Prof. Dr. Johannes Blömer
Nils Löken

July 21st, 2017
submission due: August 1st, 2017: 11 a.m.

Cryptographic Protocols

SS 2017

Handout 6

Exercises marked (*) will be checked by tutors.
We encourage submissions of solutions by small groups of up to four students.

Exercise 1:
Let R be a binary relation and V/P a three round protocol for R with special soundness and challenge space $\mathcal{C}$, Then for any $\epsilon > 0$ and any algorithm A there exists an algorithm A' with the following properties:

1. If on input $x \in L_R$ algorithm A impersonates P with probability $1/|\mathcal{C}| + \epsilon$, $\epsilon > 0$, then A' oun input x and with probability $\epsilon^2/4$ computes a witness $w \in W(x)$.
2. If A runs in time t then A' runs in time $\mathcal{O}(t + t')$, where t' is the running time of the extractor E for V/P

Exercise 2:
For group signature schemes, we consider the notion of strong exculpability: No subset S of group members, even if they collude with the group manager and the party that executes the Gen algorithm, can create a signature that can be traced to a group member not in S.
Discuss general strategies how to augment group signature schemes in order to achieve strong exculpability.

Exercise 3:
Let $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ be a public key encryption scheme secure against chosen-plaintext attacks. Consider scheme $C = (\mathrm{Gen}, \mathrm{Commit}, \mathrm{Open})$, that works as follows:

$\mathrm{Gen}(1^n)$: run $\Pi.\mathrm{Gen}(1^n)$ to obtain (pk, sk). Output $pp := pk$

$\mathrm{Commit}(pp, m)$: pick randomness r uniformly at random from an appropriate domain. Compute $c := \mathrm{Enc}(pp, m; r)$, i. e. make all random choices of Enc depend on r. Set $d := (r, m)$. Output (c, d).

$\mathrm{Open}(pp, c, d)$: parse $d = (r, m)$. If $\mathrm{Enc}(pp, m; r) = c$, output m otherwise output $\perp$.

Prove or refute: C is perfectly binding and computationally hiding.