Practical Evaluation of Correlated GGM Trees in FAEST Vector Commitments



In the ongoing NIST competition for standardizing additional Post-Quantum digital signatures, one of the most promising candidate is FAEST. It is instantiated by using only symmetric cryptography primitives in the Vector Oblivious Linear Evaluation in-the-Head (VOLEitH) paradigm, a zero-knowledge proof technique inspired by secure multi-party computation. Thanks to this design, FAEST achieves competitive signature and public key sizes, while relying on well-established symmetric primitives, and it has recently been updated to version 3.

One of FAEST's main building block is a batched all-but-one vector commitment (BAVC) constructed using a large Goldwasser-Goldreich-Micali (GGM) tree, whose generation requires a significant number of hash calls. A recent paper [1] proposed BACON, a new BAVC construction based on correlated GGM trees. By reducing the number of primitive calls required to generate the tree, BACON is expected to improve the efficiency of the commitment scheme and, potentially, that of FAEST. However, the authors provide only a theoretical performance analysis and do not include an implementation, thus casting shadows on its practical performance.

The objective of this thesis is to implement BACON and evaluate its practical performance against the BAVC used in the FAEST reference implementation [2]; afterwards, the student will assess if BACON is suitable for deployment in secure cryptographic implementations and investigate whether its design introduces additional attack surfaces compared to the BAVC baseline. In order to reach these goals, the student will first study the FAEST scheme, BACON, and the relative literature. If feasible within the available time, the implementation will be integrated into FAEST v3 to evaluate its effect on complete signature generation. The student is expected to be familiar with either C or RUST.

Practicalities

Promotor:	Prof. Dr. Ir. Vincent Rijmen		
	Dr. Svetla Nikova		
Daily supervisor:	Dilara Toprakhisar	dilara.toprakhisar@esat.kuleuven.be	office B01.05
	Sina Bagheri	sina.bagheri@esat.kuleuven.be	office B01.11
	Andrea Natale	andrea.natale@esat.kuleuven.be	office B01.11
Nature of the work:	40% literature, 10% theoretical work, 50% software		
Number of students:	1		

[1] https://ieeexplore.ieee.org/abstract/document/11354736
[2] https://github.com/faest-sign/faest-ref

 © 2026 – 2027 COSIC