Plaintext ciphertext

June 25 2020, by David Bradley

Credit: CC0 Public Domain

Writing in the *International Journal of Ad Hoc and Ubiquitous Computing*, Yu-Chi Chen of the Department Computer Science and Engineering, at Yuan Ze University, in Tauyuan, Taiwan , has revisited the concept of plaintext checkable encryption with check delegation that could be utilized in the context of security and privacy in the realm of big data and cloud computing.

Achieving a specific computing over ciphertext, plaintext checkable encryption (PCE) is a relatively new concept explains Chen. It supports the specific functionality between ciphertext and plaintext. "Given a target plaintext, a ciphertext and a public key, anyone can perform a check algorithm (called Check) to test whether the ciphertext encrypts the target plaintext with the public key," he explains.

It allows the user to send search instructions to a database, for instance, that are encrypted so that a third party, such as the service provider themselves, cannot see the search terms, but the server has to know that the search is encrypted in a valid way so that it can send back encrypted results; this is where the check function plays its role.

The new work builds on these concepts and offers a new way to approach them with secure public keys and generic constructions.

More information: Yu Chi Chen. Plaintext checkable encryption with check delegation revisited, *International Journal of Ad Hoc and Ubiquitous Computing* (2020). DOI: 10.1504/IJAHUC.2020.107822

Provided by Inderscience