Inventas Technical Review

- Lokotech ASIC designers have completed a full cycle industry standard SPICE simulation run
- Investas has reviewed the SPICE simulation run and concluded:
  - "The report indicates that the relative differences between the cases is presented correctly. Thus, it is fair to state that the results presented in the report gives a good indication of the expected benefits of the updated hash function".
- Inventas was established in 1997 and originated from the NTNU and SINTEF communities in Trondheim
- Completed more than 3.000 projects for their customers
- For information about Inventas, see: www.inventas.no

INVENTAS

Review of Salsa20/8 Simulation Report

Background
Lokotech has used a third-party company to perform a comparison between their suggested implementation of the Salsa20/80 hash function and an older version of the same function. This document is an evaluation of the work and findings presented in their report.

Findings
Received document:

- Lokotech Simulation Report 20191115

The report describes the assumptions and background for the simulations as well as their findings.

Simulations of Lokotech's Verilog design was compared to simulations of an existing Verilog design of the Salsa20/8 hash function. The same test data sets were used for simulating both implementations. Power simulations were based on synthesized versions of the two designs.

The performance numbers for speed and efficiency are impacted by assumptions, simplifications and the quality of the simulation models. However, the report underlines measures taken to reduce the impact of inaccurate models:

- Much effort that has been put into making the two design cases comparable.
- The same SRAM memory design was used for both simulations
- The results are presented as a ratio relative to the old architecture.

The report states that further efficiency improvements can be obtained by using a low-power library. This is a credible statement but will most likely not benefit the new function more than the old implementation.

Conclusion
The report indicates that the relative differences between the cases is presented correctly. Thus, it is fair to state that the results presented in the reports gives a good indication of the expected benefits of the updated hash function.