A proposal to provide prove of honesty of tournament organizer

The problem

After a session of hands is played the players can be suspicious of the hands. Were they random, or were they rigged? Currently there is no way for the tournament organizers to prove that they are honest.

Thoughts

It should be possible using crypto techniques to solve this problem

First method

In theory the organizer could blatantly rig hands, move cards around, organize triple squeezes etc. This is easily circumvented. Let us assume we use (a slightly modified) BigDeal, as we will in this whole document. The way BigDeal works is that it first gets, through keyboard input or otherwise, a bunch of randomness. It uses a piece of software, called a cryptohash, to make a 160 bit number out of this randomness. This 160 bit number looks something like this(in hexadecimal digits): 3C223ED17E17F45229AD618F0FA98FE567D2D31D.

Now BigDeal generates a series of hands using this starting number. Because of the cryptographic techniques it is not possible to reverse this process, so you cannot first come up with a series of hands and then make such a starting number from it.

So method one could be to print this starting number at the bottom of the hand records, so people could use their own version of BigDeal to test if it actually generates this series. For this they need the same modified BigDeal, and supply it with the starting number using a normally hidden option.

This method guarantees that a series of hands comes out of BigDeal.

Second method

Now we have the guarantee that the hands come out of BigDeal, but nothing still prevents the organizer to generate many more sets than needed, pick the interesting ones, put the wildest series in the evening sessions or any other subterfuge he could think of.

This can also be fixed. First it is important to realize that the starting number of BigDeal need not be purely random. What is needed is uniqueness and unpredictability. This is normally achieved by being random and being a big number, but other methods could work as well. Again important to realize is that the series of hands coming out of BigDeal will have the correct statistical properties no matter what starting number is used(as far as one can say this about a finite set).

So method two runs as follows. The organizer generates the Tournament Secret(TS), preferably again a large number, but any other secret is OK, as long as it is guaranteed unique. The organizer also names all the series of hands in the tournament, like for example

Bermuda Bowl 2024 Vatican City/Round Robin 13

and so for all the series, call it Session Name(SN). Now we have a secret(TS), and a list of names(SN). The organizer now publishes all this information, for example by Email and/or the tournament website. A slight modification is needed here, because the secret needs to remain secret until the tournament is played, otherwise the players would be able to generate the hands before they play them.

The modification is that enough information is published to check the secret after the tournament, without giving it away before. Again we use cryptographic techniques. We make a crypto-checksum of the secret, using MD5, SHA-256, RIPEMD-160, or any other well-known and publicly available checksum software, and we publish the checksum, and not the secret itself. Because of the crypto-checksum technique it is not possible for players to find out the secret before the tournament.

To generate a series of hands we now use the secret(TS) and the name of the session(SN) to generate a starting value and make the hands.

After the tournament the secret itself is published, and now players can check the hands using exactly the technique that the organizer used. They can also check the correspondence of the secret and the published check-sum.

Third method

Now there is only one trick left for the organizer. He could generate many secrets, check all the resulting series of hands, and pick the ones he likes best. He publishes the secret for this series of series. What can we do about this? The only way to make sure this cannot be done is to make sure that the organizer does not have all the information when he publishes the secret. Other information is needed after this moment.

One way, described in Budapest, is to let the participants join in. They could send information after the publishing of the secret. Another way would be to take a well-known piece of information, but one only becoming known after publishing of the secret. The closing Dow Jones Index a week after publishing the secret should do.

No matter how it is done we now have the Delayed Information(DI). For each series the organizer now uses the TS, DI and SN together to generate the starting value.

This Third Method is the proposed method.

Security

No player can generate the hands before the tournament because for that the TS is needed, and they only have the crypto-checksum of it, which is not reversible. The players do have the DI and the SN, but that is not enough.

The organizer can generate the hands after the DI becomes available, but by that time he cannot change TS and/or SN anymore, so he cannot influence the hands.

When, after the tournament, the TS is published all players can generate the hands just like the organizer did and verify that no foul play was involved.

Details

Very occasionally a set must be redealt because it leaked by an error. In that case you deal again, now using for example
Bermuda Bowl 2024 Vatican City/Round Robin 13a,
and explain to the players why it was necessary to make this new set.

Wrap up

I think this is the simplest I can come up with to solve the whole problem. It looks complicated but this can all easily be automated. At the championships in Budapest I proposed something similar, but not as good. At that time there was not perceived a problem worth solving. By now perhaps there might be interest.