THEOREM

IF DDH HOLDS WITH RESPECT TO $\mathsf{Gen}_{\mathbb{G}}$, THEN THE DH KEY-EXCHANGE PROTOCOL IS SECURE AGAINST KE^{eav}.

PROOF

LET'S JUST START FROM THE EXPRESSION WE WANT TO SHOW BOUNDED BY $1/2+\varepsilon(n)$:

$$\Pr\left(KE^{eav}_{A,\Pi}(n)=1\right) \overset{\Pr(A)=\Pr(A|B)\cdot\Pr(B)+\Pr(A|\bar{B})\cdot\Pr(\bar{B})}{=}$$

$$\Pr\left(KE^{eav}_{A,\Pi}(n)=1 \mid b=0\right)\cdot\Pr(b=0)+\Pr\left(KE^{eav}_{A,\Pi}(n)=1 \mid b=1\right)\cdot\Pr(b=1)$$

$$\frac{1}{2}\left[\Pr\left(KE^{eav}_{A,\Pi}(n)=1 \mid b=0\right)+\Pr\left(KE^{eav}_{A,\Pi}(n)=1 \mid b=1\right)\right]$$

$$\frac{1}{2}\left[\Pr\left(A(\text{transcript},r)=0\right)+\Pr\left(A(\text{transcript},k)=1\right)\right]$$

$$\frac{1}{2}\left[\Pr\left(A(\mathbb{G},q,g,g^x,g^y,g^z)=0\right)+\Pr\left(A(\mathbb{G},q,g,g^x,g^y,g^{xy})=1\right)\right]$$

$$\frac{1}{2}\left[\left(1-\Pr\left(A(\mathbb{G},q,g,g^x,g^y,g^z)=1\right)\right)+\Pr\left(A(\mathbb{G},q,g,g^x,g^y,g^{xy})=1\right)\right]$$

$$\frac{1}{2}+\frac{1}{2}\left[\Pr\left(A(\mathbb{G},q,g,g^x,g^y,g^{xy})=1\right)-\Pr\left(A(\mathbb{G},q,g,g^x,g^y,g^z)=1\right)\right]$$

THANKS TO THE DDH ASSUMPTION, WE KNOW THAT THIS IS NEGLIGIBLE, I.E. A FUNCTION ε WHICH IS A NEGLIGIBLE FUNCTION

$$\frac{1}{2}+\frac{1}{2}\varepsilon(n)$$

THIS IS NEGLIGIBLE

$\boxtimes$