Crypto&Security 2020/21, Mirosław Kutyłowski, Politechnika Wrocławska
Exam – training questions

The questions are harder and require more time to solve than the questions on Feb 3. However, it is highly recommended to spend time on them. The real questions will be somehow related (regarding ideas).

Problem area: Privacy

1) concern the classical Schnorr Identification protocol where $X = g^x$ is the private key for Alice:
step 1: Alice sends to the Verifier a commitment $r = g^k$ for k chosen at random
step 2: Verifier presents a challenge c
step 3: Alice computes $s = k + c \cdot x$ mod q and sends s back to the Verifier
step 4: the Verifier accepts if $g^s = r \cdot X^c$
Is it possible for the Verifier to prove that he has interacted with Alice?

2) Concern TOR where there are n active connections opened and n TOR servers (a big number of people volunteered to instal TOR servers). The adversary is monitoring the whole traffic (but cannot break encrypted messages). How strong is anonymity in this case?

3) Read the verification procedure for Idemix. Why does it prove that the user has received a credential with the presented attribtes?

Problem area: Cache attacks

4) Assume that we have to compute AES with a lookup table implementation. The defense strategy is to encrypt with the proper secret key K and in the same time with the key $K' = \mathrm{Hash}(K)$. The computations go in parallel. How good is this idea?

Problem area: Quantum cryptography

5) Assume that an eavesdropper can guess with probability $\frac{2}{3}$ each random bit chosen by of Alice and Bob. Have does it influence BB84 protocol. Is it of any use in such a situation?

Problem area: PUF

6) Assume that you have a SRAM PUF where at the power-up the memory state is $r \otimes e$ where e is an error vector of weight at most k (r contains n bits). Design a identification protocol based on this PUF. The verifier should be able to learn that a given device is authenticated twice.

Problem area: disk encryption

7) Somebody implemented XEX misunderstanding the notation and has replaced multiplication with addition. For the sector I, block J the plaintext gets encrypted according to
$X = \mathrm{Enc}_K(I) \oplus \alpha^J, C_j = \mathrm{Enc}_K(P \oplus X) \oplus X$
What influence on security could it have?

Problem area: communication

8) Somebody propoed the following modification of the CBC mode: the block C_n is computed not only based on the plaintext block P_n and cipherblock C_{n-1} but as follows
$C_n = \mathrm{Enc}_K(P_n \oplus C_{n-1} \oplus C_{\lceil n/2 \rceil})$
Does it help against the attacks over CBC encryption discussed during the lecture?

ps: in some cases I am curious about the answer. I have some intuitions and observations but maybe you shall see what I do not. These are not the questions from any textbook etc. They are Sunday afternoon problems…