Secure and Efficient Initialization and Authentication Protocols for SHIELD

Chenglu Jin and Marten van Dijk

Secure Computation Laboratory
Department of Electrical & Computer Engineering
University of Connecticut

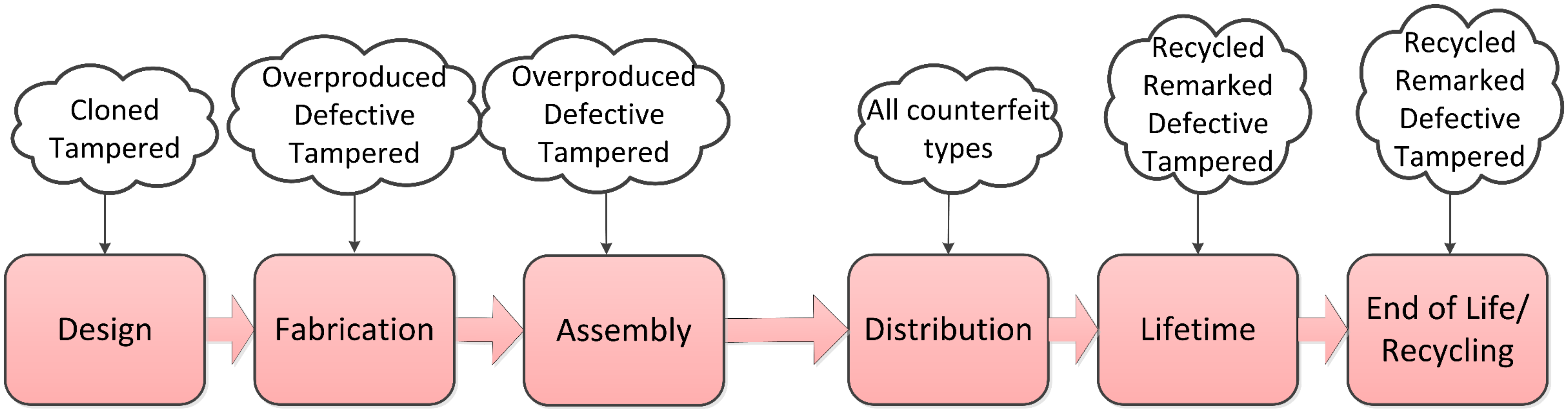
Email: chenglu.jin@uconn.edu

Outline

- Motivation
- SHIELD
- Adversarial Models
- DARPA's Authentication Protocol
- Try-and-Check Attack
- Proposed Authentication Protocol
- Security Properties and Performance Improvements
- Initialization Protocol
- Conclusion

UCONN

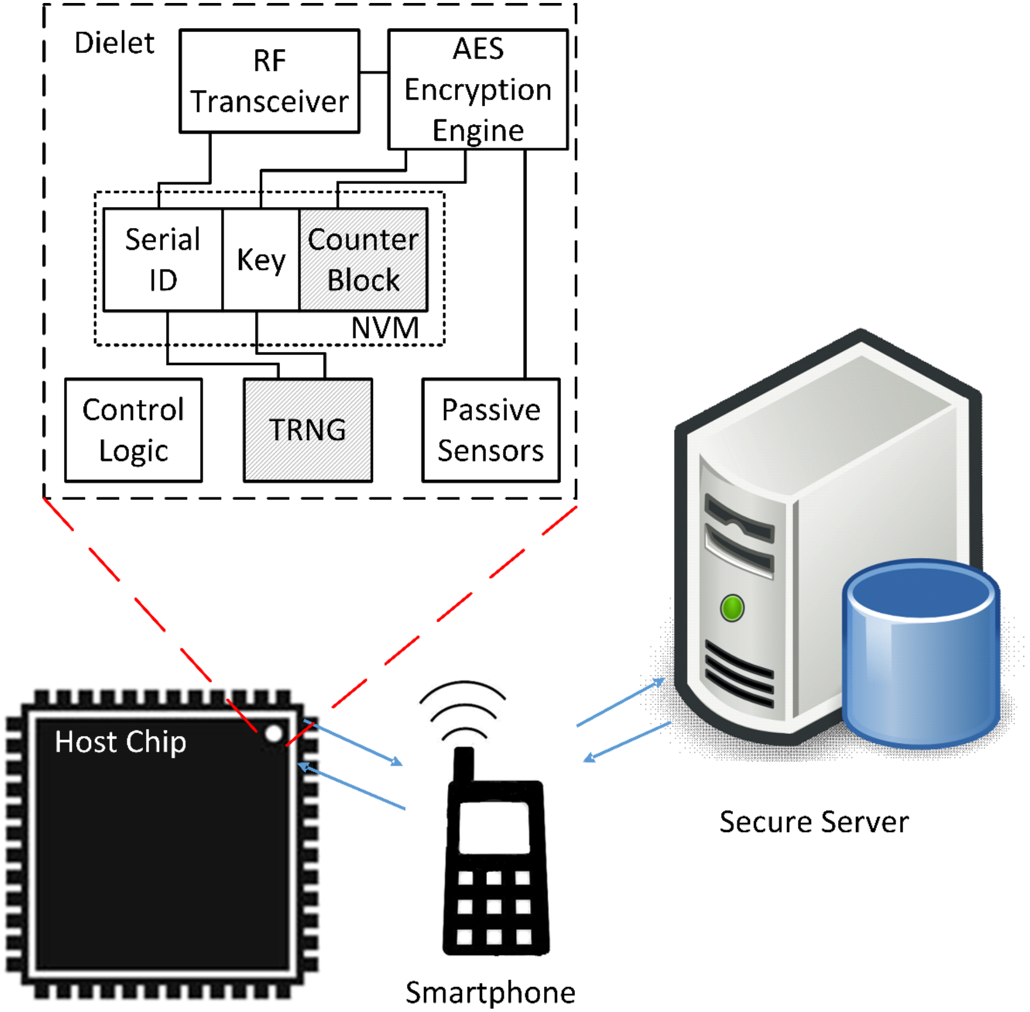
Motivation



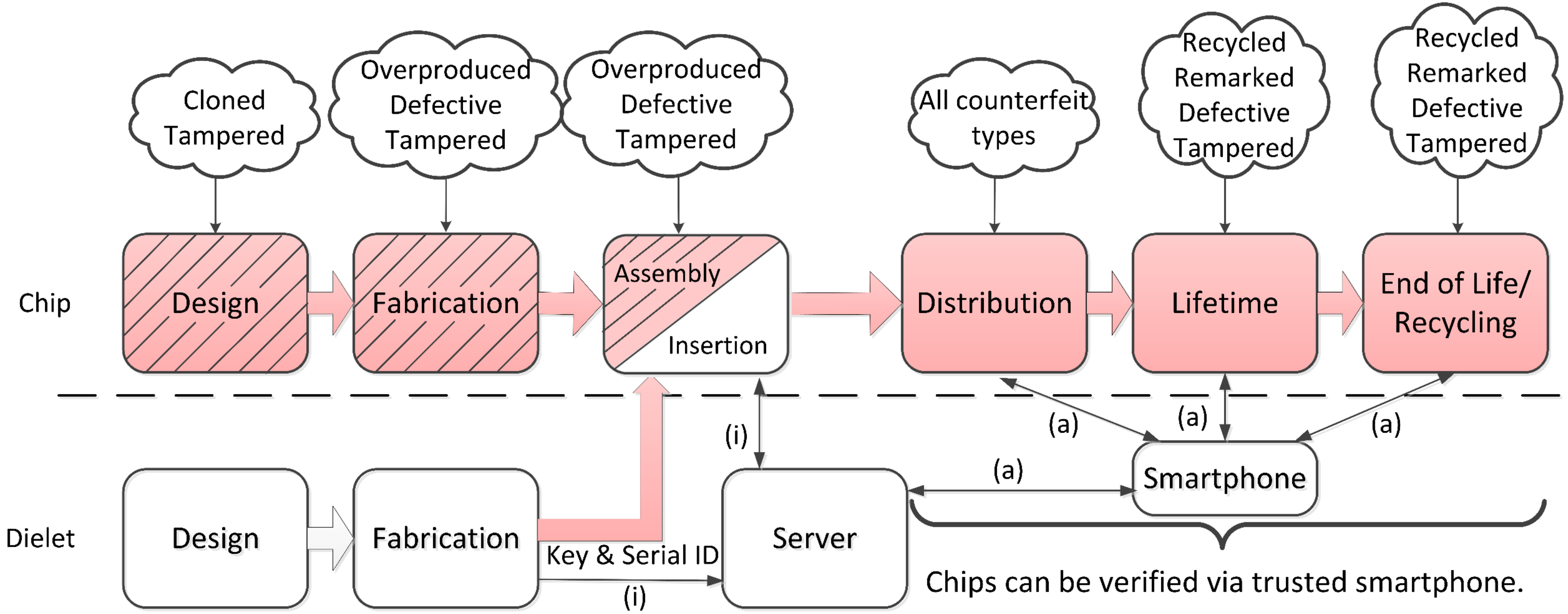
- Nowadays, untrusted IC supply chain introduces a variety of security threats.
- Many countermeasures are proposed. Usually they are specific for one security vulnerability in the supply chain.

SHIELD

- SHIELD (Supply Chain Hardware Integrity for Electronics Defense) was proposed by DARPA in 2014.
- A dielet chip inserted in the host package of a legitimate chip, in order to verify the host chip remotely.



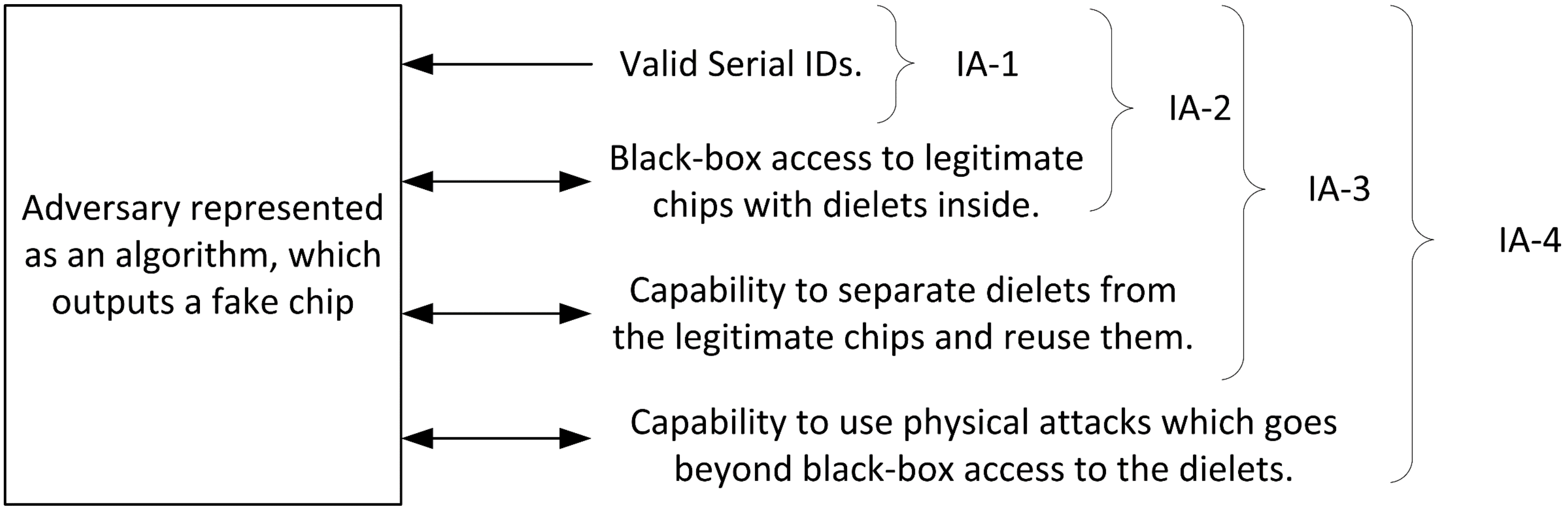
SHIELD Protected IC Supply Chain



UCONN

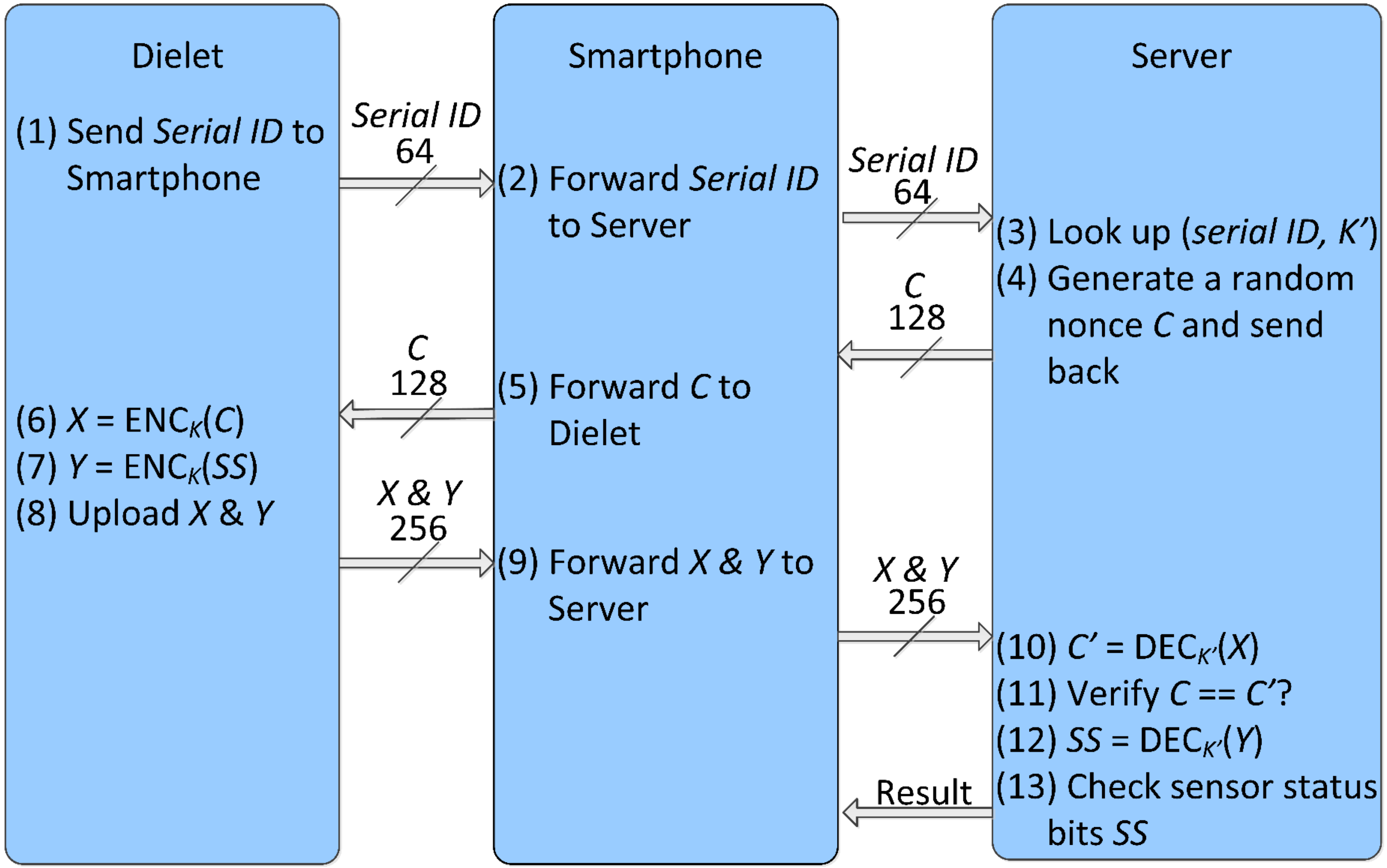
Adversarial Models

- Denial of Service (DoS):
  - Single dielet DoS: allowed by DARPA
  - Batch mode DoS: needs protection
- Impersonation Attacks (IA):



DARPA's Authentication Protocol

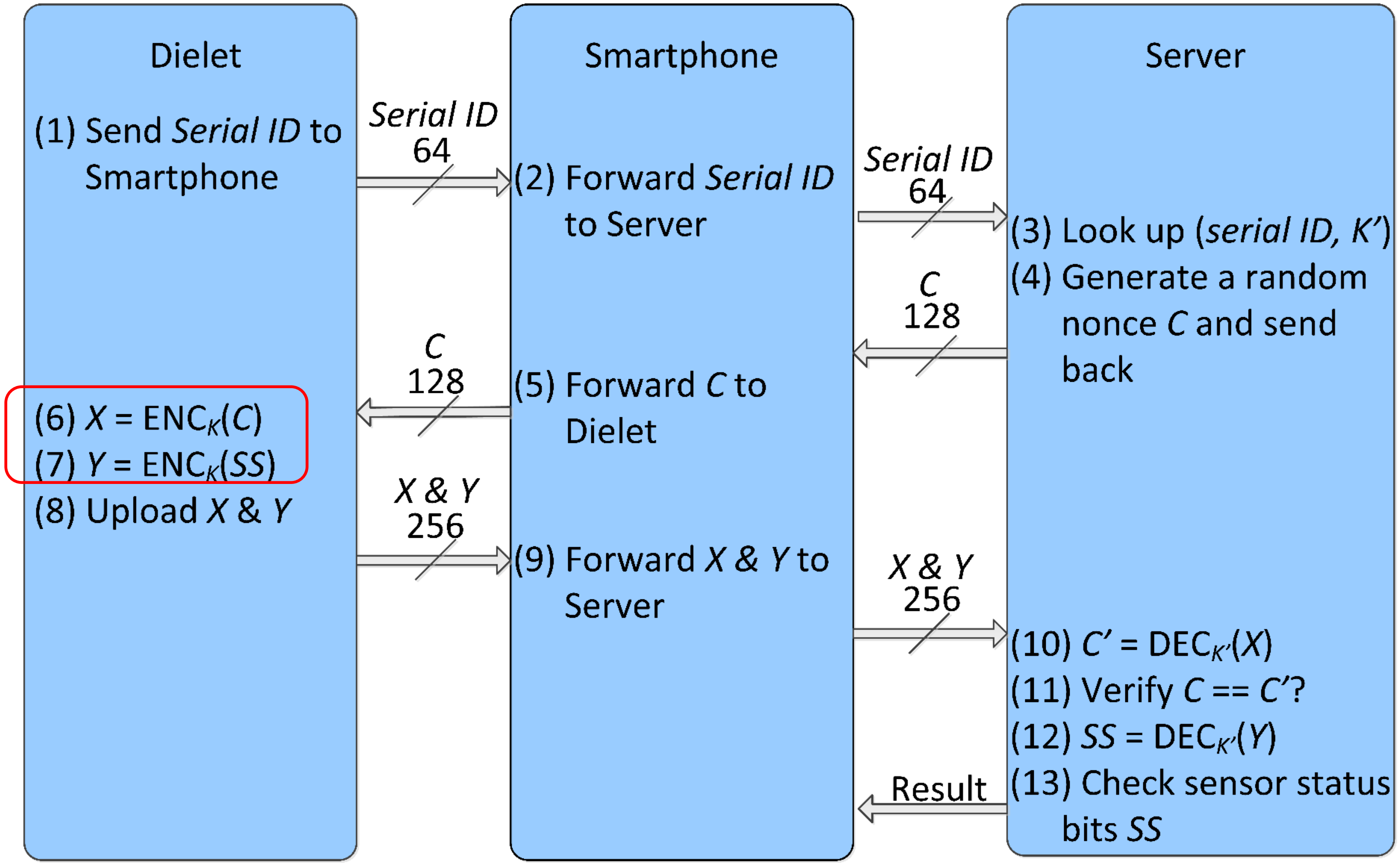
Authentication Protocol



UCONN

DARPA's Authentication Protocol

Authentication Protocol



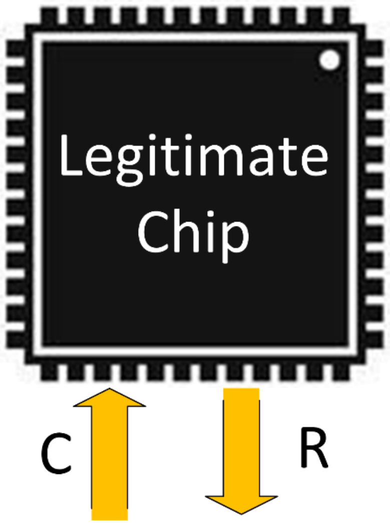
Deterministic Encryption!

Try-and-Check Attack

- Try-and-Check attack is one IA-3 attack, which nullifies the effectiveness of DARPA's authentication protocol in that the adversarial events will not be recorded and detected by the verifier.

Try-and-Check Attack

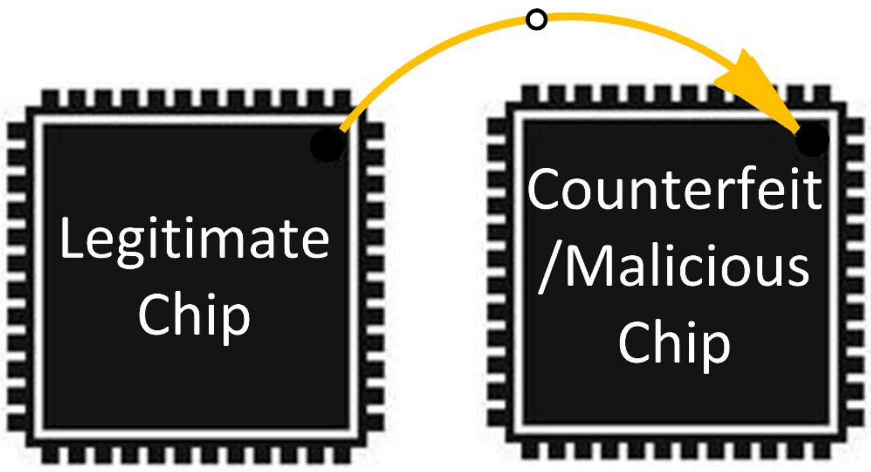
- Try-and-Check attack is one IA-3 attack, which nullifies the effectiveness of DARPA’s authentication protocol in that the adversarial events will not be recorded and detected by the verifier.
- 1. Apply Challenge C to a legitimate chip with a legitimate dielet inside, and store the response R = Enc(C) | Enc(S). S is the sensor status.



R = Enc(C) | Enc(S)

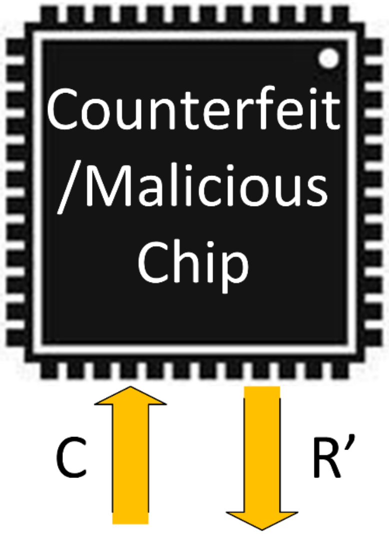
Try-and-Check Attack

- 2. Try to separate the dielet from the legitimate chip, and embed it into a counterfeit or malicious chip. This separation process may alter the sensor status S on the dielet.



Try-and-Check Attack

- 3. Check R = R’ ? If R = R’, it means that sensor status is not altered (S = S’). Therefore the attackers can conclude that this counterfeit/ malicious chip can be authenticated in the supply chain without being detected.



R’ = Enc(C) | Enc(S’)

How to fix this loophole?

- Use probabilistic encryption instead of deterministic encryption.

How to fix this loophole?

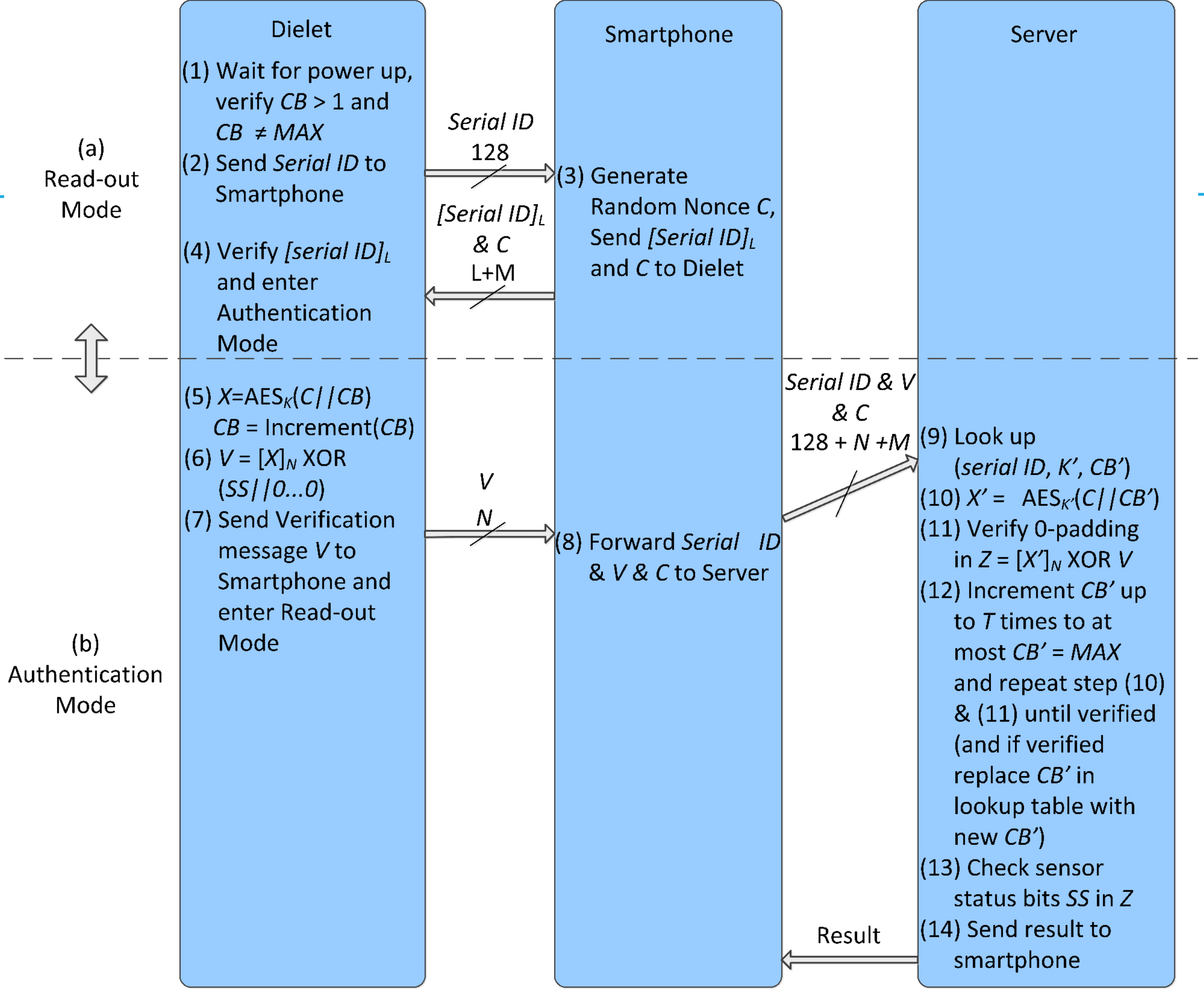
- Use probabilistic encryption instead of deterministic encryption.
- We suggest AES Counter Mode Encryption as an efficient solution.
- R = Enc(C|Counter) XOR S.

How to fix this loophole?

- Use probabilistic encryption instead of deterministic encryption.
- We suggest AES Counter Mode Encryption as an efficient solution.
- R = Enc(C|Counter) XOR S.
- Because this incremental counter value is never repeated, the same sensor status S will not generate the same response. This prevents Try-and-Check attack.

Proposed Authentication Protocol

UCONN


Dielet
Smartphone
Server
(a)
Read-out
Mode
(1) Wait for power up, verify CB > 1 and CB ≠ MAX
(2) Send Serial ID to Smartphone
Serial ID
128
(3) Generate Random Nonce C, Send [Serial ID]L and C to Dielet
[Serial ID]L
& C
L+M
(4) Verify [serial ID]L and enter Authentication Mode
(b)
Authentication
Mode
(5) X=AESK(C||CB)
CB = Increment(CB)
(6) V = [X]N XOR (SS||0...0)
(7) Send Verification message V to Smartphone and enter Read-out Mode
V
N
(8) Forward Serial ID & V & C to Server
Serial ID & V
& C
128 + N +M
(9) Look up (serial ID, K', CB')
(10) X' = AESK'(C||CB')
(11) Verify 0-padding in Z = [X']N XOR V
(12) Increment CB' up to T times to at most CB' = MAX and repeat step (10) & (11) until verified (and if verified replace CB' in lookup table with new CB')
(13) Check sensor status bits SS in Z
(14) Send result to smartphone
Result

Security Benefits

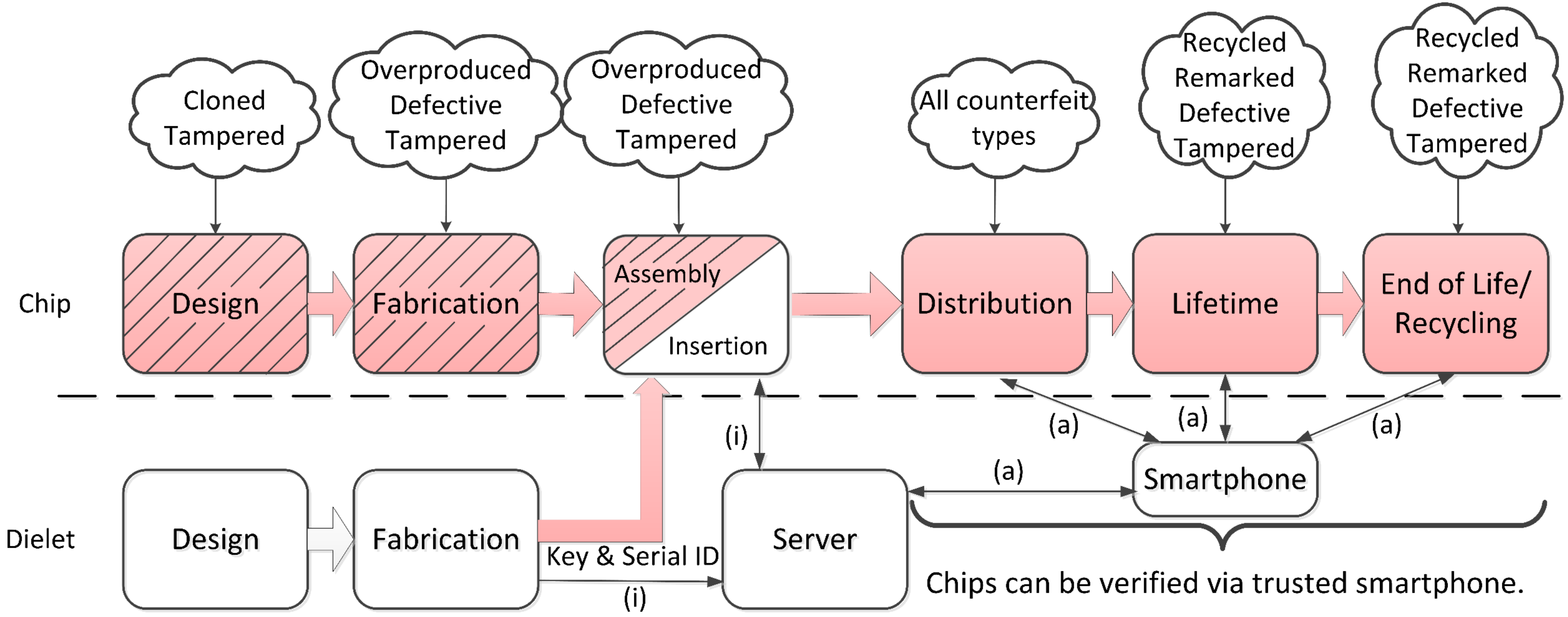
- Protect against IA-1, IA-2 and IA-3 attacks.
  - DARPA's protocol is vulnerable to Try-and-Check attack.
- Increase the difficulty of IA-4 attacks by limiting the power traces and incrementing counter values.
- Prevent batch mode DoS attack by adding a read-out mode before authentication mode.
- The counter of AES counter mode can be used as an indicator of suspicious offline behavior.

Performance Benefit

- Reduce the power consumption
  - Number of transmitted bits: 258 bits instead of 448 bits.
  - Number of encryptions: one encryption instead of two encryptions
- Speed up the protocol execution by halving the number of communication rounds with the server.

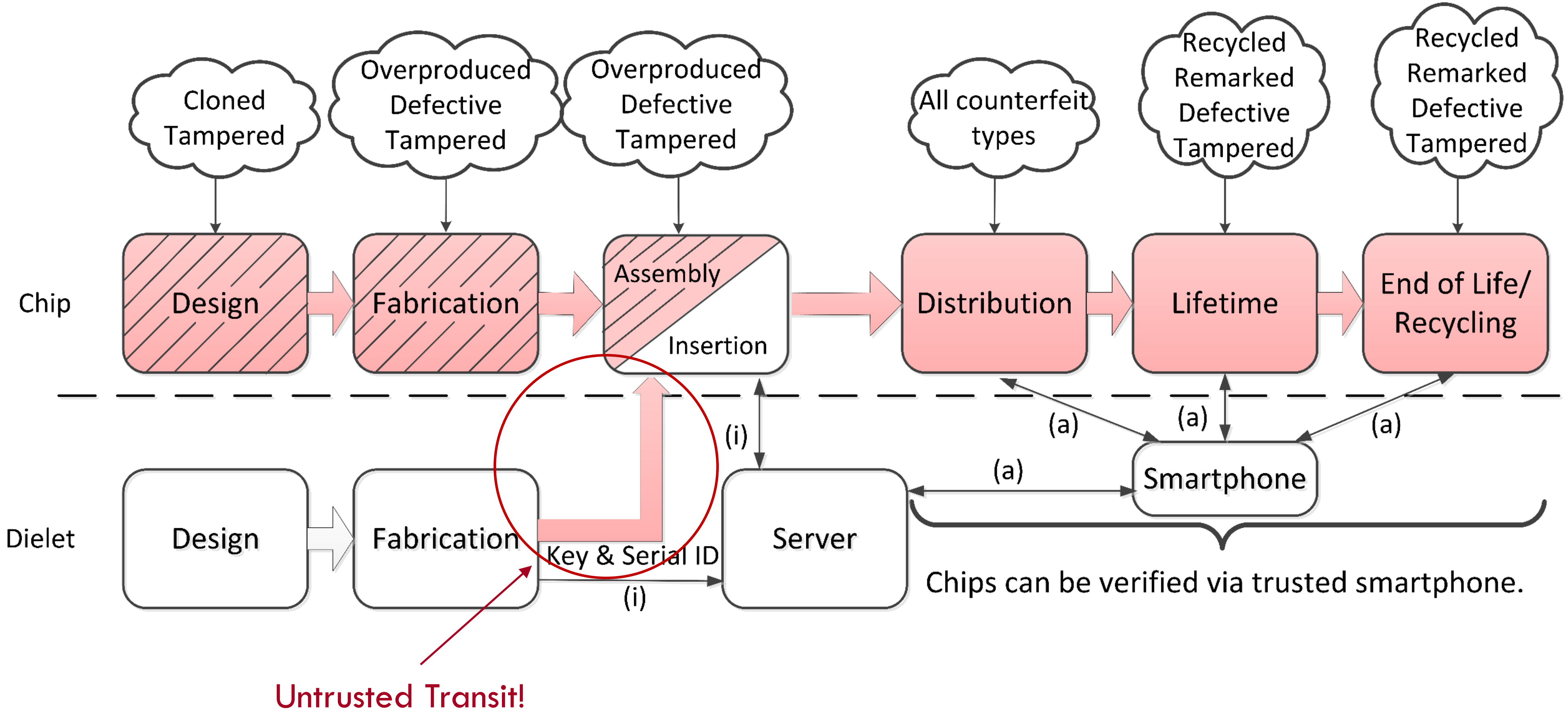
Dielet Initialization

- The main threat comes from the untrusted transit between dielet fabrication facilities and insertion facilities.

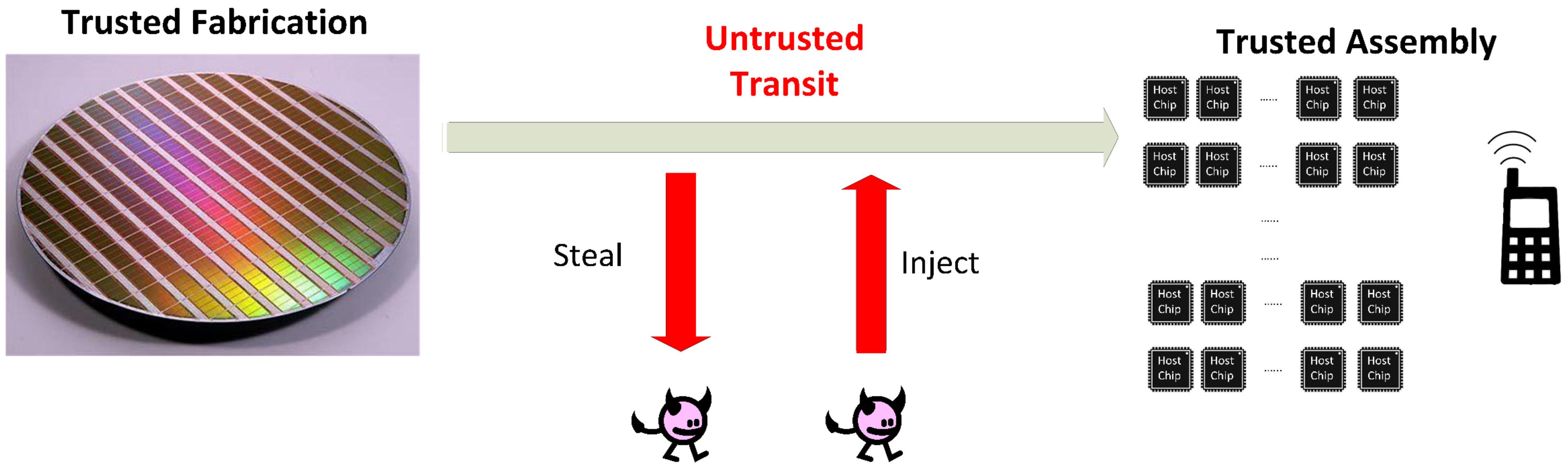


Dielet Initialization

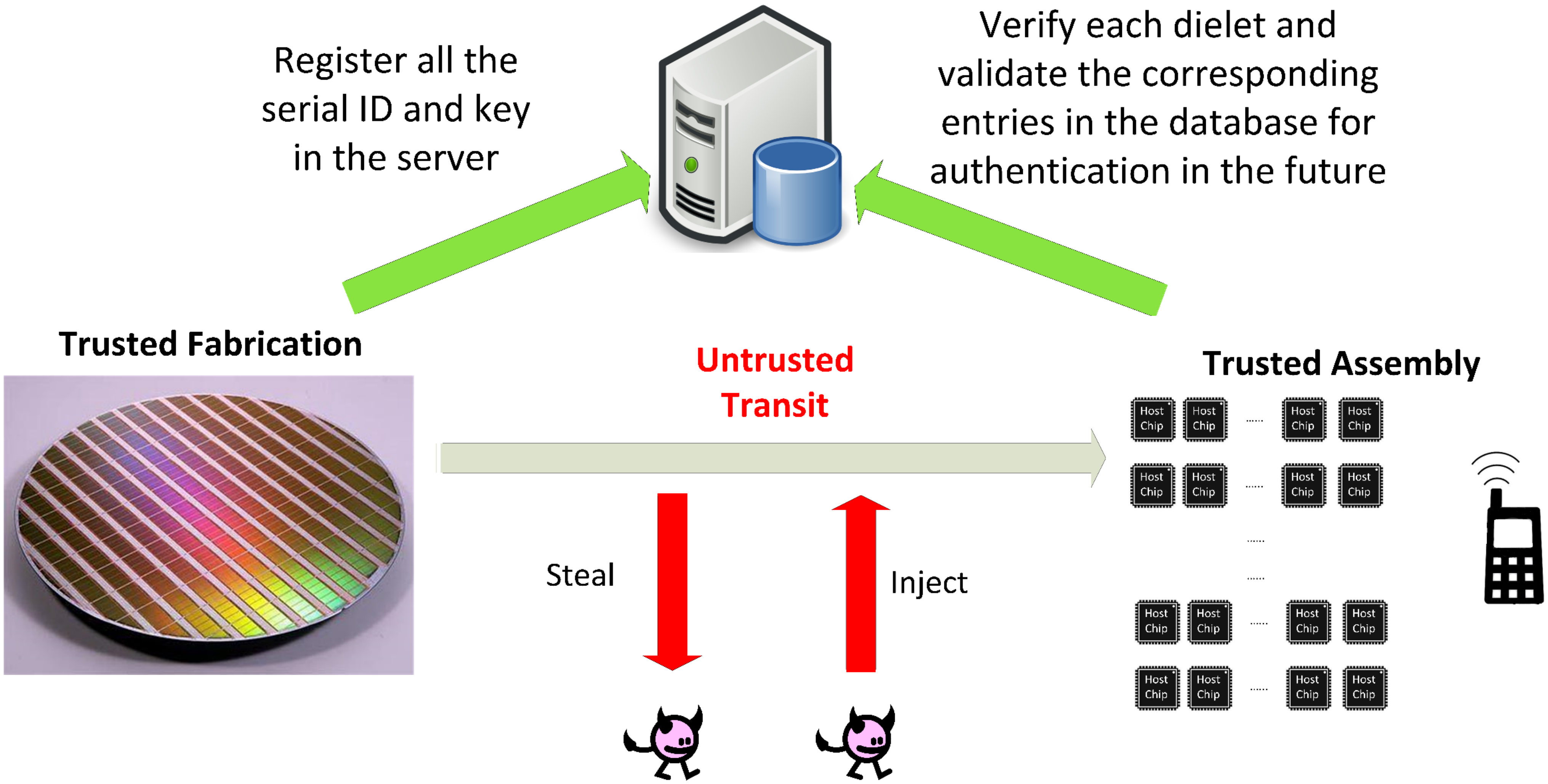
- The main threat comes from the untrusted transit between dielet fabrication facilities and insertion facilities.



Initialization Protocol



Initialization Protocol



Benefits

- Due to a one-time initialization and two-phase activation construct in our initialization protocol, transits between trusted fabrication and trusted assembly facilities can be untrusted.
- On-board TRNG allows dielets to efficiently generate the secret keys and serial IDs in parallel.

Conclusion

- We introduce a "try-and-check" attack which nullifies the effectiveness of one of SHIELD's main goals of being able to detect and trace adversarial activities with significant probability.
- We introduce an improved authentication protocol which resists the try-and-check attack, compared to DARPA's example authentication protocol.
- We introduce the first concrete initialization protocol.
- The additional area utilization for our authentication and initialization protocols compared to DARPA's authentication protocol is only 4% of the allowed area of the dielet ($0.01mm^2$) in 32nm technology.
- Our findings and rigorous analysis are of utmost importance for the team which received DARPA's funding for implementing SHIELD.

ePrint available at: http://eprint.iacr.org/2015/210

Thank you!