Towards ML-KEM & ML-DSA on OpenTitan

Amin Abdulrahman[1] Felix Oberhansl[2] Hoang Nguyen Hien Pham[3,4] Jade Philipoom[5,6] Peter Schwabe[1,7] Tobias Stelzer[2] Andreas Zankl[2,8]

May 14, 2025

[1]Max Planck Institute for Security and Privacy (MPI-SP) [2]Fraunhofer Institute for Applied and Integrated Security (AISEC)
amin@abdulrahman.de, peter@cryptojedi.org firstname.lastname@aisec.fraunhofer.de
[3]BULL SAS [4]Université Grenoble Alpes [5]zeroRISC [6]OpenTitan
nguyenhien.phamhoang@gmail.com jadep@zerorisc.com
[7]Radboud University [8]Technical University of Munich (TUM)

A Paradigm Shift

[Res21; App20; Com22; Goo22; Cor19; Clo25; Gmb; FSS20]

A Paradigm Shift

[Res21; App20; Com22; Goo22; Cor19; Clo25; Gmb; FSS20]

A Paradigm Shift

[Res21; App20; Com22; Goo22; Cor19; Clo25; Gmb; FSS20]

A Paradigm Shift

IACR Transactions on Cryptographic Hardware and Embedded Systems
ISSN 2569-2925, Vol. 2020, No. 4, pp. 239–280. DOI:10.13154/tches.v2020.i4.239-280

RISQ-V: Tightly Coupled RISC-V Accelerators for Post-Quantum Cryptography

Tim Fritzmann[1], Georg Sigl[1] and Johanna Sepúlveda[2]

[1] Technical University of Munich, TUM Department of Electrical and Computer Engineering, Chair of Security in Information Technology, Munich, Germany, {tim.fritzmann,sigl}@tum.de
[2] AIRBUS Defence and Space GmbH, Taufkirchen, Germany, johanna.sepulveda@airbus.com

[Res21; App20; Com22; Goo22; Cor19; Clo25; Gmb; FSS20]

A Different Direction

*How efficient can we make **PQC***

A Different Direction

*How efficient can we make **PQC***
*on an **existing pre-quantum platform***

A Different Direction

*How efficient can we make **PQC***
*on an **existing pre-quantum platform***
with modest hardware changes?

Target: OpenTitan

- Open source silicon root of trust (RoT)
- Led by lowRISC, contributions from zeroRISC, Google, ETH Zurich, and many more
- Performs security critical operations
  - → Hardware support for many cryptographic operations
  - → Hardening against side-channel attacks
- Coming to, e.g., Google's 2025 Chromebooks [SO25]

Target: OpenTitan

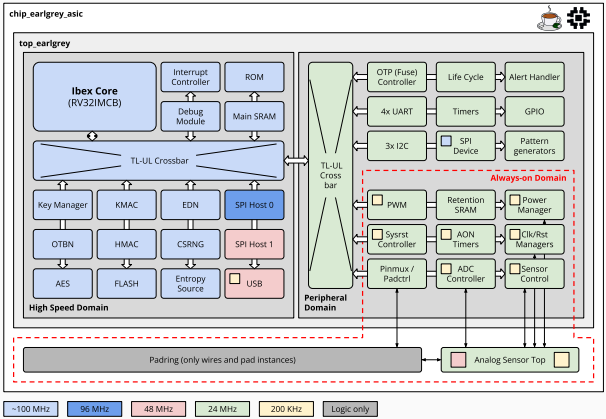


Figure 1: Overview OpenTitan Earl Grey [Ope23]

Target: OpenTitan

- Accelerator for SHA-3 and SHAKE

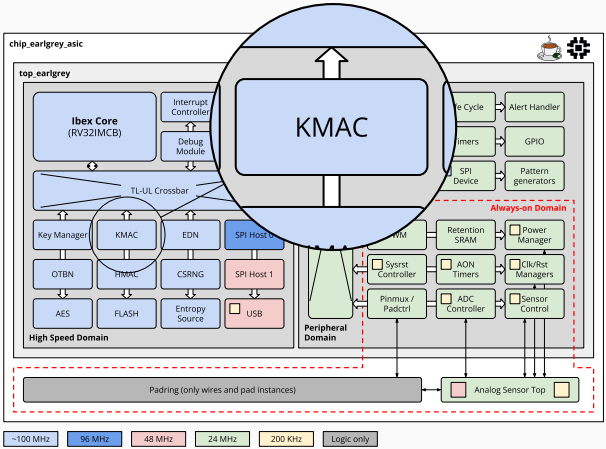


Figure 1: Overview OpenTitan Earl Grey [Ope23]

Target: OpenTitan

- Accelerator for SHA-3 and SHAKE
- OpenTitan Big Number

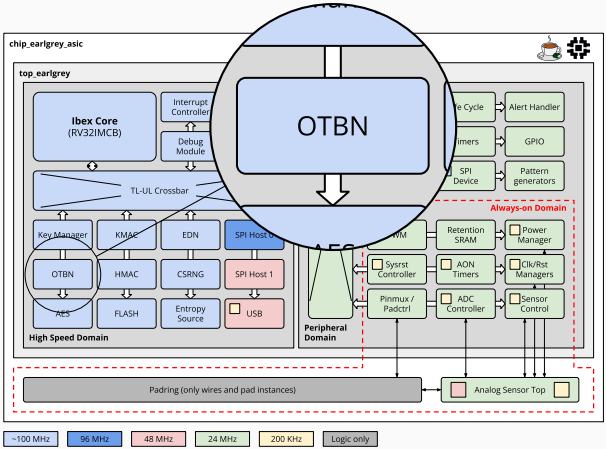


Figure 1: Overview OpenTitan Earl Grey [Ope23]

Target: OpenTitan

- Accelerator for SHA-3 and SHAKE
- OpenTitan Big Number
  - 32 256-bit registers

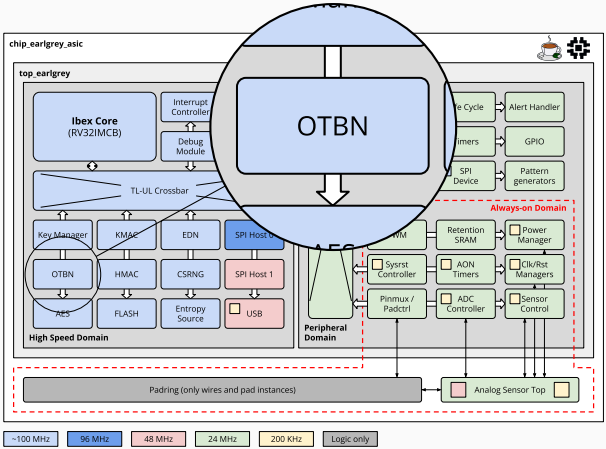


Figure 1: Overview OpenTitan Earl Grey [Ope23]

Target: OpenTitan

- Accelerator for SHA-3 and SHAKE
- OpenTitan Big Number
  - 32 256-bit registers
  - Reduced RV32I ISA

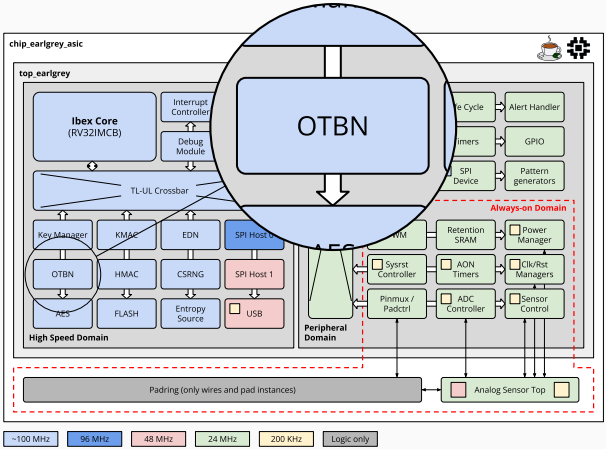


Figure 1: Overview OpenTitan Earl Grey [Ope23]

Target: OpenTitan

- Accelerator for SHA-3 and SHAKE
- OpenTitan Big Number
  - 32 256-bit registers
  - Reduced RV32I ISA
  - “Generic” big-number ISA for ECC & RSA

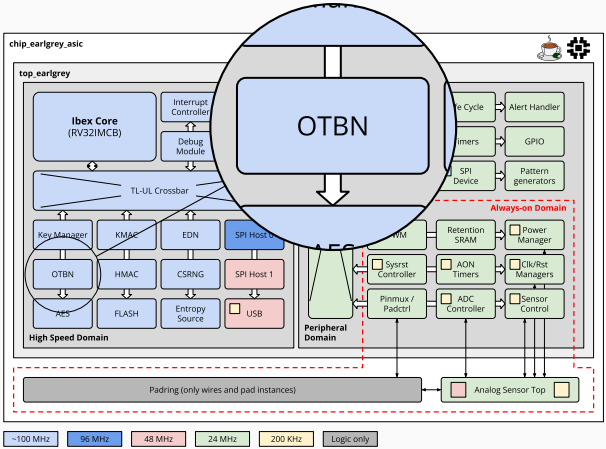
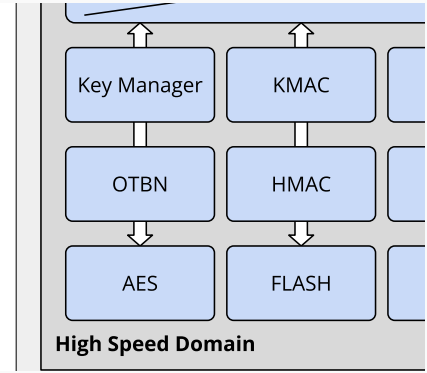


Figure 1: Overview OpenTitan Earl Grey [Ope23]

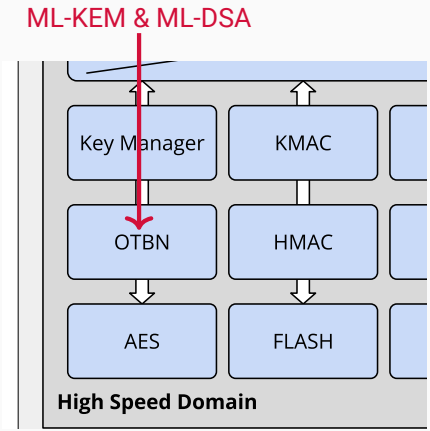
Our Contributions



Our Contributions

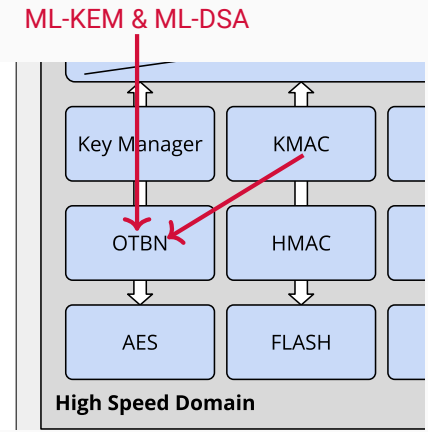
1. First implementation of **ML-KEM** and **ML-DSA** on unmodified[a] OTBN

[a] Enlarged memories required



Our Contributions

1. First implementation of **ML-KEM** and **ML-DSA** on unmodified[a] OTBN
2. Interface to **KMAC** accelerator

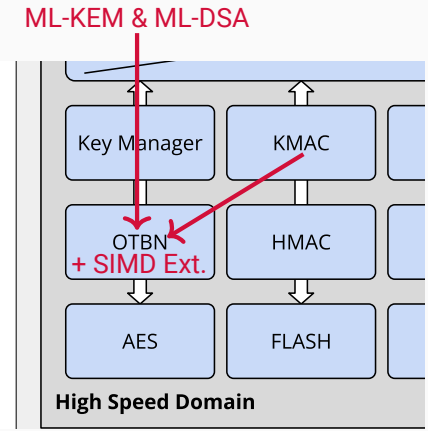


[a] Enlarged memories required

Our Contributions

1. First implementation of **ML-KEM** and **ML-DSA** on unmodified[a] OTBN
2. Interface to **KMAC** accelerator
3. ISA extensions to utilize wide registers using **SIMD** on OTBN
   → Applicable to ML-KEM and ML-DSA but also beyond

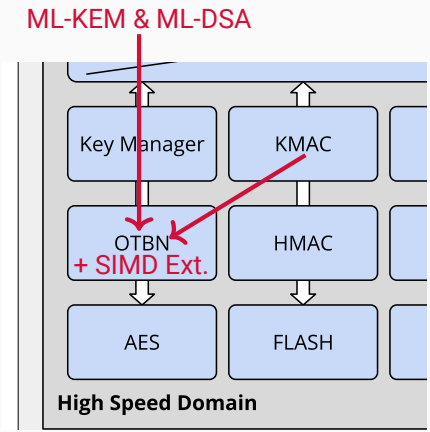
[a] Enlarged memories required



Our Contributions

1. First implementation of **ML-KEM** and **ML-DSA** on unmodified[a] OTBN
2. Interface to **KMAC** accelerator
3. ISA extensions to utilize wide registers using **SIMD** on OTBN
   → Applicable to ML-KEM and ML-DSA but also beyond
4. Hardware implementation maximizing **resource-sharing** with pre-existing components

[a] Enlarged memories required



Implementation: High Level Overview

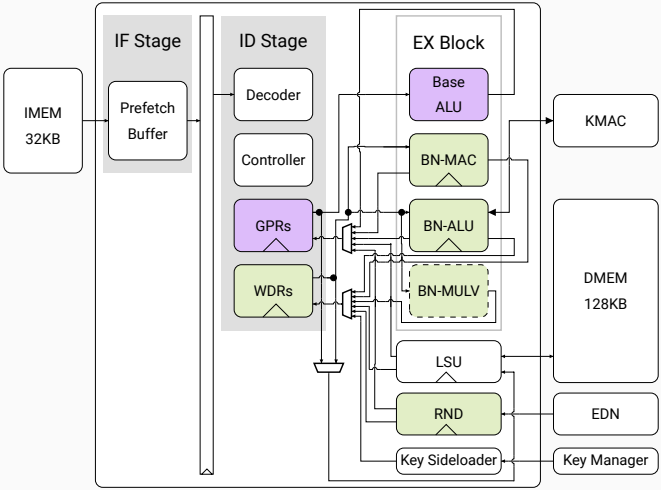


Figure 2: Simplified diagram of the modified OTBN pipeline.

Implementation: High Level Overview

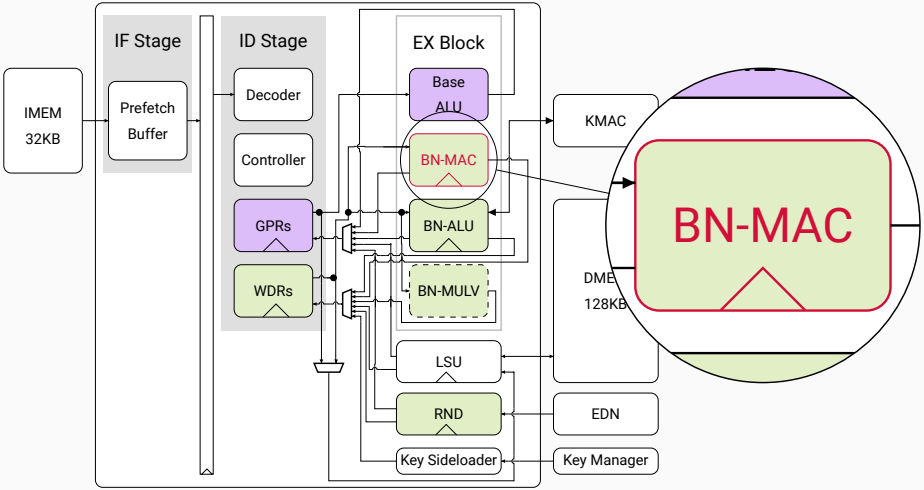


Figure 2: Simplified diagram of the modified OTBN pipeline.

Implementation: High Level Overview

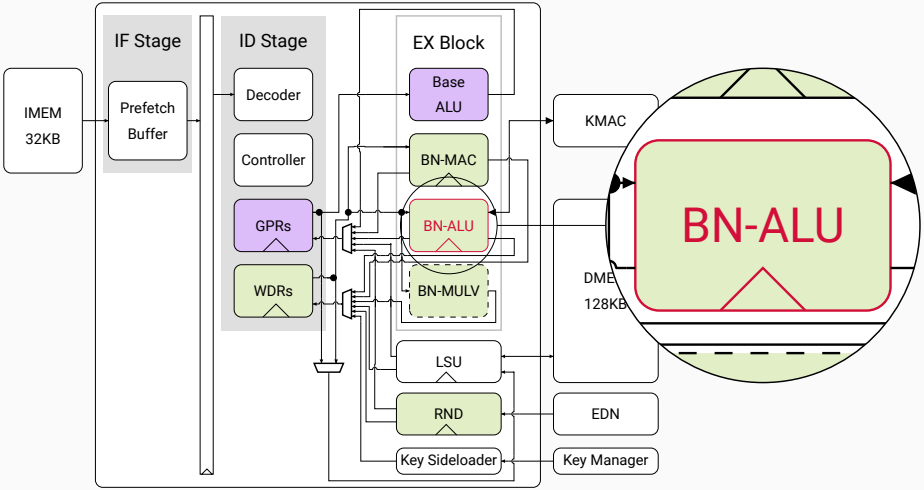


Figure 2: Simplified diagram of the modified OTBN pipeline.

Implementation: High Level Overview

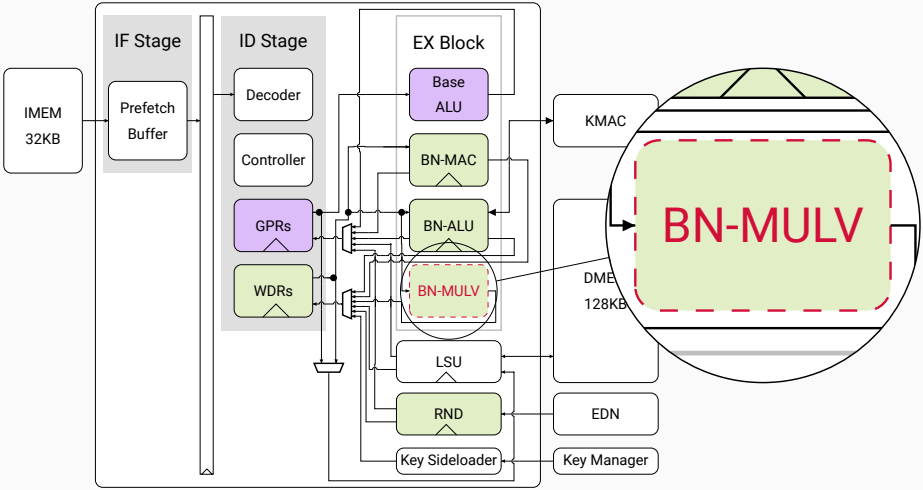
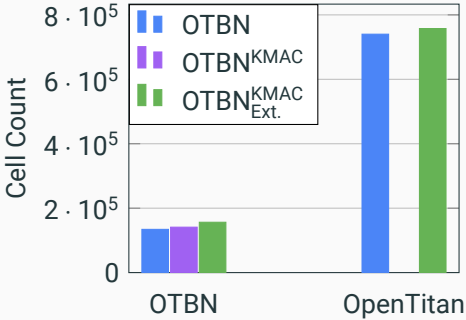


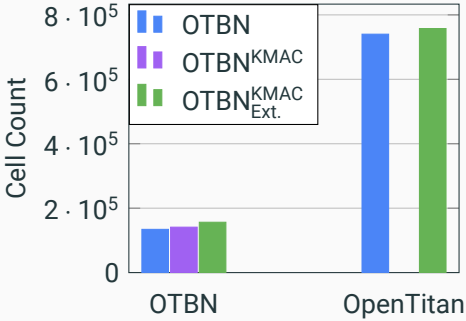
Figure 2: Simplified diagram of the modified OTBN pipeline.

Results

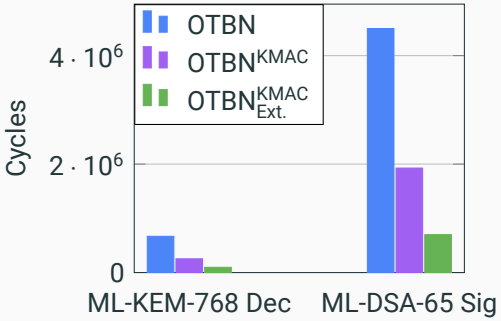


- Cell count-increase of $<$**17%** for OTBN
- Cell count-increase of $<$**3%** for OpenTitan

Results

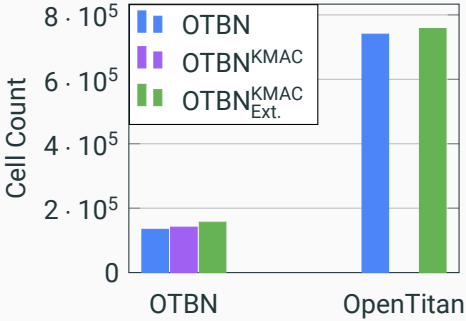


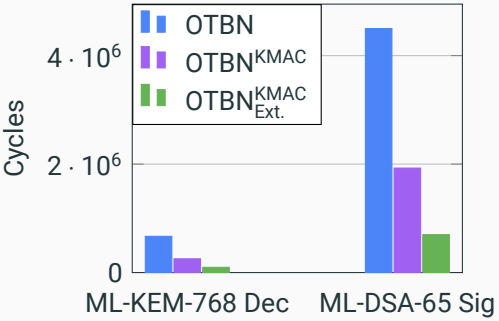
- Cell count-increase of $<$**17%** for OTBN
- Cell count-increase of $<$**3%** for OpenTitan



- Target Freq.: **6–9**$\times$ speedup for ML-{KEM,DSA}
- Max. Freq: **4–6**$\times$ net-speedup for ML-{KEM,DSA}

Results





- Cell count-increase of $<$**17%** for OTBN
- Cell count-increase of $<$**3%** for OpenTitan

- Target Freq.: **6–9**$\times$ speedup for ML-{KEM,DSA}
- Max. Freq: **4–6**$\times$ net-speedup for ML-{KEM,DSA}

$\rightarrow$ ML-KEM-768 Dec in 0.8 ms, ML-DSA-65 Sig in 7 ms @ Target Freq.

OpenTitan is Going PQC

ia.cr/2024/1192

github.com/PQC-OpenTitan/towards-ml-kem-and-ml-dsa-on-opentitan

opentitan.org

References

[App20] Signal App. ***Signal Logo.*** https://github.com/signalapp/Signal-Desktop/blob/87d6a55ce87a3f09e34da1dbc9e69f400ac7e32d/images/signal-logo.svg. 2020.

[Clo25] Inc. Cloudflare. ***Press Kit.*** https://www.cloudflare.com/press-kit. 2025.

[Com22] Zoom Video Communications. ***The logo of Zoom Video Communications - company responsible for the Zoom software.*** https://zoom.us/docs/doc/Zoom-logos.zip. 2022.

Bibliography ii

[Cor19] Mozilla Corporation. ***Firefox Logo*.** https://phabricator.services.mozilla.com/D41016. 2019.

[FSS20] Tim Fritzmann, Georg Sigl, and Johanna Sepúlveda. **"RISQ-V: Tightly Coupled Accelerators for Post-Quantum Cryptography".** In: *IACR TCHES* 2020.4 (2020), pp. 239–280. ISSN: 2569-2925. DOI: 10.13154/tches.v2020.i4.239-280. URL: https://tches.iacr.org/index.php/TCHES/article/view/8683.

[Gmb] Nitrokey GmbH. ***Nitrokey 3A NFC Hacker*.** https://shop.nitrokey.com/de/shop/nk3anh-nitrokey-3a-nfc-hacker-404.

[Goo22] Google. ***Google Chrome logo*.** https://www.google.com/chrome/static/images/chrome-logo.svg. 2022.

Bibliography iii

[Ope23] OpenTitan Team. ***Datasheet - OpenTitan Documentation.*** 2023. URL: https://opentitan.org/book/doc/introduction.html (visited on 12/10/2023).

[Res21] IBM Research. ***IBM Quantum System One in Germany for the Fraunhofer Institute.*** https://www.flickr.com/photos/ibm_research_zurich/51248690716/. 2021.

[SO25] Cyrus Stoller and Miguel Osorio. ***Fabrication begins for production OpenTitan silicon.*** https://opensource.googleblog.com/2025/02/fabrication-begins-for-production-opentitan-silicon.html. 2025.