ETH Zürich, D-INFK
Spring 2019

Prof. Ueli Maurer
Fabio Banfi
Daniel Jost
Jiamin Zhu

Cryptography Foundations
Notes from March 20

The following document serves as complementary material to the reading assignment.

1 On the Hardness of the CDH Problem

For most groups the computational Diffie-Hellman problem can be proven to be as hard as the discrete logarithm problem. In this section, we consider a cyclic group $\mathbb{G} = \langle g \rangle$, where $p = |\mathbb{G}|$ is prime with $p = 2^k + 1$ for some $k \in \mathbb{N}$. We now show that if we have an algorithm that solves the CDH problem with probability 1 in this group, then we can construct an algorithm that solves the discrete logarithm problem with probability 1 as well.

First, observe that for an element $a = g^x \in \mathbb{G}$, we either have $x = 0$ or $x \in \mathbb{Z}_p^*$, since p is prime. The case of $x = 0$ can be easily checked by our DL solver, thus assume in the following that $x \in \mathbb{Z}_p^*$. Hence, if h is a known generator of $\mathbb{Z}_p^*$, i.e., $\langle h \rangle = \mathbb{Z}_p^*$, then we can rewrite a as $a = g^x = g^{h^y}$ for some y. Note that $|\mathbb{Z}_p^*| = 2^k$ and, thus, we know from Exercise **3.2 d)** an algorithm to solve the discrete logarithm in $\mathbb{Z}_p^*$ with respect to h. Furthermore, observe that this algorithm is generic, i.e., only needs to be able to multiply (and thus exponentiate) and compare elements. We can consider g^{h^y} to be an encoding of h^y, i.e., define $\text{enc}\colon \mathbb{Z}_p^* \to (\mathbb{G} \setminus \{e\}), x \mapsto g^x$. Using our assumed CDH solver we can furthermore compute on this encoding since $\text{enc}(a \cdot b) = g^{a \cdot b}$. Hence, we can use the algorithm from Exercise **3.2 d)** to compute y from $a = g^x = g^{h^y}$, and thus also compute $x = h^y$.

More abstractly we have defined the group $\mathbb{G}' := \langle \mathbb{G} \setminus \{e\}; \star \rangle$ with $g^a \star g^b := g^{ab}$ (which we can compute using the assumed CDH solver). Then, we used that $\mathbb{Z}_p^* \to \mathbb{G}', x \mapsto g^x$ is group isomorphism, i.e, $\mathbb{G}' \cong \mathbb{Z}_q^*$, to reduce the problem of computing the discrete logarithm in $\mathbb{G}$ to computing the discrete logarithm in $\mathbb{Z}_p^*$.

One can prove that the computational Diffie-Hellman problem is as hard as the discrete logarithm problem in groups of most orders. To this end, one can use a similar approach using isomorphisms based on the theory of elliptic curves, which is however more involved and not topic of this lecture.

2 Breaking the DDH Assumption in Certain Groups

In this section we show that for certain groups the DDH problem is easy to solve, even if the CDH problem might be hard.

2.1 Using the Legendre Symbol

Consider the multiplicative group $\mathbb{Z}_p^*$ for a prime $p > 2$, which has order $|\mathbb{Z}_p^*| = p - 1$, and let g denote a generator of $\mathbb{Z}_p^*$. Since $p - 1$ is even, for a given g^x with $x \in \mathbb{Z}$ we can compute the parity, i.e, we can compute $R_2(R_{p-1}(x)) = R_2(x)$.[1]

[1] Here, $R_n(z)$ denotes the remainder of z modulo n.

Hence, given g^a and g^b, we can compute

$$R_2(R_{p-1}(a)) \cdot R_2(R_{p-1}(ab)) = R_2(a)R_2(b) = R_2(ab) = R_2(R_{p-1}(ab)).$$

Consider the distinguisher D that upon input (g^a, g^b, g^c) outputs 0 iff $R_2(R_{p-1}(a)) \cdot R_2(R_{p-1}(ab)) = R_2(R_{p-1}(c))$. If $c = a \cdot b$, then this algorithm outputs $Z = 1$ with probability 0. If c is however chosen uniformly random and independent of a and b, then the algorithm will output $Z = 1$ with probability $\frac{1}{2}$ since there are equally many even and odd numbers in $\mathbb{Z}_{p-1}$. Thus,

$$\Delta^D(\mathsf{DDH}^0, \mathsf{DDH}^1) = \Pr^{D\,\mathsf{DDH}^1}[Z = 1] - \Pr^{D\,\mathsf{DDH}^0}[Z' = 1] = \frac{1}{2} - 0 = \frac{1}{2}.$$

2.2 Using a Pairing

For two cyclic groups $\mathbb{G} = \langle g \rangle$ and $\mathbb{G}_T$ of the same order n, a *pairing* (also called bilinear-map) is a function $\mathrm{E}\colon \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ such that

1. $\mathrm{E}(g^a, g^b) = \mathrm{E}(g, g)^{ab}$,
2. $g_T \coloneqq \mathrm{E}(g, g)$ is a generator of $\mathbb{G}_T$.

It is easy to see that if there exists an efficiently computable pairing from $\mathbb{G}$ to some group $\mathbb{G}_T$, then the DDH problem is easy to solve in $\mathbb{G}$ since the check

$$\mathrm{E}(g^a, g^b) \stackrel{?}{=} \mathrm{E}(g, g^c)$$

succeeds if and only if $c = ab \pmod{n}$ as

$$\mathrm{E}(g^a, g^b) = \mathrm{E}(g, g)^{ab} = g_T^{ab}$$
$$\mathrm{E}(g, g^c) = \mathrm{E}(g, g)^{c} = g_T^{c}.$$

Note that if $\mathbb{G} \neq \mathbb{G}_T$, then the existence of such a pairing does not exclude the CDH problem to be hard (as g^{ab} might not be efficiently computable from g_T^{ab}).

3 Groups for Which DDH is Believed to be Hard

Let p be a prime such that $\frac{p-1}{2}$ is prime as well. Such a prime is called a *safe prime*. While one can break the DDH assumption in $\mathbb{Z}_p$ (c.f. Section 2.1), it is widely believed that the parity is the only information that can be learned about the discrete logarithm. Therefore, it is believed that in $\mathcal{QR}_p$, i.e., the subgroup of $\mathbb{Z}_p$ consisting of the elements with even parity, the DDH problem is hard.

There exist also other groups based on elliptic curves where the DDH problem is believed to be hard. Those groups are however outside of the scope of this lecture.