

2)

Diffie-Hellman assumption (DHA) - given  $g, g^a$  and  $g^b$ , it is computationally infeasible to determine  $g^{ab}$ .

discrete logarithm assumption (DLA)- given  $g$  and  $g^a$ , it is computationally infeasible to determine  $a$

In a scenario where DLA does not hold, we can trivially break DHA in the following ways:

Given  $A'$  where  $g^{a^2}$  can be calculated with  $g$  and  $g^a$ ,  $a$  is determined.  $g^{a^2}$  can be calculated by  $a * g^a$ . DHA is also broken as  $g^{ab}$  can be calculated efficiently where  $g^{ab}$  is calculated by  $g^a * g^b$ . Since DLA is similar to DHA, given  $A'$  that can calculate  $a$  or  $b$  given  $g^a$  or  $g^b$  respectively, DHA is trivial broken. Hence, the square DHA would not hold either. Thus, by contrapostive, square DHA is equivalent to DHA