ETH zürich

PETs H25
Exercise Session 3

David Pulido
PETs Student TA
07. October 2025, Zurich

Outline

1. Further Motivation (3 min)
2. Reminder: Extra Resources (2 min)
3. Refresher on ZKP’s (Simulators and Extractors, 10 min)
4. Exercises (30 min)
5. Questions & Feedback

Further Motivation

- Building Block for Post-Quantum Crypto
- E-Cash
- Machine Learning
- Differential Privacy Auditing (see second half of course)

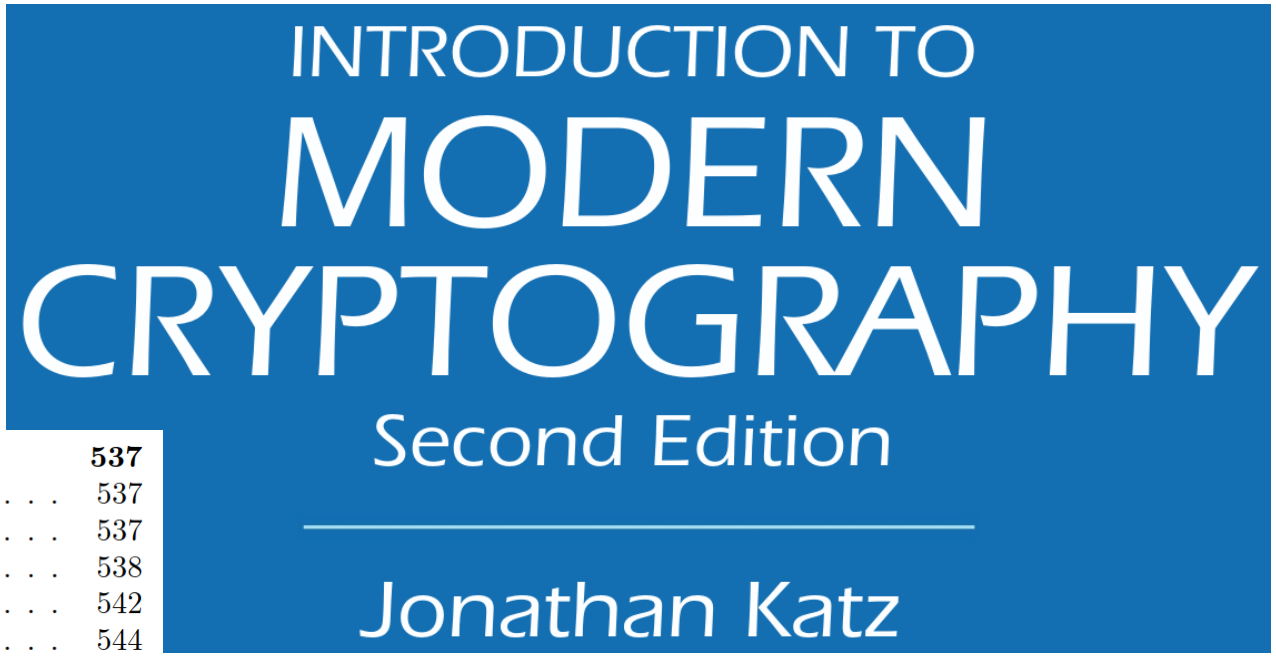
Resources (Unfinished)

A Graduate Course in Applied Cryptography

Dan Boneh and Victor Shoup

Version 0.6, Jan. 2023

Resources



ZKP – Simulator

- Computational knowledge: ability to compute something efficiently (e.g. knowing the answers of PETs homework let's you solve the problem sheet quickly)

- If the verifier could have faked the same conversation alone, they learned nothing from the real one → no new ability for efficient computation was gained

ZKP – Simulator

$\texttt{Sim}(G)$

Guess $\hat{c} \leftarrow^{\$} \{0,1\}$
  If $\hat{c} = 0$, commit to a random permutation Π of G
  If $\hat{c} = 1$, commit to a complete graph
Send the commitments to the verifier who returns c
If $\hat{c} \neq c$, abort and restart
Else, open the commitments as requested by the verifier
Output the view $(G, \texttt{Commit}, c, \texttt{Open})$

$P(G, \textbf{Ham-Cycle})$		$V(G)$
pick a random permutation Π of the n vertices; For $1 \leq i \leq j \leq n$, let $B_{ij} = 1$ if $(\Pi(i), \Pi(j)) \in E$ and $B_{ij} = 0$ otherwise;		
	$\xrightarrow{\texttt{Commit}(B_{11}), \ldots, \texttt{Commit}(B_{nn})}$	
	$\xrightarrow{\texttt{Commit}(\Pi)}$	
		$c \leftarrow^{\$} \{0,1\}$
	$\xleftarrow{c}$	
If $c = 0$, open all commitments Else, open all commitments B_{ij} where $(\Pi(i), \Pi(j))$ is in the Hamiltonian cycle.		
	$\xrightarrow{\text{Openings}}$	
		Verify commitments if $c = 0$, check that the committed graph is isomorphic to G Else, check that a cycle was opened.

Note that the simulator's first message $\texttt{Commit}$ is computationally indistinguishable from the prover's first message, as the commitments are computationally hiding.

The simulator's second message is statistically indistinguishable from the prover's second message: if $c = 0$, the simulator does exactly what the prover does, and if $c = 1$, the simulator opens all commitments of some arbitrary cycle, which is the image of the Hamiltonian cycle under *some* permutation Π.

Finally, we need to argue that the simulator is efficient. Because the commitments in the first message are computationally hiding, the verifier cannot guess $\hat{b}$ with non-negligible advantage, and thus $\Pr[\hat{b} \neq b] \leq 1/2 - \mathsf{negl}(\lambda)$. □

Knowledge Soundness & Proofs of Knowledge – Extractor

- If a prover often succeeds in convincing the verifier then it must know a witness

- PoK (existance of extractor) <=> Knowledge Soundness

Why do the simulator and extractor have special abilities?

Why do the simulator and extractor have special abilities?

- If simulator was succesful in polynomial time then simulator would be able to efficiently generate transcripts that are indistinguishable from real ones without any witness → impact on Soundess (a party with no witness could generate convincing transcripts)

- If extractor was succesful in polynomial time then a malicious verifier could potentially extract the witness too → witness leakage from provers messages (impact on Zero-Knowledge)

k-Special Soundness for 3 Round Protocols

- Given k accepting transcripts for the same instance x of L an extractor can compute a witness
- 2-Special soundness → Classic definition of sigma protocols

Sigma Protocol

- 3 Round Protocol
- Perfect completness
- Special soundness
- SHVZK

NIZK

- Under Random Oracle Model (but also more esoteric models like the Algebraic Group Model)
- Verifier doesn’t need to interact with prover since it can locally draw challenge by querying the RO

- Zero-Knowledge: stems from RO programming to match the query of the Prover/Verifier

- NIZK-PoK Knowledge soundness stems from reprogramming the RO to get two different challenges

- Bonus Question: Suppose a Sigma protocol has soundness of 1/3 what can you say about the soundness of its respective NIZK (after Fiat-Shamir)?

ETH zürich

Thank you :-)

Any Questions?