During the summer of 2016 I had the opportunity to work as an undergraduate research assistant for Professor David Jao in the C&O department. His recent work, which was also the focus of my assistantship, has been in developing new cryptographic techniques which are secure even against attacks from quantum computers. This area of research has surged in popularity in recent years, since it is now widely believed that computers which intimately harness the laws of quantum mechanics can be built, and that when built, most of the cryptography in use today will be vulnerable.

In 2011, Professor Jao and one coauthor proposed a new cryptographic scheme, often abbreviated "SIDH", which has the potential to resist such attacks. SIDH is a kind of cryptographic protocol known as a "key exchange", and allows two parties to establish a secret piece of information over an unsecured channel which can then be used to communicate securely. Crucially, the protocol involves the use of "cryptographic keys", which are pieces of data held by the two parties performing the protocol, and which contain the information necessary to complete the protocol successfully.

Recently, this protocol has emerged as a leading candidate for the development of quantum-resistant cryptosystems. One of its main advantages is in the size of its cryptographic keys, which are far smaller, and therefore easier to transmit, than other leading candidates. One of its main disadvantages is its relative speed — other proposals have implementations that run considerably faster, so although the proposal is practical, it may not be the best candidate when performance is a high priority.

My first task was to address this concern on ARM platforms. ARM is a microprocessor architecture used in the vast majority of phones. For technical reasons, efficient implementations of the SIDH protocol require code that has been specially optimized for the CPU architecture in question — code which runs quickly on Intel CPUs, for example, needs to be modified to run on ARM. The leading implementation of SIDH, which had been released by researchers at Microsoft a month prior and accepted to one of the leading conferences in the field, did not do this work for ARM. In my first two months working for Professor Jao, I was able to accomplish this task, improving the runtime by a factor of ten, and my work has since been added to the Microsoft library.

My second task was to improve the performance of certain "key compression" techniques for the protocol. One of the reasons SIDH is able to have such small cryptographic keys is due to a variety of mathematically sophisticated techniques used to reduce their size. In early 2016, such techniques were proposed, but it was found that implementing them caused the runtime of the key exchange to reach unacceptable levels. Here too I was able to improve the runtime, in this case by around a factor of eight. As a result of this work, Professor Jao and I accepted an offer to collaborate with the authors of the highly-regarded Microsoft library on these techniques. Subsequent improvements to my optimizations lead to a publication at EUROCRYPT, one of the top conferences in the field, which takes place in three weeks time. This work, too, has been added to the Microsoft library.

I am very grateful for having had the opportunity to work with Professor Jao on this exciting area of research. The work has not only been interesting, but it has given me the chance to make a meaningful contribution to the cryptographic community, which should continue to be relevant in years to come.

David Urbanik