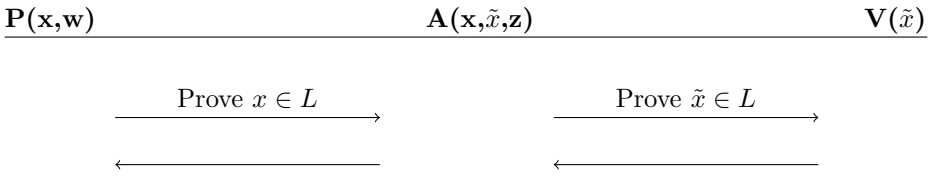
CS 294 – Secure Computation Mar 29, 2016

Lecture 19: Non-malleable zero knowledge

Instructor: Sanjam Garg *Scribe: Gil Lederman*

1 Man in the Middle in ZK

As we recall, a zero-knowledge protocol is an interactive proof $< P, V >$ for which for any (possibly malicious) verifier V^* there is a simulator S which can produce V^*'s view on its own, without access to the prover P.
Zero knowledge, by its definition, gives us assurances that V cannot take the transcript of its interaction with P proving some $x \in L$ and convince with it anyone else. However, what if some malicious verifier interacts as a *prover* with respect to another honest verifier? ZK gives us no assurances in that scenario, which in general is referred to as a *man-in-the-middle* attack. The setting is:



Where the man in the middle (MIM) is the adversary A, which has complete control over the channel between P and V - it can generate messages, choose to forward them or not, and it controls the scheduling of the messages. A tries to use its on-going interaction with P regarding $x \in L$ and auxiliary input z to convince V that another $\tilde{x} \neq x$ is in L.
With this in mind, we can define what it means for an interactive proof to be *non-malleable*, following the standard approach of comparing the real-world scenario with an ideal-world scenario. Let $mim_V^A(x, \tilde{x}, w, z)$ be the random variable describing the output of V in the MIM setting above ("real execution"), with the random tapes of P, A, V uniformly and independently chosen. Let $sta_V^S(x, \tilde{x}, z)$ be the random variable which describes V's output after interacting with a stand-alone adversary S who gets as input everything A had, but not the witness w. We can now define:

Definition 1 (Non-malleable interactive proof) *An interactive proof $< P, V >$ for a language L is said to be* non-malleable *if for every efficient man in the middle A there is a stand-alone prover S running in expected polynomial time such that for every $\tilde{x} \in \{0,1\}^{|x|}$ so that $\tilde{x} \neq x$ and $z \in \{0,1\}^*$:*

$$\Pr\left[mim_V^A(x, \tilde{x}, w, z) = 1\right] < \Pr\left[sta_V^S(x, \tilde{x}, z) = 1\right] + neg(|x|)$$

Note that we claim nothing for $x = \tilde{x}$, and indeed, in that case A could simply forward the messages between P and V (the two chess masters problem). Lastly, a proof system is non-malleable ZK if it is both non-malleable and ZK.

2 Simulation-Extractability with respect to tags

We now slightly change our proof system by adding *tags* of length $m(n)$, which can be thought of as the identity of the interaction. We will have a family of IP systems $\{< P_{TAG}, V_{TAG} >\}_{TAG \in \{0,1\}^{m(n)}}$. With tags, we can actually modify the non-malleability definition to be secure even when $x = \tilde{x}$, as long as the tags are different. However, we will instead use the stronger property defined in [1] (it can be shown to imply non-malleability) of Simulation-Extractability. With $view_A(x, z, TAG)$ being the joint view of A and the honest verifier $V_{T\tilde{A}G}$ when A verifies $x \in L$ on the left with identity TAG and proves $\tilde{x} \in L$ on the right with identity $T\tilde{A}G$, we have:

Definition 2 (Simulation-extractable protocol) *A family* $\{< P_{TAG}, V_{TAG} >\}_{TAG \in \{0,1\}^*}$ *of interactive proofs is said to be* simulation extractable *with tags of length* $m = m(n)$ *if for any MIM adversary A, there exists a probabilistic expected-time polynomial machine* `(SIM,EXT)` *such that:*

- *The ensembles* $\{\texttt{SIM}(x, z, TAG)\}_{x,z,TAG}$ *and* $\{view_A(x, z, TAG)\}_{x,z,TAG}$ *are statistically close.*
- *Let* $\tilde{x}$ *be the right hand side statement appearing in* $\texttt{SIM}(x, z, TAG)$*. If the right hand side interaction accepts and* $TAG \neq T\tilde{A}G$*, the output of* $EXT(x, z, TAG)$ *consists of a witness* w *such that* $R_L(\tilde{x}, w) = 1$*.*

We will proceed to construct a Simulation-extractable protocol for "small tags" of length roughly $\log n$, and will then use the small tags protocol as a subroutine in the protocol with tags coming from $\{0, 1\}^n$.

References

[1] Rafael Pass and Alon Rosen. New and improved constructions of non-malleable cryptographic protocols. In *Proceedings of the Thirty-seventh Annual ACM Symposium on Theory of Computing*, STOC '05, pages 533–542, New York, NY, USA, 2005. ACM.