Private IoT Data Collection with Threshold Ascon



Image generated using Gemini.

Context. Wearables, smart meters and other small devices collect sensitive data about their users. In conventional system designs, data is encrypted on-device for a cloud service to decrypt and analyse it. Whoever controls the server controls the data (and key). Threshold cryptography removes this weak spot: the key is split over several servers that decrypt jointly, and no single server ever sees the key or the plaintext. NIST is exploring such schemes[1] and asks for threshold versions of its standards - like the lightweight cryptography family Ascon, built for exactly these small devices.

Problem. We have shown how a committee of servers can jointly run Ascon on secret-shared data[2]. The catch is speed over a real network: Ascon processes a message block after block, and in secret-sharing MPC every step costs a round of messages between the servers, so one small message takes thousands of round trips. Garbled circuits compute on hidden data in a constant number of rounds, however long the message. Whether this makes threshold Ascon practical, and how it then compares to the widely deployed AES-GCM, has not been measured thus far.

Goal. The goal of this thesis is to evaluate Ascon-AEAD128 as a garbled circuit and measure it against our secret-sharing implementation and an AES-GCM baseline, in circuit size, bytes sent and wall-clock time over LAN and emulated WAN links. You start from our Ascon circuit, test vectors and benchmark scripts in the MP-SPDZ framework. Time permitting, Ascon-Hash256, security against malicious servers, or a second framework can be added.

Profile. Scoped for the 15-ECTS MANAMA thesis. Required: interest in privacy and/or cryptography, a first course in cryptography and comfort with Python (MP-SPDZ circuits are written in a Python dialect); C++ helps for a second framework. No MPC background needed: if you follow most of the paper linked in footnote 2, you are a good fit. You gain hands-on experience with garbled circuits, MPC frameworks and performance measurement.

Practicalities

Promotor:	Bart Preneel		
Daily supervisor:	Peter Schwarz	peter.schwarz@esat.kuleuven.be	office B01.21
	Aysajan Abidin	aysajan.abidin@esat.kuleuven.be	office 01.13
Nature of the work:	30% literature, 15% theoretical work, 55% software		
Number of students:	1		

[1] https://doi.org/10.6028/NIST.IR.8214C
[2] https://doi.org/10.1145/3733802.3764050

 © 2026 – 2027 COSIC