Clash Formal

Ecosystem formally verifiable IT

Dr. Christiaan Baaij, **Dr. Felix Klein**

20.01.2025 – Kickoff

QBayLogic.
The key to FPGA-ASIC design

QBayLogic: Who we are?

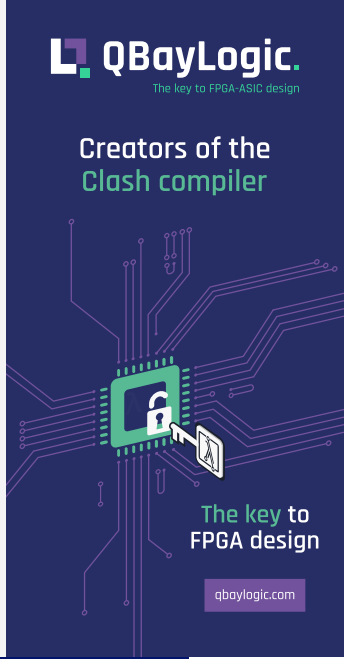
Member of CHIPTECH TWENTE

- Founded in 2016, a **spin off of Twente University**: research since 2009, Located in Enschede (Twente region, The Netherlands (East))
- Focus on innovative FPGA chip design: inventors of the **Clash Compiler**
- Headcount: from 2 (2016) to 20 (2025): project management, research, FPGA- & RTL design, (embedded) software and tool development

- Member of **ChipTech Twente**: a strong cluster of semiconductor-related companies in IT, electrical & mechatronic engineering, microelectronics, nanotechnology, photonics, quantum technology and microfluidics
- Participant of the Dutch Semiconductor Innovation mission 2023 to Japan and the Dutch Trade mission 2023 to the USA

QBayLogic: Our Expertise

- **FPGA based Development:**
  IP Design in VHDL, (System)Verilog, **Haskell/Clash**
- **ASIC Design:** RTL Development, Simulation
- **FPGA/ASIC Validation and Verification**
- **Systems-on-Chip:**
  QSys, IP-designer Vivado, IP-blocks, LiTex, RISC-V
- **Workflow Design & Setup:** CI / CD / CT
- **(Research related) Product Development:**
  from the idea to the first prototype
- **Project Planning & Management**



QBayLogic: Customers

Member of CHIPTECH TWENTE

AIRBUS

esa

AXIGN An MPS Company

Bronkhorst®

DEMCON

Myrtle.ai

TNO innovation for life

POSITRON

Haskell: more than just a programming language

- **Functional Language**
  - based on the lambda calculus
  - independent from any computer architecture specifics
- **Strongly Typed**
  - bugs can be catched even before running the program
  - properties can be expressed and ensured via the types
- **Research Use**
  - various papers, tools and research about (and using) the language
  - popular at universities (introductory courses to computer science)
- **Industrial Use**
  - *Meta, Microsoft, Standard Chartered, Tesla, Klarna, Galois, Serokell, ...*
  - popular for applications with strong safety and security requirements

Haskell: a versatile all-rounder

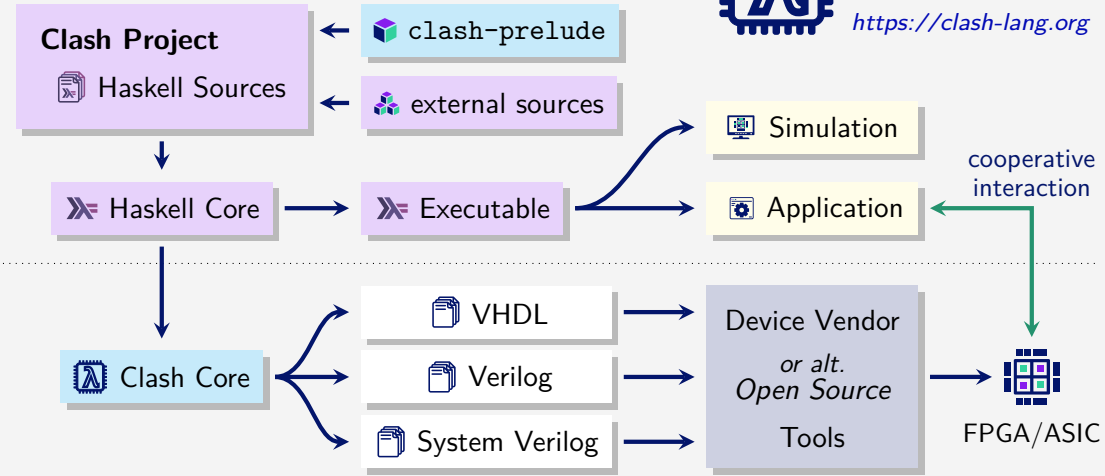
- **Web Frameworks:** IHP, Obelisk, Snap, Yesod, ...
- **Build & Package Management:** Cabal, Nix, Shake, ...
- **Embedded & Distributed Systems:** Ivory, Copilot, Cloud Haskell, sparkle, ...
- **Graphics & Music & Art:** Gloss, Diagrams, Haskore, Tidal Cycles, ...
- **Formal Verification**
  - Haskell has its own, built-in, type based constraint system
  - Correctnes Proofs / Proof Assistants: `hs-to-coq`, `agda2hs`, Haskabelle, ...
  - Refinement Types: Liquid Haskell
  - Automated Reasoning: `sbv`, `yices-painless`, ...
- **Hardware:** Bluespec, Lava, ForSyDe, **Clash**
- ...

Clash Compiler: Haskell → Hardware

Clash

A modern, functional, open source hardware description language

https://clash-lang.org

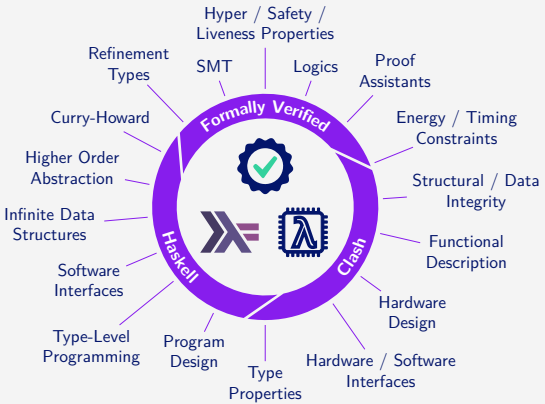


Clash Formal

Ecosystem formally verifiable IT

Project Goal

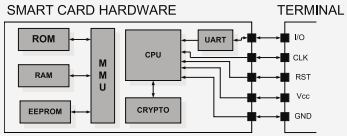
"The applicability of tools and methods for ***formal verification****, such as proof assistants or automated solvers, not only for functional program verification, but in the same extend for checking* ***functional circuit designs*** *in Haskell / Clash."*



What does this mean in particular?

- **Research Questions (50%):**
  - To which extend can we reuse the existing solutions for software verification in Haskell to also verify hardware designs in Clash?
  - To which extend can we utilize the type system of Haskell to describe the properties to be verified?
  - Can the properties that are specificed this way be shared and used in a cooperative manner between the hardware and the software, running on that particular hardware in the end?
- **Development (50%):**
  - Extension of the existing Clash compiler / ecosystem with user friendly tools for the construction of formally verified designs (open source).
  - Smart Card Demonstrator (open source)

Smart Cards

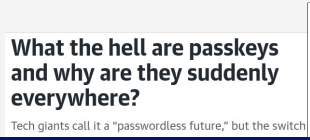


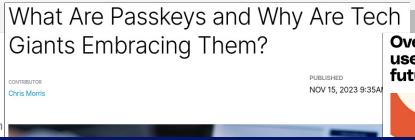
- dedicated hardware tokens for security relevant data management (passwords, identities, ...)
- hand-held mini-computer:
  CPU, memory, crypto core, custom operating system
- various applications & interfaces
- open standards:

fido ALLIANCE

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

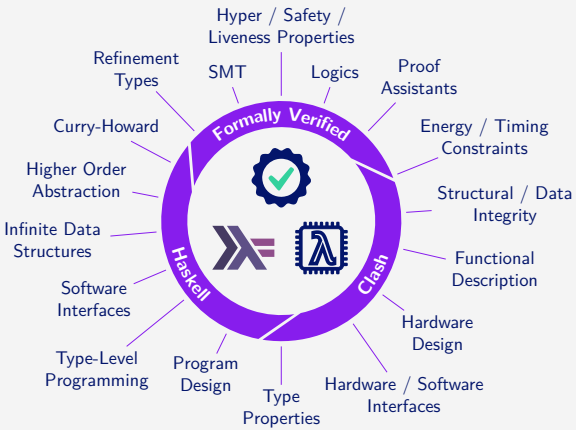
- **Passkeys** will be the technology of the future!





Clash Formal

Ecosystem formally verifiable IT



Clash

A modern, functional, open source hardware description language

https://clash-lang.org