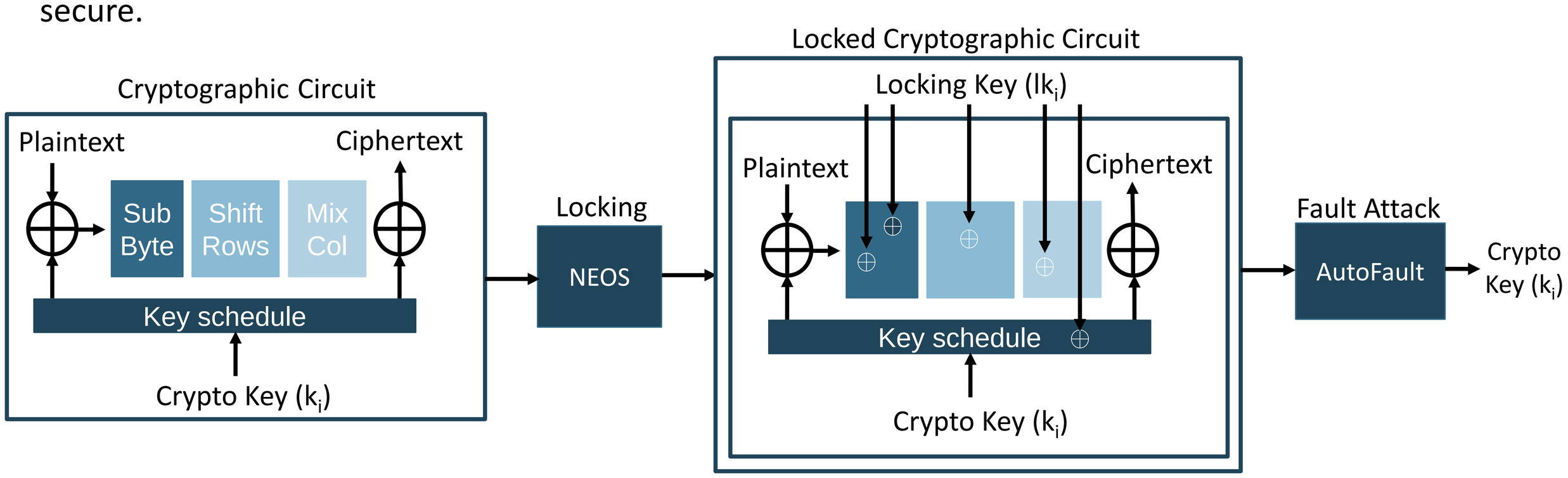
Towards Secure Composition of Logic Locking and Fault Attack Resistance

Devanshi Upadhyaya, Ilia Polian

Universität Stuttgart

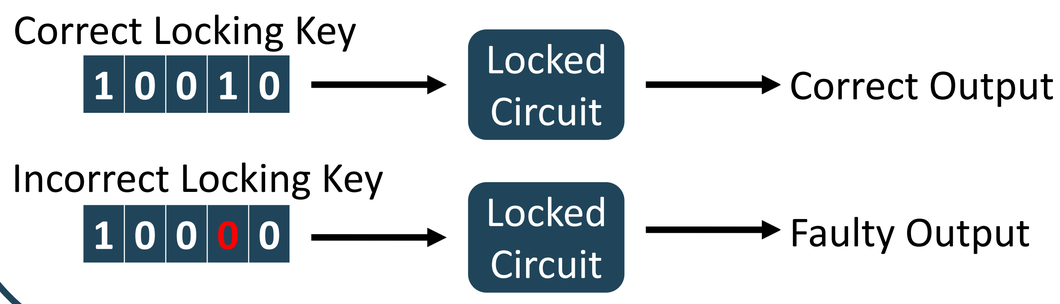
Motivation

- Cryptographic circuits need to be protected against both: physical attacks and supply-chain threats.
- Logic locking: Popular supply-chain protection against supply-chain threats like IP piracy, overproduction, counterfeiting, reverse engineering.
- Can logic locking make a crypto implementation more vulnerable against fault attacks?
- Intuition: A circuit with wrong locking key implements a function that might not be cryptographically secure.



Background on Logic Locking

- A simple locking technique[1] protects a combinational circuit using an n-bit locking key.
- To do this, n new XOR/XNOR gates are introduced
  - We select n wires and match them with the key bits.
  - For each selected wire, it's driver is disconnected from the sink and either an XOR or an XNOR gate is inserted.
  - The choice of an XOR or an XNOR gate depends on the chosen value of the matched key bit.
- A locked circuit will not generate correct output unless activated using the correct key.



Locking Assisted Fault Attack

- We use a tool NEOS[2] from University of Florida to lock a cryptographic circuit.
- Attack Scenario:
  - Use the cryptographic circuit with an incorrect locking key to perform "encryption".
  - Repeat with and without a fault injection.
  - Solve for the cryptographic key using faulty/fault-free ciphertexts.
  - Use algebraic fault-attack (AFA) framework AutoFault[3] from Universities of Stuttgart and Freiburg.
- The success rate depends upon the applied locking method.
- The secret cryptographic key can be derived with,
  - A simple locking technique: random insertion of locking gates and
  - Modification of the locking key.

References

1. J. A. Roy et al, "EPIC: Ending Piracy of Integrated Circuits," *2008 Design, Automation and Test in Europe*, Munich, 2008, pp. 1069-1074, doi: 10.1109/DATE.2008.4484823.
2. K. Shamsi et al, "NEOS". Available at: <https://bitbucket.org/kavehshm/neos/src/master/> [Accessed 31 August 2020].
3. M. Gay et al, "Hardware-Oriented Algebraic Fault Attack Framework with Multiple Fault Injection Support,"*2019 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, Atlanta, GA, USA, 2019, pp. 25-32, doi: 10.1109/FDTC.2019.00012.