1. One of the big breakthroughs achieved by pairing-based cryptography is the identity-based encryption. In such systems it possible to encrypt messages with arbitrary identifying information like an e-mail address.

Let $H_1 : \{0, 1\}^* \rightarrow \mathbb{G}_1$ and $H_2 : \mathbb{G}_T \rightarrow \{0, 1\}^\kappa$ be hash functions. Original protocol [Boneh and Franklin 2001] for identity-based encryption is as follows:

- Trusted authority picks a master secret key $s \leftarrow \mathbb{Z}_q$ and publishes a master public key $\text{pk} \leftarrow [s]_2$.
- User with identity $id$ has a public key $\text{pk}_{id} \leftarrow H_1(id)$ and authority can generate user’s secret key as $\text{sk}_{id} \leftarrow s \cdot \text{pk}_{id}$.
- Let $m \in \{0, 1\}^\kappa$ and $r \leftarrow \mathbb{Z}_q$, then $\text{Enc}(m; r) = (m \oplus H_2(r \cdot \text{pk}_{id}) \cdot \text{pk}), [r]_2$.

How to decrypt the ciphertext?

2. Another popular construction in pairing-based cryptography is the BLS signature scheme [Boneh, Lynn, Shacham, 2001]:

- Signing key is $s \leftarrow \mathbb{Z}_q$ and verification key is $\text{vk} \leftarrow [s]_2$.
- For $m \in \{0, 1\}^*$ signature is $\text{Sig}(m) = s \cdot H(m)$ where $H : \{0, 1\}^* \rightarrow \mathbb{G}_1$ is a hash function.
- To verify that $\sigma$ is a signature for message $m$, we check the equation $\sigma \cdot [1]_2 = H(m) \cdot \text{vk}$.

A nice property of BLS is that it allows to aggregate signatures, that is, instead of separately verifying signatures $\sigma_1, \ldots, \sigma_n$ for respective messages $m_1, \ldots, m_n$ it is sufficient to verify $\sigma_{\text{agg}} := \sum_{i=1}^{n} \sigma_i$. Show how to do this. Can you think of an attack for the naive aggregation approach?