# Summer School on Proof Techniques Used in Symmetric Cryptography

July-August(29-3), 2018, Bertinoro (Italy)

Navid Ghaedi Bardeh

I got funding from COINS research school to attend Summer School on proof techniques used in symmetric cryptography in Bertinoro, Italy, in July 2018.
The summer school's aims were at bringing together PhD students, postdoc researchers. It was a great opportunity to meet researchers from the common field of research. Well-known cryptographers were invited:

- Joël Alwen, IST Austria & Wickr
- Mihir Bellare, UC San Diego
- Yevgeniy Dodis, NYU
- Phillip Rogaway, UC Davis
- Pooya Farshim, ENS
- John Steinberger, Tsinghua
- Krzysztof Pietrzak, IST Austria
- Stefano Tessaro, UC Santa Barbara

The summer school topics varied, however, the main topics included:

**Mihir Bellare:** Symmetric encryption revisited. Cryptography in the age of mass surveillance.
**Phil Rogaway:** Crafting definitions: (1) adept secret-sharing; (2) garbled circuits; (3) robust authenticated encryption; (4) indistinguishability up to correctness.
**Stefano** Tessaro**:** Techniques for indistinguishability proofs from H-coefficient to the expectation and chi-squared methods. Applications to multi-user security.
**Pooya Farshim:** Introduction to indifferentiability.
**John Steinberger**: Indifferentiability of block ciphers.
**Yevgeniy Dodis:** Random oracles with auxiliary input. The compression and pre-sampling techniques. Bounds in multi-instance security. Extensions to the generic-group, random-permutation, and ideal-cipher models.
**Krzysztof Pietrzak:** Time/space lower bounds (Hellman, Rainbow tables, etc.). A proof of the $S \times T \geq N$ lower bound for inverting random functions/permutations as an illustration of the compression technique. Proofs of Space (the "beyond-Hellman type") as a modern application of this technique.
**Joël Alwen:** Pebbling games and their applications in crypto and ex-post-facto pebbling reductions.

Full program of the summer school, as well as presentation slides can be downloaded from the webpage of the program[1].

The most interesting lecture for me was “Indifferentiability of block ciphers” given by John Steinberger. This lecture was interesting for me because he explained very well the concept of Indifferentiability of block ciphers. He also showed us how to probe that a Feistel network is indifferentiable from a random permutation. The technics that he used is really similar to what I am doing in my research now. It was about yoyo game. The Yoyo game was introduced by Biham et al. against Skipjack (Feistel block cipher). The idea was simple: suppose that a plaintext pair has a specific property. It is possible to generate other plaintext pairs that has the same property by exchanging a specific word of their ciphertexts and decrypt new ciphertext pair.

Mihir Bellare also gave an interesting lecture about “Symmetric encryption revisited. Cryptography in the age of mass surveillance”. This lecture was interesting for me because he reviewed the definitions of symmetric encryption very well. Also, he gave us the definition of Nonce-Based Symmetric Encryption which I have not heard about this before. He explained well problems we face from theoretical definitions to practical ones. I have learned a lot about his lecture.

The school organizers also organized dinner at some restaurants, so I got chance to explained and discussed my research topic with famous professors. I also got some ideas from them. Also, I found a PhD student that we are going to collaborate together on a research topic.

Overall this school was a very nice event, which really interested me on indifferentiability on block cipher. I got to meet new friends within cryptography, and I also got to discuss some important problems within my research with the top researchers in cryptography, which gave a lot of new ideas and approaches which help me a lot in my work.

I am deeply grateful for COINS supporting me to go to Summer School on proof techniques used in symmetric cryptography

[1] https://spotniq.school