Researcher showcases fundamentals for more efficient cryptography implementations

Researchers who are interested in pushing the limits of public-key cryptography should expand their understanding of the basics.

Technology Innovation Institute

ABU DHABI, UNITED ARAB EMIRATES, February 25, 2022 /EINPresswire.com/ -- Researchers who are interested in pushing the limits of public-key cryptography should expand their understanding of the basics. "People often question the utility of pairing-based cryptography and complain it is too slow, so any speedups we can achieve are useful," said Michael Scott, a senior cryptographic researcher at the Technology Innovation Institute in the United Arab Emirates.

> People often question the utility of pairing-based cryptography and complain it is too slow, so any speedups we can achieve are useful."
>
> *Michael Scott, Senior cryptographic researcher at TII*

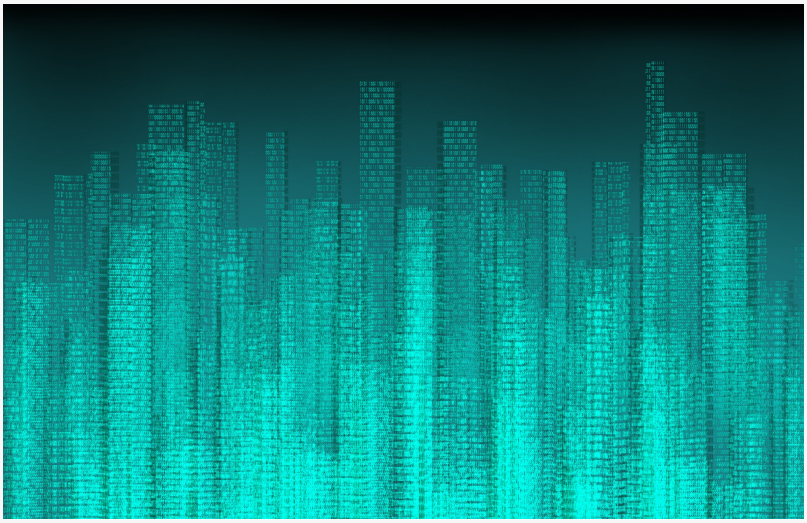
He recently elaborated on some of the best practices he learned over several decades in implementing cryptographic algorithms. It is particularly important for researchers pushing the edge to brush up on finite field arithmetic which underpins most public-key cryptography implementations currently deployed such as RSA.

Cryptographic developers need to choose the fastest algorithms which can be organized into the fastest implementation, while at the same time ensuring safety. The starting point lies in finding the best algorithms for doing the calculations. The next step is to implement these algorithms into and working applications. However, sometimes the best algorithms from a mathematical perspective turn out to be less useful when it comes to implement them into code.

The new kid on the block

Older cryptographic techniques often use base field arithmetic. Pairing-based cryptography techniques often require considering the extension-field arithmetic which have a variety of important differences compared to basic field arithmetic. "Pair-based cryptography is the new kid on the block," said Scott.

Researchers also must consider constant time as part of their implementations. Otherwise, an implementation may leak information that could support side-channel attacks.



Researcher showcases fundamentals for more efficient cryptography implementations

“This is really about exploring the classic issues in base fields and how these issues might be extended to considerations with extension fields,” Scott said, referring to the tricks he elaborates on in the recent paper.

The math has been out there for a while but not widely studied. Scott was able to tease apart some best practices in working with extension fields, over several decades in implementing these kinds of algorithms.

Building a new foundation

This is particularly important for non-cryptographers who might be looking at a mathematical description. They need to be able to take this description and convert it into a computer program. This is not easy without domain knowledge. A better understanding of the fundamentals can help them identify what kind of approach will be fastest in practice.

For example, there are many cases where the asymptotically optimal algorithm from a mathematics perspective may not be implementable as a computer program. A better understanding of the foundations in implementing algorithms for pair-based cryptography can guide awareness of the size of the numbers involved. This can lead to implementations that run more efficiently in each cycle and with the minimum number of cycles.

Ensuring constant time

Researchers also need to consider the constraints around ensuring constant time. If a program takes longer to process some codes than others, the variations in processing can leak information. Implementing the algorithm to run in constant time ensures that the execution

profile is completely independent of the cryptographic data.

"Sometimes you need to compromise on speed to achieve constant time," said Scott.

This concern is relatively new in cryptography. It was not widely understood until about a decade ago. Now cryptographers are hyperaware of this. There are other ways of blocking leakage, but constant time is the best, said Scott. For example, it's possible to mask the calculations by introducing random data to mask variability, but that can create additional problems.

In the paper, Scott also elaborates on how these tricks can be applied to improving hash-to-curve algorithms. This is an interesting example of the importance of constant time. In some applications, it is desirable to take someone's email, convert it into a number, and represent it as a point on an elliptic curve. The traditional method is to hunt and peck incrementally until this number fits on the curve, however, this leaks information.

Scott demonstrated how to directly implement a formula that can take the email address and drop it onto the curve in one step. This kind of approach is more efficient and can execute the operation as efficiently as possible and also execute in constant time.

Keeping it simple, fast, and clean

Another example of how researchers can put these principles into practice is to explore ways to combine common cryptographic calculations for quadratic residuosity, inverses, and square roots. It turns out that all three of these calculations are closely related.

With the right approach it is possible to do a basic calculation and from that calculate any of these three. This is roughly 3 times faster than calculating each of these separately. "You get three for the price of one," Scott said.

In general, the field of pair-based cryptography is mature enough that many implementations have been standardized. But even these implementations sometimes have room for improvements when researchers are willing to go back to experiment with applying a deeper understanding of extension fields to new implementations. Scott found that by applying the tricks he discovered to a standard implementation of a hash-to-curve algorithm, he was able to speed the standard implementation by 20%.

"This could be useful for any researcher that finds their extension field related calculations are taking more time," Scott said. "It's also important that the algorithms that appear in the standards are optimal, simple, fast, and clean."

About Technology Innovation Institute (TII)
Technology Innovation Institute (TII) is the dedicated 'applied research' pillar of Advanced Technology Research Council (ATRC). TII is a pioneering global research and development centre

that focuses on applied research and new-age technology capabilities. The Institute has seven initial dedicated research centres in quantum, autonomous robotics, cryptography, advanced materials, digital security, directed energy and secure systems. By working with exceptional talent, universities, research institutions and industry partners from all over the world, the Institute connects an intellectual community and contributes to building an R&D ecosystem reinforcing Abu Dhabi and the UAE's status as a global hub for innovation.
For more information, visit www.tii.ae

Tania Ameer
APCO Worldwide
+971 52 672 5138
email us here
