The following are notes from the Crypto Academic Workshop at Edge City.

## Problem Description

There are several problems that need to be solved to make the TEE trust model palatable for a wide set of Web3 use cases. One of these is defense against hardware trojans - i.e. hardware that is maliciously buit to deviate from spec, potentially compromising any system running on top of it. The goal of this discussion was to arrive at a sort of “decentralised quality assurance protocol”, which provides some guarantees over hardware correctness under more reasonable assumptions than the honesty of the manufacturer, a sole party.

We assume any analysis must be destructive.

Note that it is insufficient for a prospective buyer to purchase superfluous TEEs and conduct their own sampling and analysis. Manufacturers and TEE operators may collude and we assume a TEE operator must also convince multiple counterparties of the correctness of their hardware.

This is separate form (but related to) defense against manufacturers keeping copies of hardware secrets and phsyical tamper resistance.

For more background on hardware trojan detection, you can readthis or this.

## Notes:

We did not arrive at a protocol, but have several constructive thoughts to share.

- Once a verifier claims that they have some conclusion after analysis, how do we verify this given that the process employed is destructive? Can we stop halfway through the process and use the remaining parts of the chip to support a claim of misbehaviour? If not, we need to guard against verifiers making spurious claims.
- If we can stop the manufacturing process halfway, how can we associated the semi-destroyed chip with its identity? Presumably the identity is derived from platform secrets, but if the chip is no longer functional, these may no longer be used in an authentication protocol.

- If we can stop the manufacturing process halfway, how can we associated the semi-destroyed chip with its identity? Presumably the identity is derived from platform secrets, but if the chip is no longer functional, these may no longer be used in an authentication protocol.

- The analysis is very hard to pull off as even subtle deviations in chip design can open channels for information exfiltration [must add link].
- A QA protocol may begin something like this:
- 
  1. all chips in a batch are registered on-chain.

- all chips in a batch are registered on-chain.

- 1a) (optionally) some intentionally modified chips are also registered on chain, along with a commitment to show that these are indeed tampered with
- 
  1. a verifiable randomness beacon is used to shuffle and randomly select devices for analysis

- a verifiable randomness beacon is used to shuffle and randomly select devices for analysis

- 2a) (optionally) Whistleblowers are allowed to put down some collateral to identify chips that ought to be analysed
- 
  1. results of analysis are posted on chain

- results of analysis are posted on chain

- 3a) (if step 1a is followed) the committed list of intentionally compromised chips is revealed.
- 
  1. purchasers registers their desire to purchase chips on chain. Again, using a randomness beacon we randomly select from the remaining chips and assign to the buyers.

- purchasers registers their desire to purchase chips on chain. Again, using a randomness beacon we randomly select from the remaining chips and assign to the buyers.

-

1. all chips in a batch are registered on-chain.

- all chips in a batch are registered on-chain.

- 1a) (optionally) some intentionally modified chips are also registered on chain, along with a commitment to show that these are indeed tampered with
-
    1. a verifiable randomness beacon is used to shuffle and randomly select devices for analysis

- a verifiable randomness beacon is used to shuffle and randomly select devices for analysis

- 2a) (optionally) Whistleblowers are allowed to put down some collateral to identify chips that ought to be analysed
-
    1. results of analysis are posted on chain

- results of analysis are posted on chain

- 3a) (if step 1a is followed) the committed list of intentionally compromised chips is revealed.
-
    1. purchasers registers their desire to purchase chips on chain. Again, using a randomness beacon we randomly select from the remaining chips and assign to the buyers.

- purchasers registers their desire to purchase chips on chain. Again, using a randomness beacon we randomly select from the remaining chips and assign to the buyers.

- As indicated above, we can defend against lazy verifiers by intentionally inserting compromised chips into the testing process. This would require a manufacturer to comply, potentially increasing attack surface area.
- In the protocol above, it is unclear how to handle the cases in which:
- the verifier is assigned a chip that is on the list of (supposedly) intentionally modified chips, but the verifier does not flag it
- the verifier flags a chip which is not on the test list as malicious

- the verifier is assigned a chip that is on the list of (supposedly) intentionally modified chips, but the verifier does not flag it
- the verifier flags a chip which is not on the test list as malicious