Breaking Korea Transit Card with Side-Channel Attack -Unauthorized Recharging-

Black Hat Asia 2017

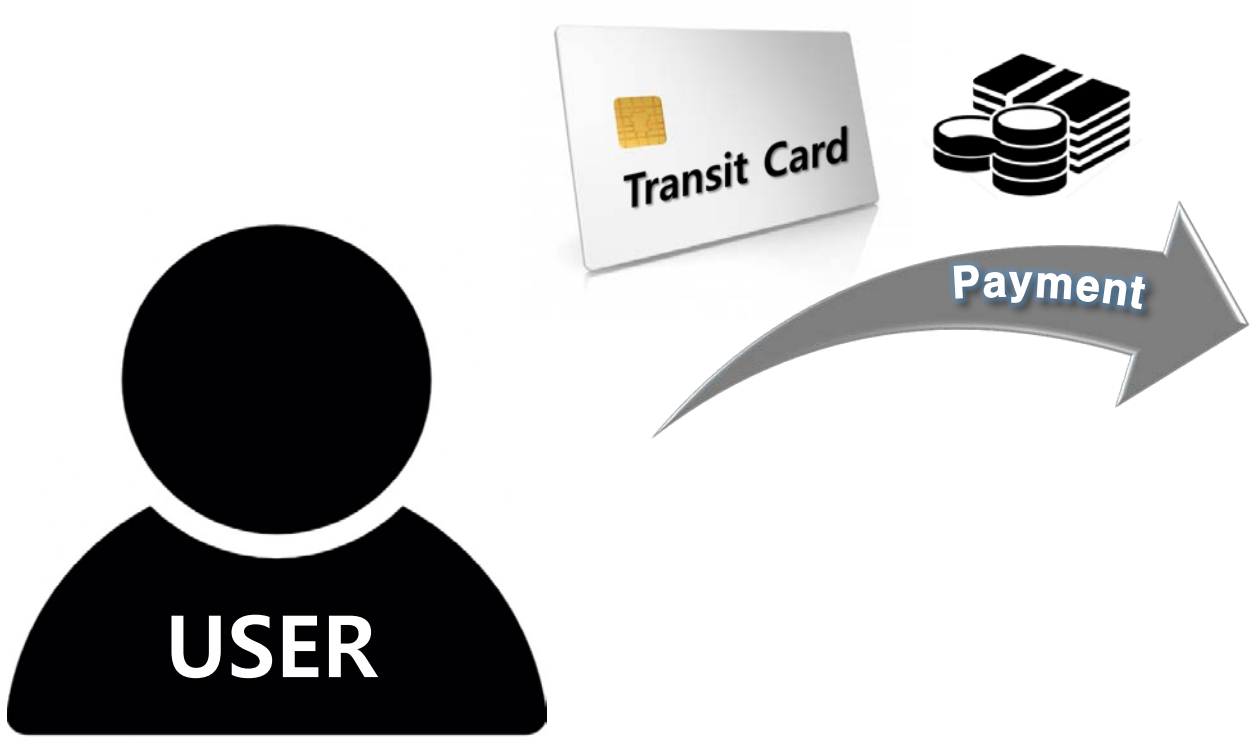
Tae Won Kim, Tae Hyun Kim, and Seokhie Hong

Outline

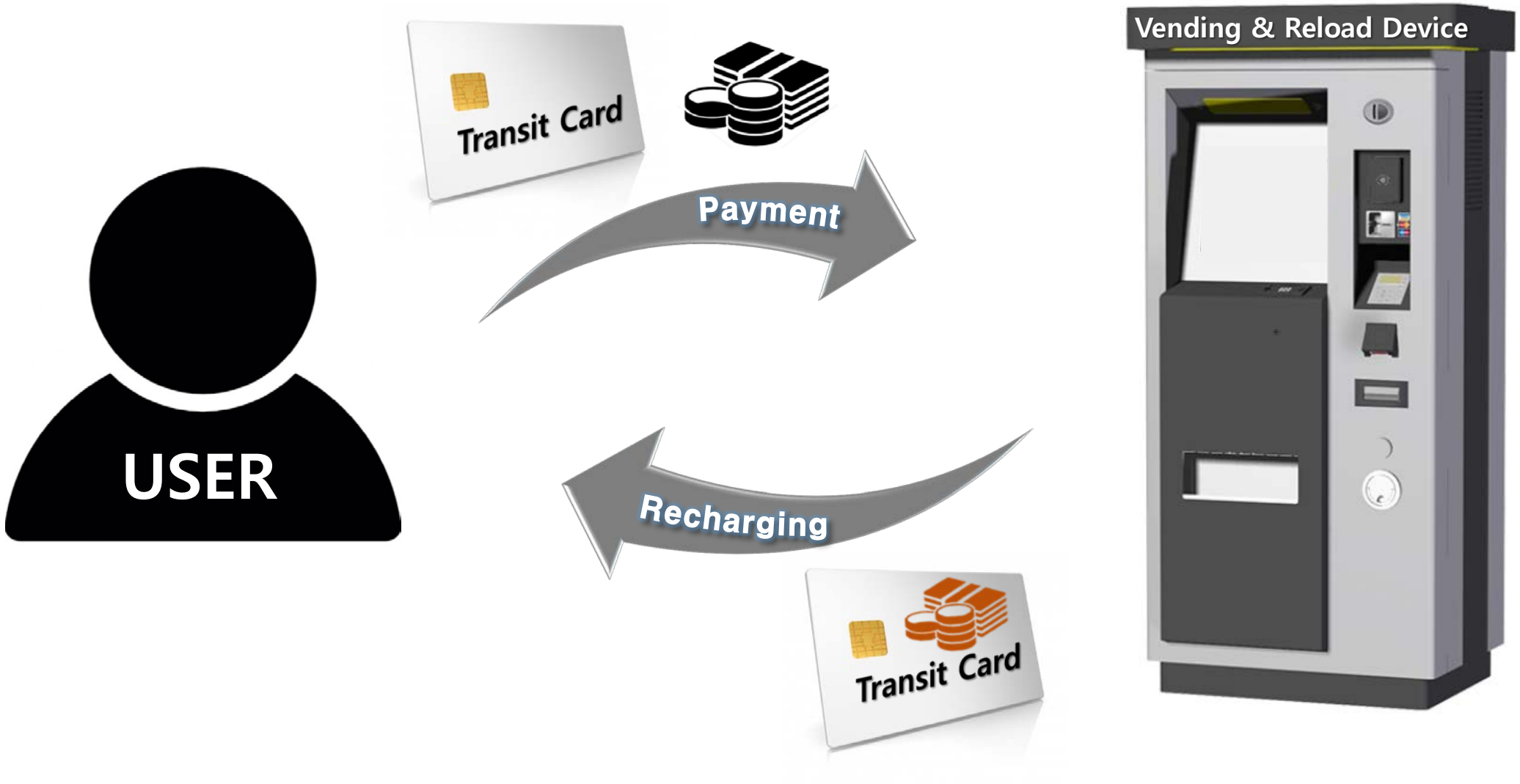
1. Attack Goal & Scenario
2. Target Device Details
   - Introduction of Target Device
   - Authentication Protocol Analysis
   - Cryptosystem
3. Key Recovery Attack
   - Attack environment & Measurement Set-Up
   - Attack Overview
   - Attack Results
4. Recharging Simulation
5. Conclusion

1. Attack Goal & Scenario
2. Target Device Details
   - Introduction of Target Device
   - Authentication Protocol Analysis
   - Cryptosystem
3. Key Recovery Attack
   - Attack environment & Measurement Set-Up
   - Attack Overview
   - Attack Results
4. Recharging Simulation
5. Conclusion

Recharging on Transit Card

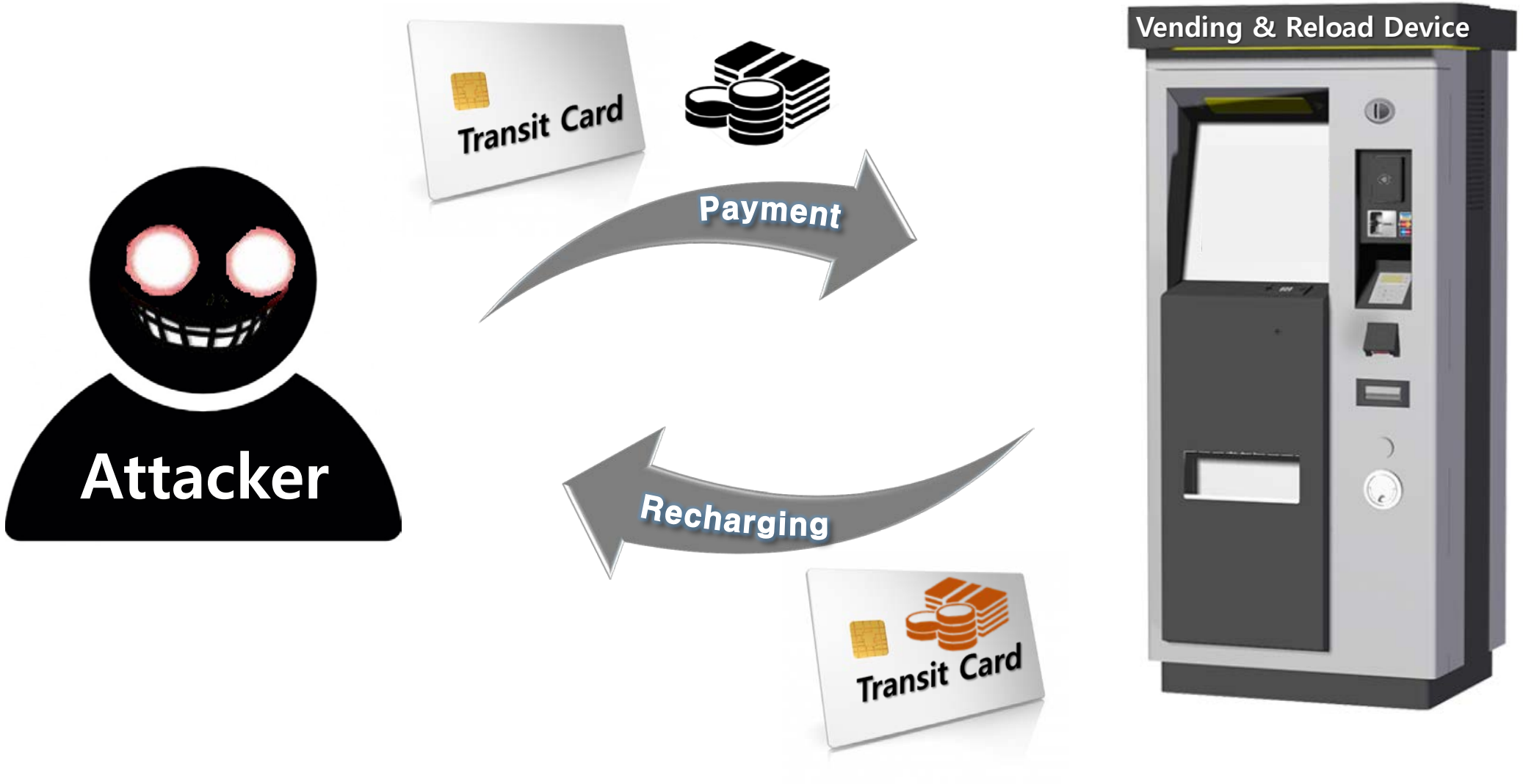


Recharging on Transit Card



Our Ultimate Goal

Free recharging as much as attacker want

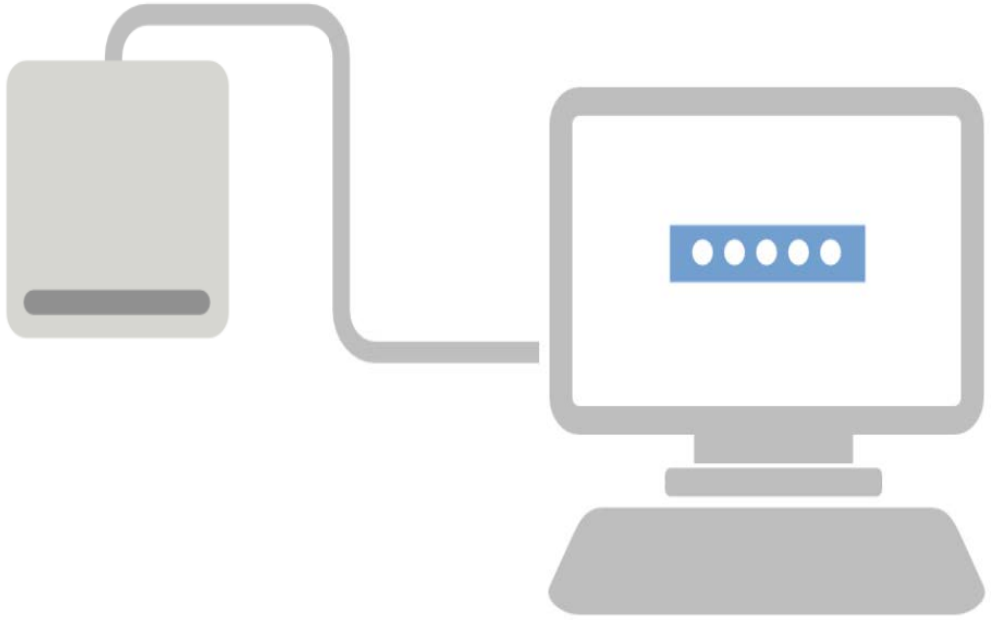


Attack Scenario toward Goal

Phase 1. **Extract authentication key for recharging using side-channel analysis attack**

Attack Scenario toward Goal

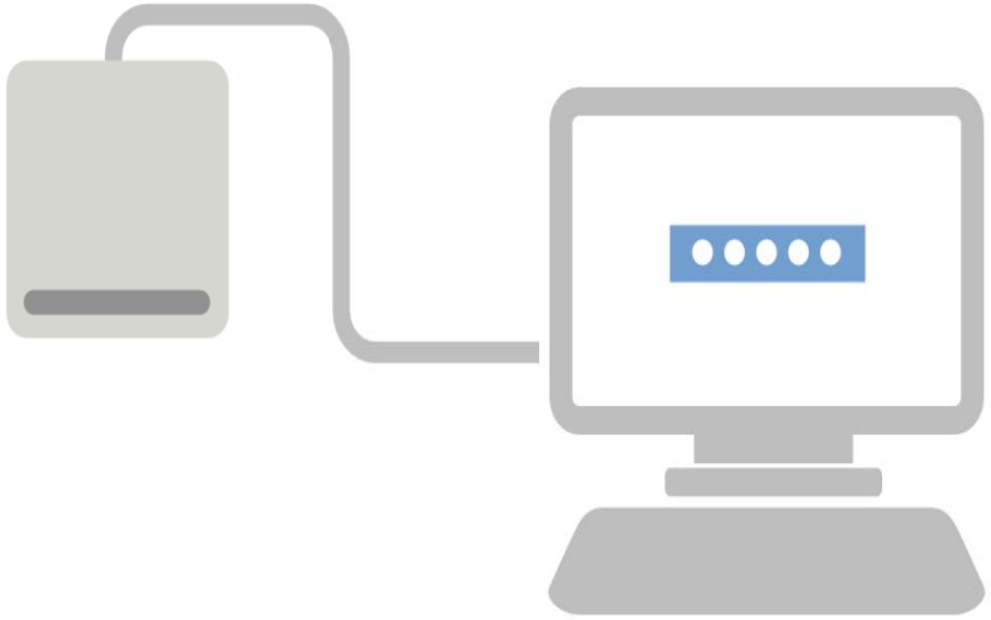
Phase 1. Extract authentication key for recharging using side-channel analysis attack



Phase 2. Design free recharging tool with restored key

Attack Scenario toward Goal

Phase 1. Extract authentication key for recharging using side-channel analysis attack



Phase 2. Design free recharging tool with restored key

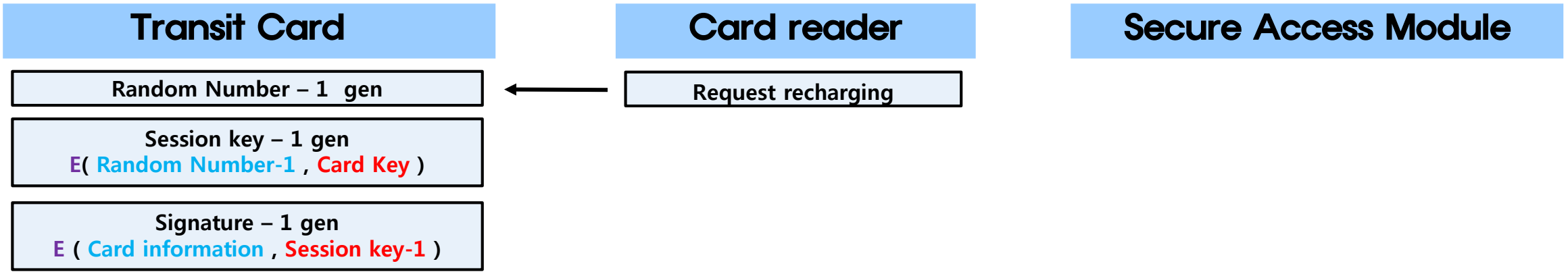
1. Attack Goal & Scenario
2. Target Device Details
   - Introduction of Target Device
   - Authentication Protocol Analysis
   - Cryptosystem
3. Key Recovery Attack
   - Attack environment & Measurement Set-Up
   - Attack Overview
   - Attack Results
4. Recharging Simulation
5. Conclusion

Target device

- Transit card
  - Pre-paid transit card for the freeway in Korea
  - Over 800 million cards were issued and used
  - Cafeteria and convenience store in the freeway service area
  - Movie theater, Airport car park etc...
- Contact Smartcard
  - Equipped with cryptographic engine in hardware level
  - Countermeasure employed against side-channel attacks
  - Support ISO/IEC 7816 standard and KS X 6924 Korea standard

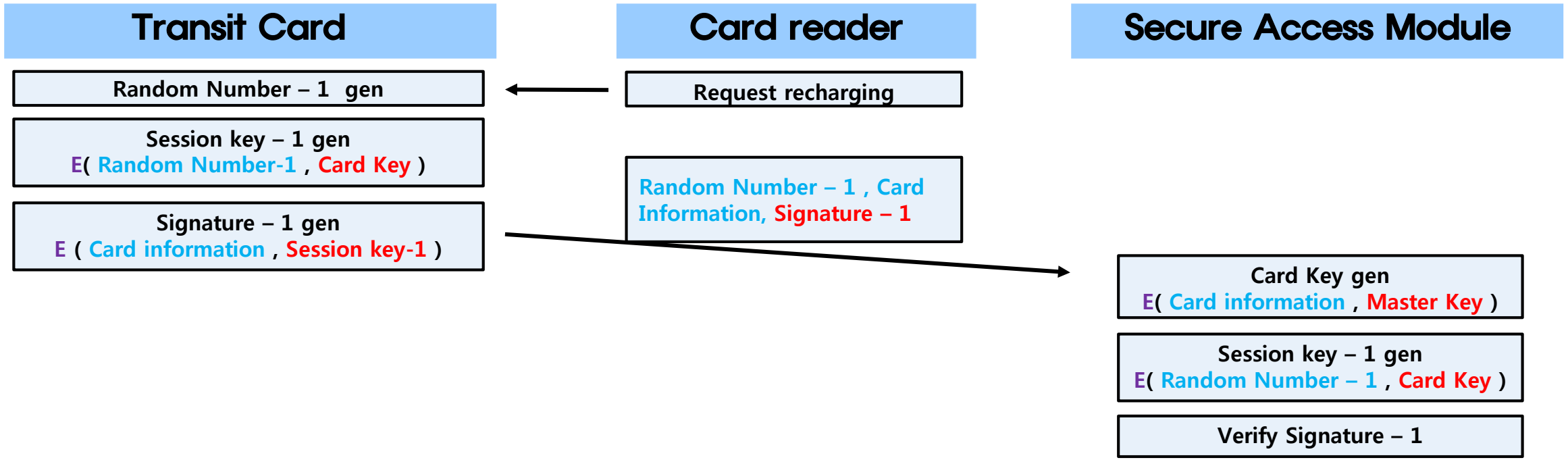
Authentication protocol for recharging

Public information
Secret information
Crypto algorithm



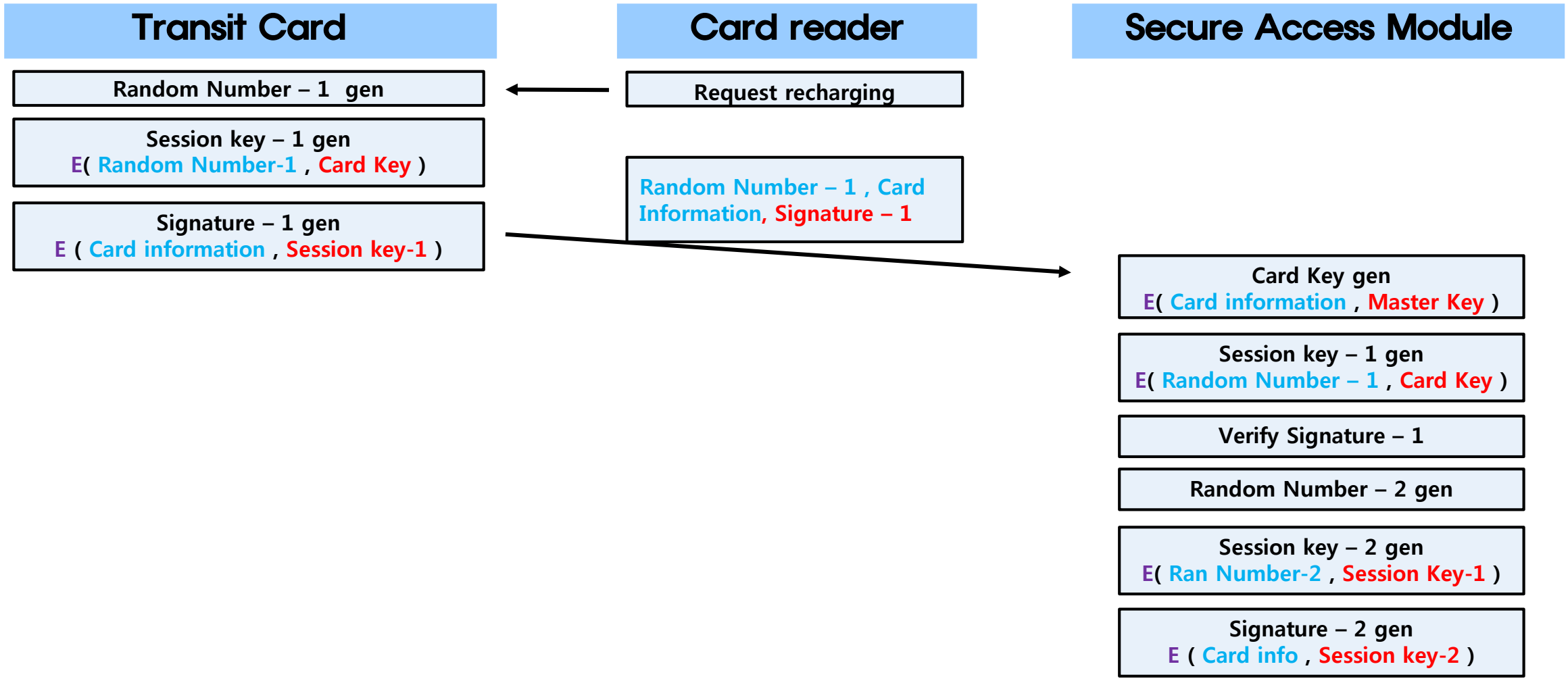
Authentication protocol for recharging

Public information
Secret information
Crypto algorithm



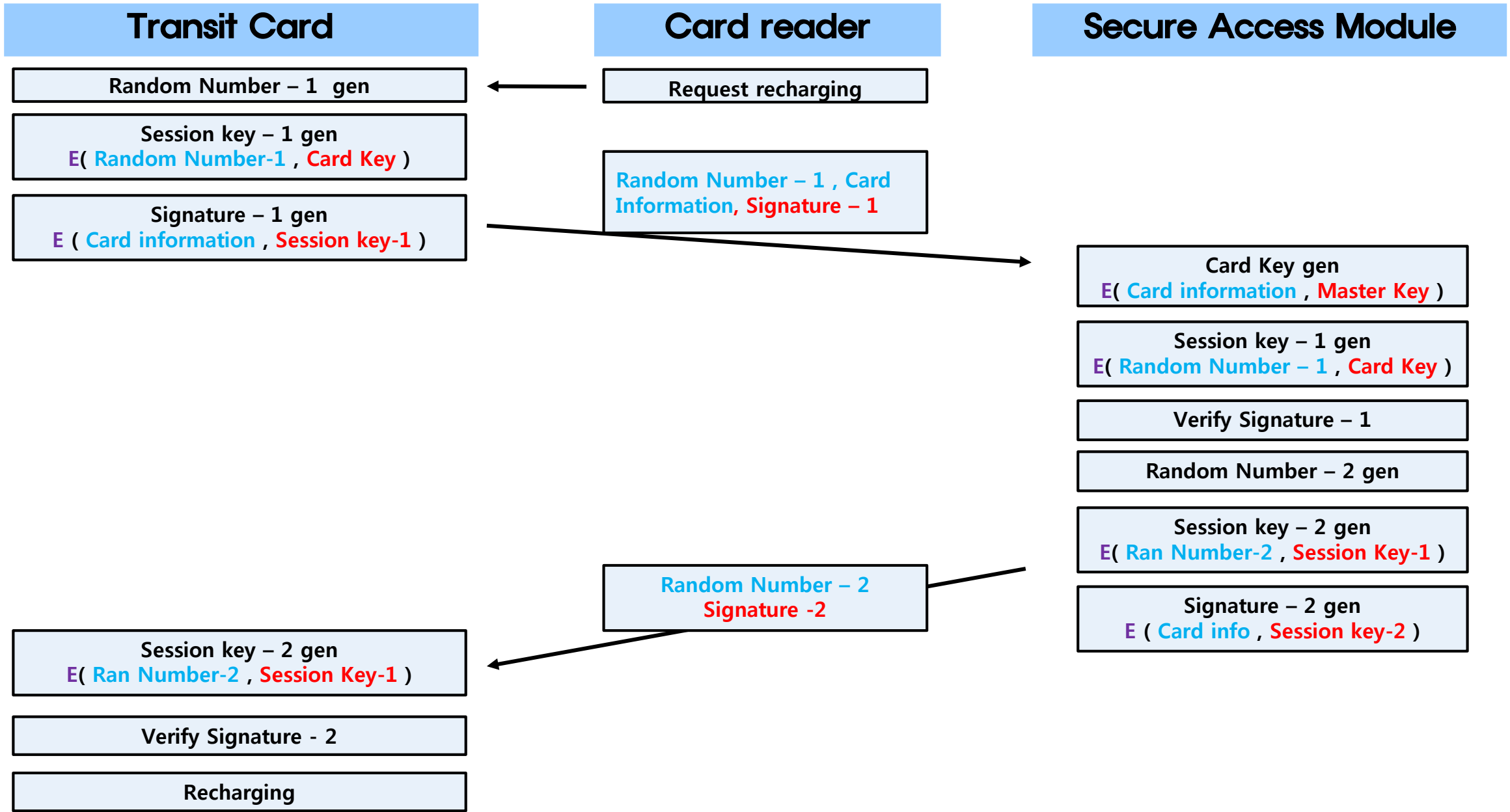
Authentication protocol for recharging

Public information
Secret information
Crypto algorithm



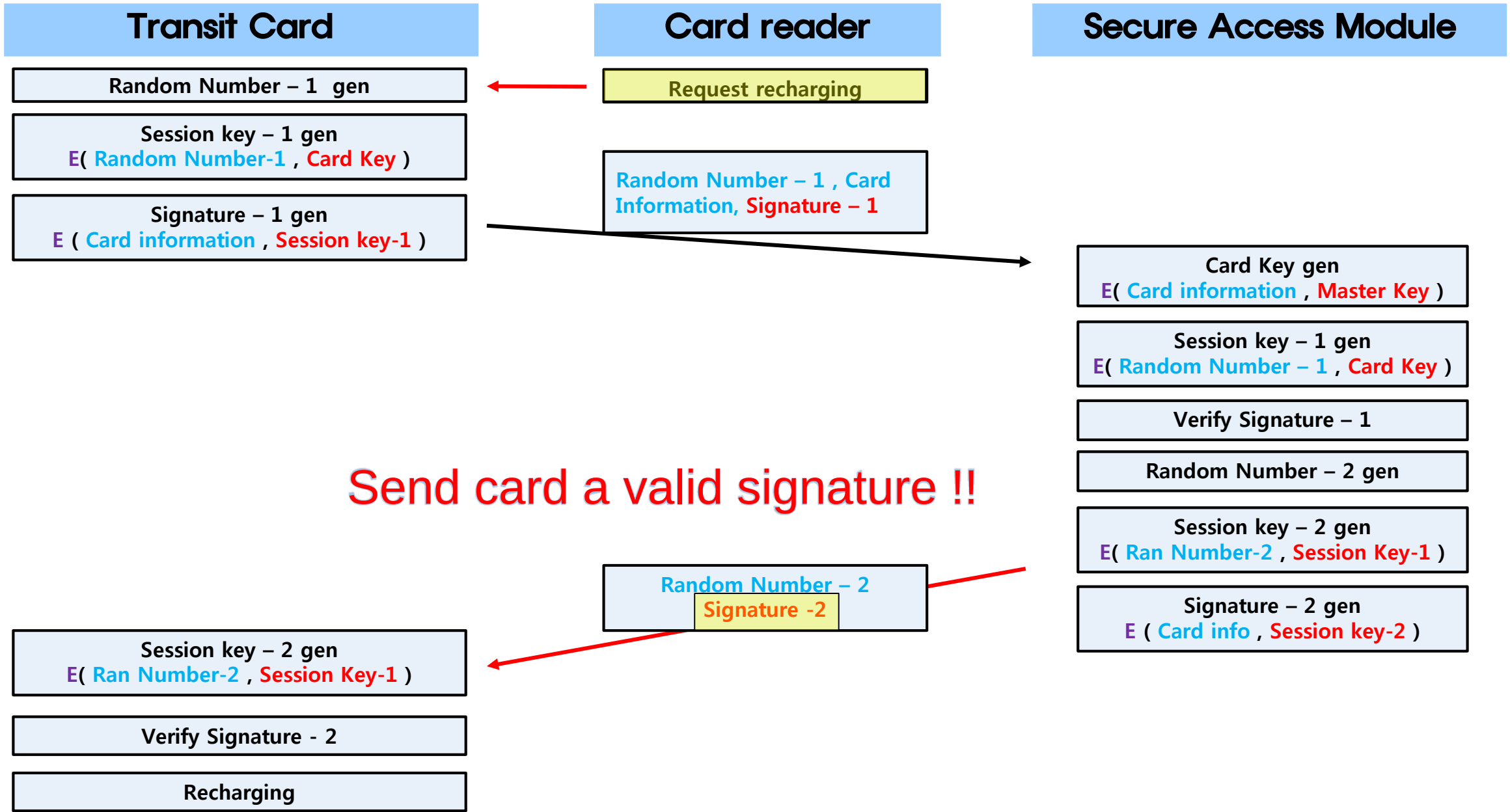
Authentication protocol for recharging

Public information
Secret information
Crypto algorithm



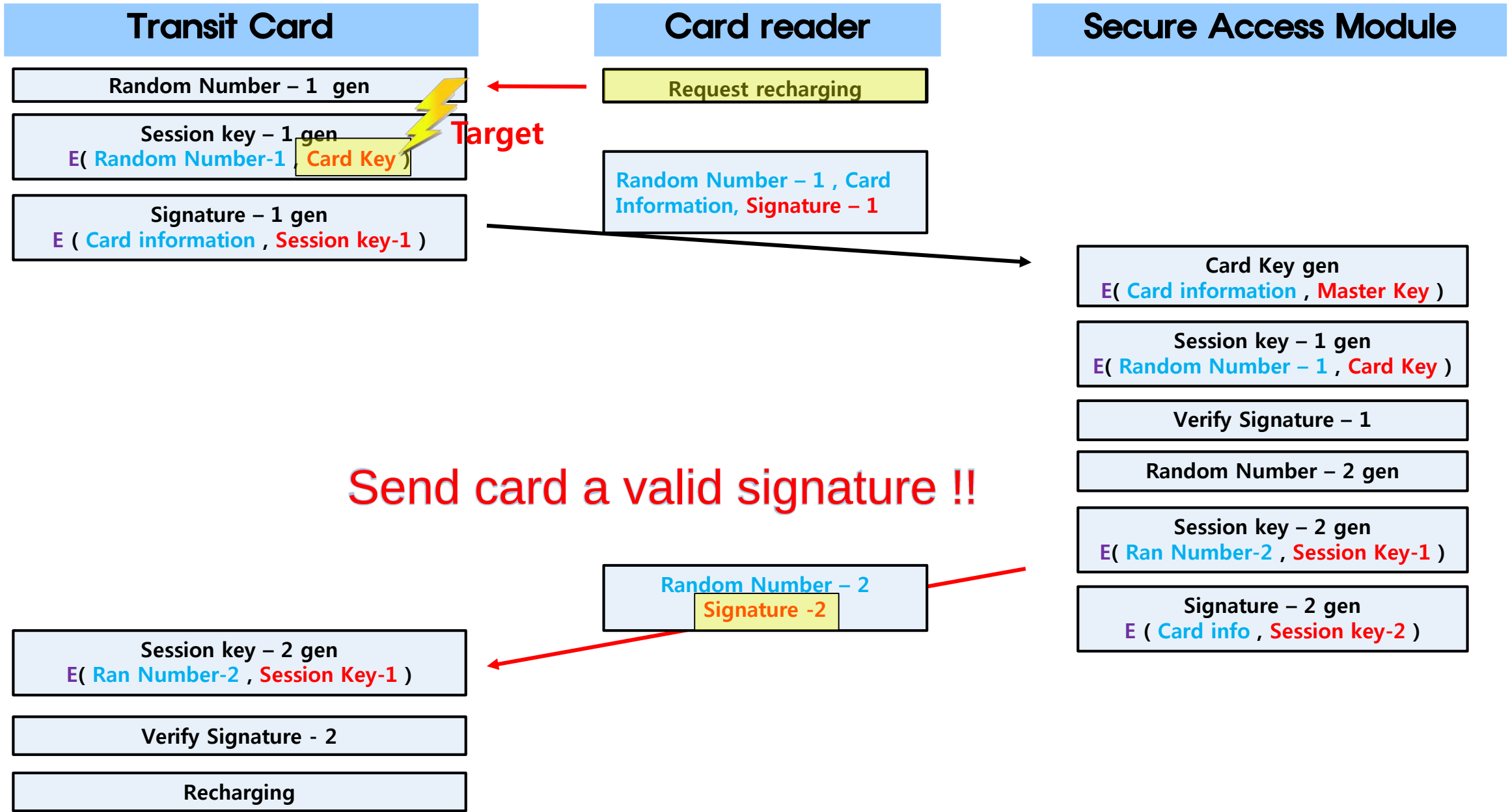
Authentication protocol for recharging

Public information
Secret information
Crypto algorithm



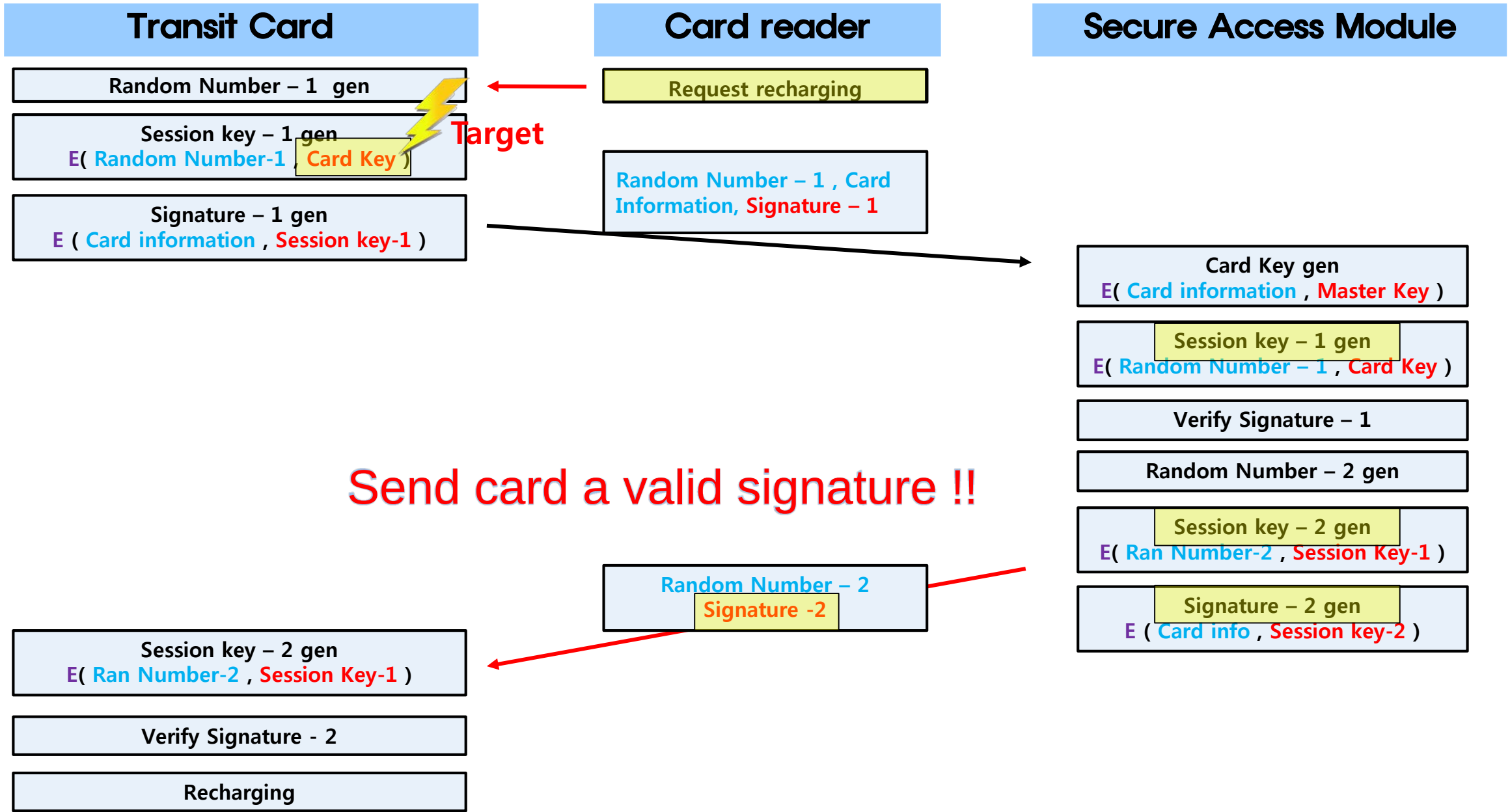
Authentication protocol for recharging

Public information
Secret information
Crypto algorithm

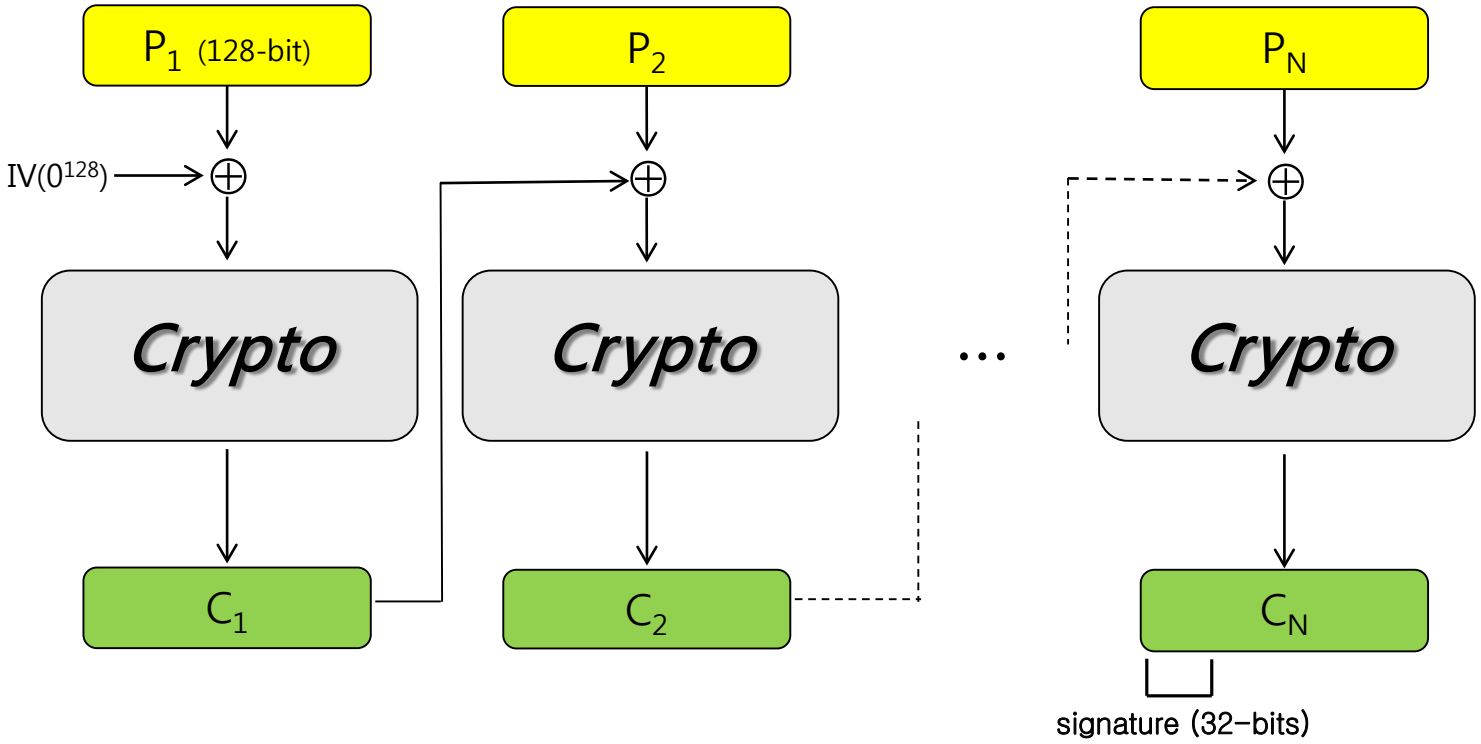


Authentication protocol for recharging

Public information
Secret information
Crypto algorithm



Crypto Algorithm Analysis



- Sign & verify

  => performs crypto Algorithm

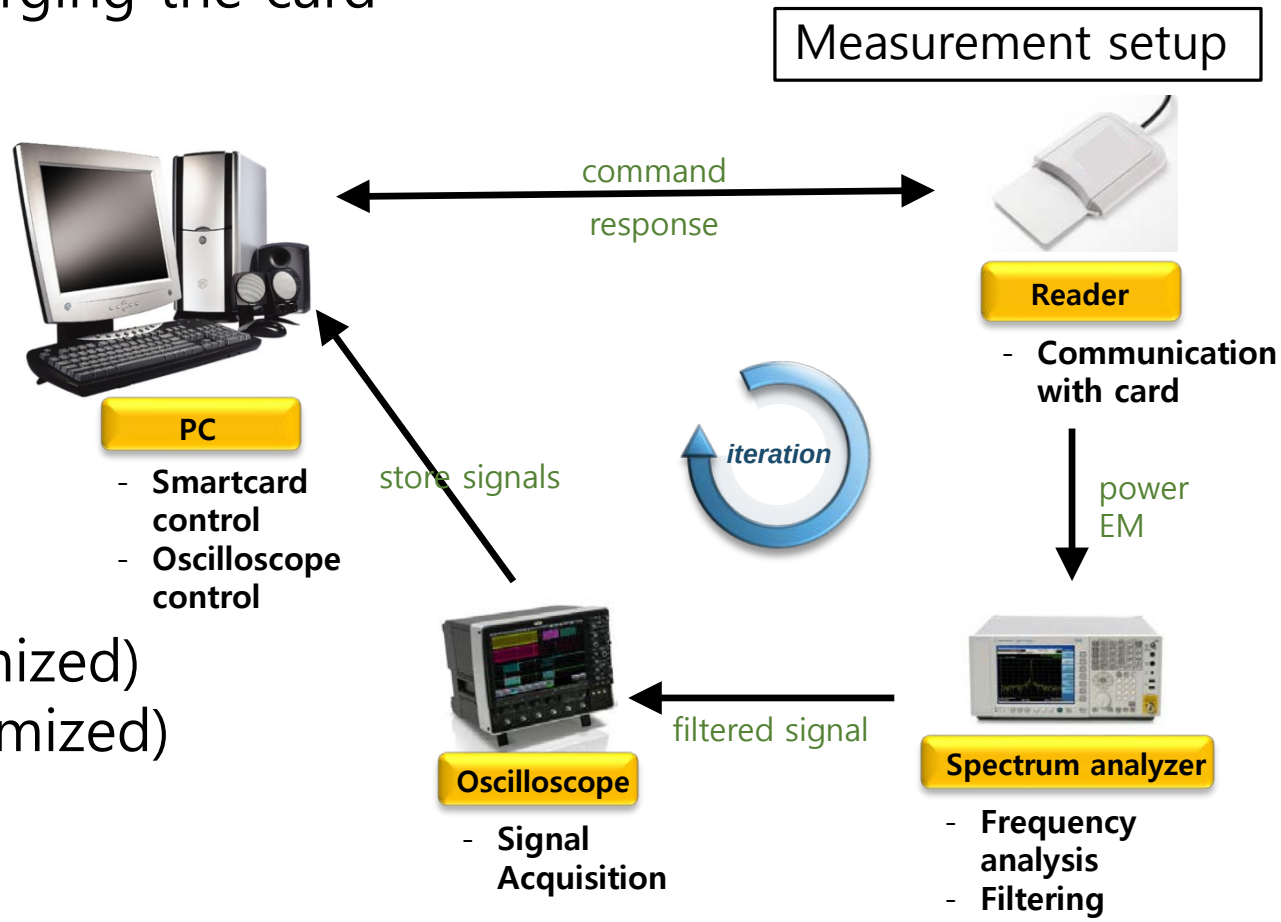
- 128-bit Block cipher & operation mode
  - Crypto function => Two Triple-DES
  - Cipher Block Chaining (CBC) mode
- Initial Vector
  - 0^{128}
- Signature value
  - Most significant 32-bit of last ciphertext block
- Padding rule
  - 80 00 00 00 …

Outline

1. Attack Goal & Scenario
2. Target Device Details
   - Introduction of Target Device
   - Authentication Protocol Analysis
   - Cryptosystem
3. Key Recovery Attack
   - Attack environment & Measurement Set-Up
   - Attack Overview
   - Attack Results
4. Recharging Simulation
5. Conclusion

Attack Environment

- Attack under the secure transit card
  - APDU commands for recharging the card
- Hardware
  - Board
  - Card reader
  - Oscilloscope
  - Spectrum Analyze
- Software
  - For the acquisitions(Customized)
  - Signal preprocessing(Customized)
  - Analysis(Customized)
  - Matlab

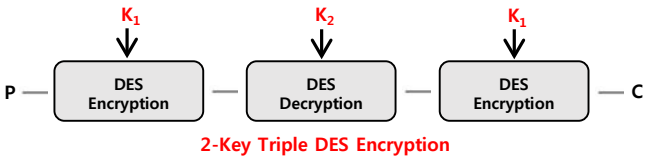


Attack Overview

Phase 1 : Locate the positon of T-DES

1. I/O signal analysis
2. Visual Inspection
   - Find similar patterns
3. Plaintext CPA
   - Find location of relating plaintext
   - Can deduce location of target operation from plaintext location

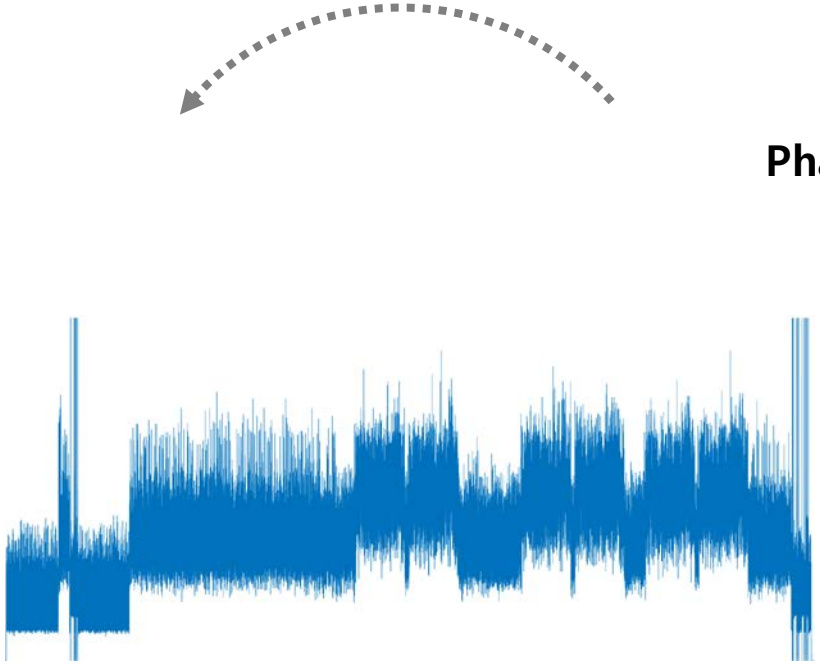
Attack Overview



2-Key Triple DES Encryption

Phase 2 : DPA Attack for key recovery

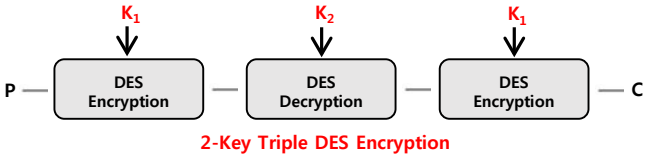
1. Pre-processing
   - Compression
   - Alignment
2. First Round attack in the DES
   - 48-bit Key recovery
   - 6-bitwise CPA
3. Correction of error
   - Prevent error propagation
   - Method based on BS-CPA
4. 2-15 Round attack
   - 56-bit full-key recovery
   - 32-bitwise CPA



Phase 1 : Locate the positon of T-DES

1. I/O signal analysis
2. Visual Inspection
   - Find similar patterns
3. Plaintext CPA
   - Find location of relating plaintext
   - Can deduce location of target operation from plaintext location

Attack Overview



2-Key Triple DES Encryption

Phase 1 : Locate the positon of T-DES

1. I/O signal analysis
2. Visual Inspection
   - Find similar patterns
3. Plaintext CPA
   - Find location of relating plaintext
   - Can deduce location of target operation from plaintext location

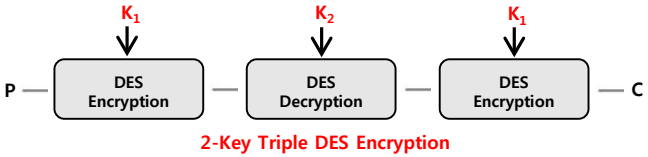
Phase 2 : DPA Attack for key recovery

1. Pre-processing
   - Compression
   - Alignment
2. First Round attack in the DES
   - 48-bit Key recovery
   - 6-bitwise CPA
3. Correction of error
   - Prevent error propagation
   - Method based on BS-CPA
4. 2-15 Round attack
   - 56-bit full-key recovery
   - 32-bitwise CPA

Phase 3 : Verification of restored the key

- Compare the signature value through card response with the signature value generated by recovered key
- This is only way to confirm the validity

Attack Overview



2-Key Triple DES Encryption

Phase 1 : Locate the positon of T-DES

1. I/O signal analysis
2. Visual Inspection
   - Find similar patterns
3. Plaintext CPA
   - Find location of relating plaintext
   - Can deduce location of target operation from plaintext location

Phase 2 : DPA Attack for key recovery

1. Pre-processing
   - Compression
   - Alignment
2. First Round attack in the DES
   - 48-bit Key recovery
   - 6-bitwise CPA
3. Correction of error
   - Prevent error propagation
   - Method based on BS-CPA
4. 2-15 Round attack
   - 56-bit full-key recovery
   - 32-bitwise CPA

Phase 3 : Verification of restored the key

- Compare the signature value through card response with the signature value generated by recovered key
- This is only way to confirm the validity

If fail, return to the beginning

Repeat until the key is found

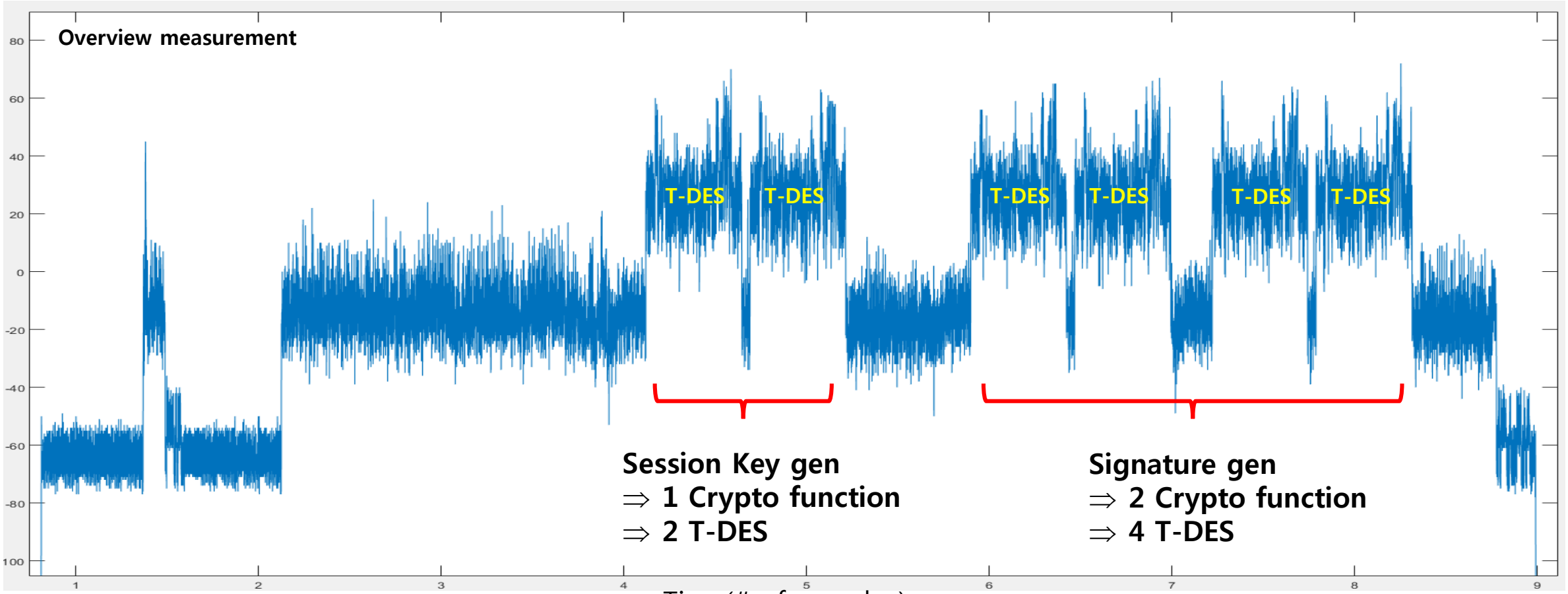
Tremendous trials and errors!!

Some Problems for Key Recovery

- Hiding Countermeasure
  - Pre-processing for mitigation
    - Filtering, Alignment
  - Increases the number of traces
- Alignment
  - Align, whenever guess the location of target operation
  - There is no good reference pattern
    - By effect of hiding countermeasure
  - Need elaborated work
    - One or two point of misalignment leads to attack failure
- More requirement of time cost, memory
  - Compression of trace
  - Parallel processing

Visual Inspection

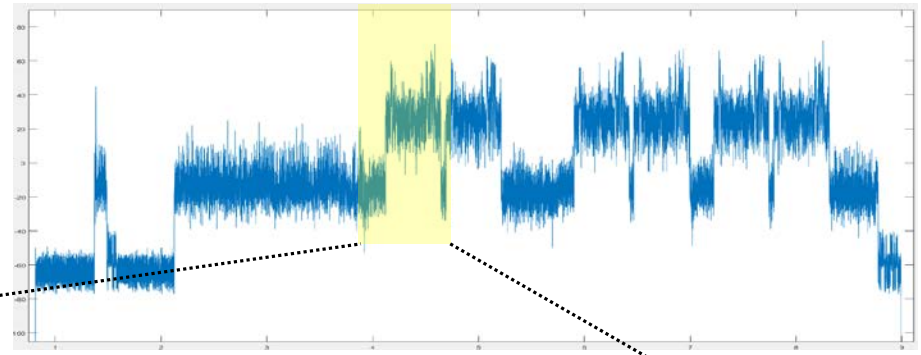
- Search for similar patterns
- Execution of three crypto function
  =>6 T-DES

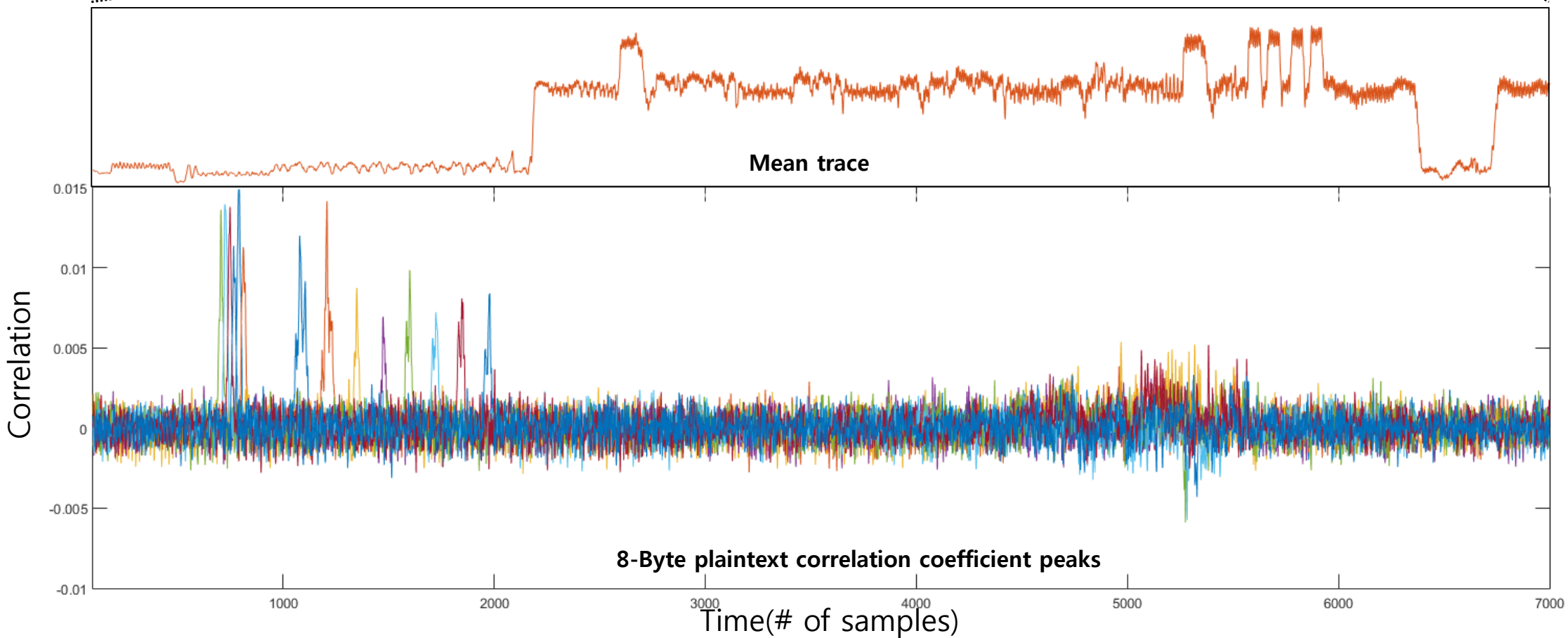


Plaintext CPA

- Perform after alignment
- Result of CPA

  => Indicate location relating to plaintext

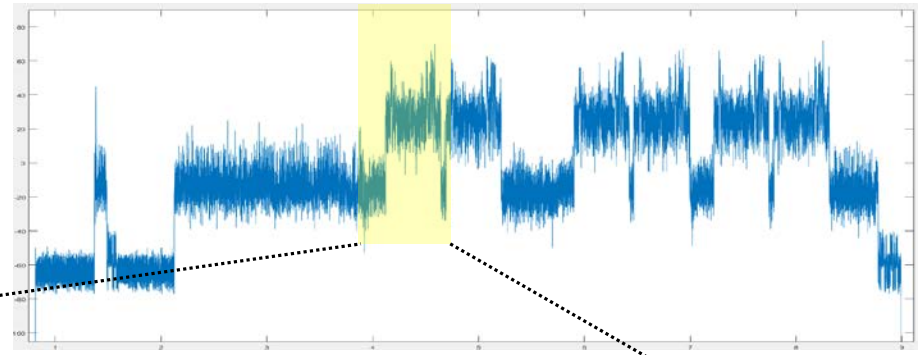


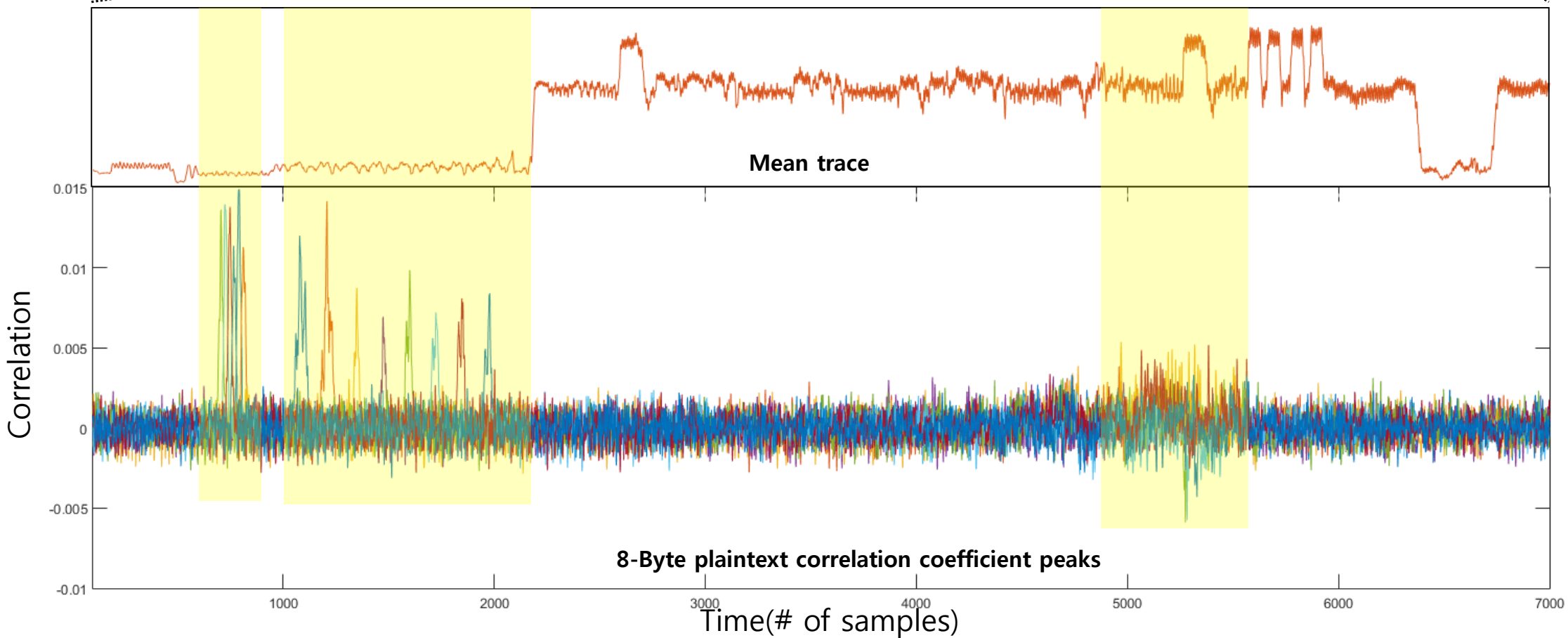


Plaintext CPA

- Perform after alignment
- Result of CPA

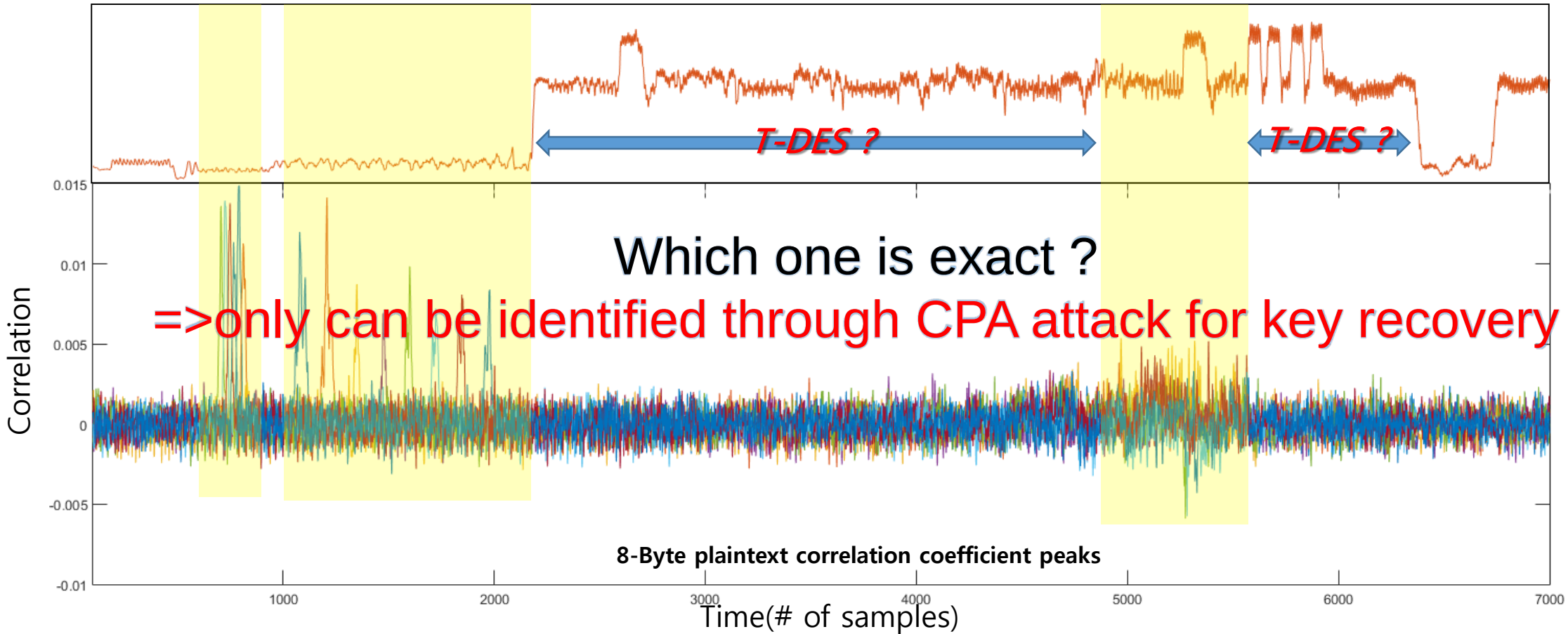
  => Indicate location relating to plaintext





Plaintext CPA

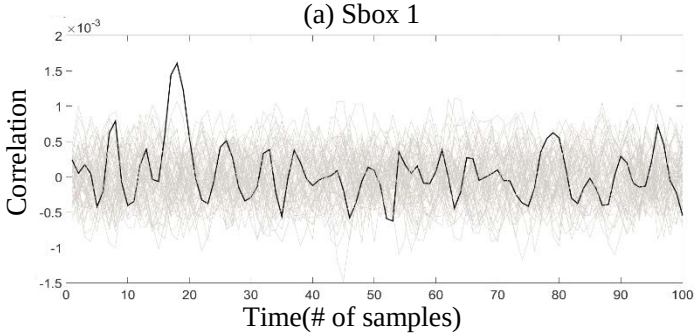
- Two possible intervals for target operation



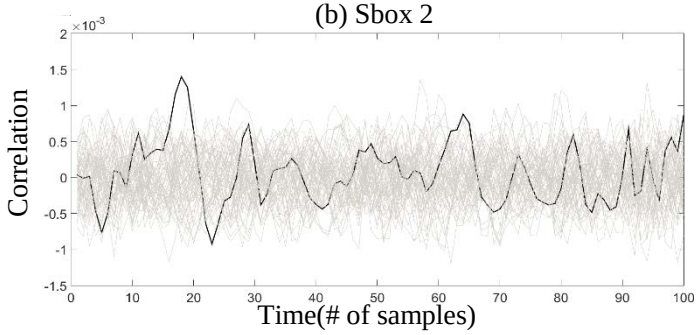
48-bit key recovery

- Correlation Coefficients for the first Round of DES

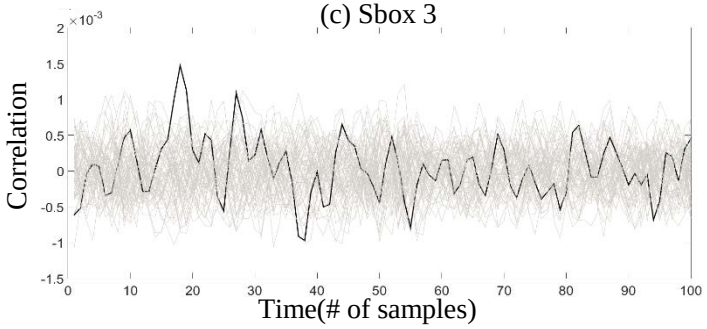
(a) Sbox 1



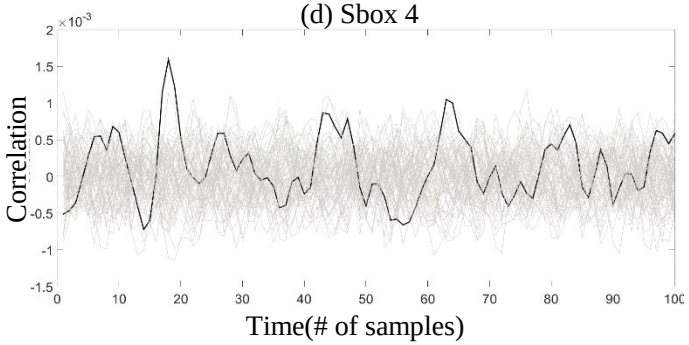
(b) Sbox 2



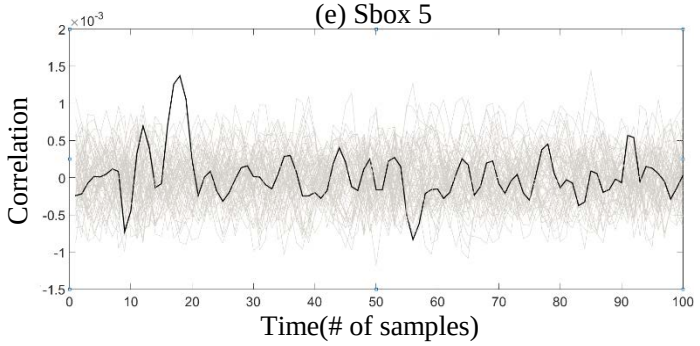
(c) Sbox 3



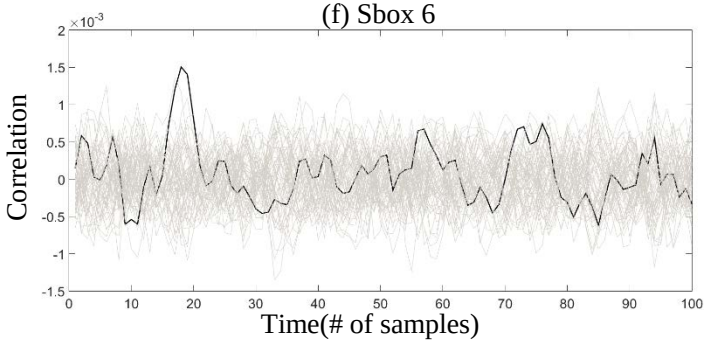
(d) Sbox 4



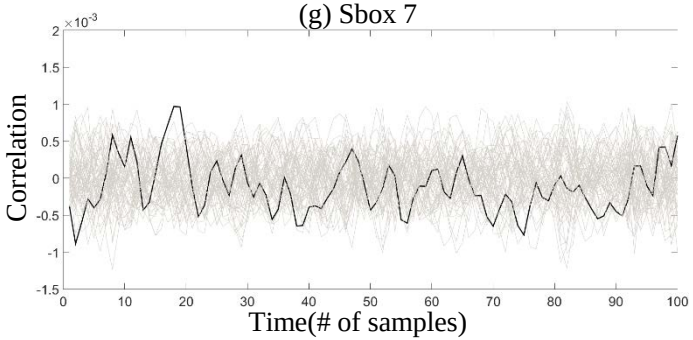
(e) Sbox 5



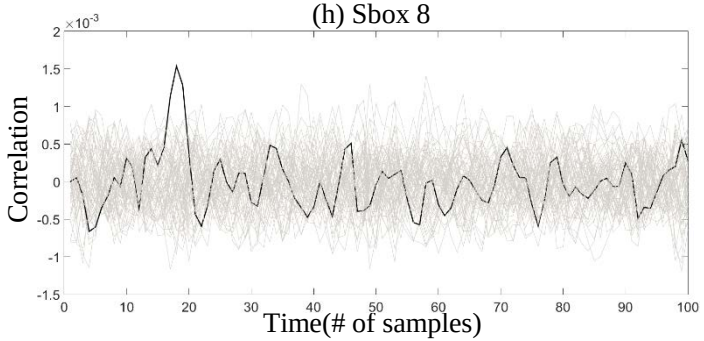
(f) Sbox 6



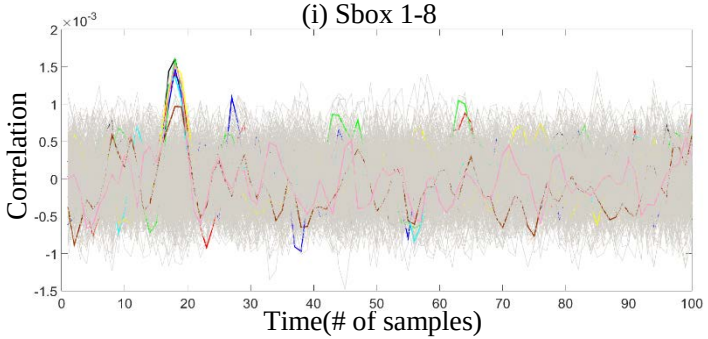
(g) Sbox 7



(h) Sbox 8

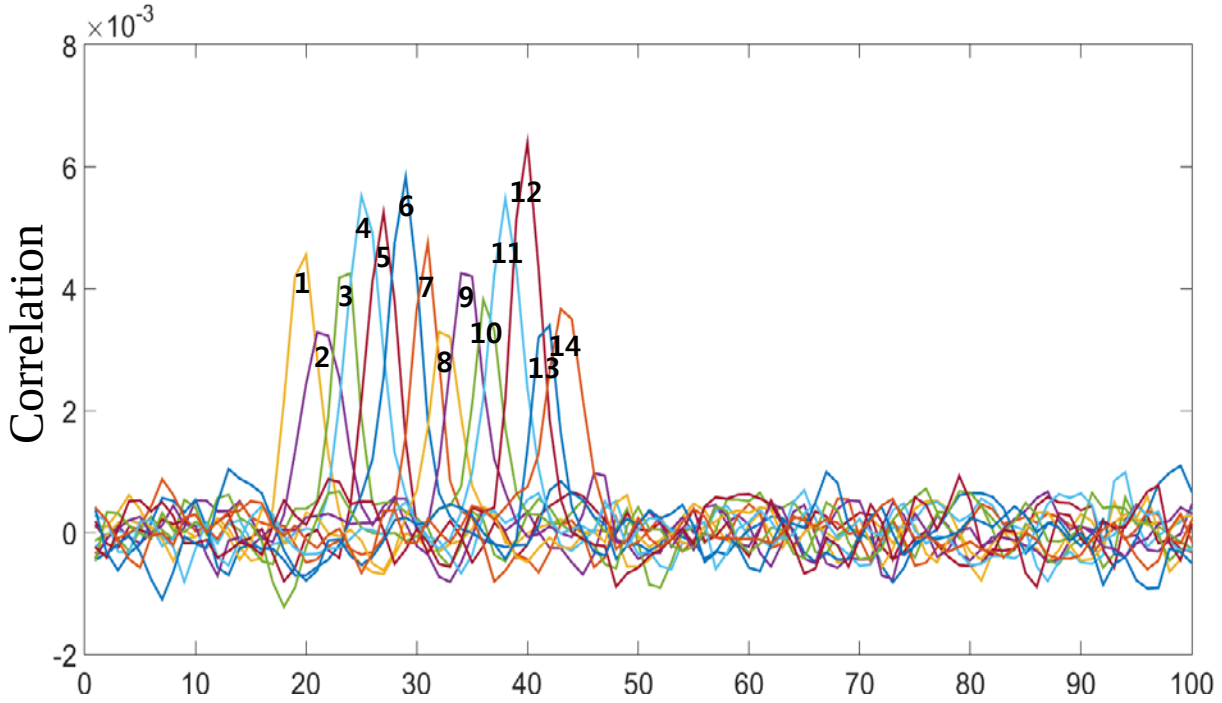


(i) Sbox 1-8

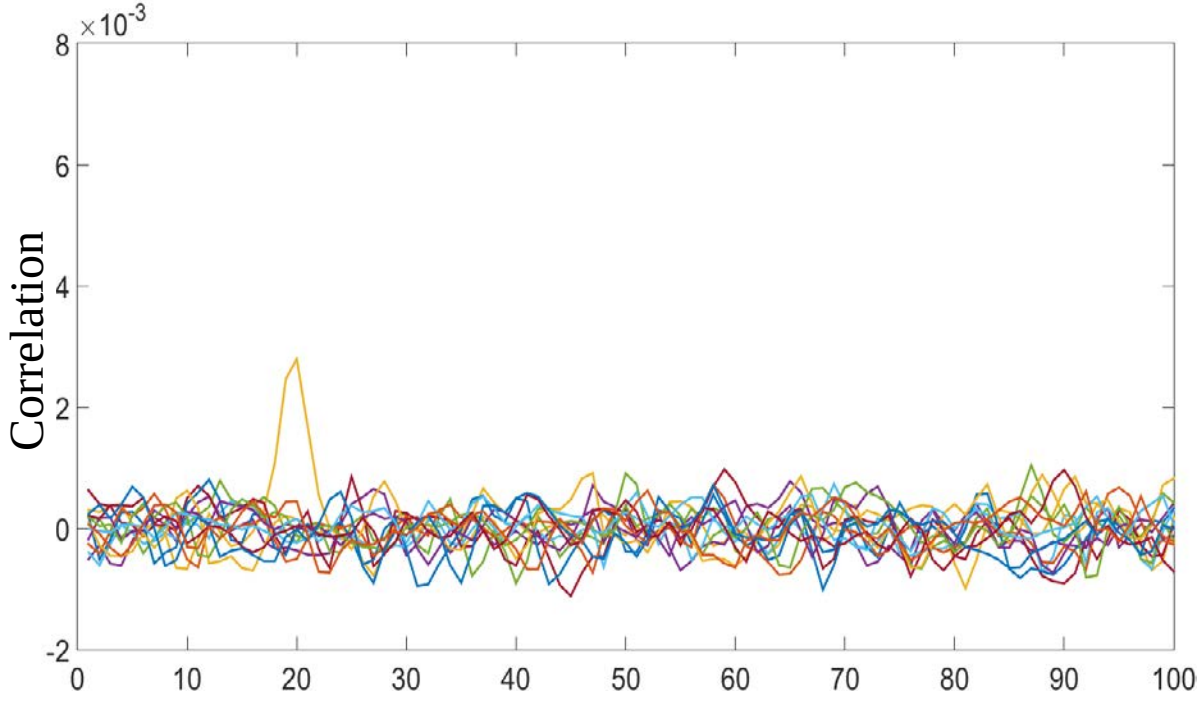


Full Key Recovery

- Correlation coefficients for the Hamming distances between rounds(2-15) of the T-DES
- Correct key guess => Observe 14 peaks

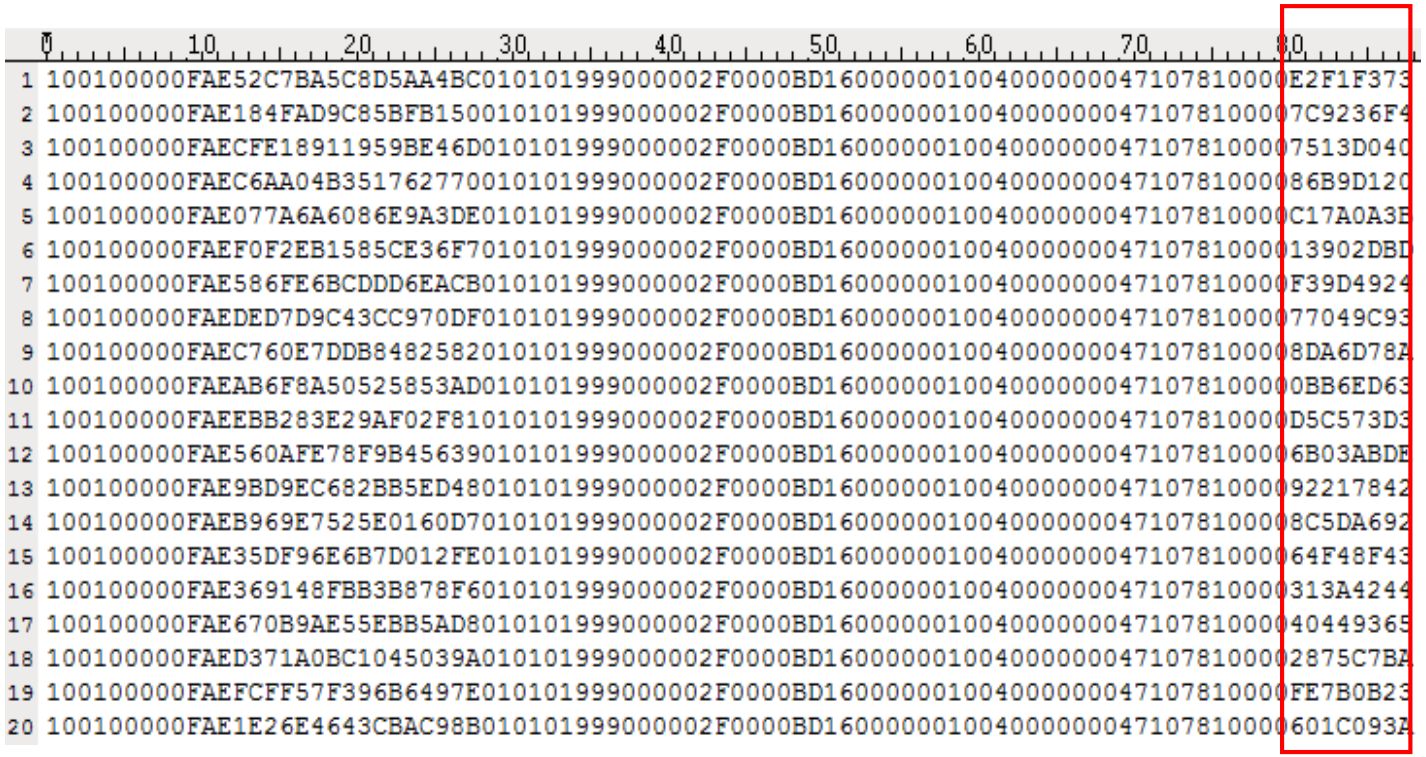


correct key guess



incorrect key guess

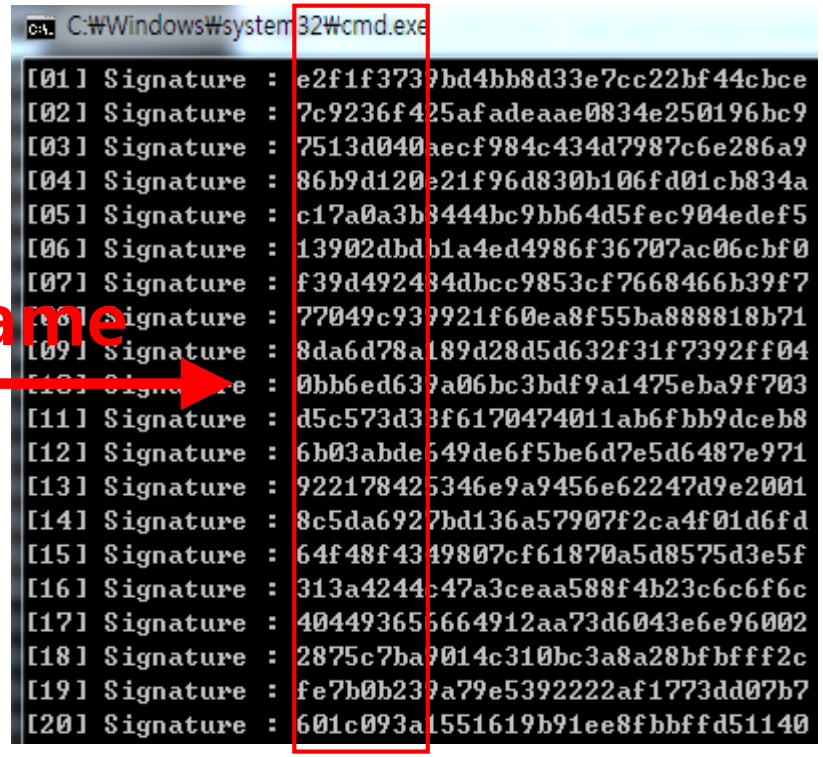
Verification of Restored Entire Key



```
1  100100000FAE52C7BA5C8D5AA4BC010101999000002F0000BD160000001004000000047107810000E2F1F373
2  100100000FAE184FAD9C85BFB150010101999000002F0000BD160000001004000000047107810000 7C9236F4
3  100100000FAECFE18911959BE46D010101999000002F0000BD160000001004000000047107810000 7513D040
4  100100000FAEC6AA04B3517627700101019990000002F0000BD160000001004000000047107810000 86B9D120
5  100100000FAE077A6A6086E9A3DE010101999000002F0000BD160000001004000000047107810000 C17A0A3B
6  100100000FAEF0F2EB1585CE36F7010101999000002F0000BD160000001004000000047107810000 13902DBD
7  100100000FAE586FE6BCDDD6EACB010101999000002F0000BD160000001004000000047107810000 F39D4924
8  100100000FAEDED7D9C43CC970DF010101999000002F0000BD160000001004000000047107810000 77049C93
9  100100000FAEC760E7DDB84825820101019990000002F0000BD160000001004000000047107810000 8DA6D78A
10 100100000FAEAB6F8A50525853AD010101999000002F0000BD160000001004000000047107810000 0BB6ED63
11 100100000FAEEBB283E29AF02F8101010199900002F0000BD160000001004000000047107810000 D5C573D3
12 100100000FAE560AFE78F9B4563901010199900002F0000BD160000001004000000047107810000 6B03ABDE
13 100100000FAE9BD9EC682BB5ED4801010199900002F0000BD160000001004000000047107810000 92217842
14 100100000FAEB969E7525E0160D7010101999000002F0000BD160000001004000000047107810000 8C5DA692
15 100100000FAE35DF96E6B7D012FE010101999000002F0000BD160000001004000000047107810000 64F48F43
16 100100000FAE369148FBB3B878F6010101999000002F0000BD160000001004000000047107810000 313A4244
17 100100000FAE670B9AE55EBB5AD8010101999000002F0000BD160000001004000000047107810000 40449365
18 100100000FAED371A0BC1045039A010101999000002F0000BD160000001004000000047107810000 2875C7BA
19 100100000FAEFCFF57F396B6497E010101999000002F0000BD160000001004000000047107810000 FE7B0B23
20 100100000FAE1E26E4643CBAC98B010101999000002F0000BD160000001004000000047107810000 601C093A
```

Response values from the card including signatures

Same

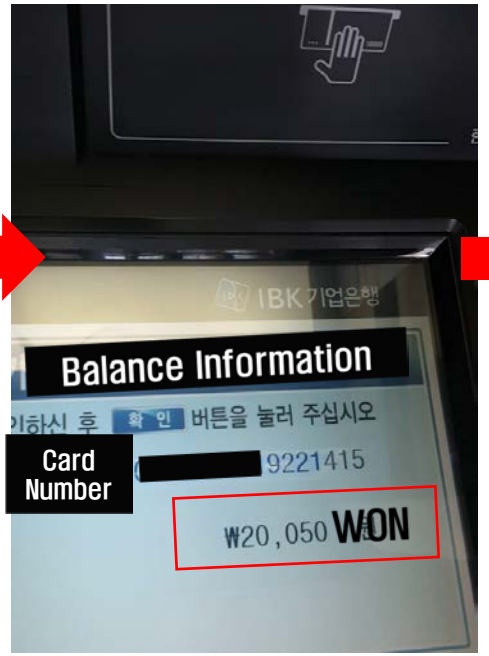


```
C:¥Windows¥system32¥cmd.exe
[01] Signature : e2f1f3739bd4bb8d33e7cc22bf44cbce
[02] Signature : 7c9236f425afadeaae0834e250196bc9
[03] Signature : 7513d040aecf984c434d7987c6e286a9
[04] Signature : 86b9d120e21f96d830b106fd01cb834a
[05] Signature : c17a0a3b8444bc9bb64d5fec904edef5
[06] Signature : 13902dbdb1a4ed4986f36707ac06cbf0
[07] Signature : f39d492484dbcc9853cf7668466b39f7
[08] Signature : 77049c939921f60ea8f55ba888818b71
[09] Signature : 8da6d78a189d28d5d632f31f7392ff04
[10] Signature : 0bb6ed639a06bc3bdf9a1475eba9f703
[11] Signature : d5c573d38f6170474011ab6fbb9dceb8
[12] Signature : 6b03abde649de6f5be6d7e5d6487e971
[13] Signature : 922178425346e9a9456e62247d9e2001
[14] Signature : 8c5da6927bd136a57907f2ca4f01d6fd
[15] Signature : 64f48f4349807cf61870a5d8575d3e5f
[16] Signature : 313a4244c47a3ceaa588f4b23c6c6f6c
[17] Signature : 4044936565664912aa73d6043e6e96002
[18] Signature : 2875c7ba9014c310bc3a8a28bfbfff2c
[19] Signature : fe7b0b239a79e5392222af1773dd07b7
[20] Signature : 601c093a1551619b91ee8fbbffd51140
```

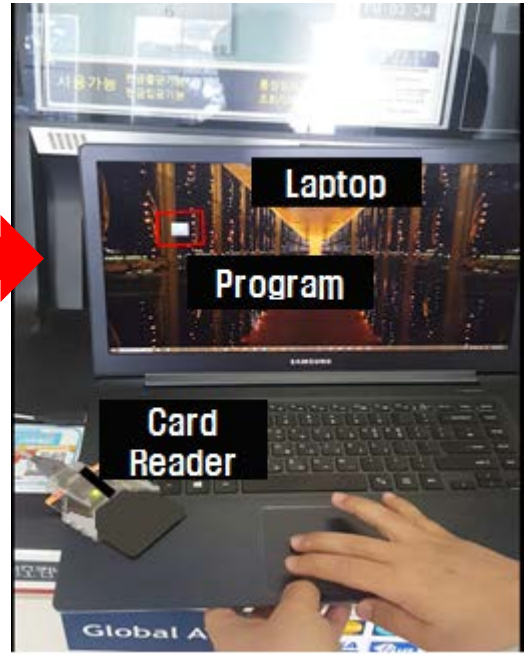
Generated signatures by ourselves

1. Attack Goal & Scenario
2. Target Device Details
   - Introduction of Target Device
   - Authentication Protocol Analysis
   - Cryptosystem
3. Key Recovery Attack
   - Attack environment & Measurement Set-Up
   - Attack Overview
   - Attack Results
4. Recharging Simulation
5. Conclusion

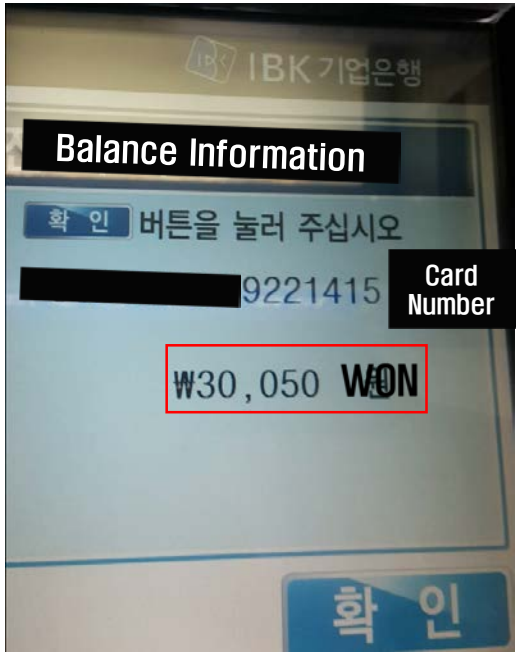
(a) Before recharging,
check balance with ATM



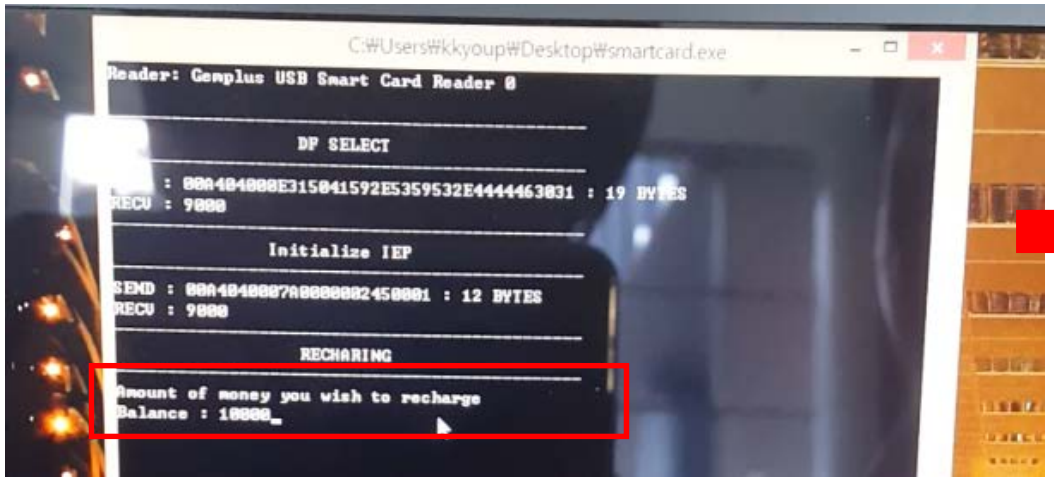
(b) Balance : 20,050 (₩)



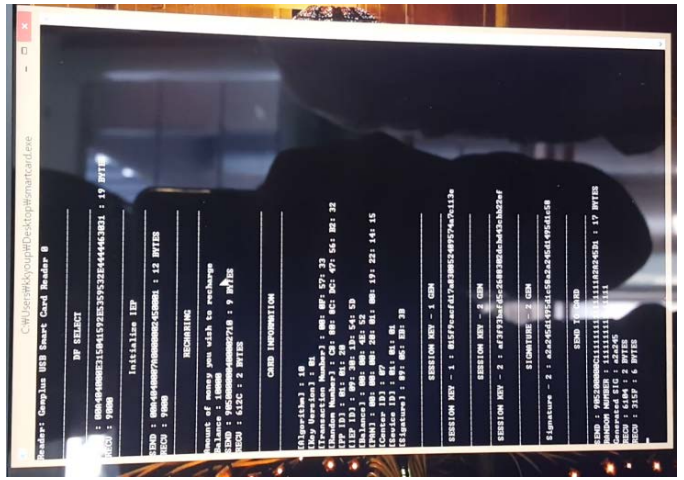
(c) Recharging Tool



(f) After recharging,
Balance : 30,050 (₩)



(d) Execution of our recharging program.
Insert amount of money you wish to recharge => 10,000 (₩)



(e) Completion of recharging

1. Attack Goal & Scenario
2. Target Device Details
   - Introduction of Target Device
   - Authentication Protocol Analysis
   - Cryptosystem
3. Key Recovery Attack
   - Attack environment & Measurement Set-Up
   - Attack Overview
   - Attack Results
4. Recharging Simulation
5. Conclusion

Conclusion

- Demonstrated that side-channel analysis attack is serious threat in real-world
  - Hacking the Korea transit card in a black-box manner
  - Showing financial damage through unauthorized recharging balance
- Practical attack
  - Trials and errors
    - Approx. six months
  - Current extracting key in same device
    - Approx. 63 hours (trace collection : 58 hours + Attack : 5 hours)
- Further works
  - For black box attack, combination of reverse engineering and side-channel attack
  - Go on attack for any commercial devices!

More details ?

Could please see white paper

&

Questions ?

ktw@sntworks.kr

Thank you ☺

SNTWORKS

KOREA UNIVERSITY