Faster GCD calculation shines a light on cryptographic alternatives

TII Researchers at Cryptography Research Centre have implemented an approach for running GCD efficiently in a constant amount of time.

Technology Innovation Institute

ABU DHABI, DUBAI, UNITED ARAB EMIRATES, February 10, 2022 /EINPresswire.com/ -- Students often learn about calculating the greatest common divisor (GCD) in elementary school. The same calculation can also help craft various cryptographic algorithms. Consequently, security researchers have been exploring different ways of running this calculation more efficiently on computers.

> Cryptographic applications commonly need to execute same calculation repeatedly, so a minor difference in performance of a calculation can make a big difference on how quickly the calculation works."
>
> *Victor Mateu, principal cryptography researcher, TII*

Researchers at the Technology Innovation Institute's (TII) Cryptography Research Centre have implemented one such approach for running GCD efficiently in a constant amount of time. Now they have followed up that research to identify the fastest way to compute a cryptographic computation, called a modular inverse for integers, more quickly.

A vital aspect of the original algorithm is that it can run the calculation without varying the amount of time for calculating different numbers. This reduces the risk that hackers might reverse engineer a secret key by analyzing the differences in time, which is called a timing attack.

"Cryptographic applications commonly need to execute the same calculation repeatedly, so a minor difference in the performance of a calculation can make a big difference on how quickly the calculation works. In the latest work, the researchers found they could increase the speed of this calculation by about ten times than what was previously considered state-of-the-art," said

Victor Mateu, principal cryptography researcher at TII.

They have also optimized the new algorithm to run more efficiently on different kinds of FPGA chips, which tend to be faster than CPUs for these kinds of calculations. “The best algorithm we know has been implemented with the faster technology we now have,” Mateu said. “As far as we know, this will remain state-of-the-art for a while.”

Faster GCD calculation shines a light on cryptographic alternatives

Use in post-quantum cryptography

Concerns about how quantum computers may crack encryption code have driven a wave of research and standardization efforts for post-quantum cryptography. These algorithms are designed to be more resistant to attacks that use quantum computers. Some of these newly proposed algorithms could benefit from modular inverse calculations.

Mateu says that researchers have tended to shy away from using this calculation because it tends to be less efficient than other approaches involving multiplication. The latest research has closed this gap from about 1/100th to only 1/10th as fast as the multiplication approaches. Even though it is slower, cryptographic researchers want to keep their options open with regards to new cryptographic algorithms. Knowing different approaches’ technical characteristics can help prioritize alternatives if problems are discovered in the leading approach.

Some cryptographic algorithms, such as ElGamal, make wide use of modular inverse calculations and thus will realize significant performance improvement with a calculation. ElGamal is already being used in electronic voting systems and confidential computing applications.

Mateu expects this to remain at the top of the field for modulo inverse for some time. This also marks a milestone in collaboration with the University of Yale to set up more cooperative research to improve classic and post-quantum cryptography.

“This is the beginning of a larger collaboration that will include post-quantum research,” Mateu said.

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

About Cryptography Research Centre (CRC)
Cryptography Research Centre – one of the seven research centres at Technology Innovation Institute in Abu Dhabi (TII) – designs the building blocks of advanced cryptographic algorithms that enable data confidentiality, integrity, privacy, and non-repudiation. The Centre works in partnership with leading research advisors and institutions to research new cryptographic primitives covering design, analysis, implementation and implementation hardness, and the development of security protocols.
For more information, visit https://cryptography.tii.ae

Tania Ameer
APCO Worldwide
+971 52 672 5138
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
Other
