Introduction to Security Reduction

Lecture 0: Subject Introduction

Adversary

My IQ is up to 186.

My interest is breaking schemes.

You want me to help you solve problem?

Fool me first!

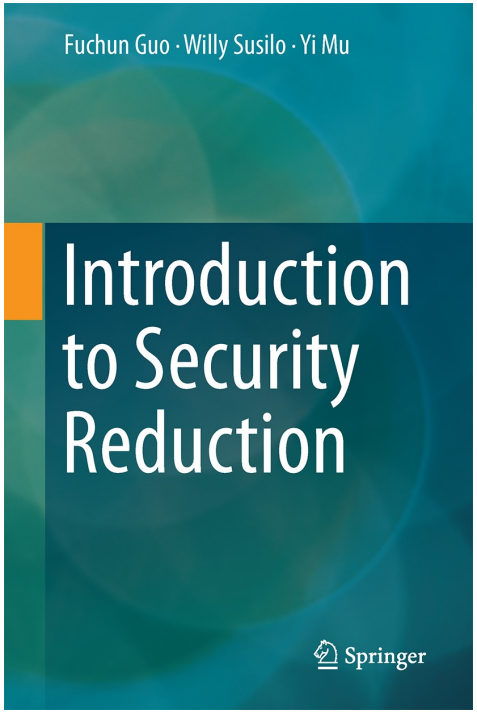
Lecture Slides: Sponsored by

Lecture Slides: Dedication to

Xiaoming (1958-2016)

About this Subject

Most contents in this subject are obtained from the following book:



Fuchun Guo, Willy Susilo, and Yi Mu. “Introduction to Security Reduction”. Springer International Publishing, 2018.

Topics

Lecture 12: Flaws in Papers
Lecture 11: Revision of Security Reduction
Lecture 10: Security Proofs for Encryption (Computational)
Lecture 9: Security Proofs for Encryption (Decisional)
Lecture 8: Security Proofs for Digital Signatures
Lecture 7: Analysis (Towards A Correct Reduction)
Lecture 6: Simulation and Solution
Lecture 5: Difficulties in Security Reduction
Lecture 4: Entry to Security Reduction
Lecture 3: Preliminaries (Hard Problem and Secure Scheme)
Lecture 2: Preliminaries (Field, Group, Pairing, and Hash Function)
Lecture 1: Definitions (Algorithm and Security Model)

Computational Complexity Theory

Topics

Lecture 8-10 (Signature and Encryption)	
Lecture 6-7 (Simulation, Solution, Analysis)	
Lecture 5 (Difficulties in Security Reduction)	
Lecture 4 (Entry to Security Reduction)	
Lecture 3 (Hard Problem and Secure Scheme)	
Lecture 2 (Group, Pairing, Hash)	**Lecture 1** (Definition)

From bottom to Top

About the Topics

- The topics in these slides focus on contents from Chapter 3 and Chapter 4 in the book.
- The introduction logic has been revised and looks better for beginners than the contents given in the book.
- However, some concepts have to be pre-used in introduction and explained in later lectures.
- The contents in the book have been revised before put to slides.
- New contents and examples are added in these slides.
- Please follow the right contents in these slides if the contents in the book and in these slides are not consistent.

About the Contents

- Each lecture could take more than 2 hours or less than 2 hours.
- Recommend discussions on the delivered knowledge.
- Don’t waste any given example. Students must practice first!

> *“Seeing once is better than hearing 100 times, but doing once is better than seeing 100 times.”*

About Lecture 12

- This lecture is designed for student presentations.
- Students are suggested to attack insecure schemes published in papers and present the finding.
- How to find a flaw is introduced in Lecture 12.
- Knowing and understanding flaws is a very important step towards designing a secure scheme.

Before this Subject

Before learning security reduction, students should know the basics of computational complexity including

- The differences between the big O and the big Omega notations.

$$O(n^k),\ \ 2^{(O(n))},\ \ \Omega(n^k),\ \ 2^{\Omega(n)}.$$

- How to define “solving problems” in computational complexity.
- What are complexity classes $\mathcal{NP}$ and $\mathcal{P}$.

The above contents are not included in these slides.

Big O Notation in this Book

A computing problem can be solved with $O(2^\lambda)$ time complexity.

- In this book, the authors meant that the best or the known algorithm that can solve the computing problem is exponential time. We cannot or we don't know how to find a polynomial time algorithm to solve this.
- In computational complexity, it means that the upper bound time complexity is exponential time. According to the big O notation, we have the following notation is still correct.

$$f(\lambda) = \lambda^2 = O(2^\lambda)$$

ϵ Notation in this Book

- The symbol ϵ refers to probability or advantage in this book.
- Suppose there exists a probabilistic algorithm that can solve a problem with probability ϵ.
- This book didn't introduce how ϵ is calculated.

Your Feedback is Important!

These lecture slides are being updated towards perfect!

(Check Update)

I very appreciate if you can send the feedback to

Fuchun Guo: fuchun@uow.edu.au

For example, what contents should be added and what contents are incorrect in slides. Any advice will be welcome.

Note: The latex resources of these slides will not be shared.


END