ETH Zürich, D-INFK
Spring 2018

Prof. Ueli Maurer
Christian Badertscher
Fabio Banfi

Cryptography Foundations
Exercise 10

10.1 Hardness Amplification for Many Instances

Goal*: We prove the theorem on hardness amplification for many instances, which states that solving k independent copies of G is much harder to solve than a single copy of G.*

a) Generalize the proof of Lemma 4.11 to prove Lemma 4.13.

b) Prove Theorem 4.14, i.e., find a reduction ρ and show that for any $k, \delta, \delta' > 0$

$$\overline{(G^k)^\wedge} \;\leq\; \lambda\, \overline{G}\, \rho$$

for $\lambda(x) = (1+\delta)x^k + \delta'$, if G is clonable.

10.2 A Graph-Theoretic Result

Goal*: We apply the lemma from the lecture outside cryptography. We want to prove a quantitative version of the intuitive statement that the higher the density of a graph, the more vertices with substantial degree must exist in that graph.*

Let $G = (V, E)$ be a graph and let $\alpha := \frac{|E|}{|V|^2}$. Further let $\epsilon, \beta \in (0, 1)$ such that $\alpha \geq \beta^2 + 2\epsilon$. Show that at least $\beta|V|$ vertices have in-degree at least $\epsilon|V|$, or at least $\beta|V|$ vertices have out-degree at least $\epsilon|V|$.

10.3 Generic Reduction of the DL Problem to the CDH Problem

Goal*: We generalize the result from Exercise 7.2 in the generic model of computation.*

Let $\mathbb{G} = \langle g \rangle$ be a cyclic group of prime order $p := |\mathbb{G}|$ and denote the group operation by $\star$.

a) Following Section 4.8.7 of the reading assignment, formalize the abstract model of computation that models computing the DL assuming the availability of a CDH oracle.

Assuming we can compute CDH efficiently, we want to show that we can use generic DL-solvers to compute the DL efficiently in groups of prime order p under a certain condition on $p - 1$.

b) Consider Figure 1. Specify converters $\mathbf{C}_\Pi$ and $\mathbf{C}_\Sigma$ to translate operations and relation queries of any generic algorithm $\mathcal{A}$, that solves the extraction problem for (any element of) the additive group $\mathbb{Z}_{p-1}$, such that $\mathcal{A}$'s output can be used to compute the correct result for the extraction problem for the multiplicative group[1] $\mathbb{Z}_p^*$. Describe the conversion of $\mathcal{A}$'s result as a converter $\mathbf{C}_{\mathsf{out}}$.

Hint: Apply the ideas from Exercise 7.2. Assume that a generator of the multiplicative group $\mathbb{Z}_p^*$ is known.

c) Let $p - 1$ be a B-smooth number. Applying the ideas from Exercise 3.3 **f)** and **e)**, sketch a generic reduction from the DL problem to the CDH problem in $\mathbb{G}$ (relative to g) that requires only $\mathcal{O}(\sqrt{B})$ operations.

Hint: You only need to specify a concrete solver $\mathcal{A}$ to complete the overall reduction.

[1] Technically we consider the field $\mathbb{Z}_p$ in the extraction problem, but the trick from exercise 7.2 does not need the addition operation. Also, we exclude the problem instance $V_1 = 0 \in \mathbb{Z}_p$ (this case could be tested as a first step of any algorithm).

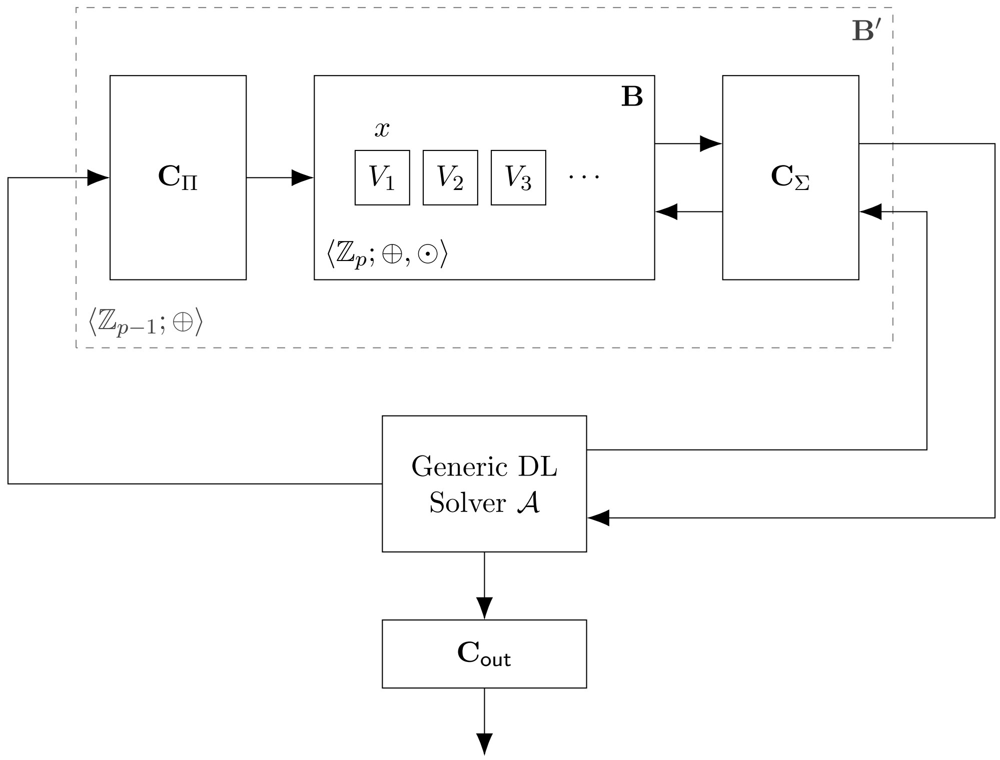

Figure 1: Illustration of the general setting.

Discussion of solutions:

14/15.5.2018 (Task 10.1 and Task 10.2)

22.5.2018 (Task 10.3)

The Monday and Tuesday sessions of each week cover the same material.