ECE 459/559
Secure & Trustworthy Computer Hardware Design

External Active Metering

Garrett S. Rose
Spring 2017

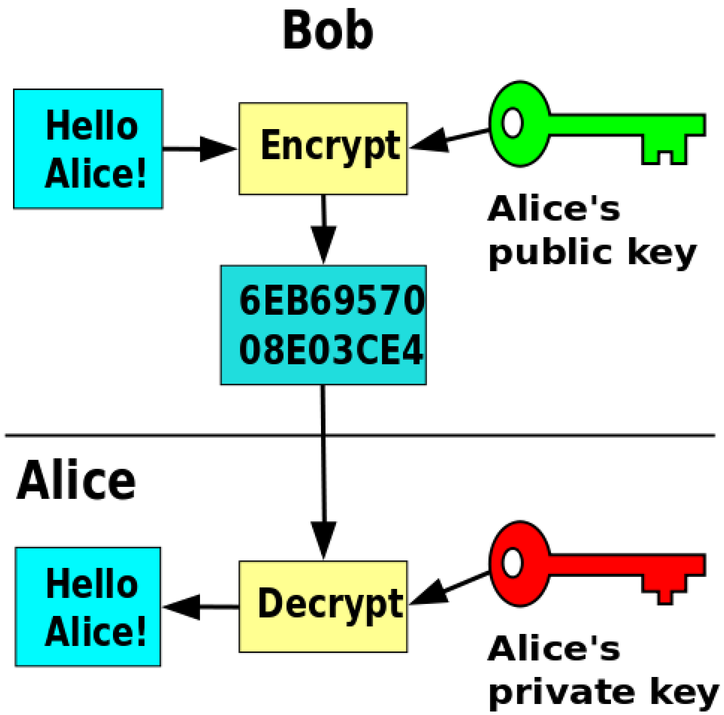
THE UNIVERSITY OF
TENNESSEE
KNOXVILLE

External Active Metering

- External asymmetric cryptographic techniques lock IC
- Cryptographic circuits rely on public and private keys to give IP owner control over activation/correct function
- Only IP owner knows private key to unlock IC functionality or testability

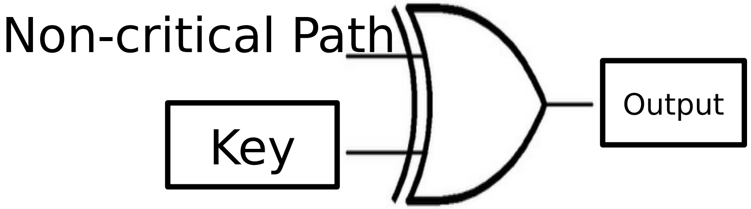
Background: Public Key Cryptography

- Uses two large prime numbers p & q to generate co-prime n=pq
- Private (d) and public (e) keys based on n, p & q calculated
  - (e, n) shared, used to encrypt message
  - Decryption can be done using (d, n)
- Security relies on magnitude of prime numbers p & q

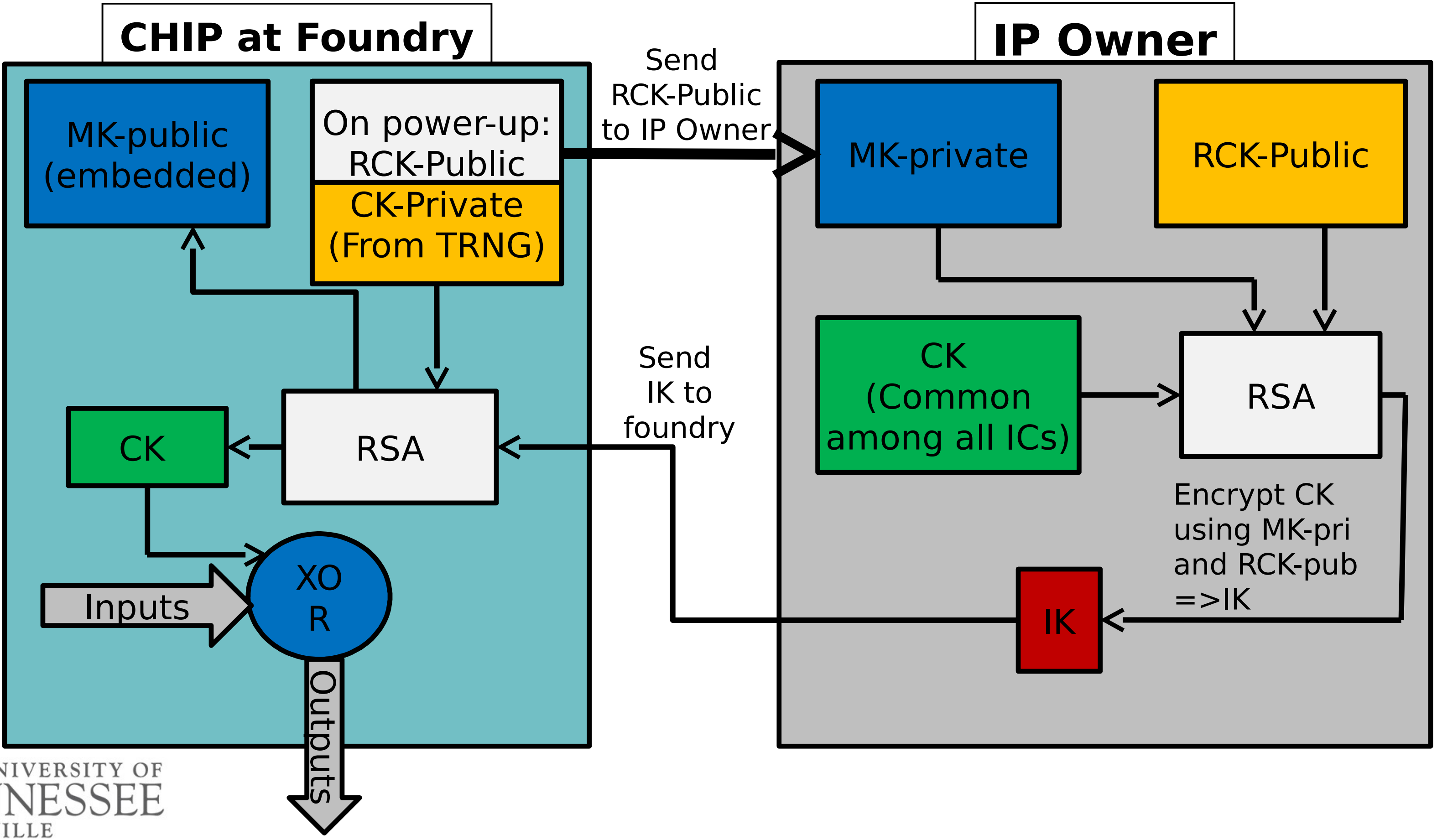


EPIC: Ending Piracy of Integrated Circuits

- Technique allows IP owner to have control over number of chips activated
- Uses public-key encryption to lock correct functionality of chip
- At gate level, XOR gates placed on selected non-critical paths
- Requires every chip be activated with external key
  - Only IP owner can generate key



EPIC High Level



EPIC

- Embedded in RTL as public Master Key (MK-Pub)
- XOR gates are controlled by Common Key
- Correct Common Key unlocks circuit's correct functionality
  - k XOR gates need a common key of length k
- TRNG (True Random Number Generator) used to generate Random Chip Keys (RCK) on start up
  - Upon power-up, each chip generates pair of private and public RCKs (RCK-private, RCK-public) which are burned into fuses
- Fab sends RCK-public to IP owner

EPIC

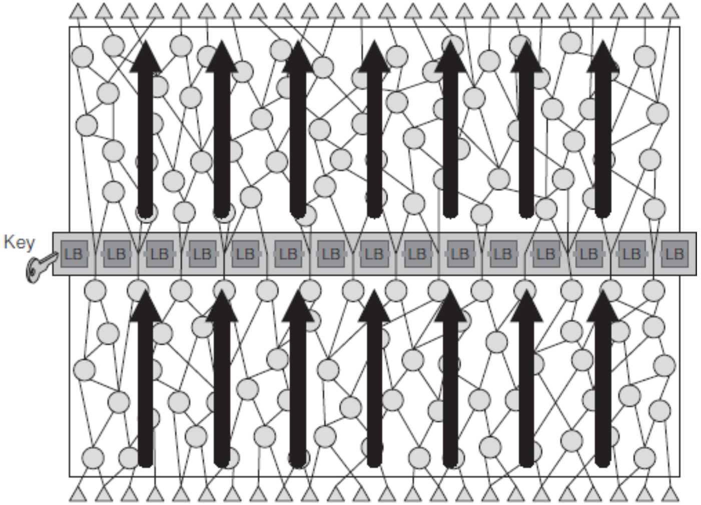
- IP owner generates Input Key (IK) by encrypting Common Key (CK) with MK-private and RCK-public
- IP owner sends Input Key to Fab
- When entered into chip, IK is decrypted using RCK-private and MK-public
- CK is obtained after decrypting which unlocks chip's correct functionality

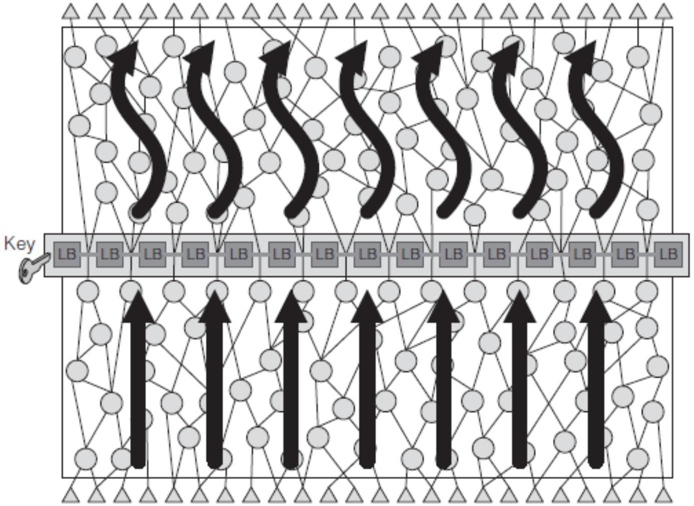
Analysis of EPIC

- Effective against cloned ICs
  - Due to TRNG, each IC has unique random key, even cloned ICs
  - ICs need IK to be functional which only IP owner can generate
- Not efficient for overproduced, out-of-spec and defective ICs
  - Overproduced:
    - Fab could claim low yield, request more IKs than needed
    - IP owner has no way to verify yield
    - Foundry can still send keys to IP owner – keys randomly generated, have no information on functionality of IC
  - Out-of-spec:
    - Foundry/assembly can send out chips that are out-of-spec
  - Defective:
    - Once IP owner sends Input Key, chip is activated
    - IP owner has no more communication with fab & chip already activated

Reconfigurable Logic Barriers (LB)

- Separates inputs from outputs such that every path from input to output passes through a barrier
- Logic barrier is a group of logic that allows correct path only if correct key is applied





Reconfigurable Logic Barriers (LB)

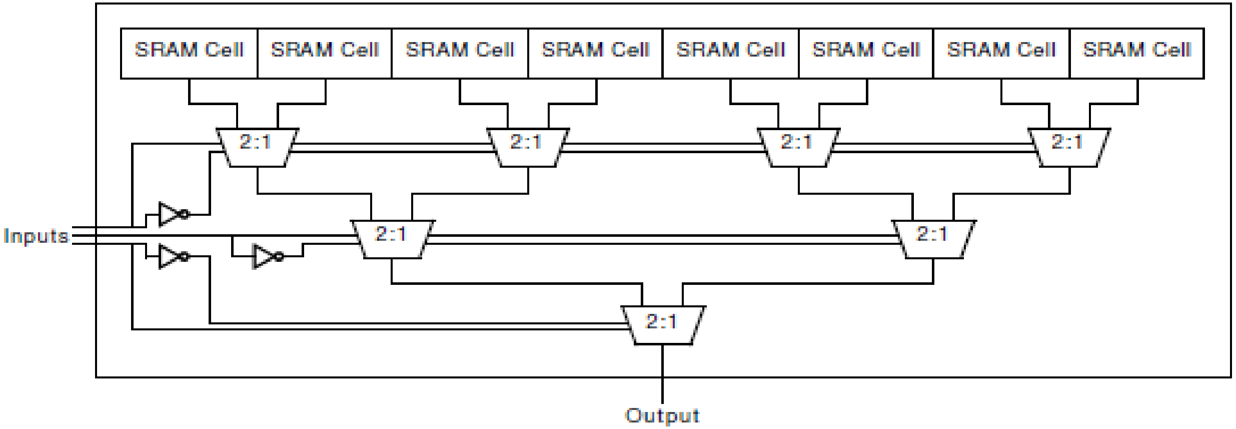
- IP owner decomposes IC functionality into F_{fixed} and $F_{reconfig}$
- F_{fixed} is given to foundry to fabricate
- $F_{reconfig}$ is location of reconfigurable logic in combination with key needed to configure them correctly
- $F_{reconfig}$ can be programmed into reconfigurable locations using a secure key

LB: Public Key Cryptography

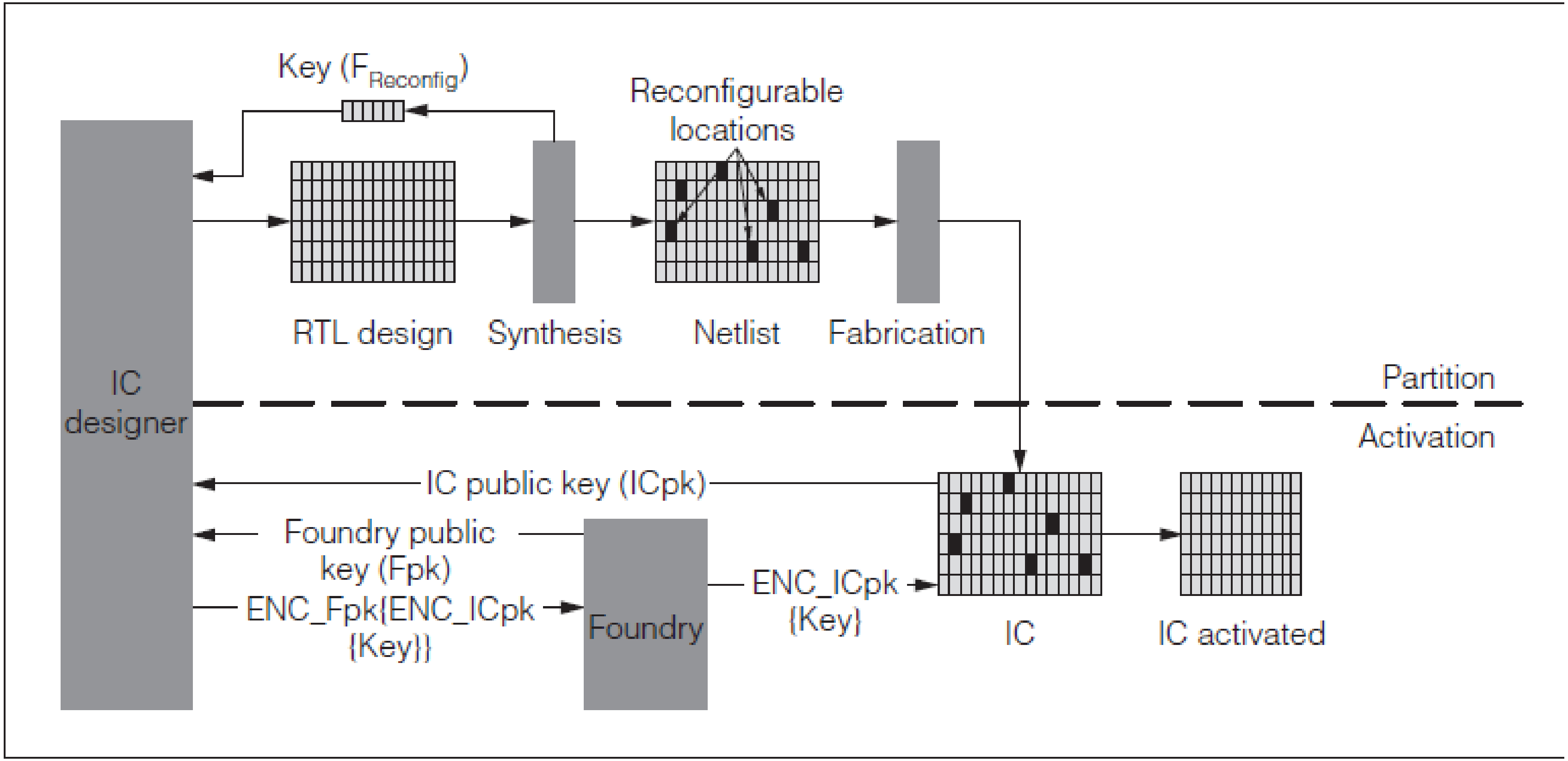
- ICs use PUFs and TRNGs to generate private and public keys
  - Public key from chip is sent to IP owner
- IP owner uses public key and its own private key to encrypt unlocking key
  - Encrypted key is decrypted on chip using IP owner's public key and chip's private key

LB: Unlocking Framework

- k-input LUTs used for logic barrier combinational locking
  - LUTs preferred over XOR gates due to their exponential number of locking combinations
  - k inputs, 2^k possible combinations
- Location of LUT based on observability and controllability



LB: Partitioning of Design

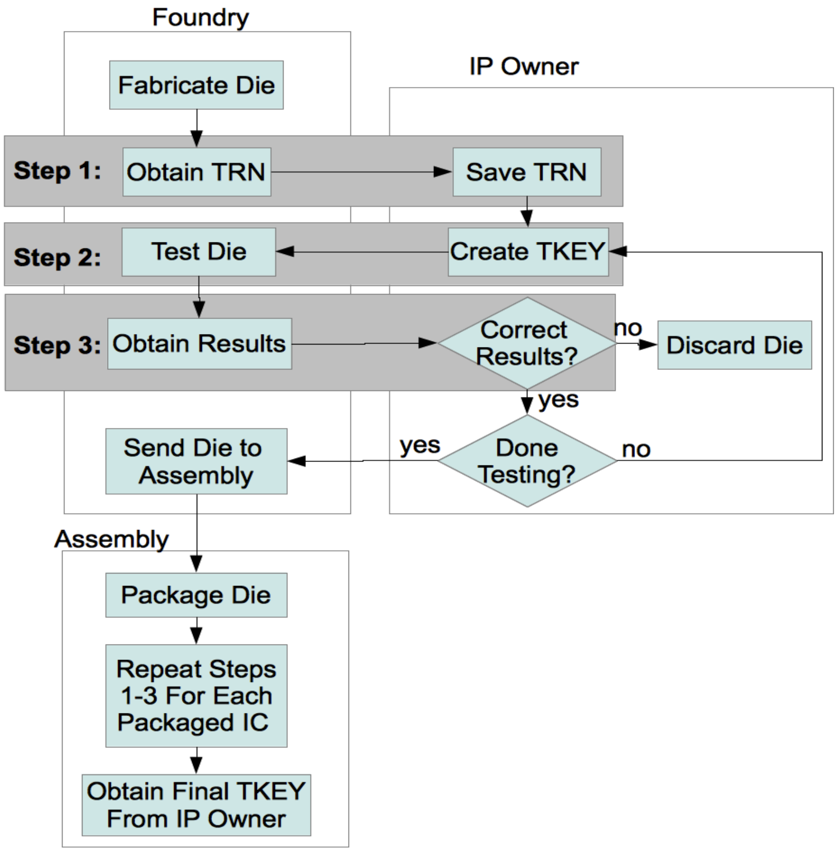


Logic Barriers Analysis

- Effective against cloned ICs
  - Chips only functional if correct keys entered which only IP owner can provide
- Ineffective against over-produced, defective and out-of-spec ICs
  - Foundry can lower yield to receive additional keys
  - Key generated by chip does not have information about its functionality (once key applied, it is functional)
- Other disadvantages:
  - Look up tables require significant area overhead – 5x more than XOR gates, timing overhead also major consideration

Secure Split-Test (SST)

- Adds multiple layers of communication between IP owner, foundry and assembly
- Ensures IP owner will know exactly how many chips pass test and how many failed
- Only chips that IP owner has deemed functional given a functional key



THE UNIVERSITY OF TENNESSEE KNOXVILLE

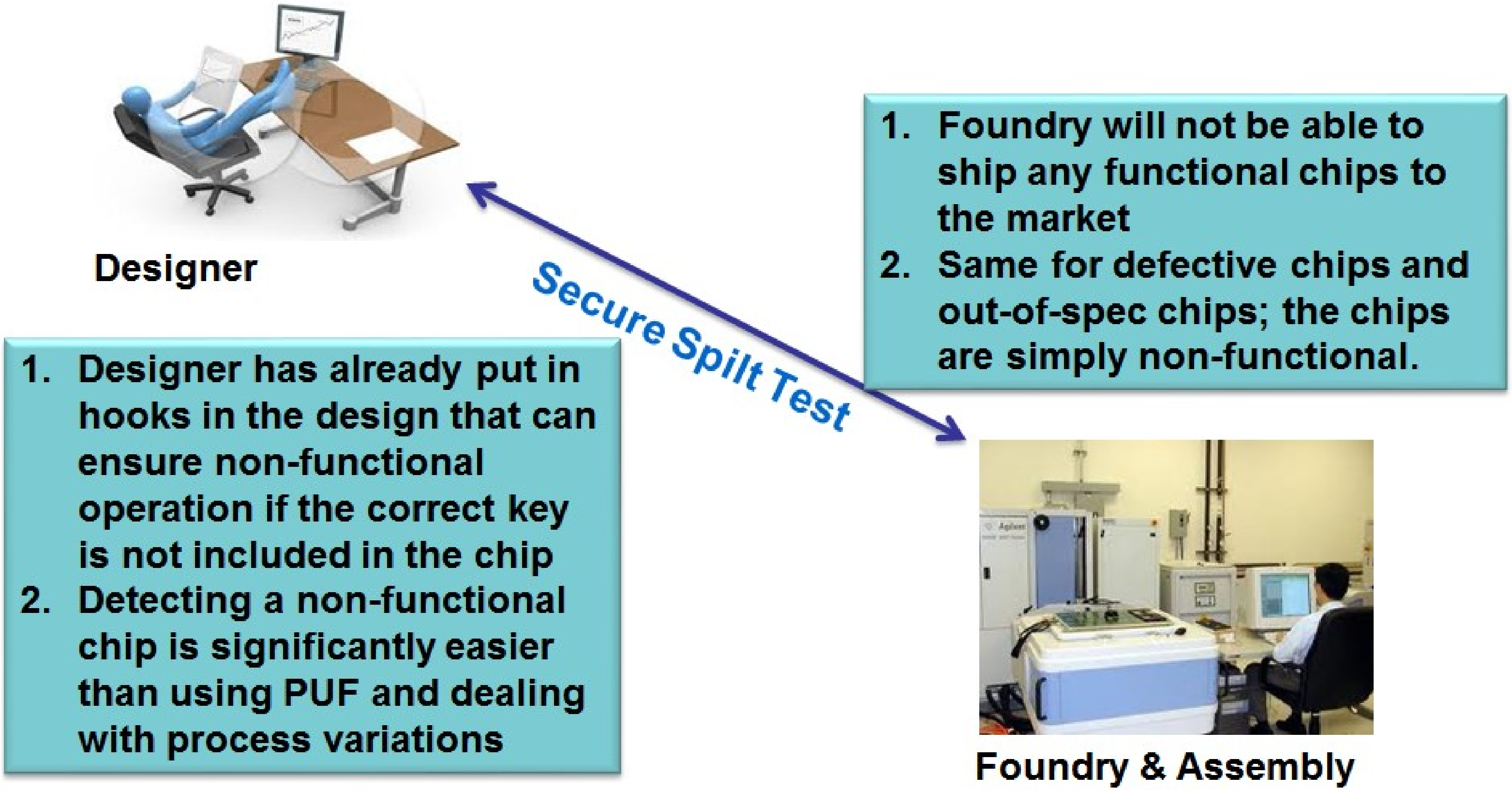
Traditional Test

Designer

Test Patterns
Test Responses

Foundry & Assembly

Secure Split-Test



Designer

Secure Spilt Test

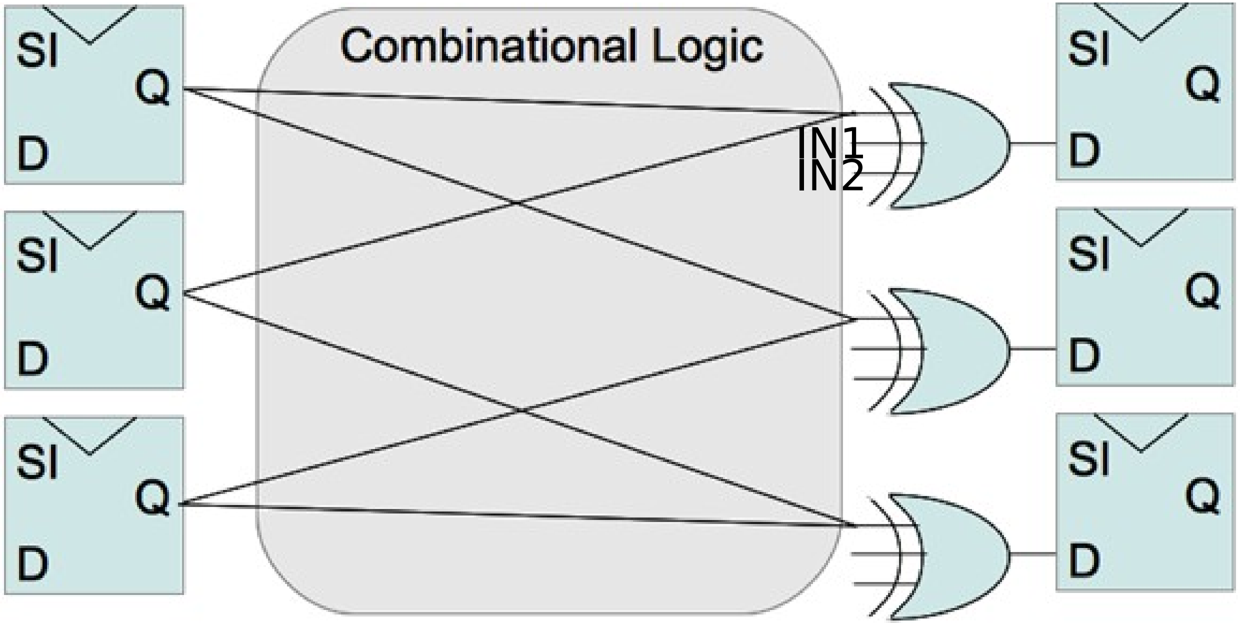
Foundry & Assembly

1. Designer has already put in hooks in the design that can ensure non-functional operation if the correct key is not included in the chip
2. Detecting a non-functional chip is significantly easier than using PUF and dealing with process variations

1. Foundry will not be able to ship any functional chips to the market
2. Same for defective chips and out-of-spec chips; the chips are simply non-functional.

XOR Mask

- Three-input XOR logic added to non-critical paths
- XOR logic additional inputs are IN1 and IN2

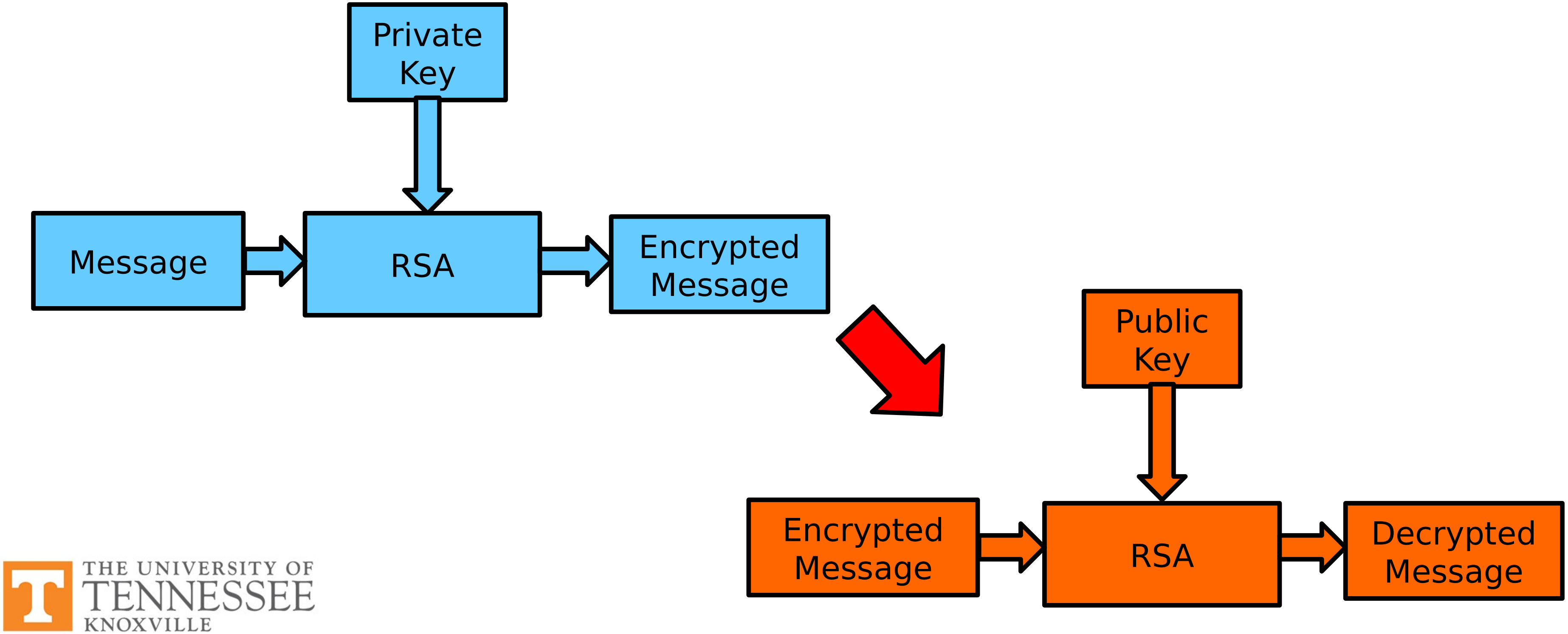


IN1: True Random Number Generator

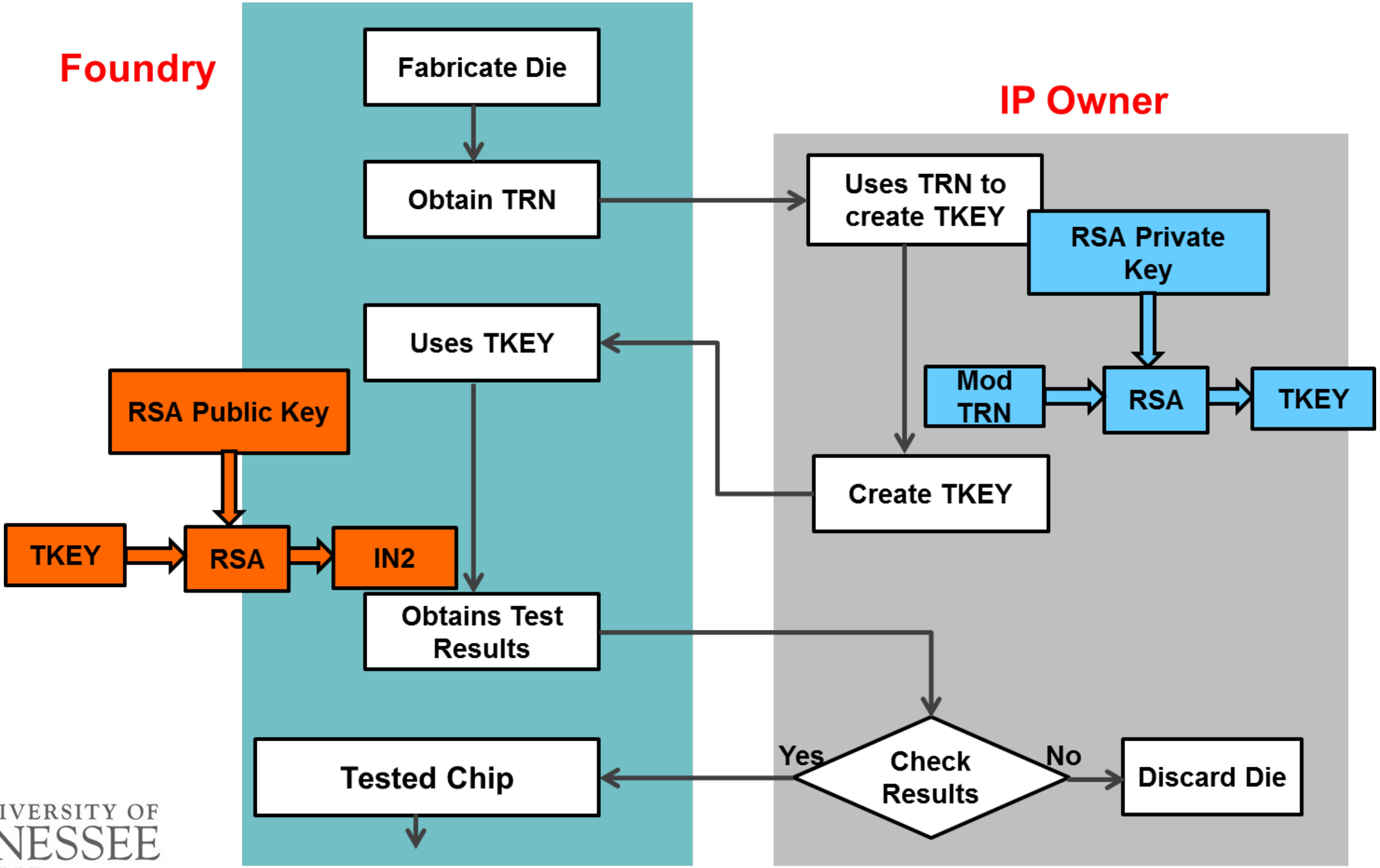
- Input IN1 is connected to a TRNG
- TRNG generates a random number TRN
- Same TRN is needed at foundry and assembly
- TRNG outputs burnt into fuses so same TRN can be read

IN2: RSA – Asymmetric Encryption

- Encryption mechanism that uses set of private and public keys to perform reversible encryption

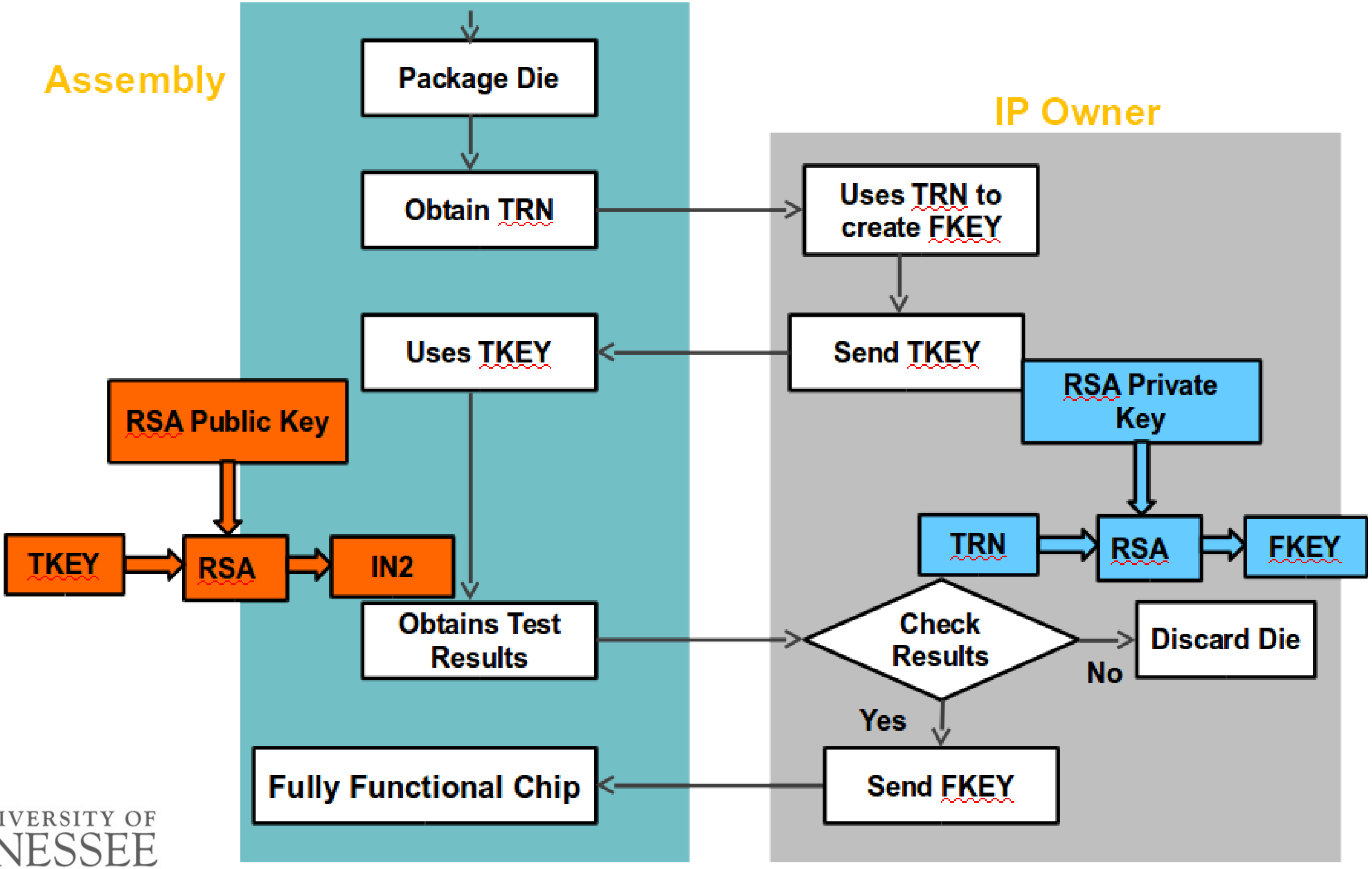


SST Communication Flow



THE UNIVERSITY OF TENNESSEE KNOXVILLE

SST Communication Flow



THE UNIVERSITY OF TENNESSEE KNOXVILLE

SST Analysis

- Effective against overproduced, cloned, and defective ICs
  - Overproduced: IP owner has control over number of TRNs and TKEY/FKEYs sent to foundry/assembly
  - Cloned: Chips not functional unless FKEY produced by IP owner
  - Defective: foundry sends test results to foundry who checks results & decides if chip has correct responses
- Prevents out-of-spec ICs
  - Some specs cannot be determined from pattern testing along If chip doesn't meet specs, could be considered passing chip
  - With addition of few sensors, specs can be tested and checked by IP owner during SST
  - IP owner then able to decide whether or not chip passes desired specs in order to prevent out-of-spec ICs going to market

Remote Activation Through FSM Modification

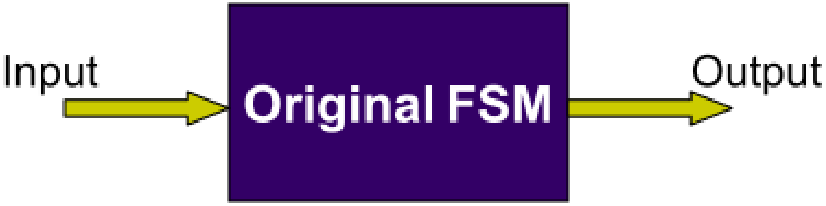
- FSM: Finite State Machine
- Sequence of inputs drive machine through different functional states
- Correct transitions give functional output

Input
Original FSM
Output

FSM

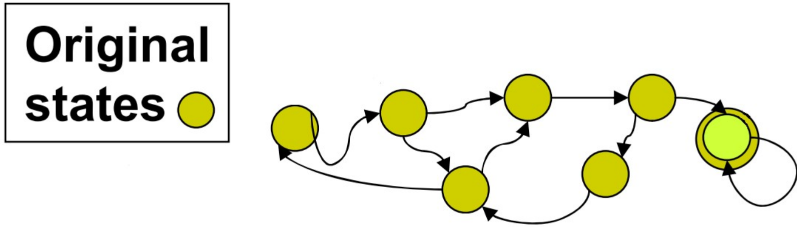
- Correct transitions give functional output

- Adding states to FSM gives IP owner controllability over sequence to reach functional states


Input

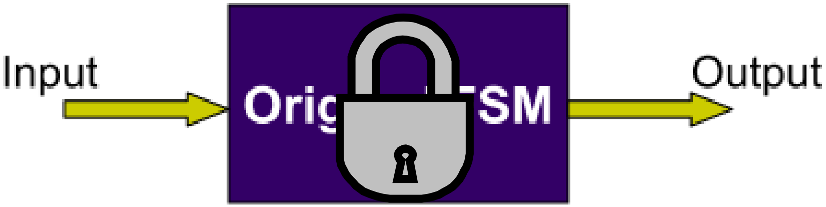
Original FSM

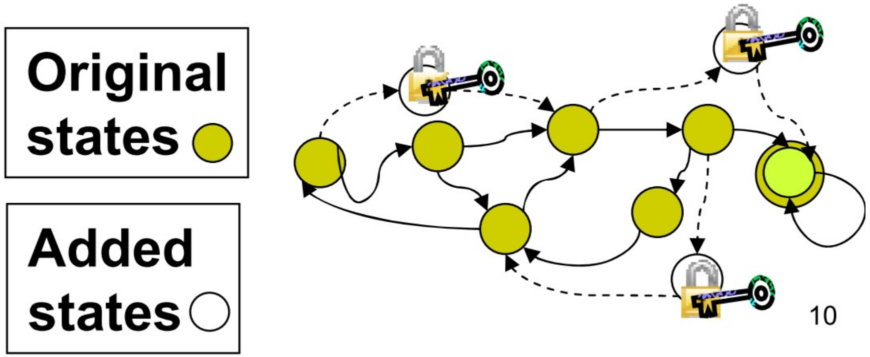
Output


Original states ●

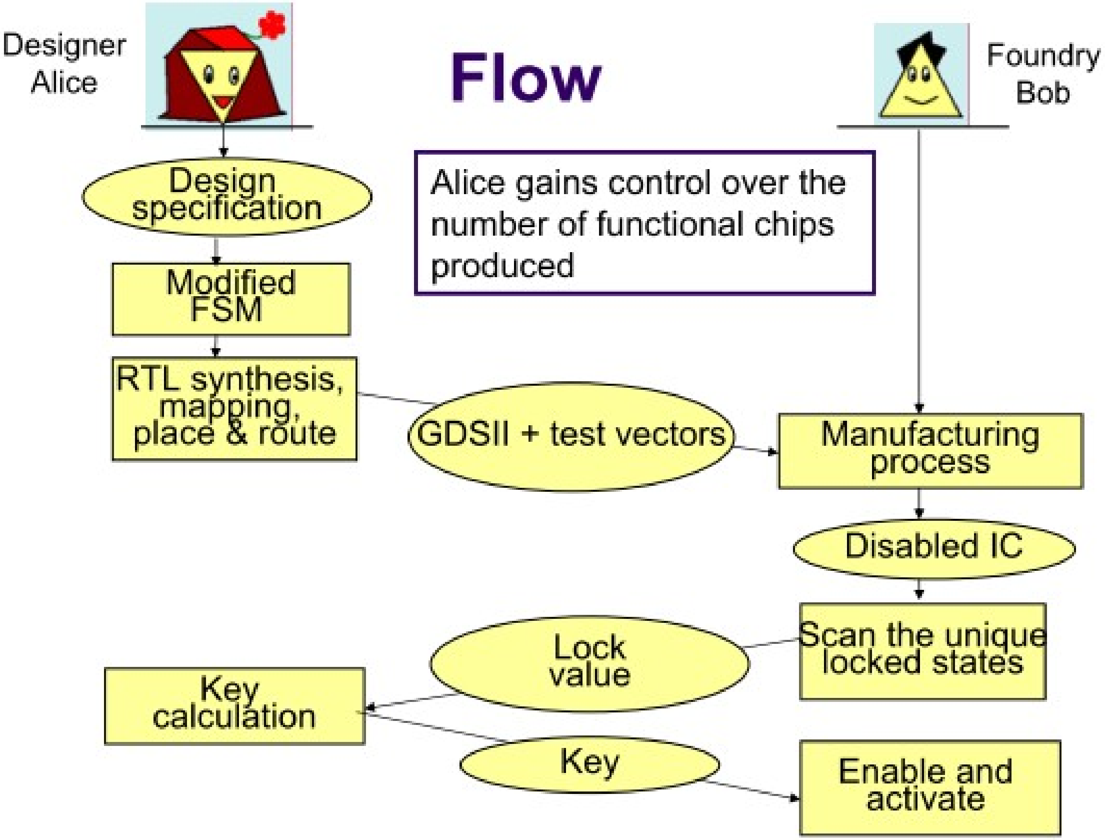
Boosted FSM

- On startup, inputs cause chip to go to one of added states
- IP owner only one with knowledge of FSM
- Only IP owner knows right sequence (key) to bring FSM back to functional states





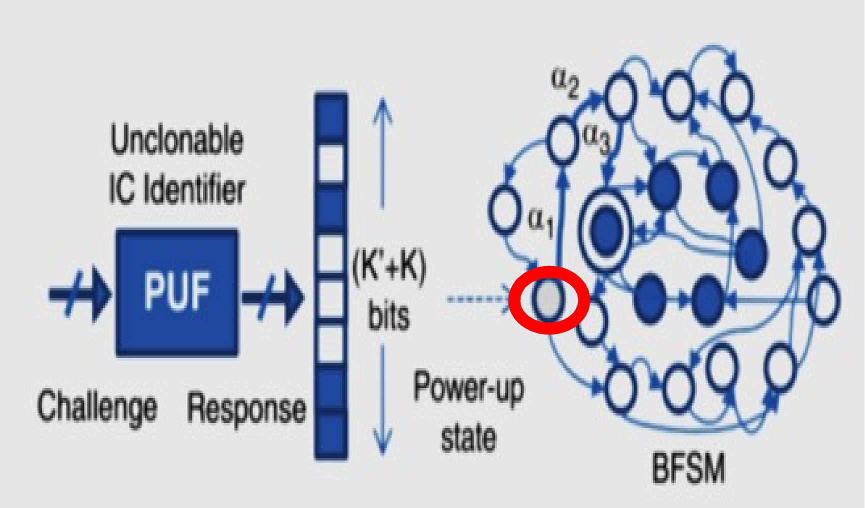
Communication Flow



Alice gains control over the number of functional chips produced

Boosted FSM

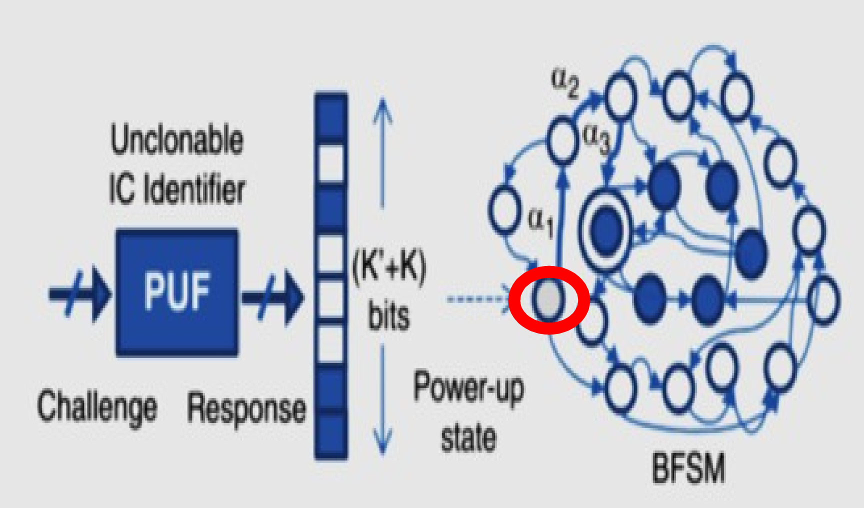
- On startup, PUF generates random sequence as input to FSM
- Due to large number of added states, high probability that starting state will be added state



Boosted FSM

- Foundry communicates current state to IP owner

- Owner knows FSM and can generate key (sequence) to reset FSM



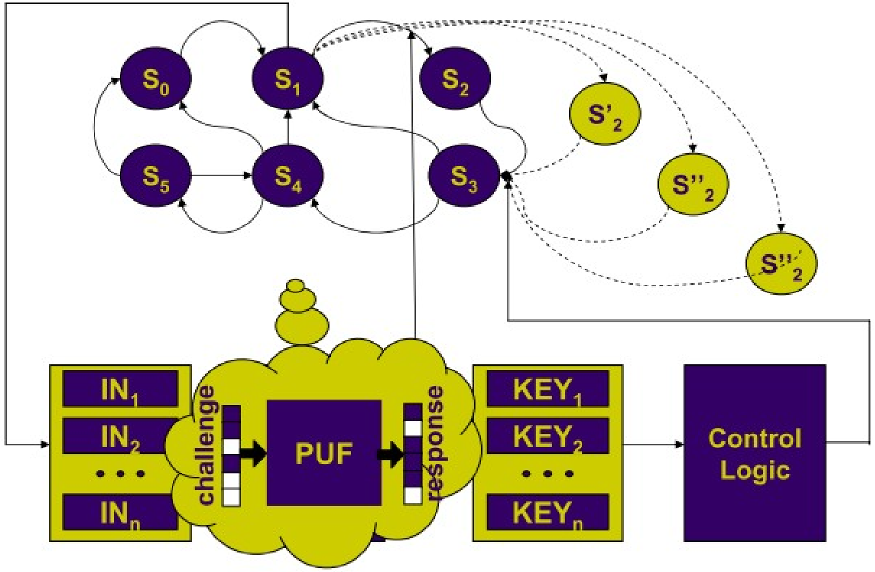
Remote Activation

- Redundant states are added

- Far less states than BFSM

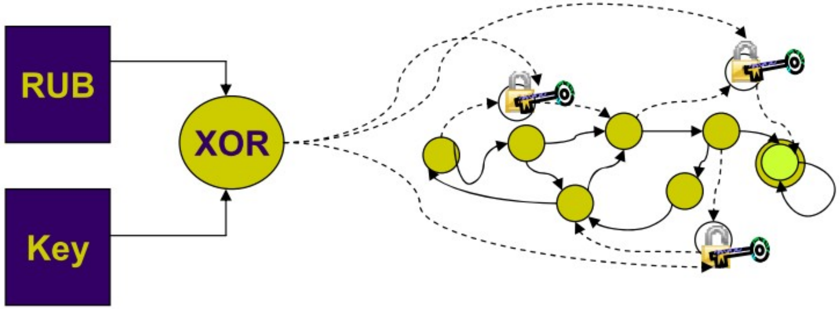
- PUF response will send FSM into one of redundant states

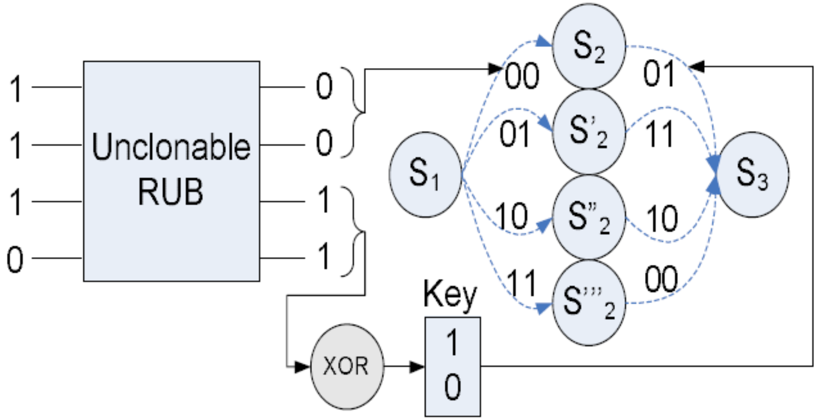
- **Challenge**: PUF not yet reliable!



Remote Activation

- RUB: Random Unique Block
- RUB must be stable – not change over time
- PUF (RUB) response sent to IP owner to generate key
- Key then used to send FSM into correct state





Analysis of Boosted FSM and Remote Activation

- BFSM requires many additional FSM states
- Remote Activation only uses a few redundant states
- Both use PUF which is affected by age, temperature, noise, etc.
- Both effective against cloned ICs but not effective against defective, over-produced, or out-of-spec ICs