ETH Zürich, D-INFK
Spring 2019

Prof. Ueli Maurer
Fabio Banfi
Daniel Jost
Jiamin Zhu

Cryptography Foundations

Exercise 5

5.1 Abstract Models of Computation

Goal: *This task is to improve your understanding of the type of results presented in the reading assignment and to apply one of the main theorems.*

Consider the following problem: Given the group $\{0,1\}^k$ with the bit-wise XOR, the goal is to extract an unknown value $x \in \{0,1\}^k$. The allowed operations are the group operation, the insertion of constant values $a \in \{0,1\}^k$, and checks for equality of two values.

a) Formalize the abstract model of computation for the above problem following the exposition in the reading assignment.

b) Provide a (non-trivial) algorithm that solves the above problem. How many operations and how many relation queries does the algorithm perform?

Hint: You might get some inspiration on which approach to follow by reading through the concrete algorithms described in the reading assignment.

c) Would a total order relation on any representation, as explained in the beginning of Section 4.7 of the reading assignment, help to improve your algorithm from subtask **b)**?

Hint: An arbitrary total ordering on the representation does not correspond to any property of the values.

d) Which Theorem of the reading assignment directly gives you a (non-trivial) lower bound on the number of operations to solve this problem (i.e., to achieve a constant success probability)?

5.2 The Proof of Theorem 4.8.4

Goal: *We study the proof of Theorem 4.8.4 from the reading assignment in more detail.*

a) Generalize the Schwartz–Zippel lemma (Lemma 4.8.1 of the reading assignments) to power of primes. That is, prove that for a prime q and any $e \geq 1$ and $t \geq 1$, the fraction of solutions $(x_1, \ldots, x_t) \in \mathbb{Z}_{q^e}^t$ of any non-trivial multivariate polynomial equation $Q(x_1, \ldots, x_t) \equiv_{q^e} 0$ of degree d is at most $\frac{d}{q}$.

b) Let q be an arbitrary prime factor of $n \in \mathbb{N}$ and let e be its multiplicity. Prove that for any generic k-step extraction algorithm $\mathcal{A}$ for $\langle \mathbb{Z}_n; \oplus \rangle$ with success probability α, there exists a generic algorithm k-step extraction algorithm $\mathcal{A}'$ for $\langle \mathbb{Z}_{q^e}; \oplus \rangle$ with probability at least α.

c) Prove Theorem 4.8.4 of the reading assignment. That is, prove that for $S \coloneqq \mathbb{Z}_n$, $\Pi \coloneqq \mathsf{Const} \cup \{+\}$, and $\Sigma \coloneqq \{=\}$, the success probability of every k-step extraction algorithm is at most $\frac{1}{2}(k+1)^2/q$, where q denotes the *largest* prime factor of n.

d) Explain in words why the same strategy cannot be applied to get bound for Theorem 4.8.6 (solving the DDH problem in the generic group model) that depends on the largest instead of the smallest prime factor.

5.3 Generic Reduction of the DL Problem to the CDH Problem

Goal: *Generalize the result from the lecture 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.

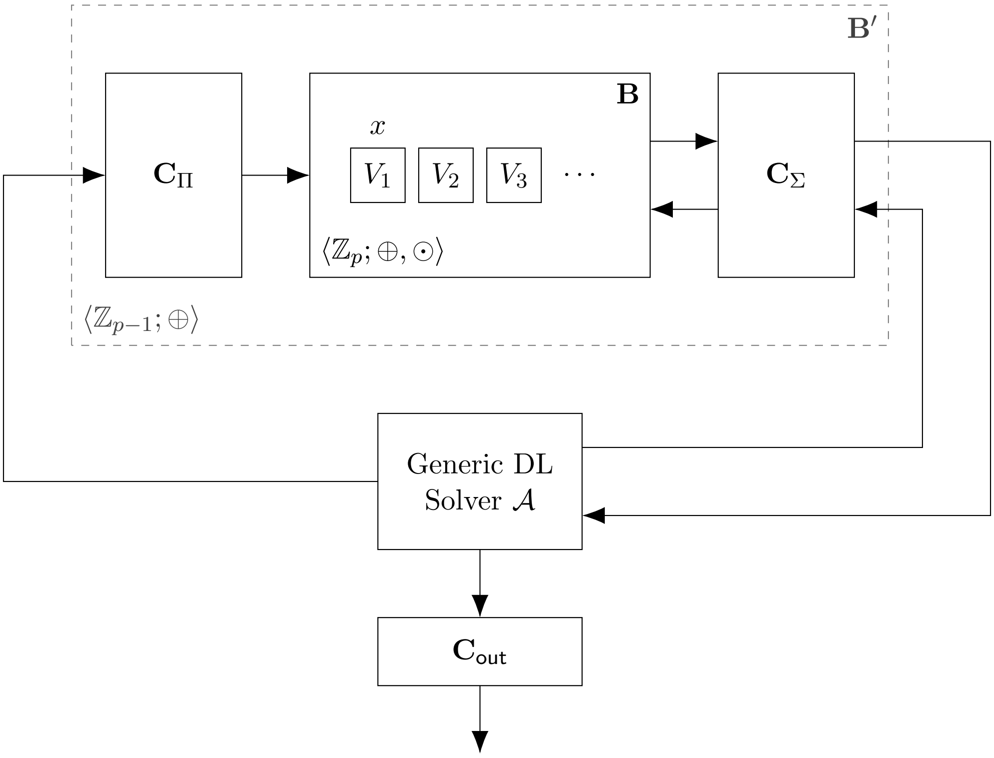
Assuming we can compute CDH efficiently, we want to show that we can use generic DL-solvers to compute the DL efficiently in groups of prime order p under a certain condition on $p - 1$.

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 the lecture. Assume that a generator of the multiplicative group $\mathbb{Z}_p^*$ is known.

c) Let $n := p - 1$ be a B-smooth number (with known factorization). Applying the ideas from Exercise **3.2 f)** and **e)**, sketch a generic reduction from the DL problem to the CDH problem in $\mathbb{G}$ (relative to g) that requires only $O(\sqrt{B} \log n)$ operations.

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



$\mathbf{B}'$
$\mathbf{C}_\Pi$
$\mathbf{B}$
x
V_1
V_2
V_3
$\cdots$
$\langle \mathbb{Z}_p; \oplus, \odot \rangle$
$\mathbf{C}_\Sigma$
$\langle \mathbb{Z}_{p-1}; \oplus \rangle$
Generic DL Solver $\mathcal{A}$
$\mathbf{C}_{\mathsf{out}}$

Figure 1: Illustration of the general setting.

[1] Technically we consider the field $\mathbb{Z}_p$ in the extraction problem, but the trick from the lecture 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).