

BLS signatures

1. BLS signatures... (choose as many options as you think are correct)

- (A) ... are known to be EUF-CMA secure in the random oracle model under the CDH assumption
- (B) ... require pairings
- (C) ... require (for security) that it is hard to factor the order of the used group G
- (D) ... can be aggregated
- (E) ... have a security reduction (as seen in the lecture) that is tight (i.e., has a loss that is constant as a function in the security parameter)

2. The security reduction of BLS that we have seen programs the random oracle such that it can sign all messages (except for one). For a hash image $H(m)$ programmed to h , what is the "trapdoor information" that the reduction knows about h so that it can compute a BLS signature on m ?

3. Like the RSA-FDH scheme, also the BLS scheme has unique signatures (such that for every pk and m , there is at most one σ for which $\text{Vfy}(pk, m, \sigma) = 1$).

- (T) True
- (F) False