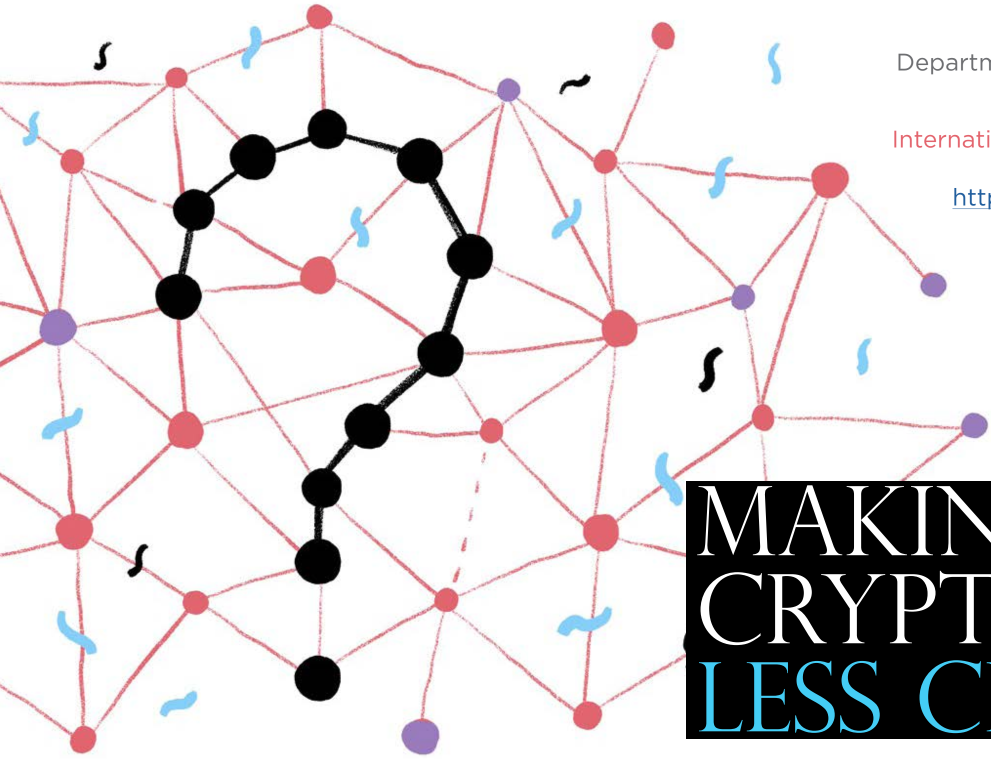


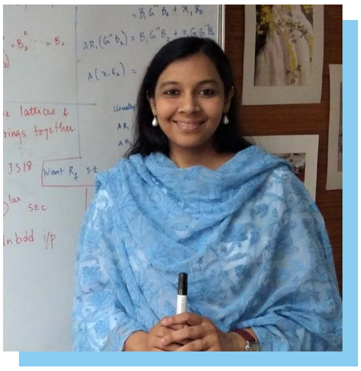
RESEARCH BY:
Dr Shweta Agrawal
Department of Computer Science and Engineering - IIT

PRESENTED IN
International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT 2019)
http://www.cse.iitm.ac.in/~shwetaag/research.html

# MAKING CRYPTOGRAPHY LESS CRYPTIC

Cryptography is a beautiful branch of mathematics which guarantees the art of secret keeping. In today's world of big data, there is a serious conflict between utility and privacy. The prime example of this conflict comes from the field of medicine -- the abundance of genetic data today makes it possible to imagine a future where medicines can be personalized, but developing this capability requires running algorithms on large scale genetic data which is highly sensitive, and may compromise the privacy of individuals. Another such example is the raging privacy debates pertaining to the biometric database in India (Aadhaar).

Resolving the conflict between utility and privacy is one of the primary challenges faced by cryptography. While traditionally designed to enable secure communication between two parties in the presence of an eavesdropper, modern cryptography has taken huge strides in expressiveness and generality, tackling paradoxical questions such as 'if is it possible to run machine learning algorithms on encrypted data' to 'is it possible to prove that I know a secret without telling you what I know?' to 'is it possible to obfuscate computer programs so that they perform the intended functionality of the program but are guaranteed to reveal nothing about the inner workings of the program, even given its code?'



Zooming in on the last question leads to the research 'program obfuscation', In here, one seeks to make a program 'unintelligible' while preserving its functionality and wishes to give strong security guarantees that no information about the underlying program is revealed. In more detail, security of such a construction guarantees that an attacker who learns anything about the inner workings of the program can be used to solve some difficult number theoretic problem. Hence, if the underlying number theoretic problem is chosen to be such that it is extremely difficult to solve, to be assured that the secrets of the program are hard to attain. In recent work to appear at Eurocrypt 2019, Dr Shweta Agrawal provided new approaches to the problem of constructing obfuscation and gave new candidate obfuscators based on novel mathematical hardness assumptions. This advances the state of the art in constructing obfuscation, and bringing it closer to resolution.

Obfuscation has wide-ranging applications in the field of cryptography, which enables new cryptographic applications. The research is still within the domain of exploring the feasibility, which means that any real-world deployment of these constructions is still a distance away. However, bridging the gap from impossible to possible is necessary before taking the step from possible to practice, and this is what the current work attempts to do.

> **"Indistinguishability Obfuscation is a cryptographic tool that allows one to transform a given program to another one that has the same functionality but an adversary cannot figure out the functionality of the transformed program by looking at it. This tool is fundamental one -- it results in just about every other cryptographic algorithm including public-key encryption, fully homomorphic encryption etc. It is therefore very desirable to have this tool. The first construction of this tool was given in 2013 based on certain hardness assumptions. Unfortunately, there were many attacks on these schemes. Besides, in follow up work, one of the sufficient assumptions, the requirement of a certain type of pseudorandom generators, was shown to be false. The present work opens us a new possibility of constructing the tool by weakening the required hardness assumptions to bring is again within the realm of possibility. It is an exciting result, making a leap in our understanding of this new domain, and could well lead to the first construction of iO tool."**
>
> **- Dr. Manindra Agrawal**
> ***(Professor at the Department of Computer Science and Engineering and the Deputy Director at the Indian Institute of Technology, Kanpur)***

Authors: Arundathi Chandrasekharan
Chennai36, International and Alumni Relations Student Council, IIT Madras