

Foundations of Cryptography
Dr. Ashish Choudhury
Department of Computer Science
International Institute of Information Technology – Bangalore


Lecture – 59
Goodbye for Now

Hello everyone, so welcome to this lecture so this is like the farewell lecture. So I have now formally finished the course so just a quick summary regarding what we have learnt in this course.

(Refer Slide Time: 00:41)

A Quick Summary

- ❑ Fundamental problem addressed in the course: **secure communication**



Secure channel

- ❖ **Two-stage solution**
 - **Stage I: Key-agreement (public-key cryptography)** --- Number-theoretic hard problems
 - **Stage II: Authenticated and private communication (private-key cryptography)** --- PRG/PRF/PRP/SPRP
- ❑ Various **attack models**
 - ❖ Ciphertext-only attack (COA)
 - ❖ Chosen plaintext attack (CPA)
 - ❖ Chosen ciphertext attack (CCA)
- ❑ A **3-stage approach** for every cryptographic primitive
 - ❖ Formal definition
 - ❖ Algorithmic construction

So the fundamental problem that we have addressed in this course is that of secure communication where the problem statement is the following we have 2 unknown parties who do not have any pre shared information say Sita and Ram meeting for the first time connected by a publicly known channel and their goal is basically to apply some algorithms and get an effect of a virtual secure channel over this publicly known channel and this virtual secure channel should ensure that this Sita and Ram are talking to each other in a secure manner.

And when I say secured that means I need to satisfy 3 properties namely privacy, integrity and authentication and we have seen a 2 stage solution to solve this problem. In stage 1 we solve the key agreement problem using public key cryptography where the goal of Sita and Ram is to agree upon a common key and to do that we use number theoretic hard problems and public key

encryption and once the key is agreed upon then in the stage 2 the Sita and Ram performs authenticated and private communication using private key cryptography or symmetric key cryptography.

And for that we have introduced several building blocks like pseudo random generator, pseudo random function, pseudo random permutation and strong pseudo random permutation we have seen various attack models both for stage 1 as well as stage 2 namely we have seen passive adversarial model and with respect to passive adversarial model we have a ciphertext only attack and chosen plain text attack whereas for a malicious or active adversary we have considered the chosen ciphertext attack model.

And for each of the cryptographic primitives that we have used in stage 1 and stage 2 we have followed a rigorous 3 stage approach. Namely in stage 1 we have formally defined what exactly we want to construct; what exactly is the definition of security for the primitive that we are interested to construct once we have the formal definition in stage 2 we give an algorithmic construction for that primitive.

And once we have the algorithmic construction in stage 3 we gave a rigorous formal security proof for the construction that we have given and show that indeed the algorithmic construction satisfies the formal definition that we have given in stage 1.

(Refer Slide Time: 03:04)



So as I said during my first lecture, cryptography is not just about solving the problem of secure communication. In this course we just focus on secure communication. But the umbrella of cryptography covers lots of advanced topics so we can do many fancy things using cryptography. For instance, we can do secure multi-party computation, where a set of mutually distrusting parties can interact with each other and perform or carry out any kind of computations securely without revealing their data to each other.

We can design a special purpose encryption schemes like non-committing encryption, deniable encryption, fully homomorphic encryption, functional encryption for specialized tasks. We have a whole lot of we have an entire branch of what we call us leakage resilient cryptography which takes into account what we call as side channel attack or side channel information. So throughout this course when we were analyzing or when we are formalizing the security requirement, we just consider that adversary has got access to encryption oracle or decryption oracle or some kind of oracle access, to the key. But it turns out that during the practical deployment of cryptographic primitives adversary might get other kinds of information or side channel information which cannot be modeled, or which were not modelled in the formal definitions that we have seen in this lecture.

For instance, it might be the case that adversary might get access to the power trace of the decryption algorithm that means how much power the decryption algorithm is consuming and

depending upon the power trace of the decryption algorithm adversary can indeed find out what exactly is the value of the decryption key. So that is the kind of side channel information which is not formally captured in the formal modeling that we have done in this course.

So it turns out that there we have a whole branch of cryptography dedicated into the design of cryptography primitives taking into account the side channel information and that branch of cryptography is called as leakage resilient cryptography. In the same way we have another branch of cryptography called Light weight cryptography where we study the design of cryptography primitives for resource constrained environments like RFID, IoT etc.

So a key bottleneck in the resource constraint environment like RFID, IoT wireless sensor networks is that the computing speed is very low and there we cannot use the typical cryptography primitives because typical cryptographic primitives operates with a key size of say 256 bits if you are in the symmetric key world or 1024 bits if you are in the public key world. But we cannot perform that much heavy computation in this resource constrained environment.

So the question is can we come up with a new set of cryptographic primitives which do not require that much amount of computation and the branch of cryptography dedicated to the study of such cryptography primitives is called as Light-Weight cryptography. So I hope that in the future I might be able to offer course covering some of these advanced topics.

(Refer Slide Time: 06:14)

Concluding Remarks

Picture copyright@Arpita Patra



So finally the concluding remarks so first of all this is the first time I am offering a new course. So during the beginning during the first few lectures it was quite inconvenient for me because this is the first time, I am doing a recording a live recording where there are no students available in the class. So I took it took some time for me to get accustomed to this setting and I must confess that my spoken English is very bad compared to my written English.

So you always might find some linguistic errors and grammatical errors. So kindly apologize kindly I beg your pardon for the same and I would also like to stress that in several lectures it has so happened that there are various typos coming and while recording. So for instance if I am supposed to say deterministic, I end up saying randomized if I am supposed to say a variable x I end up calling it y and so on.

So it becomes very difficult to rectify such minor issues by rerecording it, so I am not doing that. But I hope that depending upon the context it will be clear that they are just typos and I hope that during the transcription process where when these lectures are transcribed those typos get rectified and I would like to put some acknowledgements here. So I would like to dedicate this course to key people who have contributed in my academic development.

(Refer Slide Time: 07:45)

Acknowledgements



(Prof. Kamala Krithivasan)



(Prof. C. Pandu Rangan)



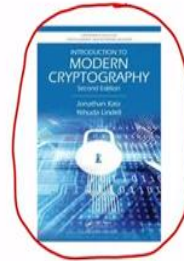
(Prof. S. A. Choudum)



(Prof. Palash Sarkar)



(Prof. Nigel Smart)



So i would like to first to dedicate the course to the first set of gurus who have actually sowed the seed of theoretical computer science and abstract thinking in me during my student days. So they are professor Kamala Krithivasan my MS supervisor who taught me automata theory professor C Pandu Rangan who was my PHD supervisor who taught me algorithms and cryptography and professor S. A. Choudum who taught me graph theory.

So these people has played a tremendous role in my academic development. I would also like to acknowledge professor Palash Sarkar and professor Nigel Smart who were my postdoctoral supervisors I learned a lot from them and what I find amazing about them is that even though by training they are theoreticians I am simply amazed by the level of practical knowledge about cryptography about applied concepts that they have and I am also super amazed by their efficiency how efficiently they handle even any kind of complicated task and last but not the least I would like to acknowledge the authors of this wonderful book Introduction to modern cryptography by Jonathan Katz and Yehuda Lindell. So the cryptography the way I know, and I have thought in this course is completely because of this wonderful text even though I have read several texts in cryptography I can confidently say that the ease and the convenience with which even highly complex topic is explained in this book I could never find in any other textbook. So as I said during my first lecture, I strongly recommend anyone who wants to do research or learn cryptography to buy a personal copy of this book and have it in their bookshelf.

(Refer Slide Time: 09:24)

Some Shameless Advertisement

- ❑ Looking for **full-time**, motivated MS (and PhD) research scholars, who want to work in cryptography
- ❖ Motivated candidates should apply in response to the **advertisements** (twice a year), published at IIITB's website
<https://www.iiitb.ac.in>
- ❖ Please do not write to me for research-assistant, internship, project positions, etc.

And finally some shameless advertisement from my sites. So I am always looking for full time motivated MS and PHD research scholars who want to work in cryptography and if you are interested you should apply in response to the advertisement for MS and PHD positions published at IIIT website. This is the website and we have admissions happening twice a year and please do not write to me for research assistant internship or project positions I am only interested in MS and PHD research scholars.

So you should apply against advertisement and if I find your application interesting then indeed you will be called for the written test and interview and so. With this I end this course i really enjoyed teaching this course and I hope to meet you sometime in the near future with another course on cryptography, Thank you, bye, bye, Jai Hind.