



: The difference on this bit can be computed by the upper and lower part of the attack