

Remote Activation of Integrated Circuits for Piracy Prevention and Digital Rights Management



Miodrag Potkonjak (UCLA); Farinaz Koushanfar (Rice U); John Lach (U of Virginia)
www.cs.ucla.edu/~miodrag; www.ece.rice.edu/~fk1; www.ece.virginia.edu/~jcl7d

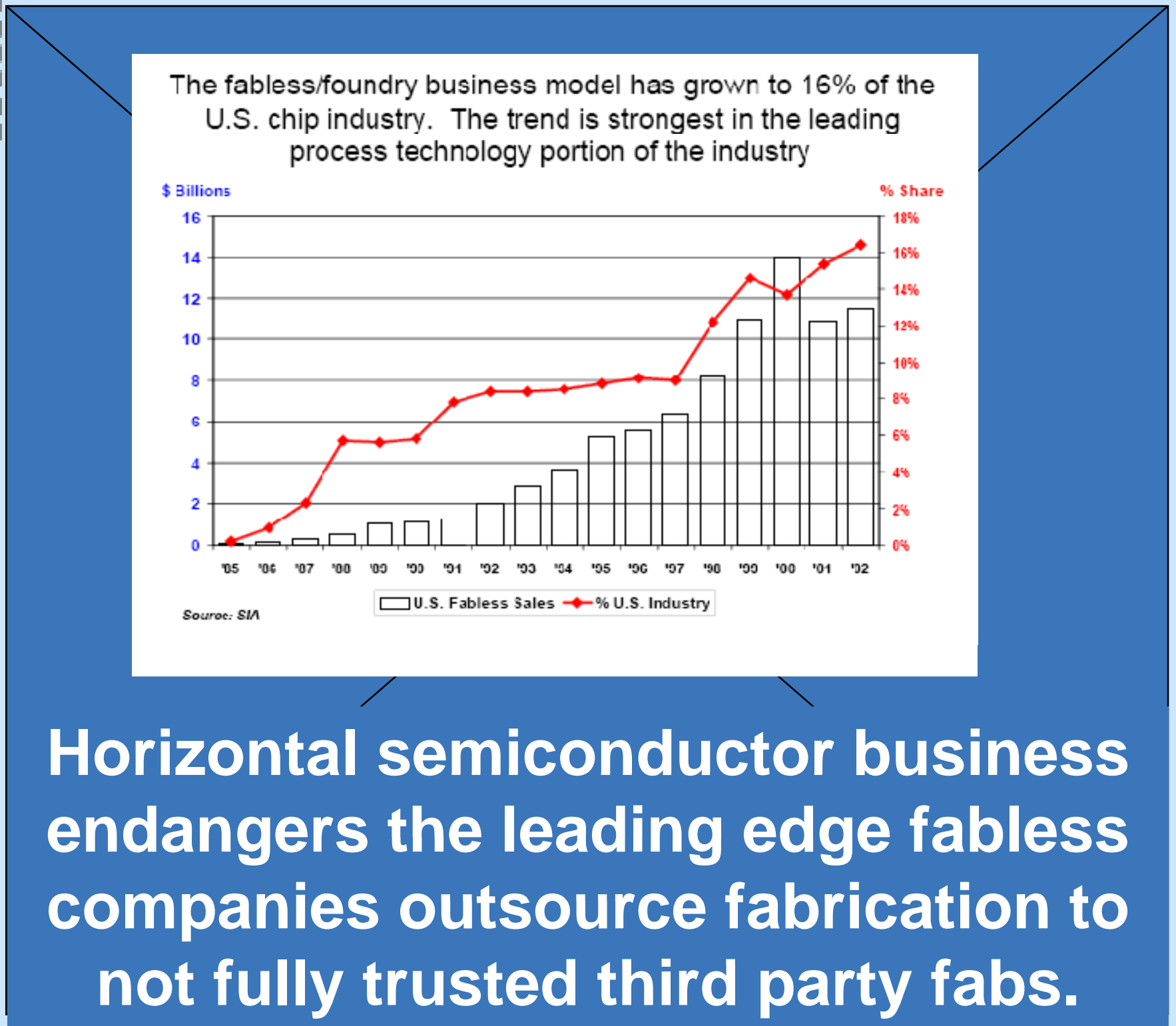
Manufacturing Variability (MV)-based Security and Protection

New generation of hardware-based security and protection techniques based on MV are emerging. Security HW based on digitally stored keys are subject to side-channel and physical attacks. MV identification is unclonable and resilient against physical and side-channel attacks.

- We introduce novel remote activation method for protecting IC intellectual property against tampering and piracy
- Each working IC is uniquely locked and can be remotely enabled/disabled
- The method uses: (1) inherent unclonable MV identification; and (2) Integration of the unique identifiers into the chip's functionality



Integration of unique IDs into the design's functionality enables a spectrum of exciting new applications, including N-variants; IP, SW, and data metering; and on-demand licensing.



Horizontal semiconductor business endangers the leading edge fabless companies outsource fabrication to not fully trusted third party fabs.

Approach and Impact

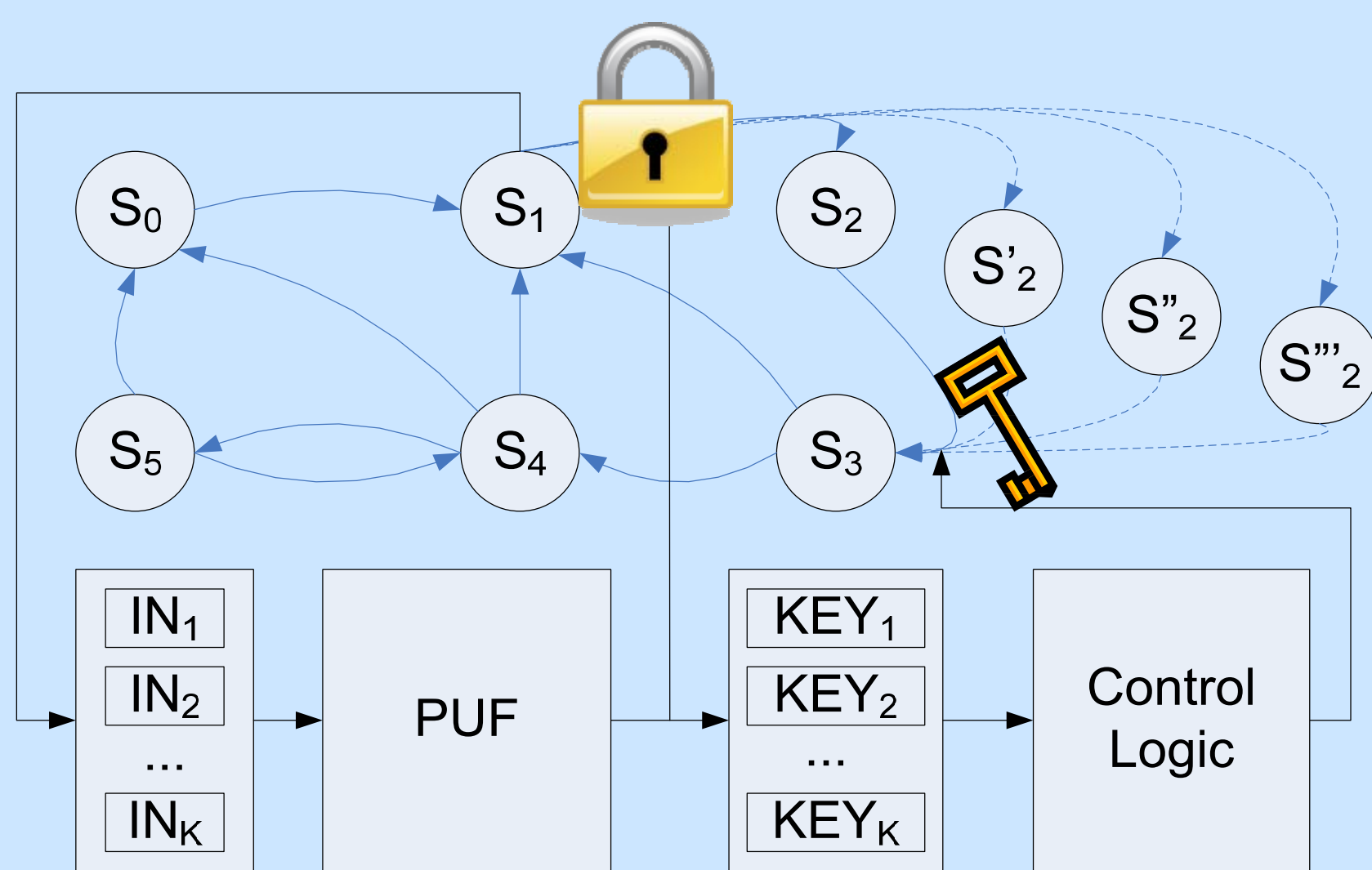
New approach

- The design files are sent to the fab
- Fab manufactures the parts, applies tests, and sends the output to designer
- Designer uses it's unique knowledge to compute the proper key for each IC
- Key stored on the IC & always checked

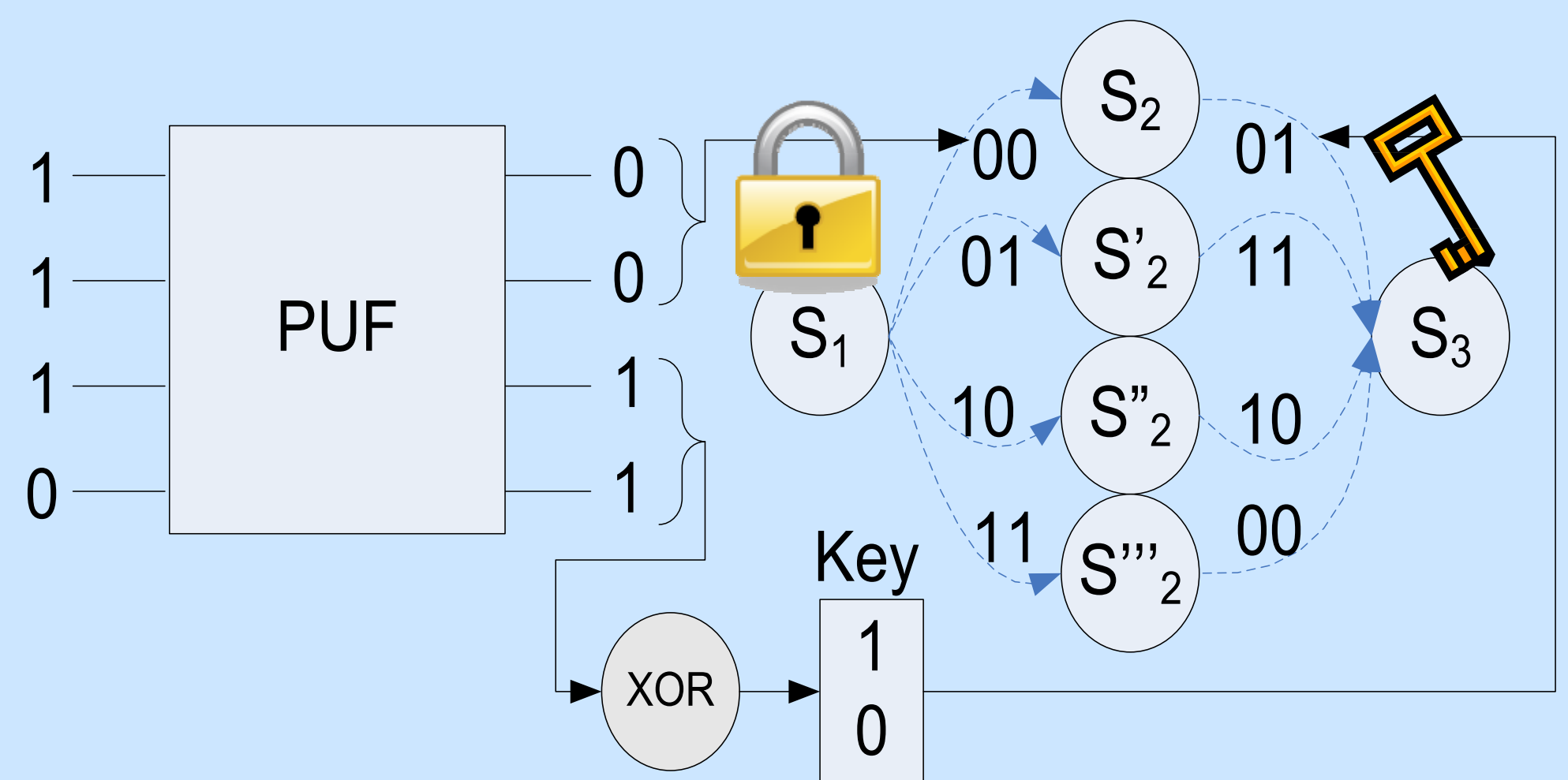
Research Impact

- The first continuous IC authentication
- Merging manufacturing variability with the functionality
- Attacks on the scheme addressed and countermeasures provided
- Low timing overhead on benchmarks

Technical description: A few states of the finite state machine (FSM) of the design are replicated and control mechanisms are added to the state transitions. A physically unclonable function (PUF) is used to create the MV-based unique IC identifiers. MV-based continuous lock/checking in action:



FSM with a lock on a replicated state (S_2), unique locking is done by the PUF.



Close-up view of the remote locking/unlocking and continuous checking.