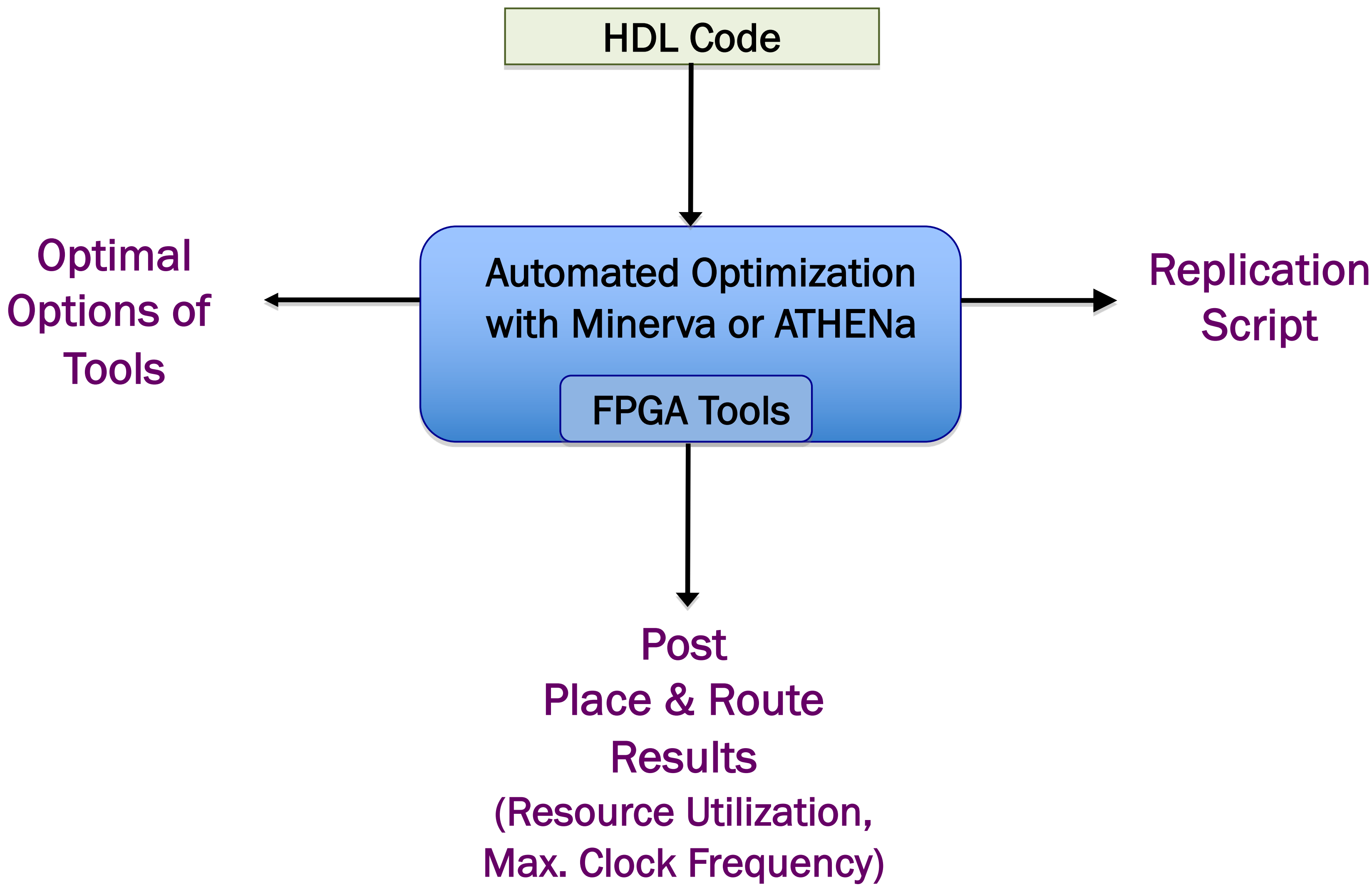
Intel

- 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



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