

The FHE.org competition: A quick update

At last, a competition just about FHE

The ingredients of the competition

1

An organizing committee
making sure all goes well

2

Competition rules
fair for everyone

3

"FHE-universal"
performance scores
any software can compete

4

A server application
submission, dashboard, etc

5

Running the server
hosting + maintenance


6

A timeline

7

A place for online chats

8

Prizes


The ingredients of the competition

1

An organization goes well

Welcoming volunteers!

2

Competition rules
fair for everyone

3

"FHE-universal"
scores
any software can compete

4

Reuse of the WhibOx app
mission, dashboard, etc

5

Google
Thanks to Stefan Kölbl!

6

A timeline

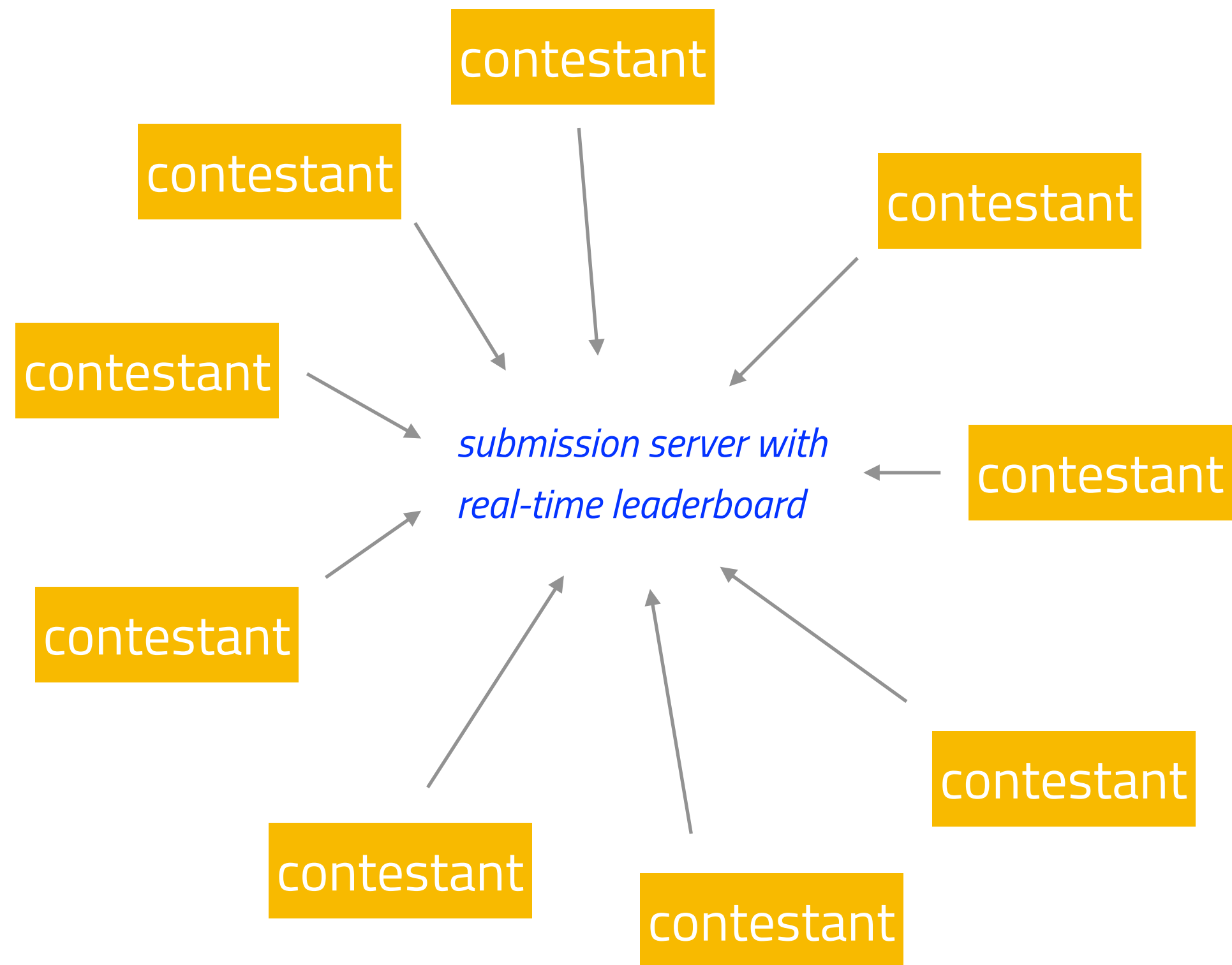
7

fhe.org discord server

8

Prizes


Competition rules

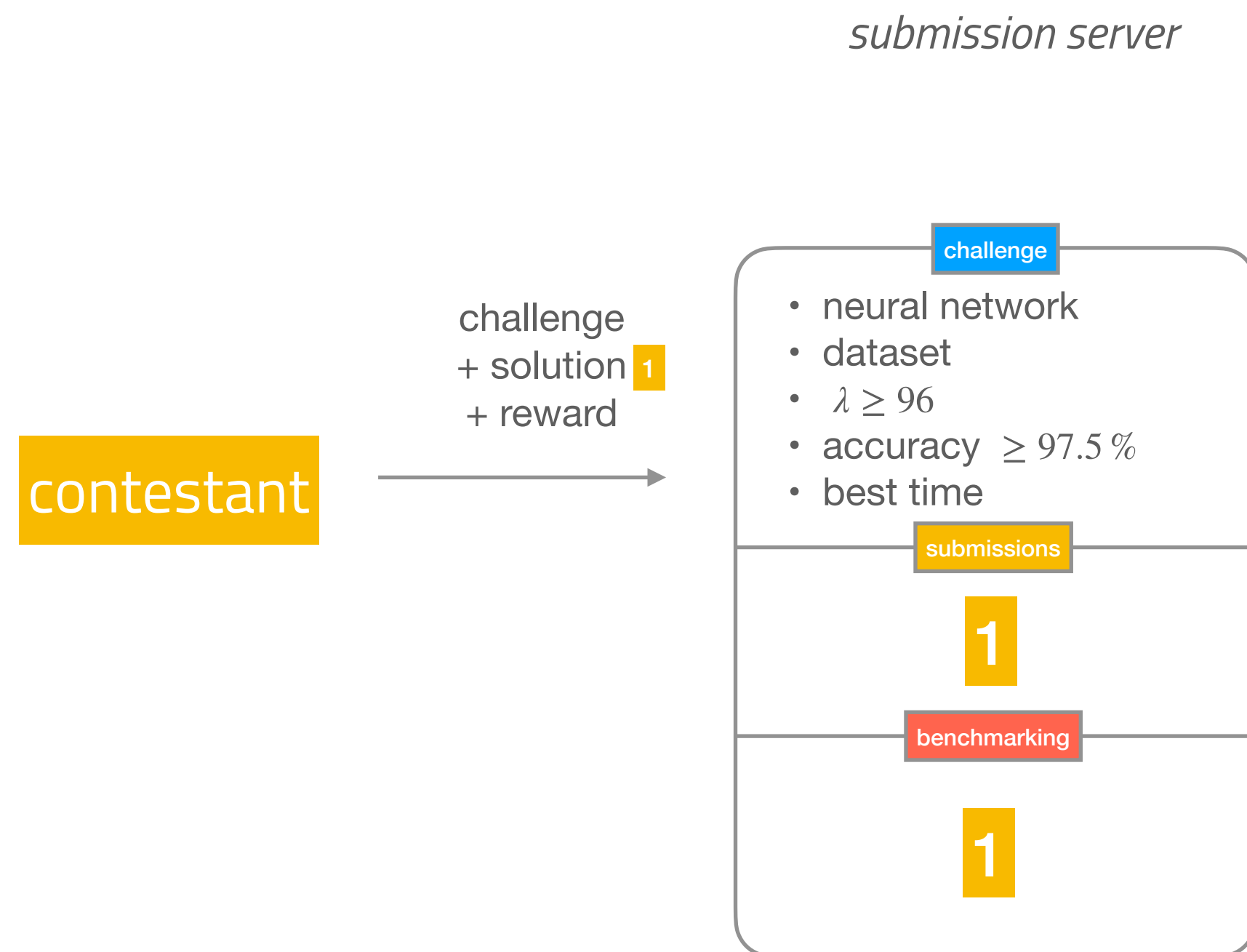


Rule 1: open to everyone,
all FHE implementations are
welcome, diversity encouraged

Rule 2: contestants may remain
anonymous (or not)

pseudonym-based

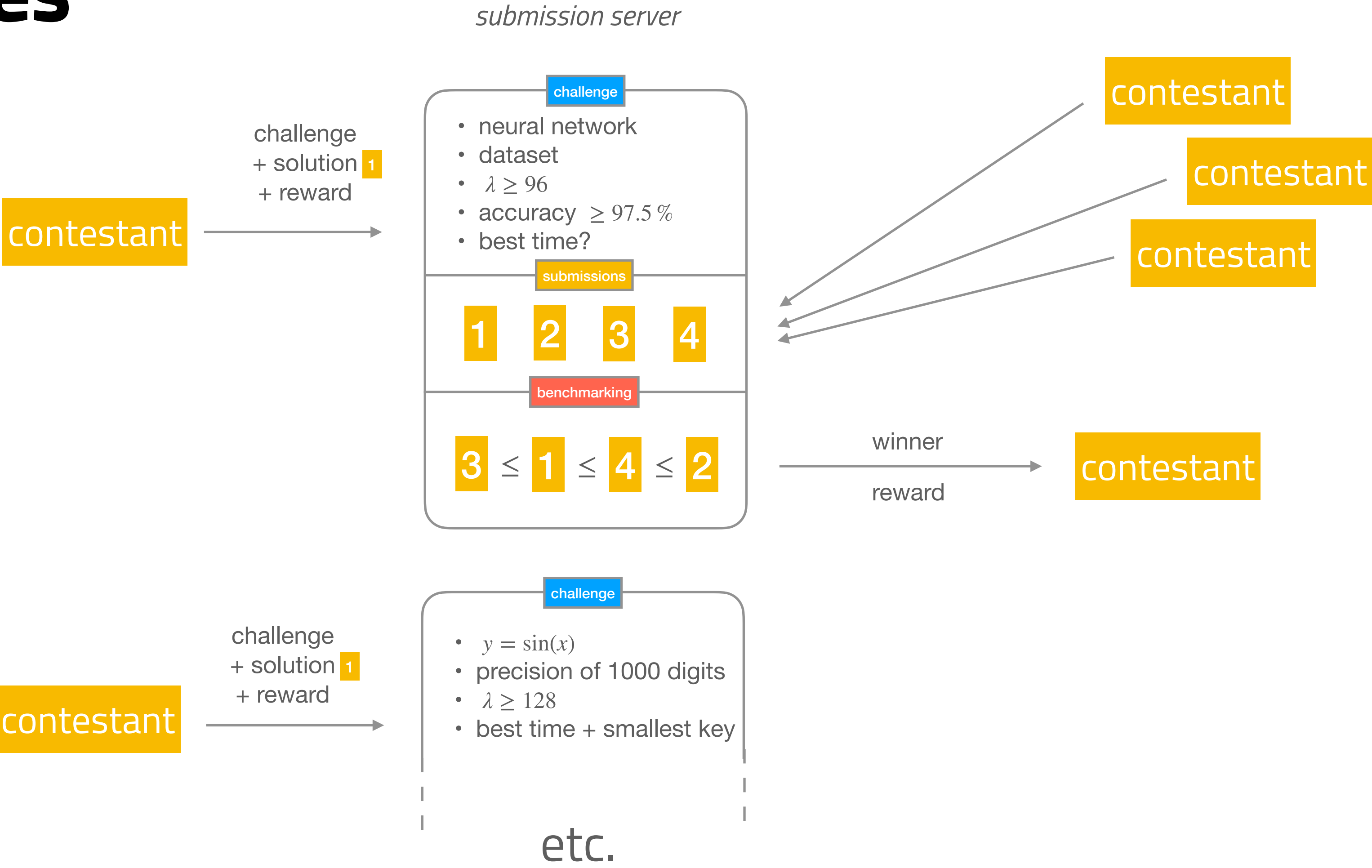
Competition rules



Rule 3: any contestant can create a separate track on a specific use-case

but a first solution is required

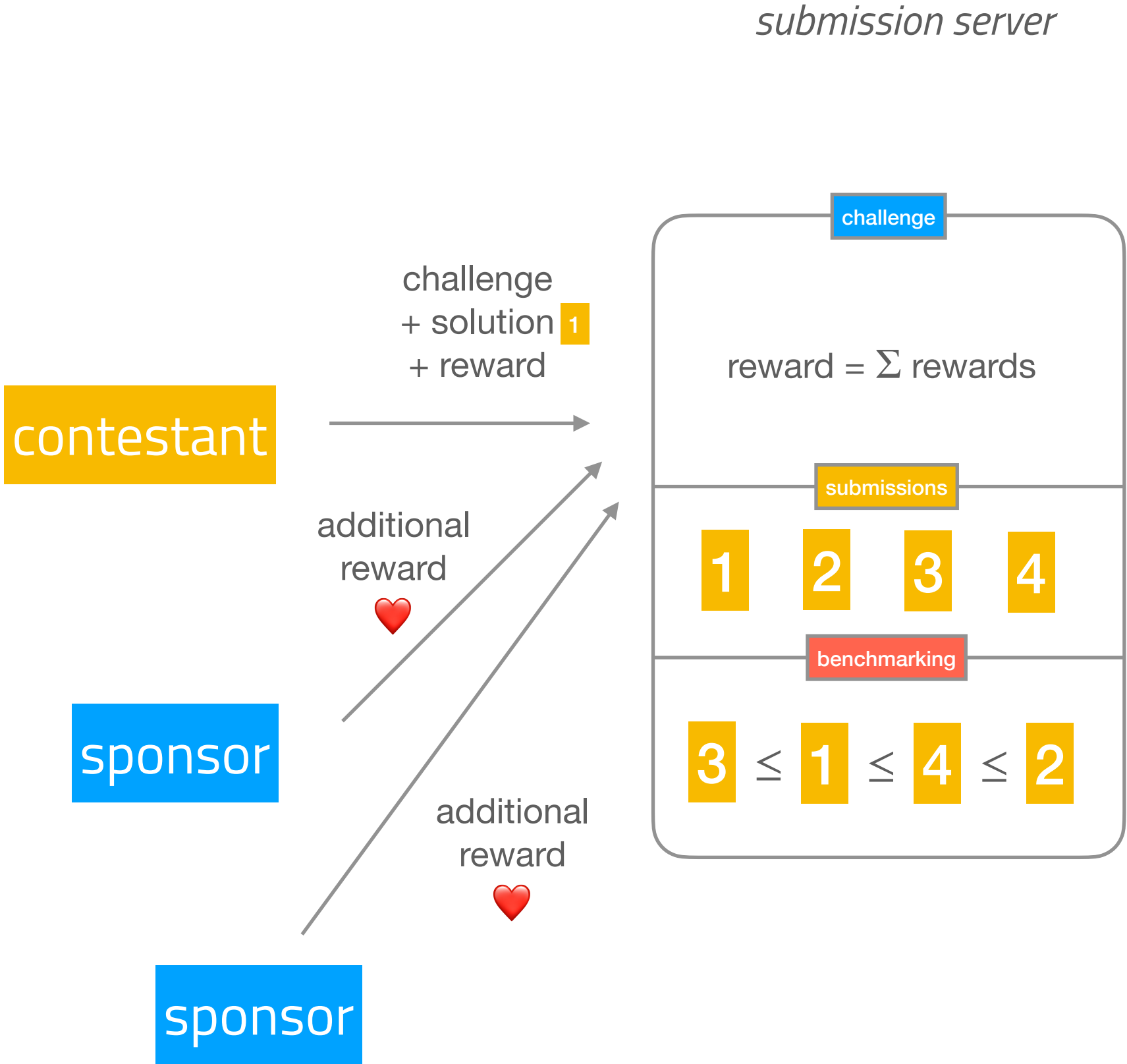
Competition rules



Rule 4: the contestant with the best score when the competition ends, wins that track

Competition rules

Sponsors



Rule 5: sponsors may add rewards to tracks they like and would like to boost

sponsors can also be anonymous

Submitting a solution

client-side
key generation
encryption
decryption

open source

closed source

server-side
homomorphic
processing

.....

- dockerized CLI **executable**
- runs on a reference architecture
 - some x86-64
 - fixed limit on RAM



Submitting a solution

client-side
key generation
encryption
decryption

open source

HEBench runs the entire cycle
key generation
random input generation
encryption
homomorphic processing
decryption
comparison / accuracy

but only benchmarks the
homomorphic processing

closed source

server-side
homomorphic
processing

.....

- dockerized CLI **executable**
- runs on a reference architecture
 - some x86-64
 - fixed limit on RAM



Submitting a solution

client-side
key generation
encryption
decryption

closed source

server-side
homomorphic
processing

.....

- dockerized CLI **executable**
- runs on a reference architecture
 - some x86-64
 - fixed limit on RAM

open source

any contestant can
download the container
and run HEBench on
her own

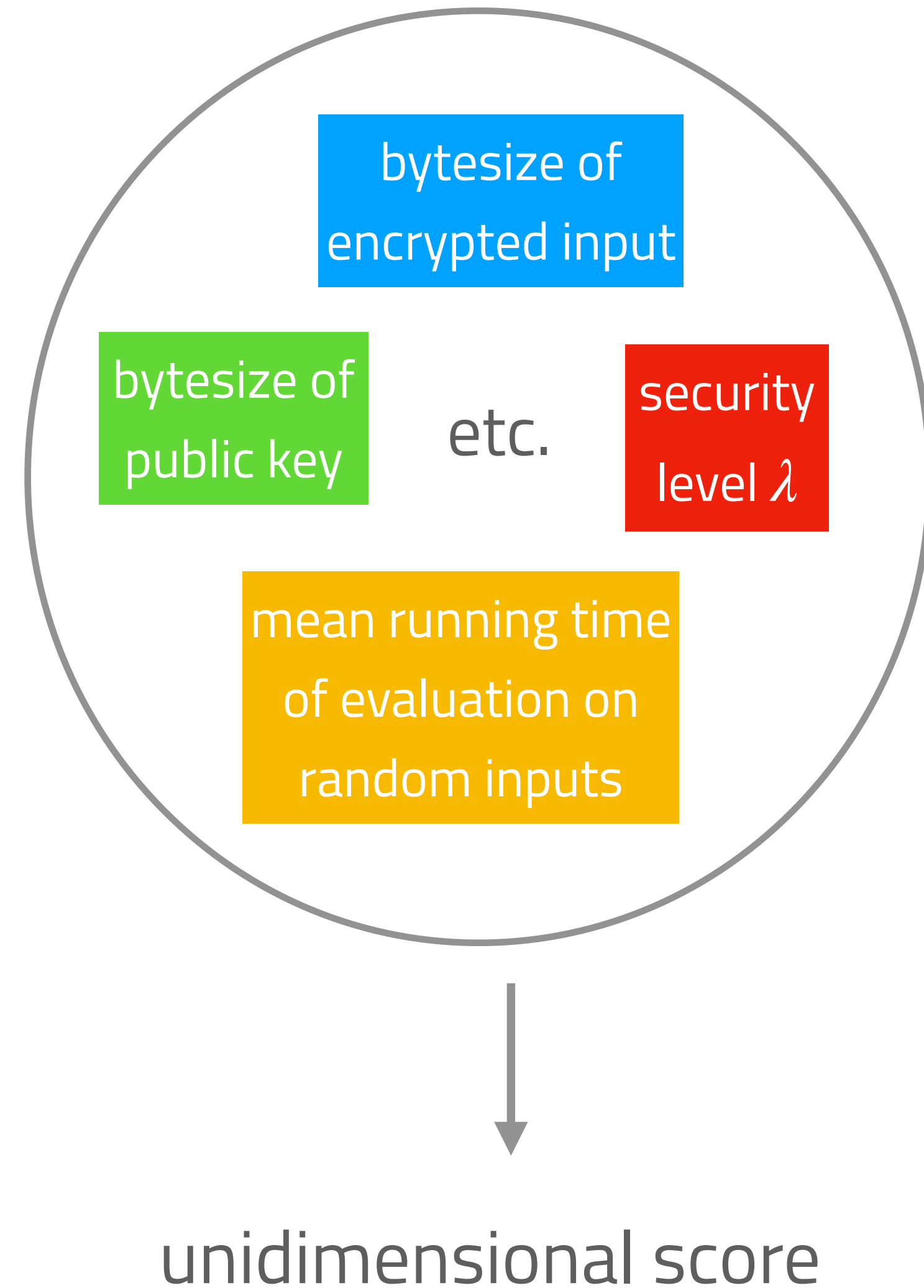
any contestant can audit
the open source part
and red-flag it if e.g. the
security claim is not met

The OC deliberates openly and
may require an update

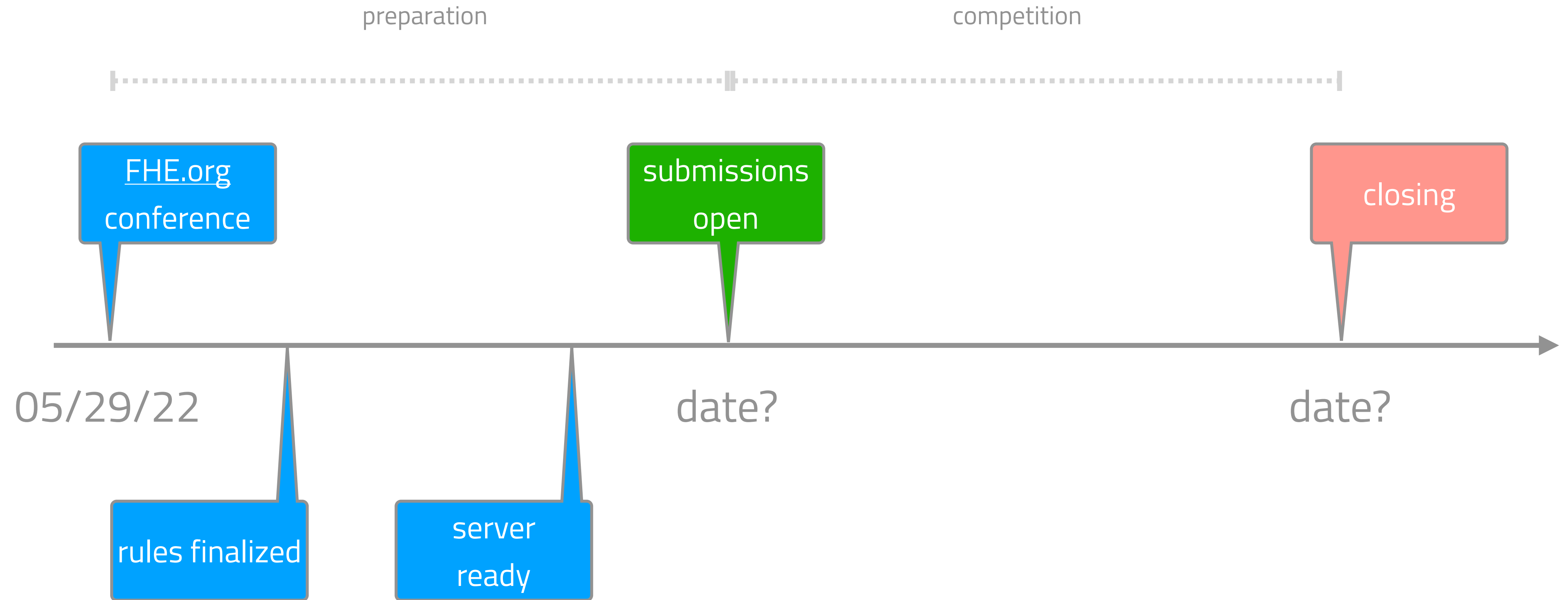


Scoring a solution

Rule 6: a posted challenge provides an arbitrary scoring function to minimize



The timeline



Want to contribute?

<https://discord.fhe.org/>

