Security Protocols and Application — Final Exam
Solution

F. Betül Durak and Serge Vaudenay

30.6.2022

- duration: 2h00
- no document allowed
- a pocket calculator is allowed
- communication devices are not allowed
- the exam invigilators will not answer any technical question during the exam
- readability and style of writing will be part of the grade
- do not forget to put your name on every sheet!

The exam grade follows a linear scale. In each exercise, each question has the same weight. Both exercises have the same weight.

1 Methodology for Efficient CNN Architectures in Profiling Attacks

This exercise is inspired from Zaid-Bossuet-Habrard-Venelli, Methodology for Efficient CNN Architectures in Profiling Attacks*, TCHES 2020, IACR, https://tches.iacr.org/index.php/TCHES/article/view/8391.*

Q.1 Power analysis is being widely studied. There are two common methods which are used to defeat them (but which do not seem sufficient to defeat the CNN-based attack). Which ones have been mentioned in the presentation?

Desynchronization and masking.

Q.2 What is the purpose of the chosen-coup pizza correlation attack?

Learn which country is of interest for the Pentagone.

Q.3 Since power is correlated to Hamming weight of processed data, why not focusing on $x_i \oplus K$ instead of $S(x_i \oplus K)$?

This is to make similar K candidates having non-similar power traces. Otherwise, we would find K up to small differences.

Q.4 The presentation showed an attack methodology based on CNN. What is the input and output of the attack? Can we output something better? How?

Input: the traces from first layer of Sbox. Output: possible value(s) for the first byte of the secret key of AES. If we iterate the attack, we can recover the other bytes of AES key.

Q.5 State two important assumptions in the threat model?

The encryption device is under the control of the attacker whereas the input data are known (i.e. not chosen).

2 Model-Checking 5G Security and 5G SUCI

This exercise is inspired from Basin-Dreier-Hirschi-Radomirović-Sasse-Stettler, Model-Checking 5G Security and 5G SUCI*, CCS 2018, ACM, https://dl.acm.org/doi/10.1145/3243734.3243846.*

Q.1 How could someone spot Russian subscribers in Lausanne?

Like with IMSI catchers, except that we focus on home network identifier $\mathsf{HN}_{\mathsf{name}}$ *which is sent in clear.*

Q.2 What is the order of magnitude of the number of mobile internet subscribers in the world?

5 billions.

Q.3 What is Tamarin?

A security protocol verification tool (also: a kind of monkey).

Q.4 SUCI is the encryption of the unique identifier in 5G. Why can't we identify user equipments based on SUCI as we did in 4G with IMSI?

It uses probabilistic public key encryption and randomized every time.

Q.5 What is the needed security property in 5G to avoid the traceability attack?

Freshness of SUCI.