Secure Cloud Computing for Medical Data

Daniel J.Bernstein, Carl Ellison, Tanja Lange, Kristin Lauter, Victor Miller,
Michael Naehrig, Eran Tromer

Challenge

We answer a recent challenge [Benaloh Lauter Horvitz Chase 2009] concerning patient privacy in electronic medical records.

Response

Our approach offers strong privacy and confidentiality, and enables autonomous delegation of priviliges in a distributed setting. We instantiate our constructions using recent the results of [Gentry 09].

The Construction

Does your doctor know the full importance of encryption?
If your data were revealed you'd suffer a conniption.
But now you can prevent him from disclosing your prescription with fully homomorphic lattice-based secure encryption!

Fully homomorphic lattice-based secure encryption

pulls together several keys in layers for ignition.

Then wraps itself recursively with clever repetition

Other steps are evident - who needs good exposition?

Cloud computing lets you spread your data with precision

Merging different servers: German, Welsh, perhaps Egyptian.

But when you finally run the scheme you end up with frustration

Doing just 2 bits per round limits the adoration.

Fully homomorphic lattice-based secure encryption

pulls together several keys in layers for ignition.

Then wraps itself recursively with clever repetition

Other steps are evident - who needs good exposition?