

Waters signatures

1. Waters signatures... (choose as many options as you think apply)

- (A) ...are unique (in the sense that for every pk and message m , there is at most one valid signature σ)
- (B) ...are randomized (in the sense that the signing algorithm uses random coins to choose certain values)
- (C) ...are EUF-CMA secure in the standard model (i.e., without random oracles) under the CDH assumption

2. Recall that Waters signatures are of the form $\sigma = (g^r, g^\alpha H(m)^r)$ for the secret key α and a random r . How can a signature be re-randomized? That is: given $(g^r, g^\alpha H(m)^r)$, how can we generate another signature $(g^{r'}, g^\alpha H(m)^{r'})$ for m for a fresh, uniformly distributed r' , without knowing α ?