Problem 6. «An aggregated signature»

Problem for a special prize!

Suppose that a big international organization, say **NSUCRYPTO association**, decided to organize its own news journal in the area of cryptography. The organization wants to publish only news that are verified by a large group of cryptographers. For this goal 10 000 leading experts in cryptography were invited to join the editorial board of the journal.

The following publishing politics was accepted. The news can be published if and only if it is signed by all members of the editorial board. But cryptographers do not want to use 10 000 individual signatures. Since they are cryptographers, they think about the aggregated postquantum signature that can not be divided into separate individual signatures.

So, **NSUCRYPTO association** kindly asks you to propose such a signature scheme. There are several requirements for it:

* the size of the signature should be not big. It can be about several kilobytes;
* the size of the public key (for checking the signature) should be small. It is desired that the key size will be constant (or close to constant) even if the number of experts is increased, say up to 20 000;
* signature verification should not take more than 2 minutes;
* the signature should be resistant to attacks that use quantum computers.