The Random Oracle Model and Fiat-Shamir

Alexander Lindenbaum

Notes are from Chapter 5 of [Tha22].

Definition 1 (Public-coin interactive proof)**.** An interactive proof where any coin tossed by $\mathcal{V}$ is visible to $\mathcal{P}$ as soon as it is tossed. Without loss of generality, these random coin flips are the only messages $\mathcal{V}$ sends to $\mathcal{P}$ (all other messages are deterministic and based on x and r, so $\mathcal{P}$ can derive them on its own). These are "random challanges."

1 The Random Oracle Model

Definition 2 (Random Oracle Model)**.** The random oracle model (ROM) is the assumption that in an interactive proof, the prover and verifier have query access to a random function/oracle $R : \mathcal{D} \to \{0,1\}^\lambda$. On input query $x \in \mathcal{D}$, R makes an independent random choice to determine $R(x)$. R keeps a record to make sure that it repeats the same response if x is queried again.

Some remarks

- An idealized setting, motivated by practical constructions of hash functions like SHA-3, computationally indistinguishable from (truly) random functions.
- Not valid in real world, since $|\mathcal{D}| \geq 2^{256}$ to ensure security. Instead, imagine it as a hash of x.
- Protocols proven secure in ROM tend to be considered secure in practice.

2 The Fiat-Shamir Transformation

Purpose: to take any public-coin IP/argument and transform it into a non-interactive, publicly verifiable protocol $\mathcal{Q}$ in ROM.

Definition 3 (Fiat-Shamir Transformation)**.** $\mathcal{P}$ takes the verifier's message in round i of $\mathcal{I}$ to be a query to the random oracle. The query point is the list of messages sent by $\mathcal{P}$ in rounds $1, \ldots, i$. $\mathcal{V}$ uses the prover's messages as in $\mathcal{I}$, and checks that the messages from $\mathcal{P}$ are hashes of previous messages.

Some remarks

- $\mathcal{P}$ can use *hash chaining*, i.e. the prover's next message is only the hash of the previous message.

- x should also always be hashed into the messages. This gives security under adversaries that can choose x.
- When Fiat-Shamir is applied to a *constant-round* public-coin IP with negligble soundness error, $\mathcal{Q}$ in ROM is sound against poly time provers.
- If $\mathcal{I}$ has *round-by-round* soundness then $\mathcal{Q}$ is sound in ROM.

References

[Tha22] Justin Thaler. Proofs, arguments, and zero-knowledge. *Foundations and Trends in Privacy and Security*, 4(2–4):117–660, 2022.