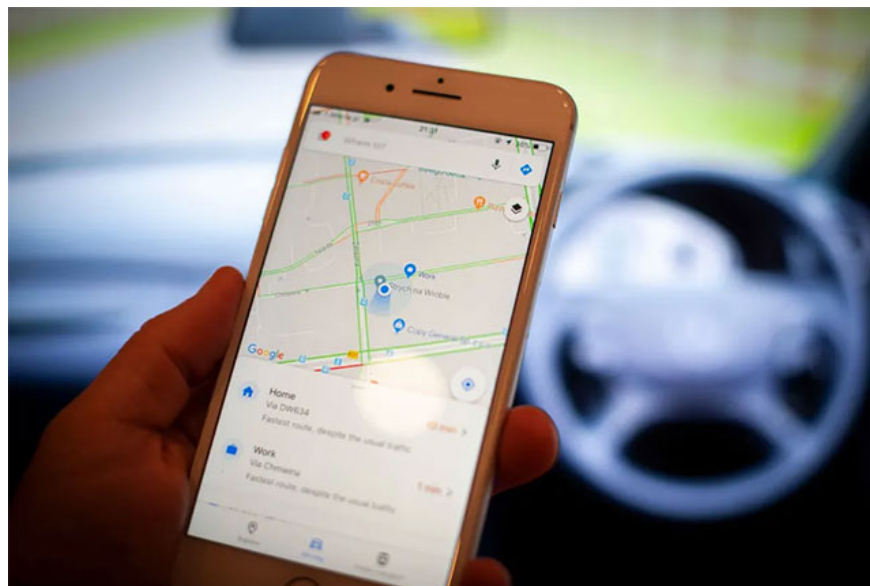


Breakthrough mathematical technology helps determine location without revealing personal information

Researchers at the Technical University of Munich (TUM) have developed a new method that allows location to be proven without revealing specific information, balancing security and accuracy.

Researchers at the Technical University of Munich (TUM) have developed a new method for proving location without revealing specific information, striking a balance between privacy and accuracy. The method, called Zero-Knowledge Location Privacy (ZKLP), uses zero-knowledge proofs and floating-point numbers to let users confirm they are in a specific area without having to provide precise coordinates.

Location tracking via mobile apps has become widespread, often without users' knowledge. This data can paint a picture of a person's habits, work and lifestyle, sometimes leading to serious privacy risks. A 2019 New York Times report showed how commercial location data can easily identify individuals, including members of former US President Donald Trump's team, revealing visits to sensitive locations like Mar-a-Lago and the Pentagon. With growing concerns about how this data could be misused, the TUM team sought to find a way to verify location information while keeping personal data private.



The ZKLP method allows users to prove they are in a general area such as a city or park without revealing their exact location. The technology is based on zero-knowledge proofs, which are used to verify a statement without revealing the data behind it. To make the method work in practice, the researchers presented the first zero-knowledge proof circuit that fully complies with the IEEE 754 floating-point arithmetic standard, ensuring correct calculations and avoiding errors common in legacy systems that rely on integer math.

This procedure is very efficient, requiring only 64 constraints for each 2^{15} single-precision float multiplication operation, significantly reducing the computational complexity compared to previous methods. Their optimized version uses 15.9 times fewer constraints when using single-precision float values and 12.2 times fewer when using double-precision, making the system much more reliable and scalable.

One major application is privacy-preserving peer-to-peer proximity verification. In this setup, two people can check whether they are close to each other without sharing their exact location. The system works very quickly. For example, person A can generate a proof of location data in just 0.26 seconds and can verify proximity to about 470 people per second. ' *Our method shows that location verification is feasible and efficient while still preserving privacy,* ' said Professor Sebastian Steinhorst, Professor of Embedded Systems and the Internet of Things.

Beyond location verification, the technology developed in this research could have broader applications in cryptography. Floating-point circuits designed for zero-knowledge proofs could be useful in secure machine learning, digital healthcare, and mobility systems, enabling accurate verification while still protecting user data. By combining accuracy and privacy, this research opens up a promising way to protect location data in an age of increasingly pervasive tracking.

You finished reading the article "**Breakthrough mathematical technology helps determine location without revealing personal information**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.