Security Protocols and Application — Final Exam

F. Betül Durak and Serge Vaudenay

30.6.2022

Family Name: . . . .

Given Name: . . . .

SCIPER: . . . .

- 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!

1 Methodology for Efficient CNN Architectures in Profiling Attacks

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?

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

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

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?

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

Family Name: . . . .

Given Name: . . . .

SCIPER: . . . .

2 Model-Checking 5G Security and 5G SUCI

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

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

Q.3 What is Tamarin?

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?

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