SoK: Something About Functionalities

***Abstract*—The abstract goes here.**

I. Introduction

UC [1]

II. Universal Composability

Brain dump below.

A. RSIM

B. GNUC

GNUC [2] deviates from UC in terms of structuring protocols, the notion of PPT, and corruptions.

Composition theorem. UC composition theorem does not hold in UC05.

Corruptions. In UC05, adversary is allowed very fine-grained corruptions, i.e., an adversary can corrupt a subroutine of a given party. If the real adversary corrupts the subroutine machine of a party, which has only one corresponding ideal machine in the ideal protocol, it is not clear whether the ideal adversary should be able to corrupt the only ideal machine. Also, an adversary can impersonate a party if it corrupts its, say, secure communication subroutine. Although this party is essentially corrupted, it is not formally considered to be.

Polynomial runtime. In UC05, a protocol is poly-time when all machines run in a number of steps that is polynomial in the difference between the length of their respective inputs minus the length of all inputs passed to its subroutines. This means that a protocol must provide enough input padding to propagate runtime throughout its subroutines, i.e., the interface of the ideal protocol must depend on the complexity of the intended implementation.

Protocol hierarchy. Every machine has an identity that uniquely identifies its position in a tree of possible protocols. A program map from identitifes to a library of programs determines a machine's program. Replacing a subprotocol means changing the library.

Hierarchical corruptions. In order to corrupt a machine, an adversary must corrupt all machines that are above that machine in the protocol hierarchy. Real corruptions always have ideal counterparts.

Polynomial runtime. Poly-time is closed under composition. If one instance of protocol is poly-time, then many instances are as well. Replacing a poly-time subprotocol in a larger protocol with a poly-time implementation, then the larger protocol is poly-time as well.

III. Conclusion

References

[1] R. Canetti, "Universally composable security: A new paradigm for cryptographic protocols," in *Foundations of Computer Science, 2001. Proceedings. 42nd IEEE Symposium on*. IEEE, 2001, pp. 136–145.

[2] D. Hofheinz and V. Shoup, "Gnuc: A new universal composability framework," *Journal of Cryptology*, vol. 28, no. 3, pp. 423–508, 2015.