

Exercise (Full proof for randomised self-reducibility of DDH). Show that for any \mathcal{B} defined as above there exists an algorithm \mathcal{A} , which has roughly the same running-time as \mathcal{B} and for any three group elements g^a, g^b, g^c , distinguish g^{ab} from g^c with roughly the same advantage as $\text{Adv}_{\mathbb{G}}^{\text{ddh}}(\mathcal{B})$. More precisely, let the following games

$$\mathcal{G}_0^{\mathcal{A}} \qquad \qquad \qquad \mathcal{G}_1^{\mathcal{A}}$$

$$\left[\begin{array}{l} c \neq ab \\ \mathbf{return} \mathcal{A}(g^a, g^b, g^c) \end{array} \right. \qquad \left[\begin{array}{l} c \leftarrow ab \\ \mathbf{return} \mathcal{A}(g^a, g^b, g^c) \end{array} \right.$$

model the distinguishing task. Then the corresponding advantage is

$$\text{Adv}_{\mathbb{G}, a, b, c}^{\text{f-ddh}}(\mathcal{A}) = |\Pr[\mathcal{G}_0^{\mathcal{A}} = 1] - \Pr[\mathcal{G}_1^{\mathcal{A}} = 1]| .$$

Show that if q is prime then for any $a, b \in \mathbb{Z}_q$, the advantage $\text{Adv}_{\mathbb{G}, a, b}^{\text{f-ddh}}(\mathcal{A})$ can be bounded from below by a multiple of $\text{Adv}_{\mathbb{G}}^{\text{ddh}}(\mathcal{B})$, while the running-time of \mathcal{A} is linear wrt the running-time of \mathcal{B} .

Solution. Recall that the weak self-reducibility construction re-randomises only the first two elements g^a and g^b of the Diffie-Hellman tuple. The corresponding correction relies on the equation

$$(a+x)(b+y) = (xy + ay + bx) + ab$$

where the first three terms on the right are correction terms, i.e., the new randomised tuple is

$$g^{a+x}, g^{b+y}, g^{xy} \cdot (g^a)^y \cdot (g^b)^x \cdot g^c \qquad \text{for } x, y \leftarrow_{\mathcal{U}} \mathbb{Z}_q .$$

Note that for fixed $ab \neq c$ the distribution of $xy + ay + bx$ is not guaranteed to be uniform over \mathbb{Z}_q . Hence also the sum $xy + ay + bx + c$ is not guaranteed to be uniform, which itself implies that a re-randomised non-Diffe-Hellman tuple is a uniformly chosen triple and thus \mathcal{B} is not guaranteed to preserve its advantage.

To avoid this pitfall, we use a more complex re-randomisation for the first two tuple elements:

$$g^a \rightsquigarrow g^{a+x}, \qquad g^b \rightsquigarrow g^{by+z} .$$

The corresponding correction is based on the equation

$$(a+x)(by+z) = xz + az + bxy + ab \cdot y$$

which leads to the following re-randomisation

$$g^{a+x}, (g^b)^y \cdot g^z, g^{xz} \cdot (g^a)^z \cdot (g^b)^{xy} \cdot (g^c)^y \qquad \text{for } x, y, z \leftarrow_{\mathcal{U}} \mathbb{Z}_q .$$

Again, note that if $ab \neq c$ then the discrete logarithm of the third element is

$$\Delta = xz + az + bxy + c \cdot y = (bx+c)y + (a+x)z .$$

To analyse the distribution of Δ further, we must use the following fact.

Lemma 0.1 Let z be an invertible element of \mathbb{Z}_q . Then the product $x \cdot z$ has uniform distribution over \mathbb{Z}_q whenever x is picked uniformly from \mathbb{Z}_q .

The claim follows from the fact that the equation $xz = y$ has a single solution for any y and thus

$$\Pr[x \leftarrow_{\mathcal{U}} \mathbb{Z}_q : zx = y] = \Pr[x \leftarrow_{\mathcal{U}} \mathbb{Z}_q : x = z^{-1}y] = \frac{1}{q} .$$

Let us continue the analysis of Δ by fixing the values of x, y . Since $z \xleftarrow{u} \mathbb{Z}_q$ we know that $(a+x)z$ is uniformly distributed whenever $a+x$ is invertible. As we assumed that the group \mathbb{G} has a prime order q , the term is uniformly distributed for any $a+x \neq 0$. The latter also implies that Δ is uniformly distributed for any fixed $x, y \in \mathbb{Z}_q$ such that $x \neq -a$. If $x = -a$ then $\Delta = (bx+c)y = (c-ab)y$. By same reasoning Δ has a uniform distribution as long as $ab \neq c$, i.e., we do not re-randomise Diffie-Hellman tuples.

As a consequence, we can conclude that the new re-randomisation takes Diffie-Hellman tuple to a random Diffie-Hellman tuple and non-Diffie-Hellman tuple to a random triple of group elements. This leads to the following random self-reduction:

$$\mathcal{A}(g^a, g^b, g^c) \left[\begin{array}{l} x, y, z \xleftarrow{u} \mathbb{Z}_q \\ \mathbf{return} \mathcal{B}(g^a \cdot g^x, (g^b)^y \cdot g^z, (g^c)^y \cdot (g^a)^z \cdot (g^b)^x y \cdot g^{xz}) \end{array} \right].$$

Notice that all parameters thrown to \mathcal{B} can be calculated in a constant time δ . Hence, the \mathcal{A} is $(t + \delta)$ -time algorithm whenever \mathcal{B} is t -time algorithm. By our extensive reasoning

$$\Pr [\mathcal{G}_0^{\mathcal{A}} = 1] = \Pr [\mathcal{Q}_0^{\mathcal{B}} = 1] \quad \text{and} \quad \Pr [\mathcal{G}_1^{\mathcal{A}} = 1] = \Pr [\mathcal{Q}_1^{\mathcal{B}} = 1]$$

where \mathcal{Q}_0 and \mathcal{Q}_1 denote ordinary DDH games. Hence, $\text{Adv}_{\mathbb{G}, a, b, c}^{\text{f-ddh}}(\mathcal{A}) = \text{Adv}_{\mathbb{G}}^{\text{ddh}}(\mathcal{B})$.