Twitter Thread by Lea Kissner



Lea Kissner
@LeaKissner

We're kicking off the Privacy Tech session at #enigma2021 with Mitch Negus speaking about "NO DATA, NO PROBLEM—GIVING NUCLEAR INSPECTORS BETTER TOOLS WITHOUT REVEALING STATE

A nuclear catastrophe hasn't occurred... yet. So we need to stay vigilant. Nuclear inspectors go in according to treaties to check what's going on and check compliance with treaty rules.

But as sophisticated analytics become more common, states will only want to share the minimum amount of information necessary under the treaty.

But perhaps we can use MPC -- secure multi-party computation

Yao's garbled circuits were first demonstrated on the millionaire's problem -- figuring out who's richer without revealing actual amounts.

Used for other things like cryptocurrency these days.

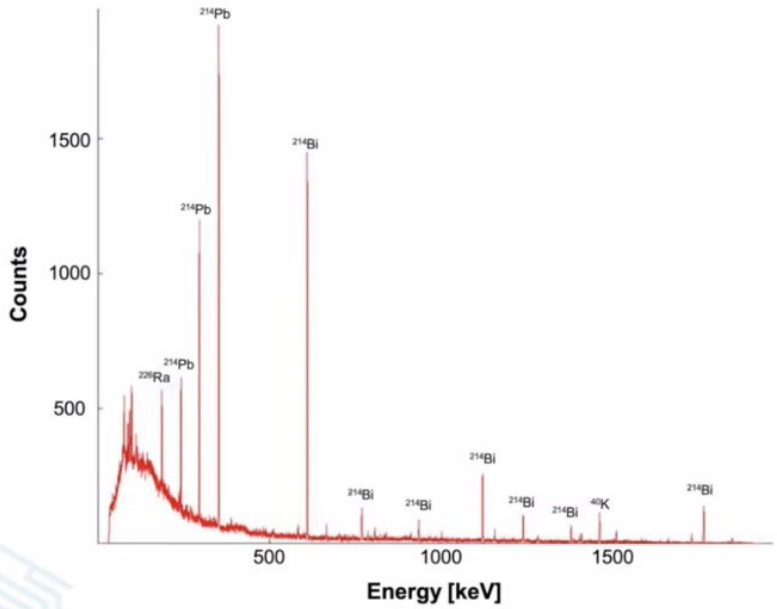
Can we use this for nuclear inspection?

MPC can be used to compute anything computed by a computer [but it's expensive!]

Every nuclear material has its own spectrum. By looking at the spectrum it tells inspectors what materials (and how much) are present at a site.

This is an example of the graph for uranium

Radiation Spectra





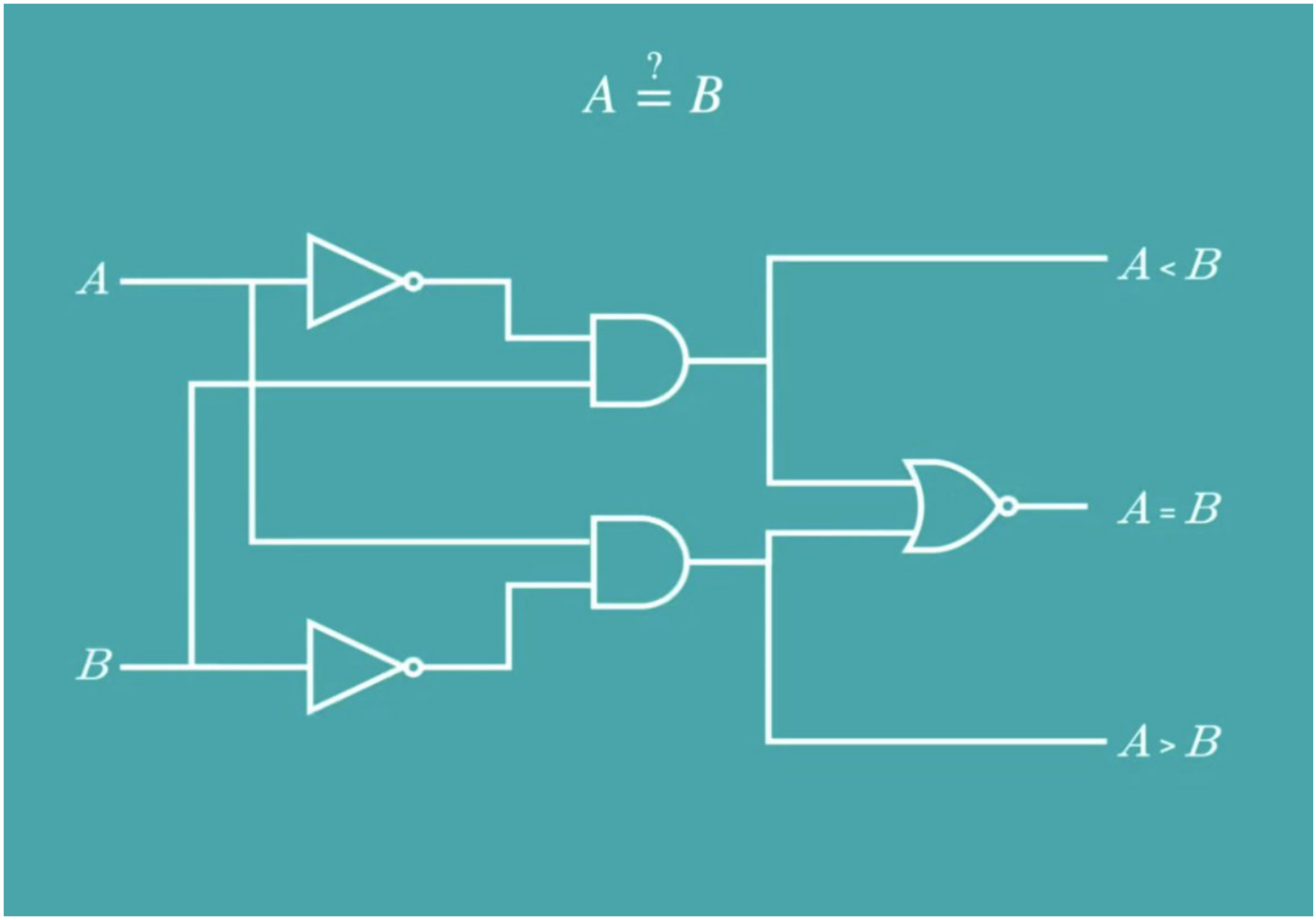


Why hasn't someone done this yet?

* It's expensive! We haven't had computers fast enough before.
* The inspectors need to be *sure* that it will work. They want tried and true, not latest and greatest.
* It's a small field with a limited budget.

MPC explainer (it's cool but not magic)

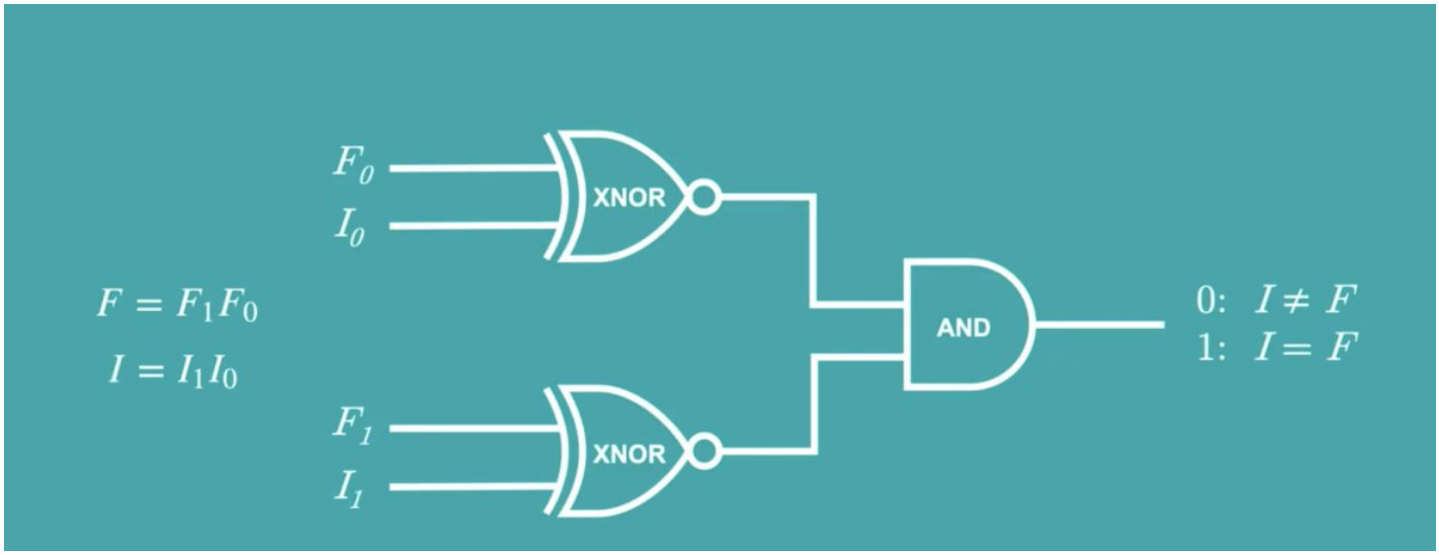
Make a circuit which does some kind of computational task, like whether A < B



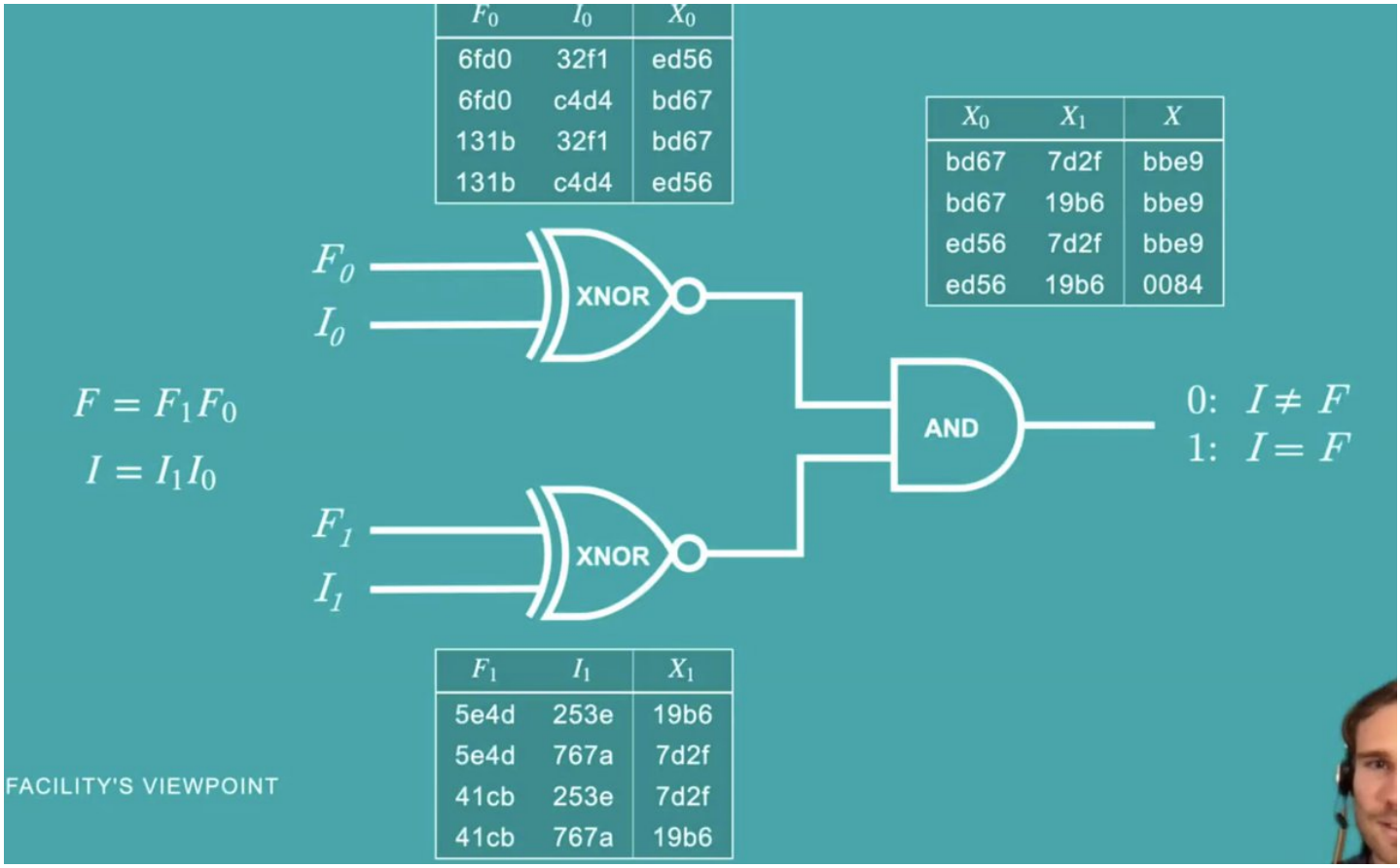
Garbled circuits build on these logic circuits.

Let's think about a case with two parties where we want to compare two inputs. That can be done with this circuit.

[accessibility apology: I'm livetweeting this really fast and can't render these diagrams in text]

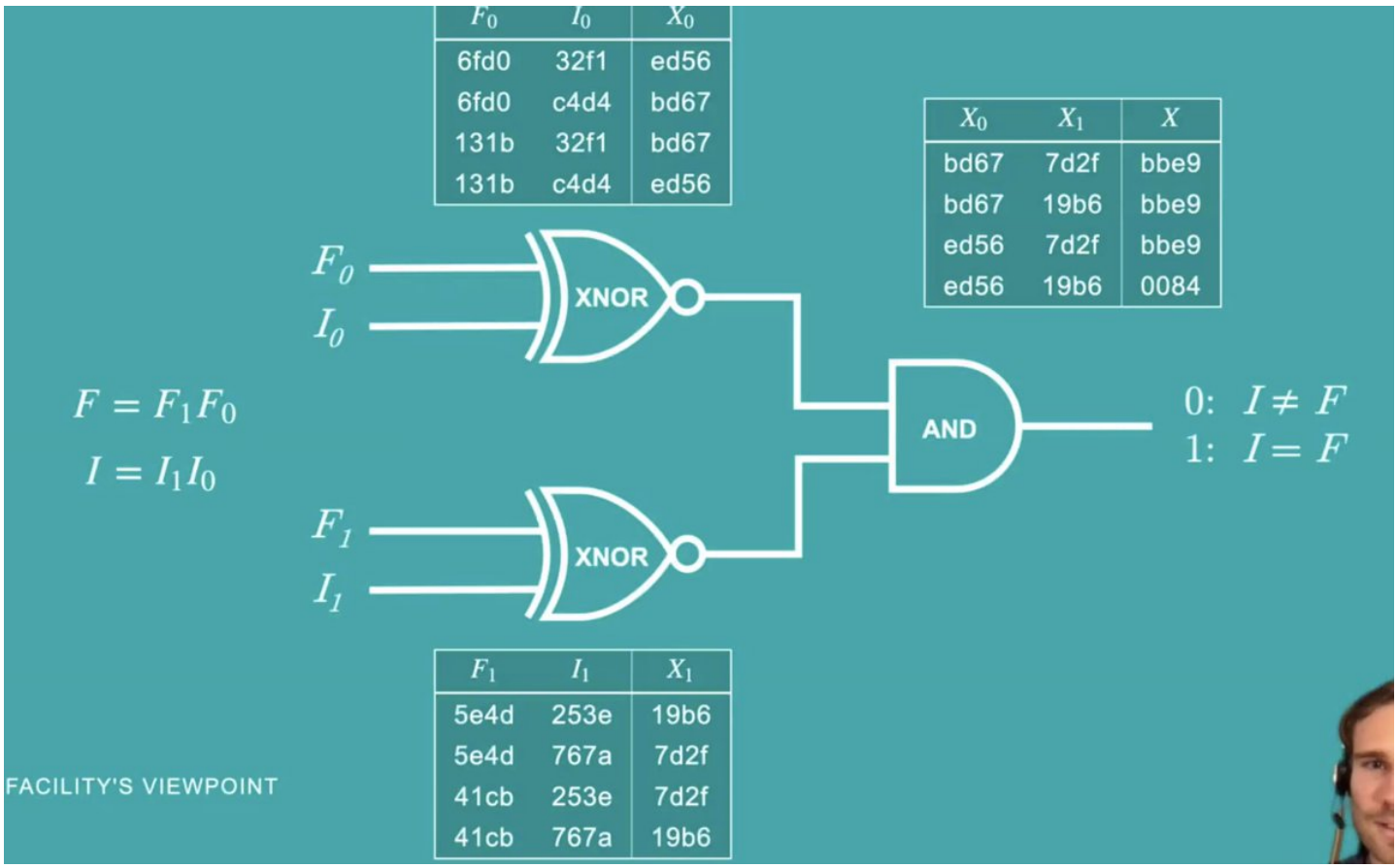


Then we stick random numbers as labels on each of the inputs



Then encrypt all the inputs -- you can only decrypt the output which gives you the correct output.

[Also go watch this talk -- it's a good explanation but very hard to livetweet]



Up until this point, everything was done by one party. They create this whole garbled circuit thingie.

Then we use this crypto thingie called oblivious transfer. That lets the other party get the keys to do the decryption of the correct output for each gate.

Eventually they get to the end, and sucess! The answer to the garbled circuit, which gives them the correct answer to the circuit.

How to use this in the real world?

Want to use pre-existing software (to give confidence to the inspectors). But not every system can work for this: they can't scale enough, they're too bleeding-edge fancy (hard to use!), etc.



So built a prototype of their own, called CipherCircuit in Python. (Yes, it's slow, but more accessible and easier to use.)

Looked for a test application -- something easier than that whole nuclear signature example!

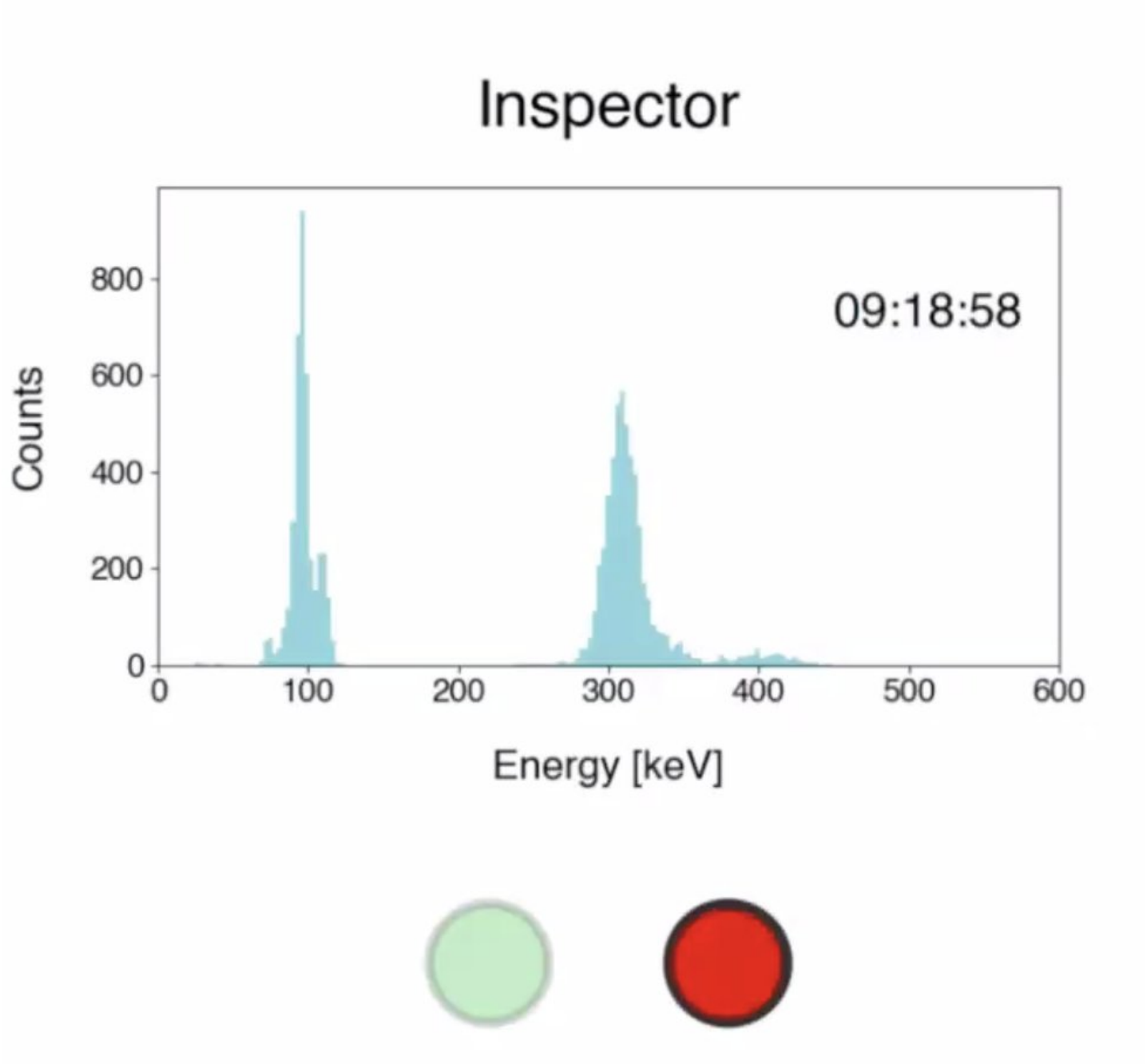
Instead did electrocardiogram analysis as a proof of concept to give the analysis without revealing the actual heartbeat.

Moved on to analyzing radiation signatures, looking for a particular movement of 233Pa along a road. Could they find this movement without ever looking at the detector's output?



[I definitely cannot render this animated data visualization please see talk.]

Spoiler: yes! They detected the spike!



It's still slow to build the circuit [... and I suspect to run it]

Can we be resilient to malicious adversaries? Maybe commitment scheme?

Believe this is more important than ever with increasing international tensions... and want to push for MPC to go mainstream

[End of talk]