idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Press release

Technische Universität München
Julia Rinner

05/15/2025
http://idw-online.de/en/news852257

Research results, Scientific Publications
Information technology
transregional, national

Hexagons for data protection: Proof of location without disclosing personal data

Location data is considered particularly sensitive – its misuse can have serious consequences. Researchers at the Technical University of Munich (TUM) have developed a method that allows individuals to cryptographically prove their location – without revealing it. The foundation of this method is the so-called zero-knowledge proof with standardized floating-point numbers.

Many smartphone apps continuously track location – often without users being aware. Based on movement profiles, providers can infer workplace, habits, and personal preferences. The potential consequences of collecting such sensitive information were highlighted by a New York Times investigation from 2019. Based on commercial location data, a device belonging to a member of President Trump's entourage could be assigned within a few minutes – including their visits to sensitive locations such as Mar-a-Lago and the Pentagon.

Location as proof – without revealing coordinates

To offer a method that protects privacy while still providing verifiable location data, researchers are turning to zero-knowledge proofs. These are mathematical proofs that can verify the truth of a statement without revealing the underlying data. The key feature for location privacy: this method allows for adjustable precision tailored to the specific application.

“The challenge is to combine privacy and precision in a way that is practically usable,” explains Jens Ernstberger, lead author of the study. The research team at the Professorship of Embedded Systems and Internet of Things achieved this by combining zero-knowledge proofs with a hexagonal spatial index. To make one’s location verifiable but not visible, the method uses a hierarchical hexagonal grid system. This grid divides the Earth’s surface into cells that can be represented at various resolutions – from broad regional levels down to individual street segments. For example, users can choose to disclose that they are in a certain city or, if more accuracy is needed, in a specific park within that city. In both cases, their exact location remains hidden.

Floating-point numbers improve position accuracy

The true innovation lies in the mathematical processing of the location data in the zero-knowledge proofs: Unlike previous systems, which are often based on error-prone integer arithmetic, the new method uses standardized floating-point numbers, which are also the representation found in modern computers. This step is crucial for ensuring computational accuracy and avoiding unintended deviations, especially during complex operations like square roots or trigonometric functions. At the same time, the new approach eliminates errors that could previously lead to incorrect results or security vulnerabilities. Thanks to smart optimizations, the proof can be computed in less than a second.

Practical use cases in everyday life

An example of an application is Peer-to-Peer Proximity Testing. This allows two people to determine whether they are in close physical proximity – without either revealing their exact position. In a prototype, a user can prove in just 0.26 seconds that they are near a specific region. At the same time, the desired level of precision can be flexibly adjusted: Instead of proving an exact location, one could demonstrate being in a particular neighborhood or park.

“Our method shows that zero-knowledge location proofs are possible and efficient while maintaining privacy,” says Prof. Sebastian Steinhorst, Professor of Embedded Systems and Internet of Things at TUM.

Beyond the direct application, the research also contributes to the broader field of cryptography: : The developed floating-point zero-knowledge circuits are reusable regardless of the specific use case and could be applied in other areas in the future – for example, in verifying physical measurement data or in secure machine learning systems. This opens up new possibilities for trusted systems, such as in digital healthcare, mobility applications, or identity protection.

contact for scientific information:

Prof. Dr. Sebastian Steinhorst
Technical University of Munich
Professorship of Embedded Systems and Internet of Things
sebastian.steinhorst@tum.de
www.tum.de

Original publication:

Ernstberger, J., Zhang, C., Ciprian, L., Javanovic, P., Steinhorst, S. Zero-Knowledge Location Privacy via Accurate Floating-Point SNARKs. IEEE Symposium on Security and Privacy (2025). DOI: 10.1109/SP61157.2025.00057

URL for press release:
https://www.tum.de/en/news-and-events/all-news/press-releases/details/hexagons-for-data-protection