Variations on
Diffie Hellman Key Exchange

Let the following key exchange protocol with input $\langle g, G, m \rangle$, which can be described by the following moves:

1. Alice selects $x_A \stackrel{R}{\leftarrow} \mathbb{Z}_m$ and sends $y_A = g^{x_A}$ to Bob.
2. Bob selects $r \stackrel{R}{\leftarrow} \mathbb{Z}_m$ and calculates $k_B = g^r$, while sending $z = y_A^r$ to Alice.
3. Alice calculates $k_A = z^{\frac{1}{x_A}}$, which is the key.

$\boxed{\text{Correctness}}$

$$k_A = z^{\frac{1}{x_A}} = ((g^{x_A})^r)^{\frac{1}{x_A}} = g^r = k_B$$

$\boxed{\text{Security}}$

We will show that the above described protocol is secure under the DDH assumption:

$$|\mathsf{Prob}[B(\langle g, G, m \rangle, g^x, g^y, g^{xy}) = 1] - \mathsf{Prob}[B(\langle g, G, m \rangle, g^x, g^y, g^z) = 1]| \leq \mathsf{negl}(1^\lambda)$$

Suppose that

$$\mathop{\mathsf{Prob}}_{key \leftarrow \mathsf{Key}(\lambda)}[V(key) = 1] = \delta$$

meaning that the Adversary can extract some part of the key.
Suppose that the protocol is not secure. Then there exists an algorithm A and a predicate V such that

$$\mathsf{Prob}[A(\tau) = V(key(\tau))] \geq \max\{\delta, 1 - \delta\} + \alpha \tag{1}$$

with α a non negligible function of λ. Then for $trans(1^\lambda) = \langle g, G, m, y, z \rangle$ we have that

$$key(\langle g, G, m, y, z \rangle) = z^{\frac{1}{\log_g y}}$$

Let

$$D_\lambda = \{\langle g, G, m \rangle \leftarrow GGen(1^\lambda); a, b \stackrel{R}{\leftarrow} \mathbb{Z}_m : (G, m, g^a, g^{ab}, g^b)\}$$

and

$$R_\lambda = \{\langle g, G, m \langle \leftarrow GGen(1^\lambda); a, b, c \stackrel{R}{\leftarrow} \mathbb{Z}_m : (G, m, g^a, g^c, g^b)\}$$

We devise a statistical test B that on input $\langle g, G, m, a, b, c \rangle$ sends $(\langle g, G, m \rangle, a, c)$ to A, which extracts σ and if $V(b) = \sigma$, then B outputs 1, else B outputs 0.

Then from (1) we have that

$$\mathop{\mathsf{Prob}}_{\gamma \leftarrow D_\lambda}[B(\gamma) = 1] \geq \max\{\delta, 1 - \delta\} + \alpha$$

and

$$\begin{aligned}
\underset{\gamma \leftarrow R_\lambda}{\mathsf{Prob}}[B(\gamma)=1] &= \mathsf{Prob}[A(\tau_\gamma)=1]\cdot \mathsf{Prob}[V(c)=1] + \mathsf{Prob}[A(\tau_\gamma)=0]\cdot \mathsf{Prob}[V(c)=0] \\
&= \mathsf{Prob}[A(\tau_\gamma)=1]\delta + \mathsf{Prob}[A(\tau_\gamma)=0](1-\delta) \\
&\leq \mathsf{Prob}[A(\tau_\gamma)=1]\max\{\delta,1-\delta\} + \mathsf{Prob}[A(\tau_\gamma)=0]\max\{\delta,1-\delta\} \\
&= \max\{\delta,1-\delta\}^*
\end{aligned}$$

and

$$|\mathsf{Prob}[B(D)=1] - \mathsf{Prob}[B(R)=1]| = |\max\{\delta,1-\delta\}+\alpha-\max\{\delta,1-\delta\}| = \alpha$$

which we have supposed to be non negligible, and therefore leads us to a contradiction since we have assumed the DDH assumption.

---

*More accurately $\mathsf{Prob}[V(c)=1]=\delta'$ but it is easy to show that $|\delta-\delta'| = \mathsf{negl}(\lambda)$