A Scientific Article and an International Conference – and she's still studying for her bachelor's degree

Student Batel Oved presented her research at a major international conference and was nominated for two awards. The research topic: an innovative method for critical cryptographic hash functions

Batel Oved, a BSc student at the Viterbi Faculty of Electrical and Computer Engineering, recently presented her research at the International Conference on Modern Circuits and Systems Technologies (MOCAST) 2022 in Bremen, Germany. The paper, on which she worked as part of her undergraduate project, was expanded into a scientific article. For that paper she was a candidate for two awards – the Best Student Paper Award and the Best Paper Award in Electronics – following the development of an innovative method for critical cryptographic hash functions.

Batel grew up in Kiryat Ekron and began her undergraduate studies three years ago. During her first year, she decided to apply for a prestigious scholarship, and the requirements included a reference from a Technion professor. Batel says, "At that point, I didn't personally know any professor, so I decided to reach out to Prof. Shahar Kvatinsky, who taught the course "Digital Systems and Computer Structure" – the first course that exposed me to the world of hardware. I sent him an email, and though I didn't get a reference for the scholarship (after all, he didn't know me personally), I did get a better offer: to hear about his research group and maybe even join it." The two met, and Batel heard "about the crazy stuff they do in the group. Of course, I wanted to be a part of it." And so, at the start of her second year, Batel joined the ASIC^2 research group, where most of the members are students studying for advanced degrees. "I learned a lot there. It started by understanding the technologies we were researching by reading articles about the field, which was incredibly challenging at first. So, I joined the research project of one of the PhD students in the group, in which we studied the practical aspects based on the theory. I had the privilege of being involved in designing a printed circuit board for a chip that was also designed by the group, and I took part in testing it in the lab."

At the end of her second year, like many of her fellow students, Batel looked for a job. "I started working at Microsoft as a chip design intern, but I didn't want to leave the research group just yet. So, I brought the final undergraduate project forward to the beginning of my third year at the university, supervised by Prof. Kvatinsky." In the project, Batel demonstrated the huge potential inherent in in-memory computation – a new approach that accelerates calculation speed and reduces the amount of energy consumed in the process."

Batel explains that the approach demonstrated is based on memristive digital processing-in-memory. "Memristors are components that store data, but also can perform logic operations by varying their resistance level. In the article, we chose to present the potential of computations of this kind on a fundamental algorithm in secure communication, specifically, the SHA-3 (Secure Hash Algorithm-3) standard. SHA-3 is a set of cryptographic hash functions, and in the article, we presented a method for their effective

implementation, while achieving very high throughput and significantly lower energy consumption compared to other solutions in the field."

Following the success of the project, which started as part of an undergraduate project, Batel worked hard on translating it into a scientific article. She was assisted in the endeavor by Prof. Kvatinsky, Ronny Ronen and Orian Leitersdorf, "who guided me along the way to understand how the world of research works, how to show the correctness and extract relevant and reliable information, how to compare the study to other studies using different technologies, and so much more. And we did succeed in authoring an article that presents impressive results."

The article was submitted and accepted to the IEEE International Conference on Modern Circuits and Systems Technologies (MOCAST) 2022, which took place in Bremen, Germany.

Click here for pictures

Captions:

1. Batel Oved
2. Professor Shahar Kvatinsky

For more information: Doron Shaham, Technion Spokesperson, +972-50-3109088