Security and Trust for Wireless Integrated Circuits

Alán Rodrigo Díaz Rizo
Hassan Aboushady, Haralampos-G. Stratigopoulos

Journée de l'EDITE 2022

SCIENCES SORBONNE UNIVERSITÉ

cnrs

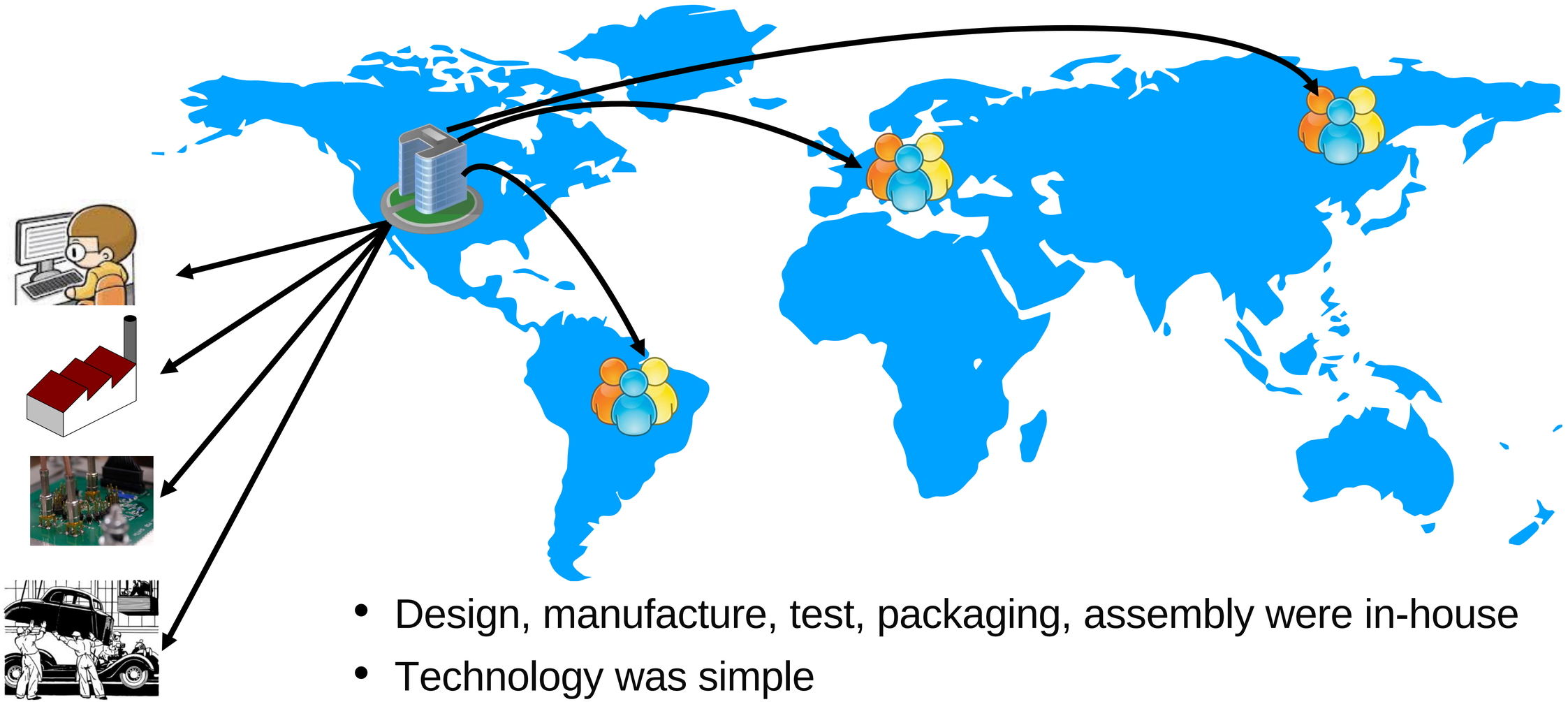
EDITE

LIP 6

Outline

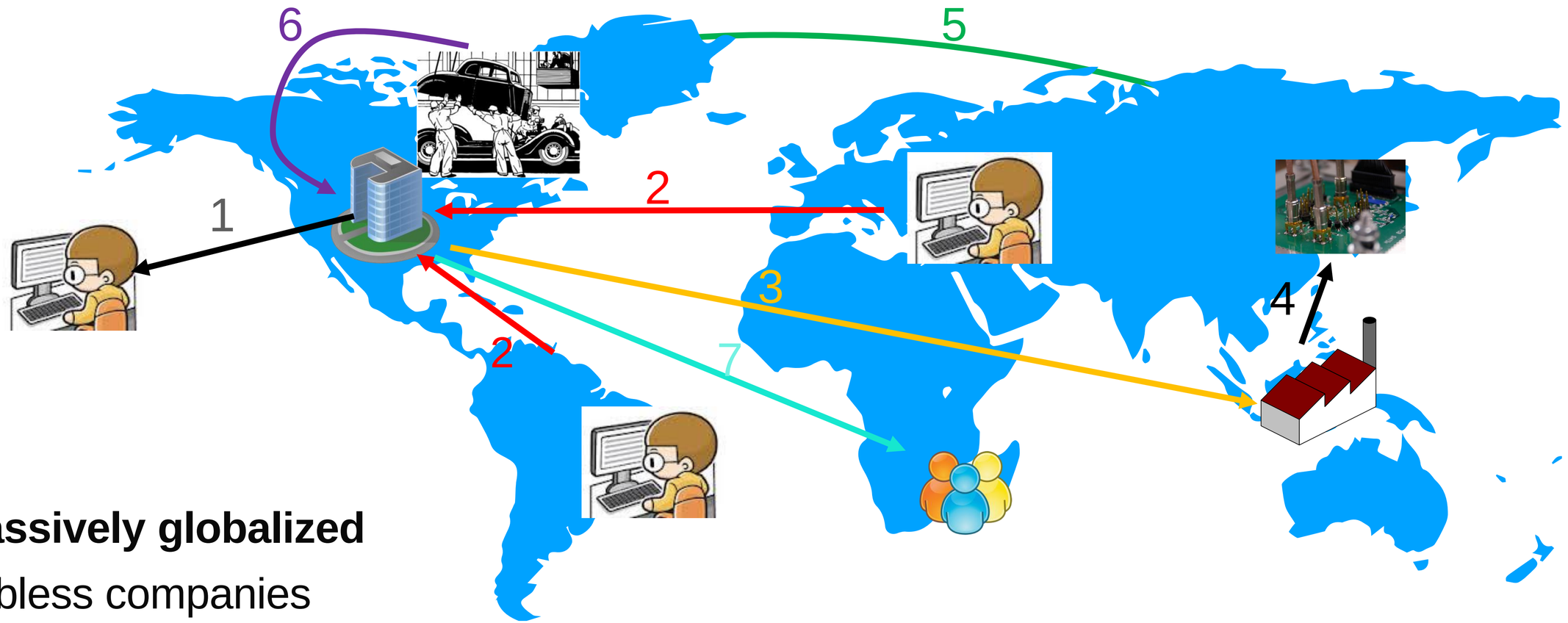
- Origin of hardware security threats: globalized Integrated Circuit (IC) supply chain
- Security threats: piracy and hardware Trojans
- The thesis is focused on RF transceivers:
  - Part I: Anti-piracy design
    - *MixLock*
    - *SyncLock*
  - Part II: Hardware Trojan-enabled covert communication channel

IC Supply Chain Before 1980s



- Design, manufacture, test, packaging, assembly were in-house
- Technology was simple
- Production costs were low

IC Supply Chain Today



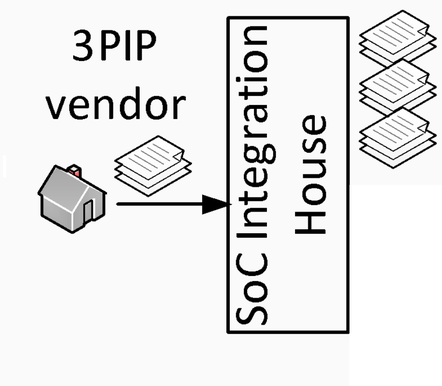
- **Massively globalized**
- Fabless companies

  Outsourcing IC production
- Companies share their IP with third entities (foundries, SoC integrators, IP brokers, etc.)

Part I : Piracy

IP/IC Piracy Threat

3PIP sells license for 1 SoC

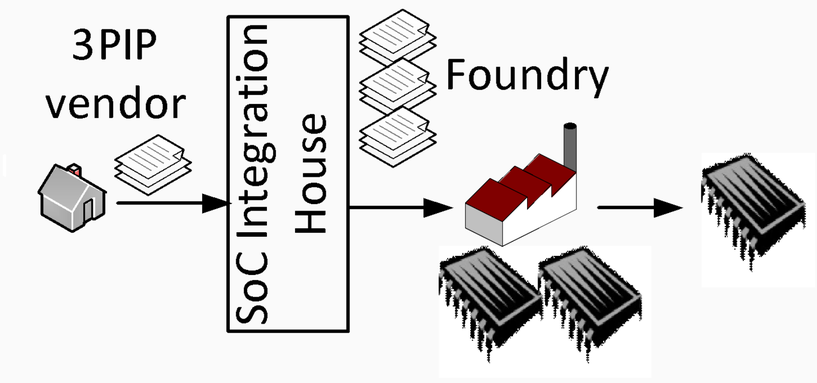


CLONING:
SoC integrator reuses IP in >1 SoCs

IP/IC Piracy Threat

3PIP sells license for 1 SoC

Design house orders N chips



CLONING: SoC integrator reuses IP in >1 SoCs

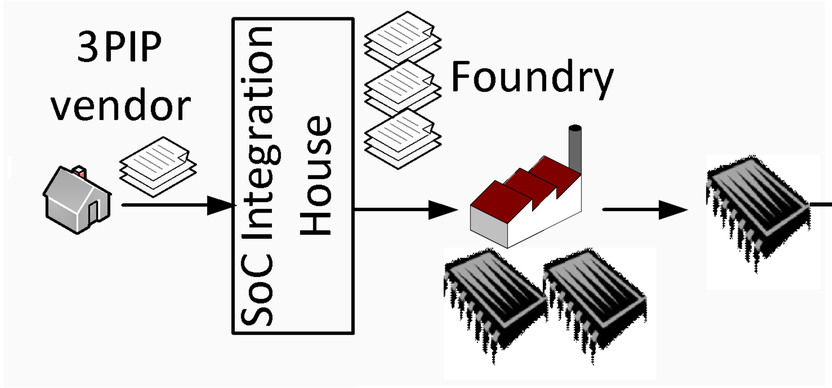
OVERPRODUCTION: Foundry overproduces >N chips

IP/IC Piracy Threat

3PIP sells license for 1 SoC

Design house orders N chips

Foundry asks to test N chips



CLONING: SoC integrator reuses IP in >1 SoCs

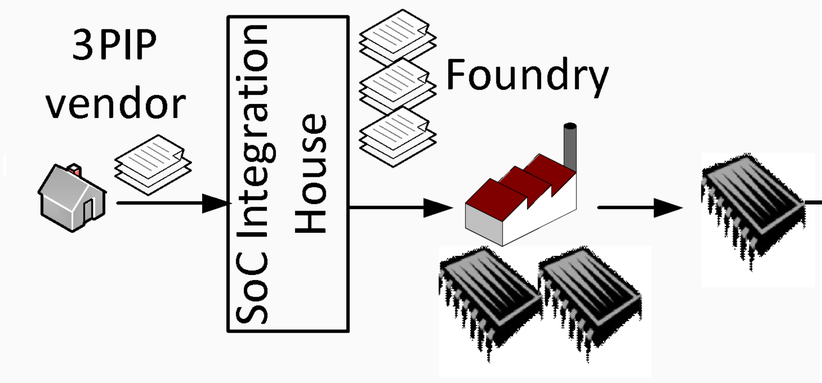
OVERPRODUCTION: Foundry overproduces >N chips

REMARKING: Test facility remarks the K<N chips that fail as passing

IP/IC Piracy Threat

3PIP sells license for 1 SoC

Design house orders N chips



Foundry asks to test N chips

Test facility

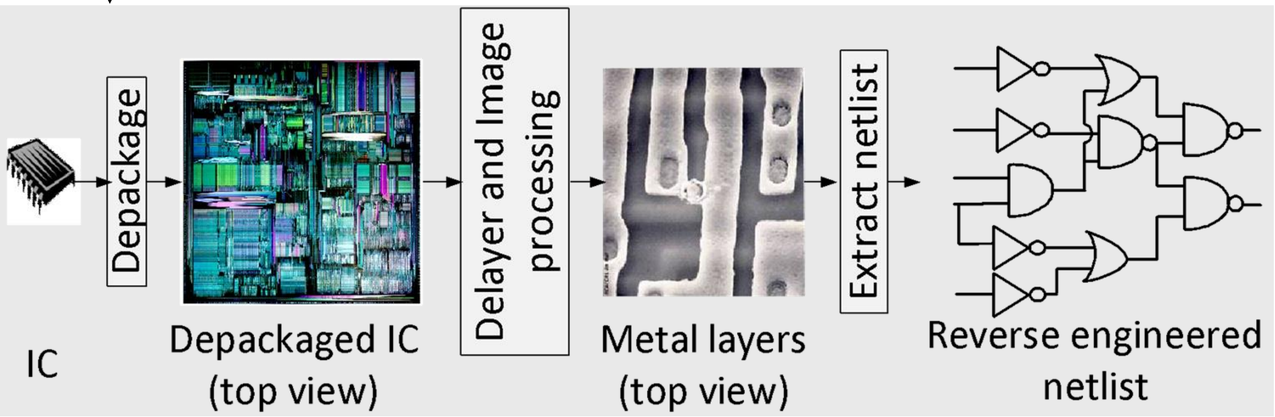
Application

CLONING: SoC integrator reuses IP in >1 SoCs

OVERPRODUCTION: Foundry overproduces >N chips

REMARKING: Test facility remarks the K<N chips that fail as passing

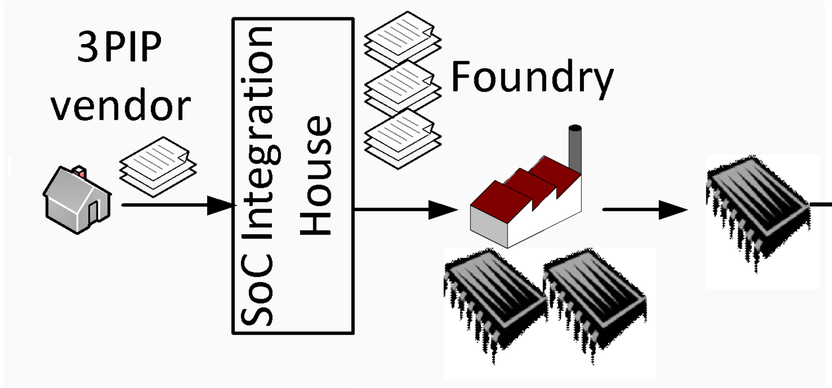
CLONING: via reverse engineering



IP/IC Piracy Threat

3PIP sells license for 1 SoC

Design house orders N chips

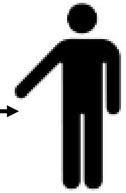


Foundry asks to test N chips

Test facility

Application

End of life



Malicious supplier

Recycled IC

Application

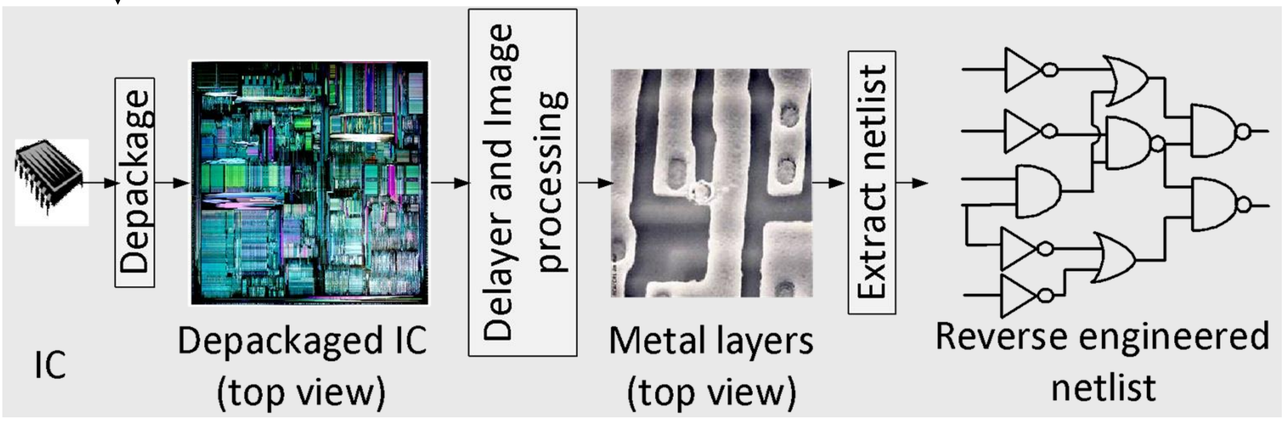
RECYCLING: Reusing aged ICs

CLONING: SoC integrator reuses IP in >1 SoCs

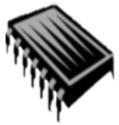
OVERPRODUCTION: Foundry overproduces >N chips

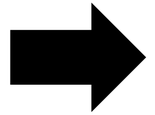
REMARKING: Test facility remarks the K<N chips that fail as passing

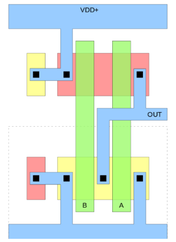
CLONING: via reverse engineering



IP/IC Piracy Facts







- $100 billion Global revenue loss [1,2]
- 1% of semiconductor sales are counterfeit ICs [1,2]
- 25% of reported incidents concern analog ICs [1,2]
- Supply chain attacks increased 4 times from 2020 to 2022 [3]
- Reverse engineering of ICs is affordable to many crime groups and governments [4]
- EU Chips Act: proposes support for innovative start-ups and certification procedures for trusted chips to guarantee quality and security for critical applications [5]
- France: Acceleration of cybersecurity is a strategic planning for the coming years [6]:

Government	Industry	Society & Consumers
• National security • Lost tax revenue • Costs of law enforcement	• Revenue loss • Loss of brand value • Costs to mitigate the risk	• Lower quality of counterfeit parts • Costs to replace failed products • Safety concerns

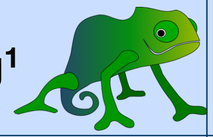
[1] USDC & USDHS, https://www.dhs.gov/publication/assessment-critical-supply-chains-supporting-us-ict-industry
[2] SEMI, https://www.nanotech-now.com/news.cgi?story_id=29151&utm_source=Nanotechnology+Now
[3] ENISA, https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
[4] Sem Eng., https://semiengineering.com/why-its-so-difficult-and-costly-to-secure-chips/
[5] European Union Chips Act Factsheet 2022, https://digital-strategy.ec.europa.eu/en/library/european-chips-act-factsheet
[6] https://www.economie.gouv.fr/strategie-nationale-acceleration-cybersecurite#

Piracy Countermeasures

[1] J. Leonhard *et al*., TCAD'21

[2] T. D. Perez and S. Pagliarini, IEEE Access'20

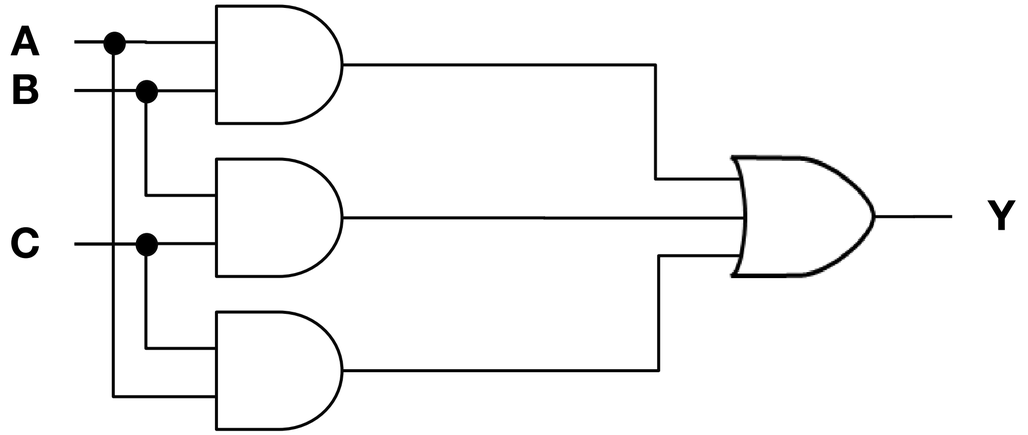
[3] K. Huang *et al*., TCAD'15

Countermeasure	Security Threat					
	Cloning by SoC integrator	Cloning by foundry	Cloning by end user	Over-producing	Remarking	Recycling
Locking 	✅	✅	✅	✅	✅	✅
Camouflaging[1] 	❌	❌	✅	❌	❌	❌
Split manufacturing[2] 	❌	✅	❌	✅	❌	❌
Age and performance monitoring[3]	❌	❌	❌	❌	❌	✅

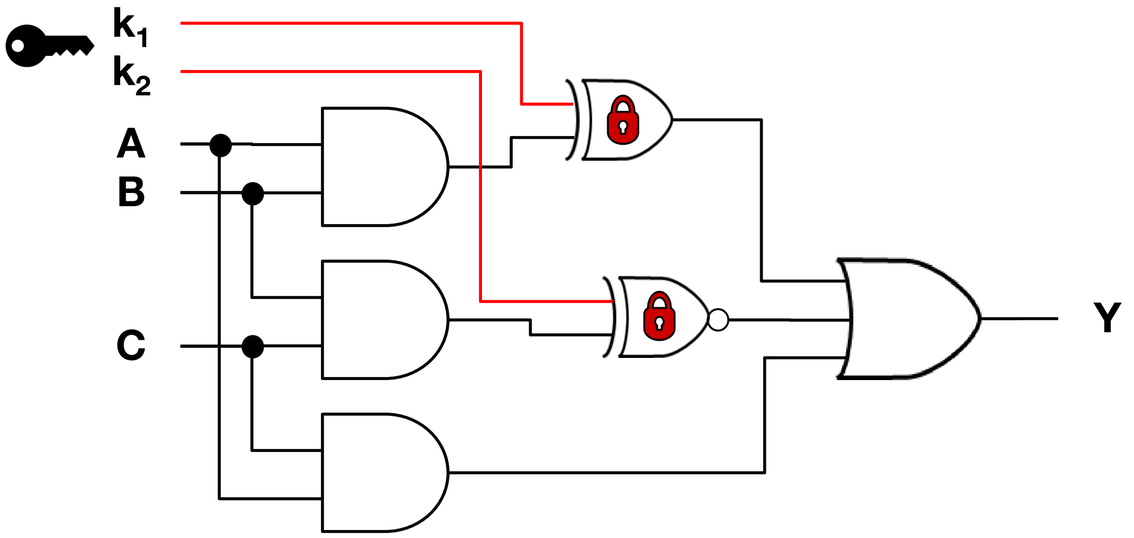
Logic Locking for Digital ICs

- Logic locking modifies the digital IC by adding new logic (key-gates) controlled by key-bits (e.g., k_1, k_2).

- Different logic locking techniques use different approaches for key-bit insertion, e.g., XOR/XNOR insertion in Random Logic Locking



Original circuit

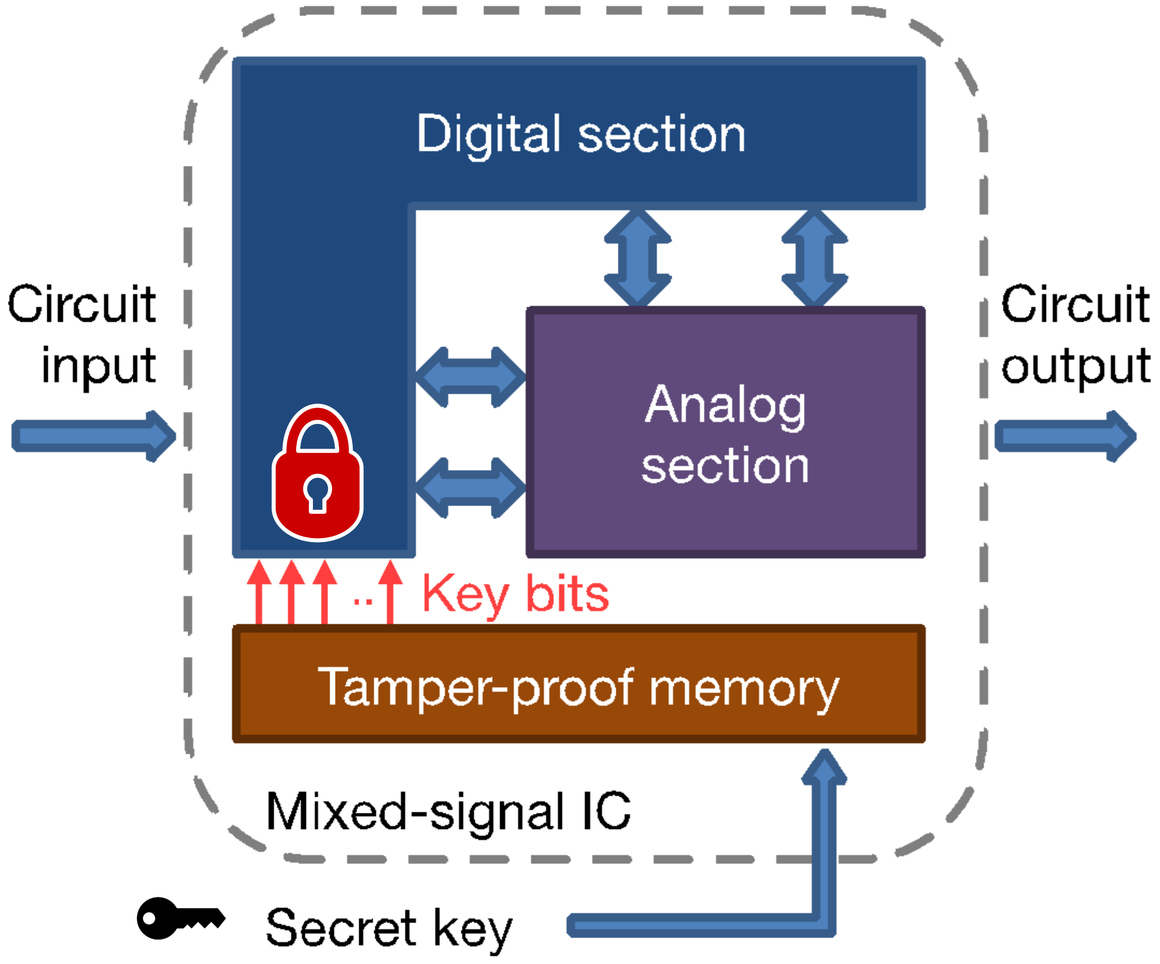


Locked circuit; secret key (k_1,k_2) = (0,1)

Roy *et al.*, Computer'10

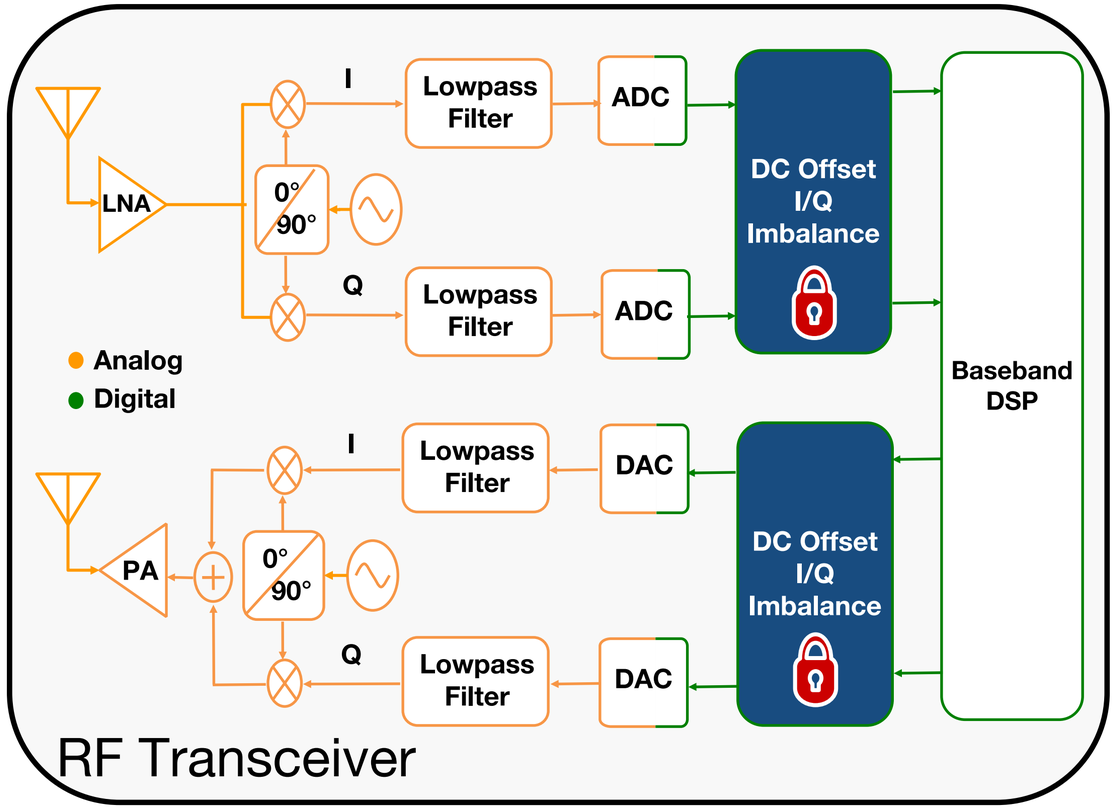
MixLock: Digitally-Assisted Security

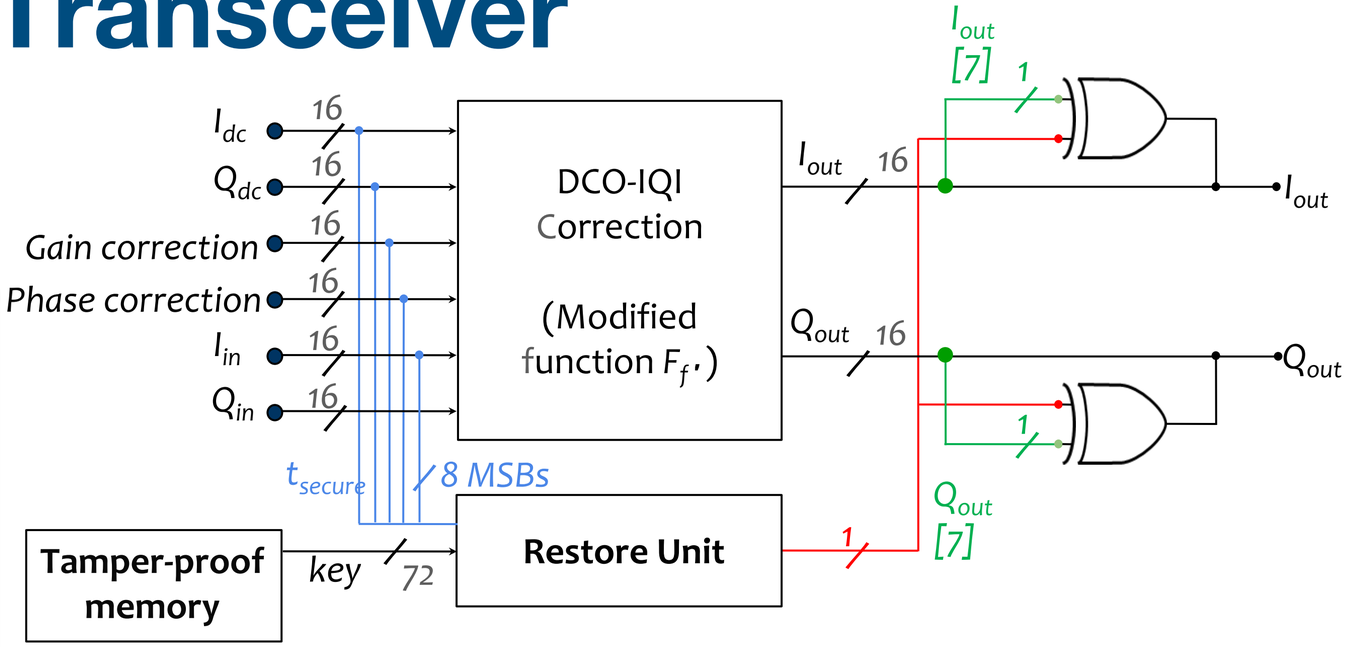
- Locking mixed-signal ICs via logic locking of their digital section
- Incorrect keys break mixed-signal performance at system level
- Apply lock in the signal path
- Widely applicable

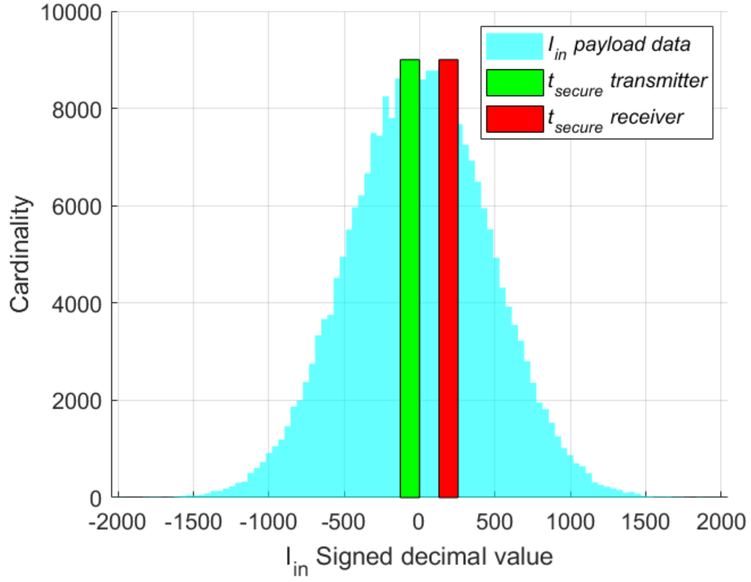


J. Leonhard *et al*., DATE'19
J. Leonhard *et al*., TCAD'22
A. R Diaz-Rizo *et al*., TCAS-II'22

Lock Insertion in RF Transceiver

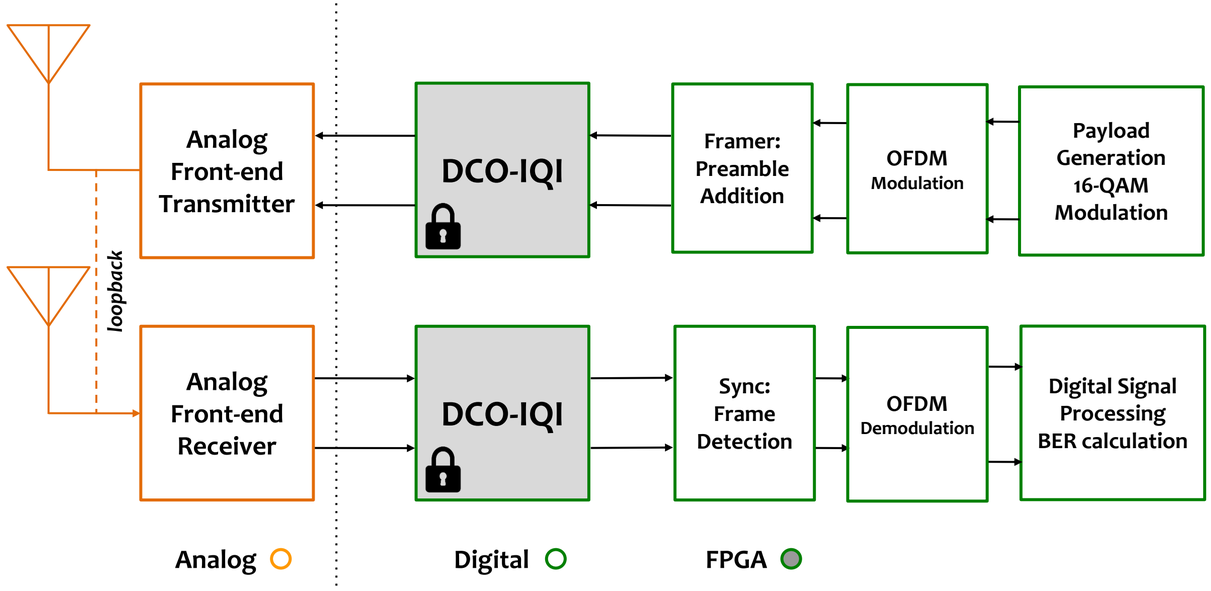


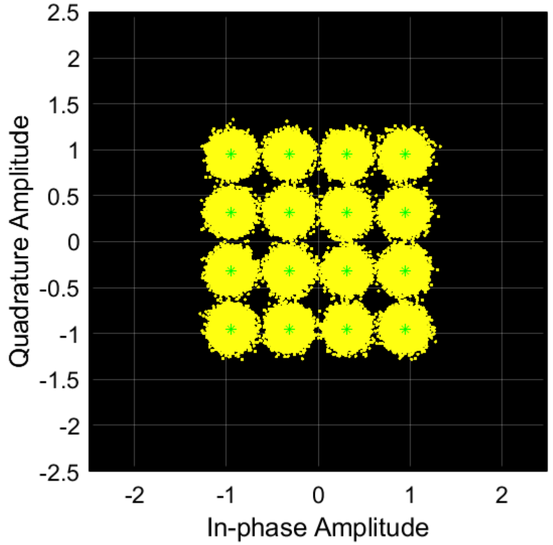




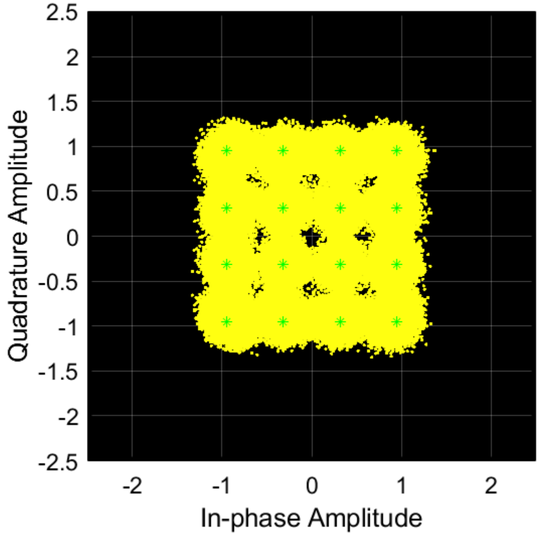
Maximize degradation for incorrect keys

Measured Locking Efficiency on bladeRF Board

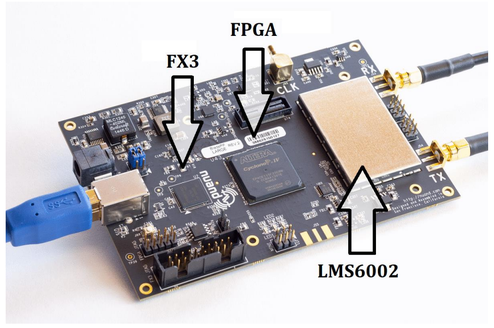




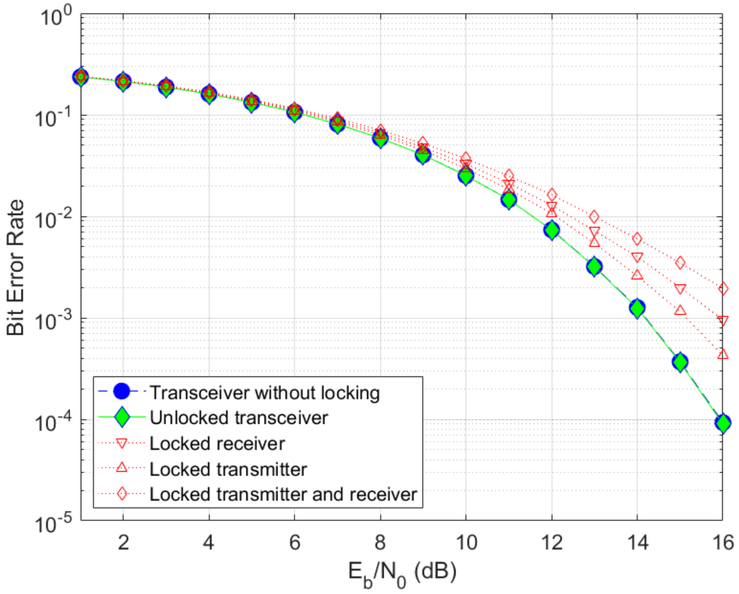
Unlocked transceiver

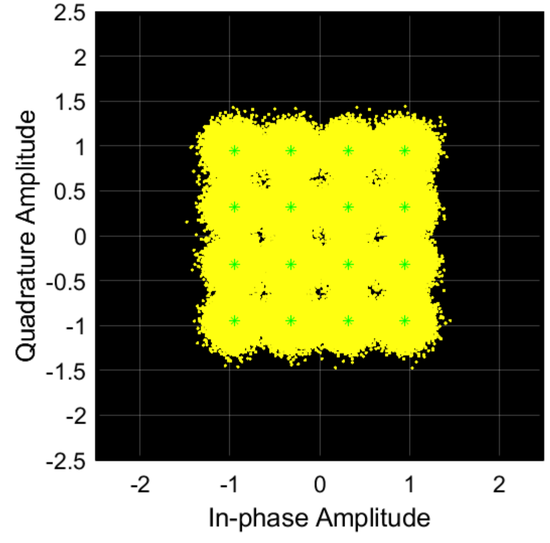


Locked receiver

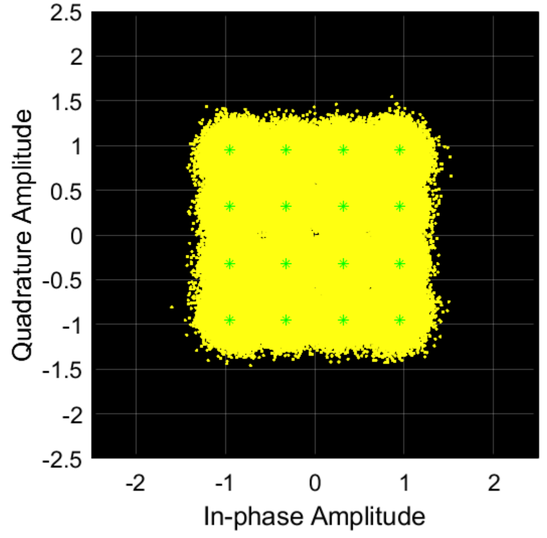


Nuand, “SDR bladeRF 2.0 micro xA9,” https://bit.ly/3z2QV1N, Online



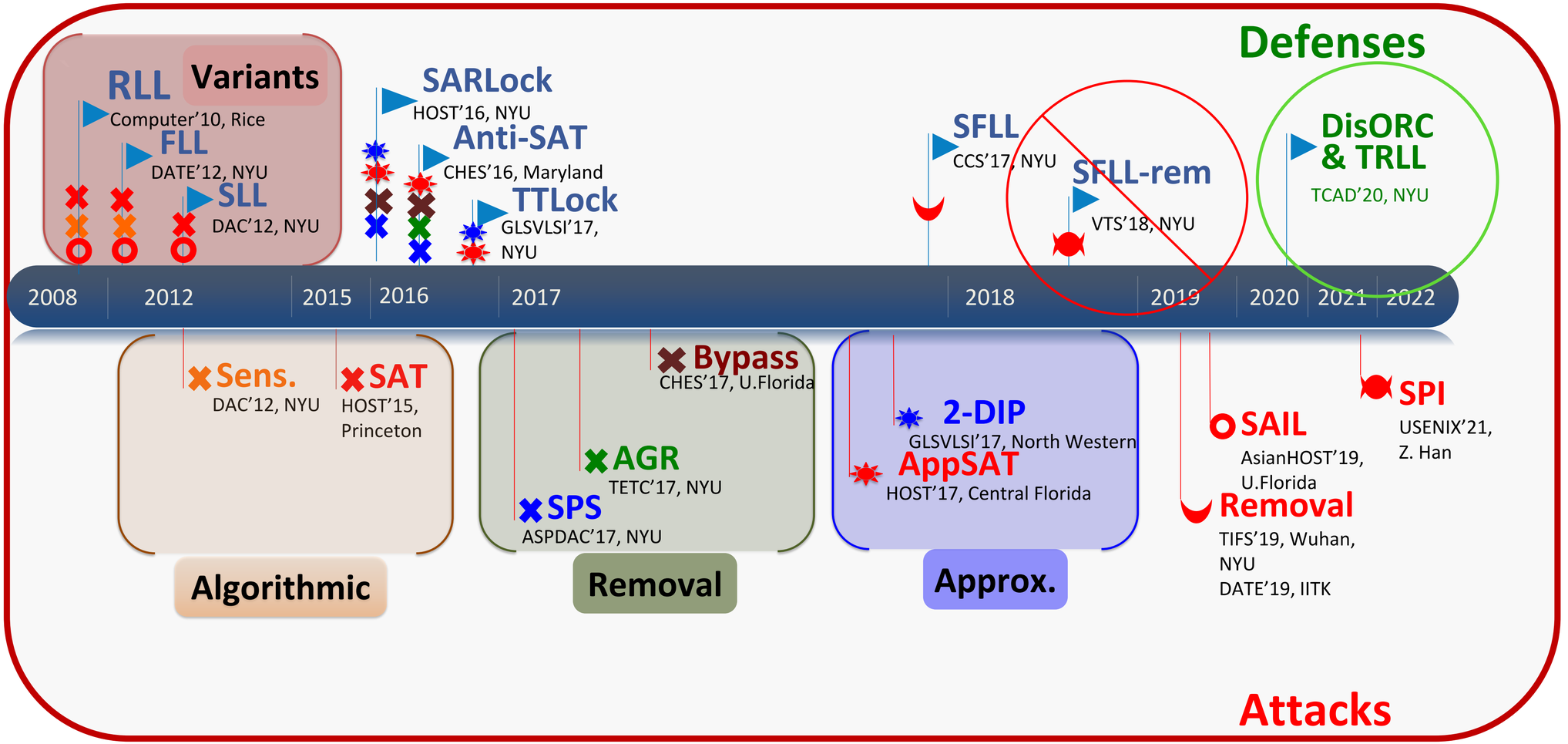


Locked transmitter

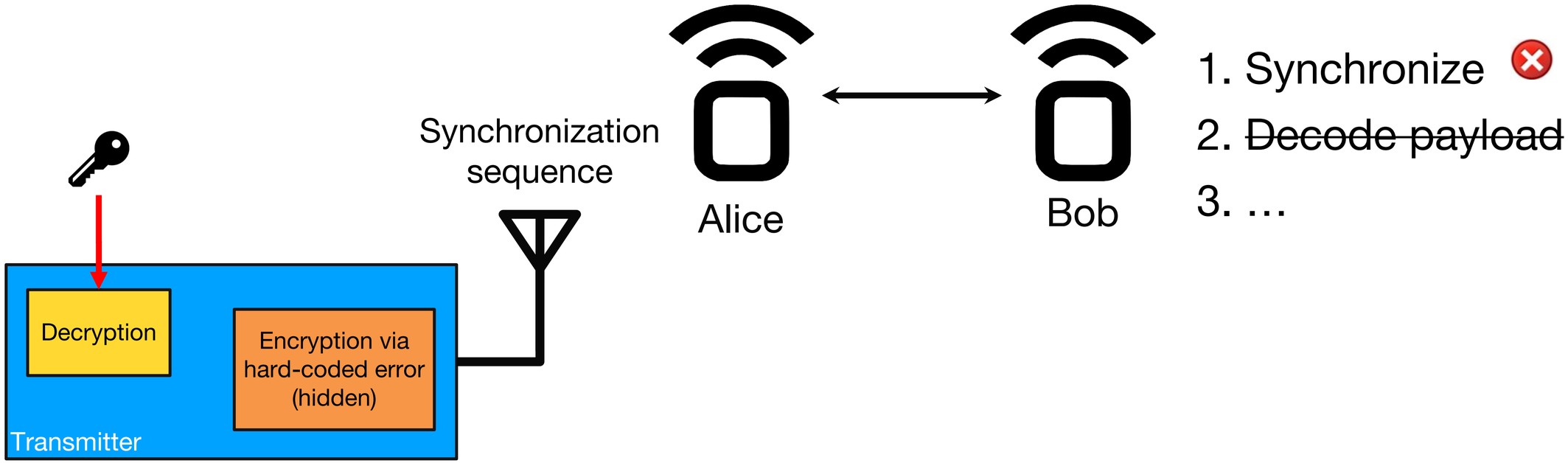


Locked transceiver

A Brief History of Logic Locking



SyncLock: Synchronization-Based Locking for RF Transceivers

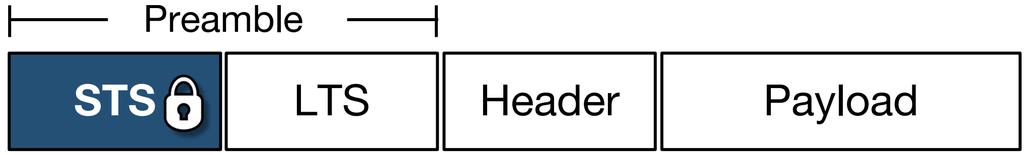


- Hard-coded error encrypting synchronization sequence
- Any incorrect key breaks the communication link

A. R. Diaz-Rizo *et al.*, TCAS-I'22

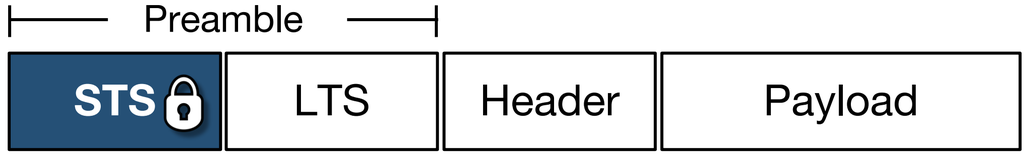
SyncLock Mechanism

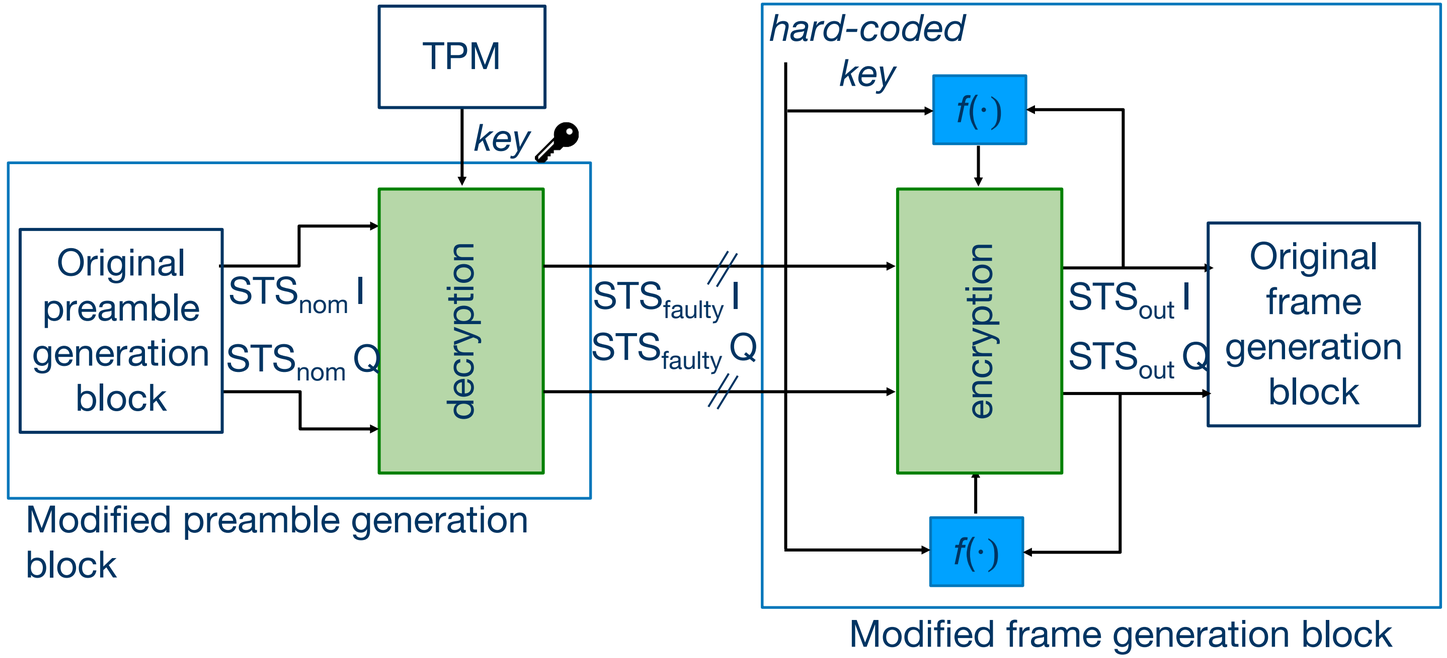
- Transmission frame of the WiFi (IEEE 802.11):



SyncLock Mechanism

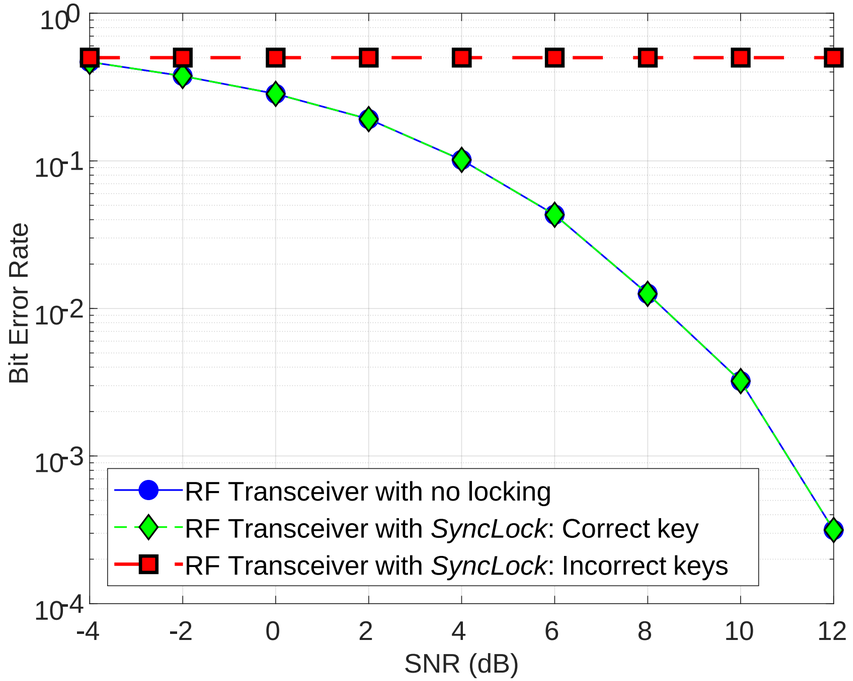
- Transmission frame of the WiFi (IEEE 802.11):



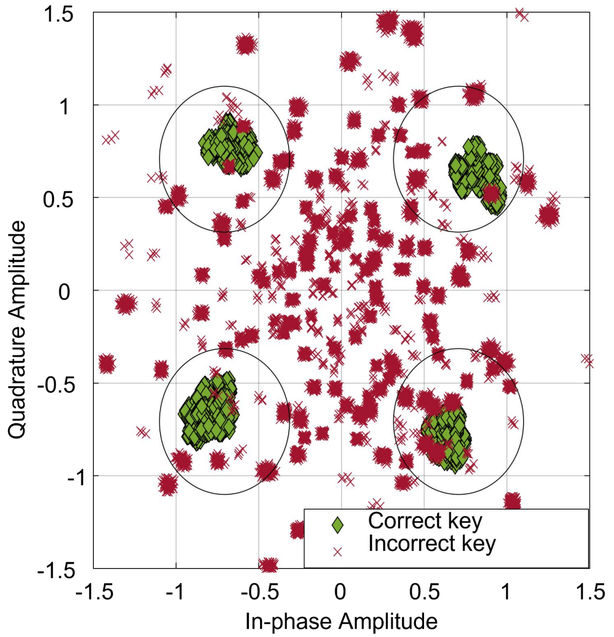


- Locking mechanism is composed of two blocks spatially separated, decryption and encryption
- decryption and encryption are implemented with XOR-based ciphers
- System equation: $STS_{out} = (STS_{nom} \oplus key) \oplus f(key_{h\text{-}c}, STS_{out})$
- $f(\cdot)$ can be any nonlinear function, e.g., $f(\cdot) = \text{circular-shift}(key_{h\text{-}c} \oplus STS_{out})$
- Correct key satisfying equation is: $key = f(key_{h\text{-}c}, STS_{nom})$

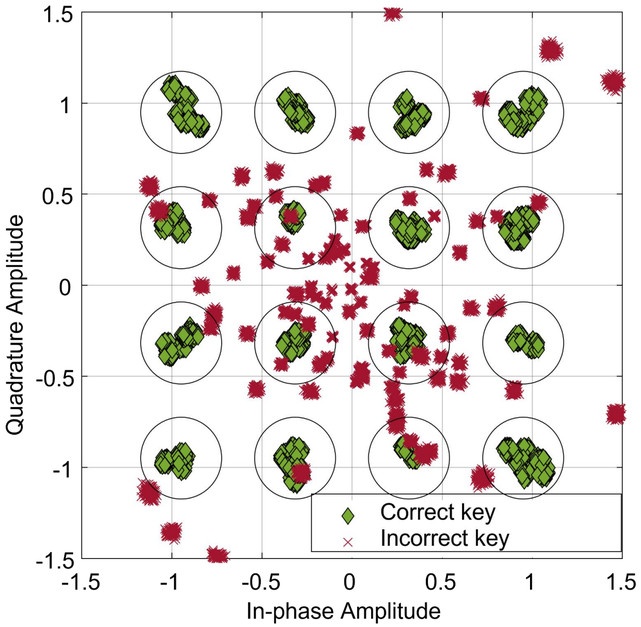
Measured Locking Efficiency on bladeRF Board

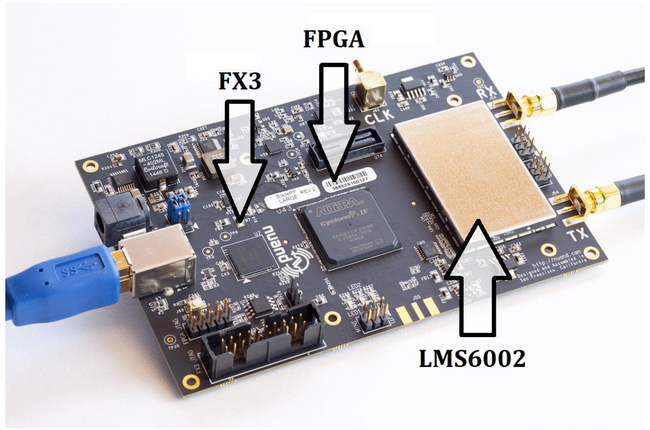


QPSK



16-QAM





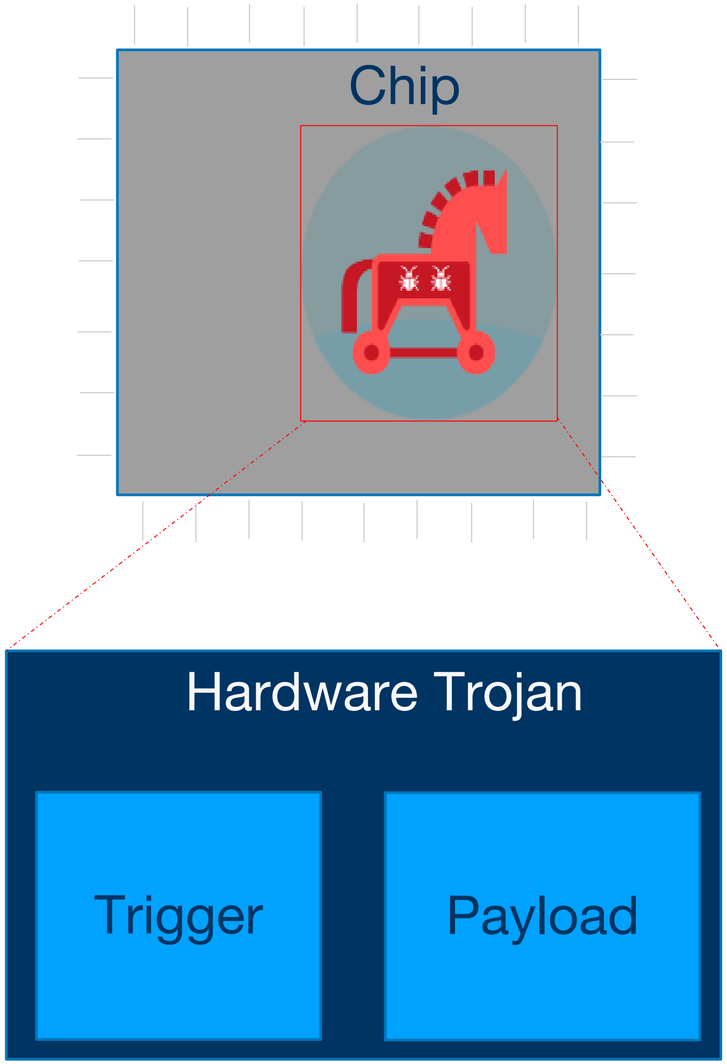
- Demonstrated in hardware using the Software Defined Radio (SDR) bladeRF board from Nuand™ [1, 2]
- IEEE 802.11 Wi-Fi RF transceiver with a direct conversion AFE architecture for both the receiver and the transmitter
- Attributes: non-intrusive, <<1% area overhead, negligible power overhead, 512 effective key-bits, any invalid key results in maximum BER

[1] Nuand, “SDR bladeRF 2.0 micro xA9,” https://bit.ly/3z2QV1N, Online.
[2] Nuand, “Open-source IEEE 802.11 compatible software defined radio VHDL modem

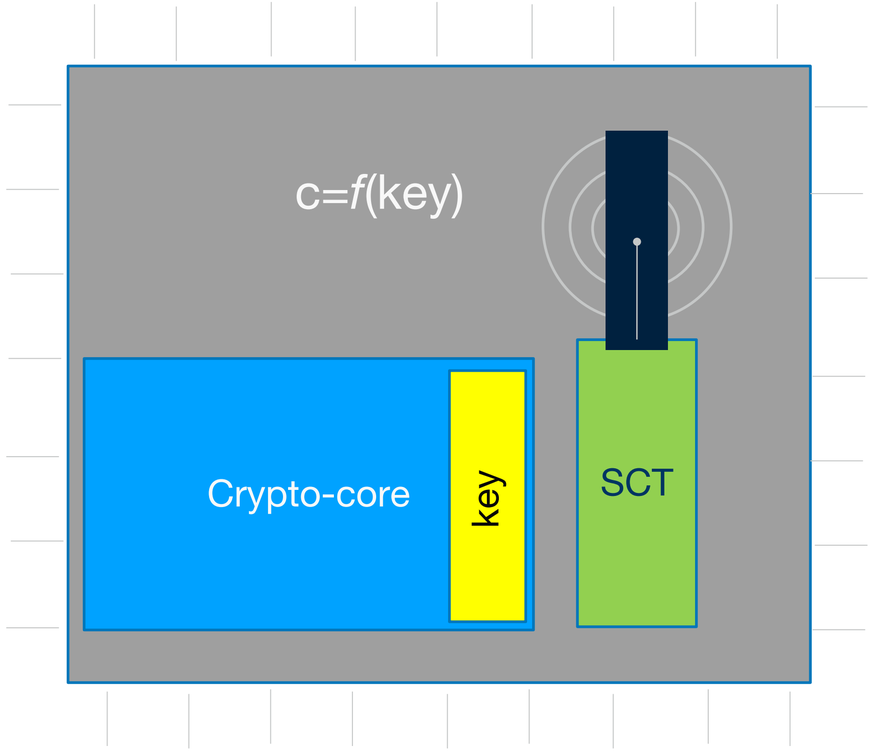
Part II : Hardware Trojans

Hardware Trojan Threat

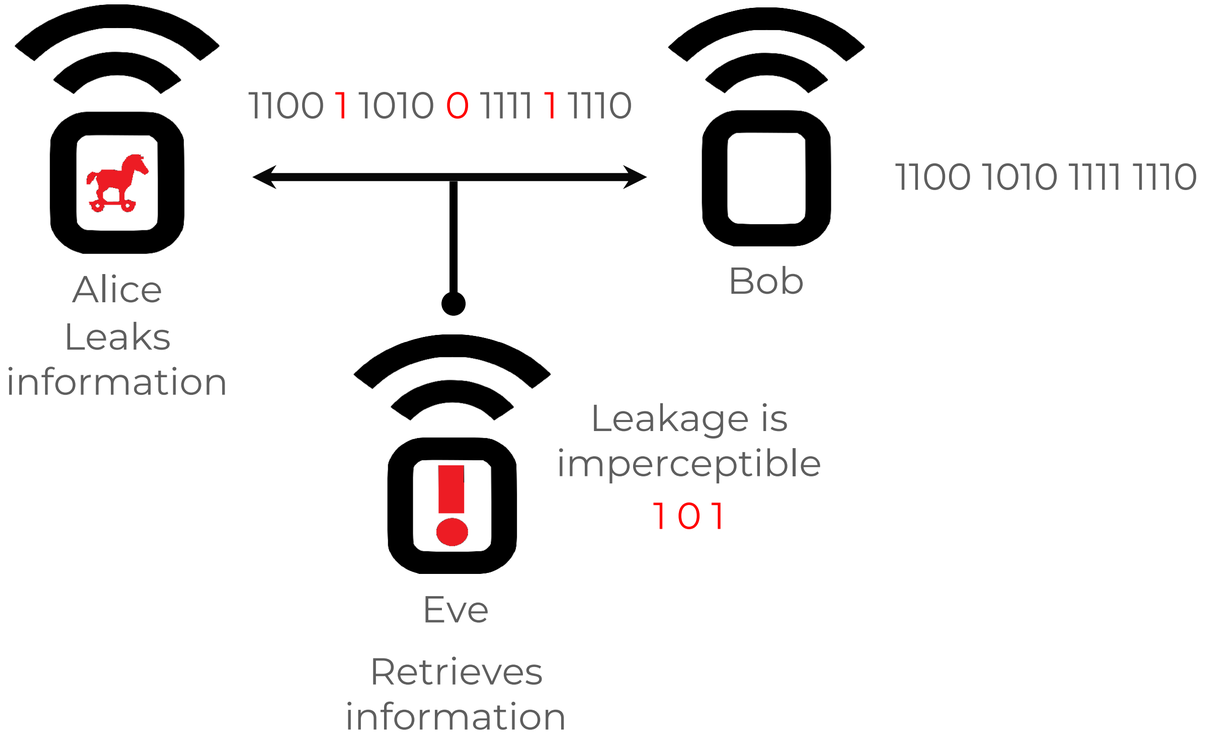
- Malicious modification of a circuit
- Hardware Trojan (HT) design:
  - Triggering mechanism (always on, rare condition is met, etc.)
  - Payload mechanism (effect):
    - Changing the function
    - Degrading performances
    - **Leaking information (cryptographic keys)**
    - Denial-of-service
- Attacker's goal: stealthy, small footprint
- Defender's goal: prevention, detection



RF Hardware Trojans: Short vs. Long Distance

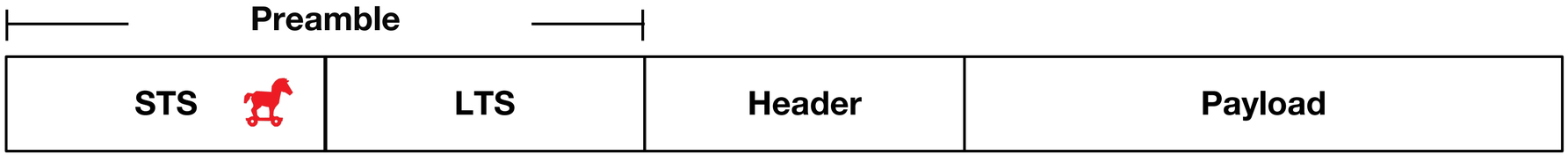


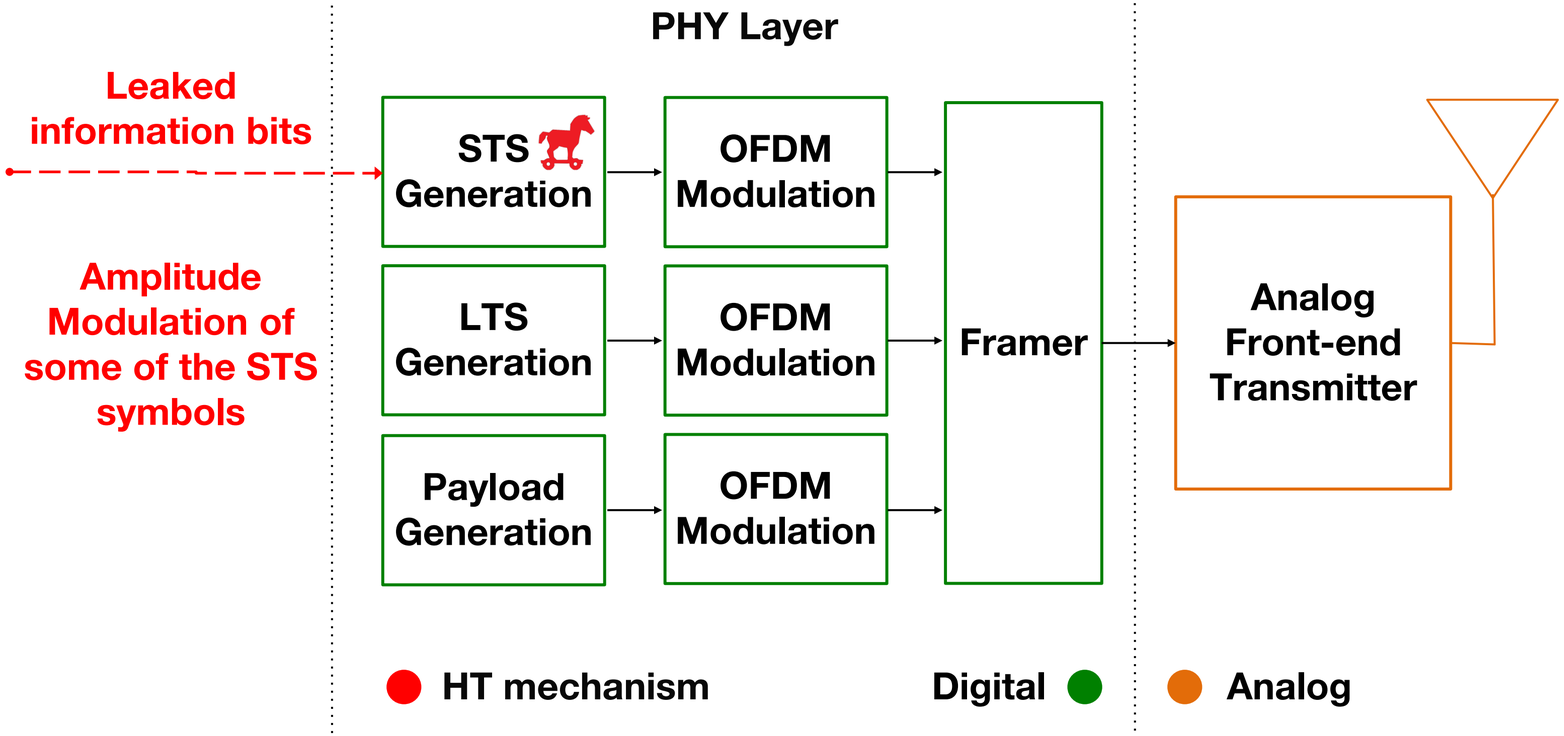
Side-Channel Trojan (SCT)
(L. Lin *et al.*, CHES'09)



Covert communication channel
(N. Kiyavash *et al.*, TIFS'13, Dutta *et al.*, Information Hiding'13, J. Classen *et al.*, CNS'15, K. S. Subramani *et al.*, TIFS'19, Y. Jin and Y. Makris, D&T'10, Y. Liu *et al.*, TVLSI'17, K. S. Subramani *et al.*, TIFS'20, S. Chang *et al.*, TODAES'20, K. Sankhe *et al.*, MILCOM'19)

Covert Communication Channel via the Preamble of Transmitted Frames

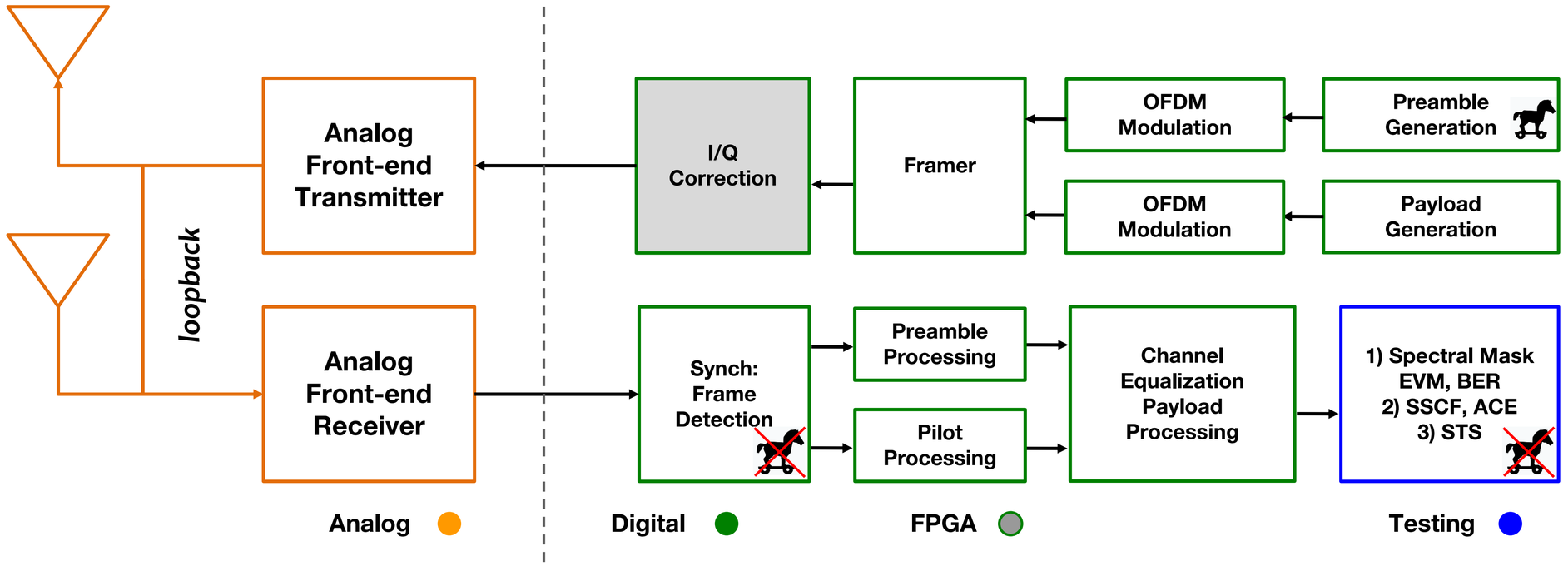




- STS field is used for detecting the start of the frame (synchronization)
- Information bits (i.e. cypher key) are leaked through STS
- Synchronization is not affected

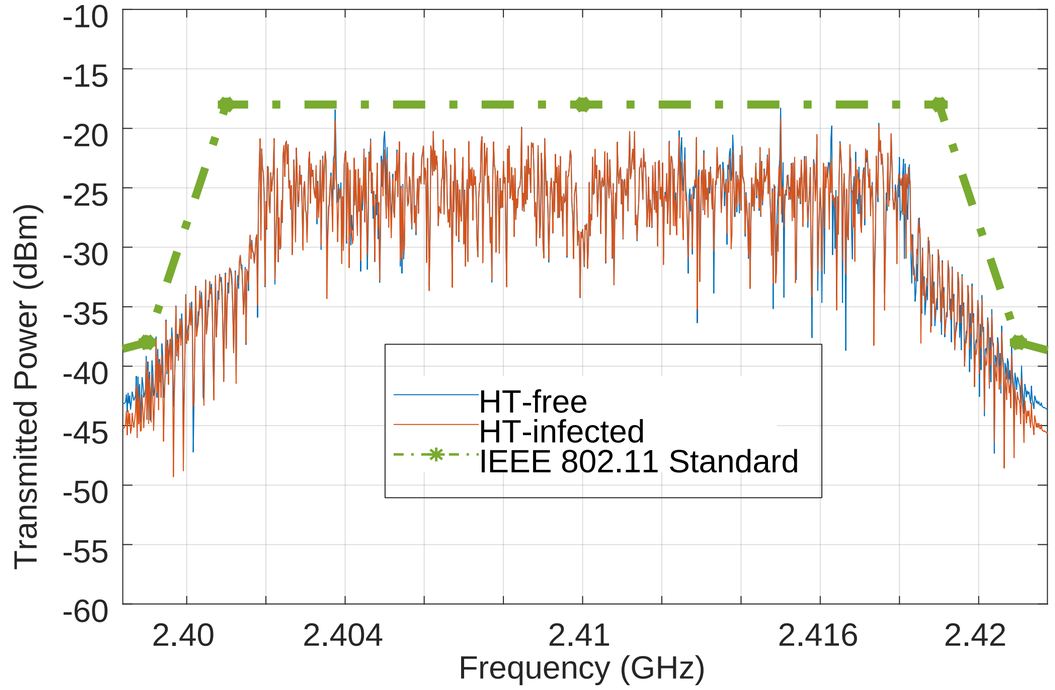
A. R. Diaz-Rizo *et al.*, TDSC'22

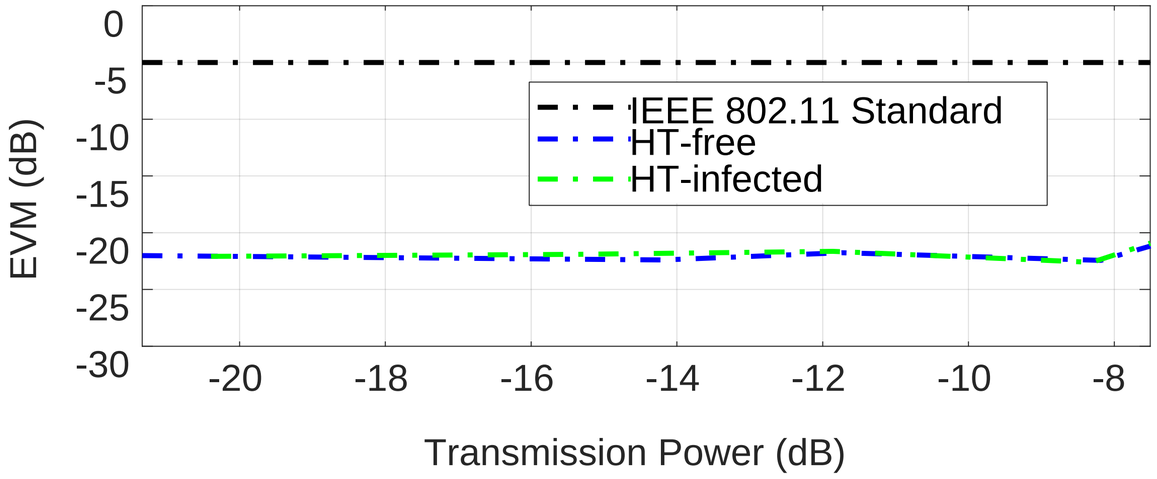
Can Alice (Tx) and Bob (Rx) Detect the Hardware Trojan?

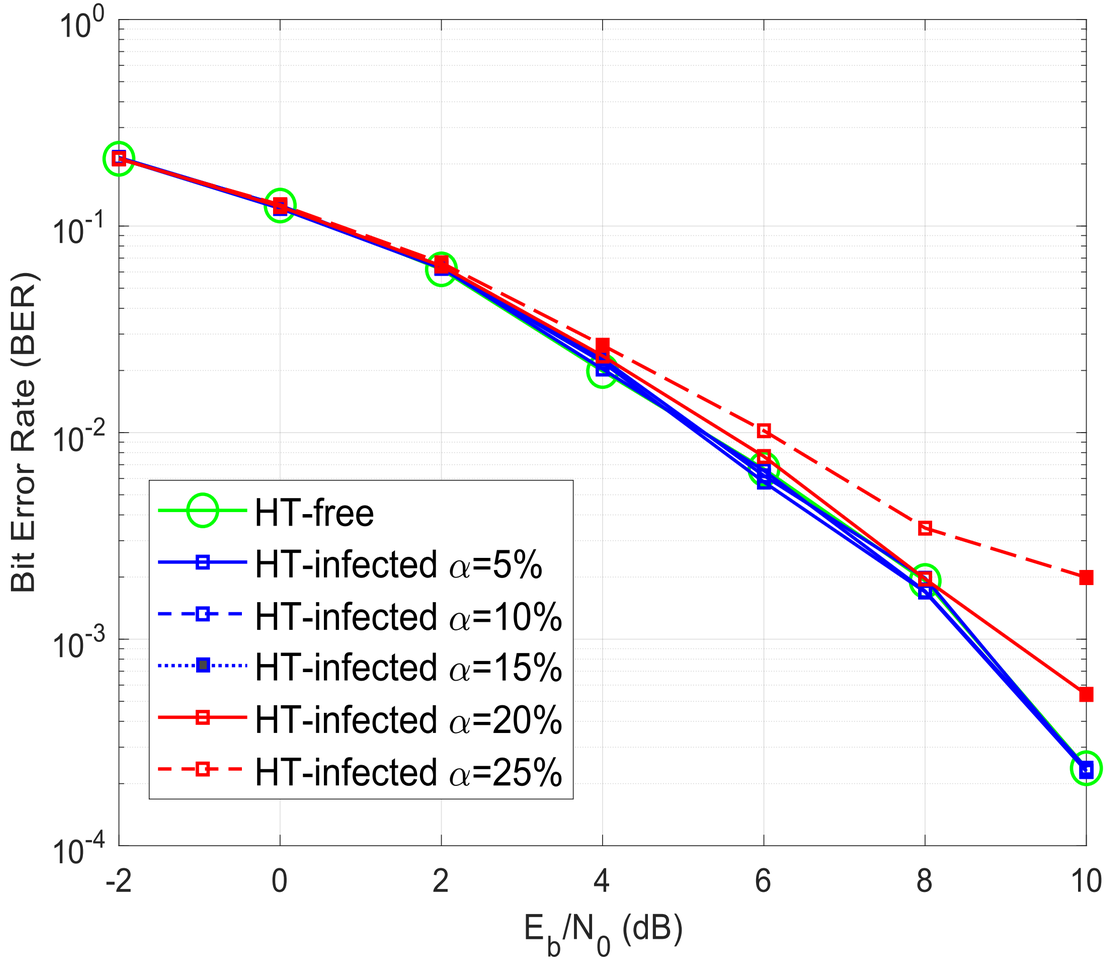


- Alice (Tx) and Bob (Rx) can perform:
  - Standard measurements: spectral mask, EVM, BER, etc.
  - Specialized measurements: Statistical Side-Channel Fingerprinting (SSCF), STS measurements, Adaptive Channel Estimation (ACE)
- All measurements performed on the bladeRF board from Nuand™

Standard Measurements







- No performance penalty
- HT undetectable for α ≤ 15%

Conclusion

- Protect the precious IP of designs against piracy is paramount
- 2 anti-piracy design techniques for RF transceivers
  - *MixLock*
    - ➢ Locking methodology of RF transceivers based on logic locking
    - ➢ Uses a generic state-of-the-art logic locking technique
    - ➢ Problem is that a counter-attack is likely to be developed
  - *SyncLock*
    - ➢ Novel domain-specific logic locking technique for RF transceivers
    - ➢ Resilient to any known attack

- HT-infected ICs can leak sensitive information
  - Leaking Wireless ICs via HT-infected synchronization
    - ➢ Novel covert communication channel
    - ➢ Undetectable by all known test-based and run-time defenses
    - ➢ We need new defenses and security-aware wireless standards

Thank you for your attention!

Questions?

alan-rodrigo.diaz-rizo@lip6.fr

MixLock Summary

- Generally applicable to any RF transceiver
- State-of-the-art logic locking can be used
- Implementation overhead DCO-IQI correction block:
  - 3.9% area, 0.3% power consumption
    (negligible overheads for entire RF transceiver)
- No performance penalty
- Fully automated
- No alterations in mixed-signal design flow
- SFLL-rem is vulnerable to attacks on logic locking*

*Z. Han *et al.*, USENIX'21

SyncLock Summary

- Generally applicable to any RF transceiver
- First domain-specific logic locking
- No performance penalty
- Tiny overhead, negligible extra power consumption
- Plug-in IP
- No alterations in mixed-signal design flow
- Effective 512-bit key
- Only one valid key
- Resilient to all known attacks
- Patent filed in October 2022

Leaking Wireless ICs via Hardware Trojan-Infected Synchronization: Summary

- HT leaks data through the synchronization sequence
- Undetectable for inconspicuous receiver
- Generally applicable to any RF transceiver
- Small HT footprint: 0.109% of PHY area
- Undetectable by all known test-based and run-time defenses
- Throughput = 8 bits*number of frames per second = 750 Kbps

(indicative for short control frames such as ACK and CTS)