An Introduction to the OpenTitan Project

G. Chadwick[1], M. Schaffner[2]

[1]lowRISC C.I.C. [2]lowRISC US

Abstract

OpenTitan[1] is an open silicon root of trust (RoT) being developed by a partnership of companies[1] stewarded by lowRISC C.I.C[2]. It comprises a number of cryptographic accelerator blocks; an entropy complex for the generation, conditioning and distribution of cryptographically secure random numbers; a number of standard peripherals (such as SPI, I2C, UART and USB) and a 32-bit RISC-V core (Ibex). In addition to being a state-of-the-art RoT, OpenTitan's open development methodology has the potential to revolutionize how silicon is developed and produced for RoT and secure microcontroller silicon and beyond.

Crucially the full development of OpenTitan is open. The live development repository is public on GitHub and it includes all RTL, testbenches and other DV (design verification) collateral such as test and coverage plans, documentation and software. Everything is made available under the permissive Apache 2.0 license.

The first discrete chip OpenTitan – codenamed Earl Grey – has taped out with engineering samples due back shortly and production planned for next year. Work is also ongoing on integrated variants, which involves OpenTitan technology being incorporated into both high performance chiplets and low power SoCs targeting smart cards, SIM cards and other embedded applications.

This talk presents a technical overview of OpenTitan, the security hardening employed, the benefits of open development and how interested parties can evaluate OpenTitan for themselves.

OpenTitan Technical Overview

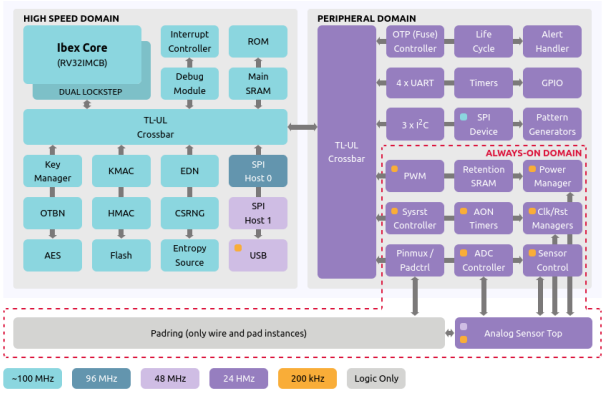

Figure 1: *OpenTitan Earl Grey*

OpenTitan Earl Grey is a secure microcontroller that can be used in a number of applications such as a platform integrity module or a trusted platform module.

Fig. 1 shows the overall structure of the OpenTitan Earl Grey discrete chip. It comprises over 30 IP blocks that have all been developed from scratch. A RISC-V 32 bit CPU core (the lowRISC Ibex core) runs the firmware to control the chip through the TileLink - Uncached Lite interconnect used to connect the blocks to the CPU.

The key security blocks are:

1. AES-128/192/256 with ECB, CBC, CFB, OFB, CTR modes
2. HMAC / SHA2-256
3. KMAC / SHA3-224, 256, 384, 512, [c]SHAKE-128, 256
4. Programmable big number accelerator for RSA and ECC (OTBN)
5. NIST-compliant cryptographically secure random number generator (CSRNG)
6. Digital wrapper for analog entropy source with FIPS and CC-compliant health checks
7. Key manager with DICE support
8. Manufacturing life cycle manager
9. Alert handler for handling critical security events
10. OTP, Flash, ROM and SRAM controllers with access controls and memory scrambling

The Earl Grey datasheet[3] in the OpenTitan documentation contains further details.

A mask ROM (hard-wired part of the chip design) contains the initial boot code and orchestrates a secure boot process with second stage boot code contained in flash. This in turn boots the main OS (also held in flash), in this case the Rust-based TockOS.

Comprehensive verification of the design has been performed to hit production silicon tape-out quality targets. Each block has its own test bench and associated tests. Additionally there is a significant (>300) set of top-level tests. A regular regression is run across all block-level testbenches and the top-level (close to 40,000 test runs total) with the results published [4] so anyone can determine the health of the project.

All of the blocks within Earl Grey have been developed under the *Comportable IP framework*[5] to allow them to be reused. In particular this allows the creation of different OpenTitan top-levels. With this capability OpenTitan integrated variants are undergoing development (and which will be made public once some initial goals are met).

[1] OpenTitan partners: Google, Rivos, Western Digital, Seagate, ETH Zurich, G+D, Nuvoton, Winbond, zeroRISC, lowRISC

Security Hardening

Significant work has been done on hardening against physical attacks, in particular to deter fault-injection and side channel attacks, with countermeasures implemented in open-source RTL and code. These complement proprietary countermeasures such as analog sensors and top-layer metal shields in a defense-in-depth strategy.

The AES and KMAC blocks utilize masking to deter side channel attacks by splitting secret values into shares derived from random numbers. The OTBN big-number accelerator can use software masking techniques and hardware blanking (where unused data and control paths are zeroed) to reduce power side channel leakage of secrets below an exploitable level. Extensive evaluation of the masking employed has been done using the Chip Whisper CW310[6] platform from NewAE[7] (a lowRISC company) along with formal techniques. Evaluation will continue with the real silicon.

For fault-injection resistance a number of techniques are employed. Extensive use is made of integrity checking with ECC codes (which protect all in-flight memory transactions as well as data at rest) and scrambling. Multi-bit encoding is utilized for various critical signals (such as enable signals for security mechanisms and finite state machine encodings) and the Ibex CPU core is implemented in a dual-core lock step configuration. Further bespoke techniques are applied in each block that are specific to that block's functionality. These techniques are enumerated in each IPs metadata description to ease verification and audit processes.

The Benefits of Open Development

Developing in the open has several key advantages. For instance, multiple organizations (potentially even commercial competitors) can easily come together to build technology that benefits them all. The diverse skill sets and experiences from those organizations can lead to solutions superior to technology developed by individual organizations in isolation.

Further, open development creates and fosters *transparency*, which is highly relevant in the security domain. Anyone can audit and evaluate OpenTitan all the way down to its RTL source code. As it has been developed from scratch they can also understand the *provenance*. An open design attracts a greater level of *scrutiny* and from an earlier point in the project (see work [8, 9] that has already helped improve OpenTitan before first silicon). Overall this produces greater *trust* in the design and resulting products.

The open design paradigm is not without its challenges - in particular for hardware there are issues around IP and certification that have to be navigated. For example, in Common Criteria Vulnerability Assessment (AVA), open RTL may receive less points for attack identification than non-public RTL. However, the OpenTitan project is well equipped to handle these challenges and we believe the cost of doing so is well worth it given the benefits gained.

Evaluating OpenTitan

There are a number of options open to those who wish to evaluate OpenTitan ahead of production silicon becoming available. Primarily, a) a full chip level simulation can be run using the open source Verilator[10] simulation (no paid-for license required) as well as commercial EDA simulators; and b) the NewAE CW340[11] is an FPGA-equipped emulation board that can fit the full Earl Grey design (and for which bitstream generation is supported by the project)

Author Biographies

Dr. Greg Chadwick is the digital design lead at lowRISC, where he has been for 4 years, with a total of 10 years experience in the silicon industry. He has worked on many parts of OpenTitan in particular doing major work on the Ibex core and the OTBN bignum accelerator. Previously to lowRISC he worked on CPUs at Arm and GPUs at Broadcom. He received his Ph.D from Cambridge University in 2011.

Dr. Michael Schaffner is a senior designer at lowRISC US. Previously, he has worked on OpenTitan and the TPU project at Google in California, and was a postdoctoral researcher at the Integrated Systems Laboratory at ETH Zurich, Switzerland. He received his MSc and PhD degrees from ETH Zurich in 2012 and 2017, where he has been a research assistant at the Integrated Systems Laboratory and Disney Research.

References

[1] *OpenTitan*. URL: https://opentitan.org.

[2] *lowRISC*. URL: https://lowrisc.org.

[3] *Earl Grey Datasheet*. URL: https://opentitan.org/book/hw/top_earlgrey/doc/specification.html.

[4] *OpenTitan DV Dashboard*. URL: https://opentitan.org/dashboard/index.html.

[5] *Comportable IP Framework*. URL: https://opentitan.org/book/doc/contributing/hw/comportability.

[6] *NewAE CW310 Board*. URL: https://rtfm.newae.com/Targets/CW310%20Bergen%20Board/.

[7] *NewAE*. URL: https://www.newae.com/.

[8] Andres Meza et al. "Security Verification of the OpenTitan Hardware Root of Trust". In: *IEEE Security and Privacy* 21.3 (2023), pp. 27–36.

[9] Pascal Nasahl et al. "SYNFI: Pre-Silicon Fault Analysis of an Open-Source Secure Element". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* (Aug. 2022), pp. 56–87.

[10] *Verilator*. URL: https://www.veripool.org/verilator/.

[11] *NewAE CW340 Board*. URL: https://media.newae.com/datasheets/NAE-CW340-OTKIT_datasheet.pdf.