Homomorphic Encryption

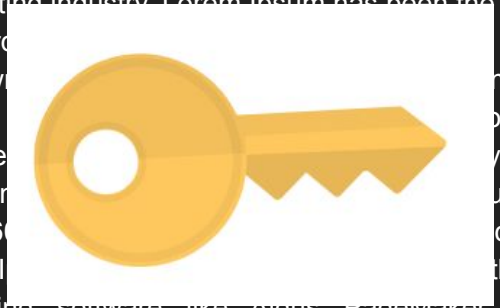
husseinnasser.com

Homomorphic Encryption

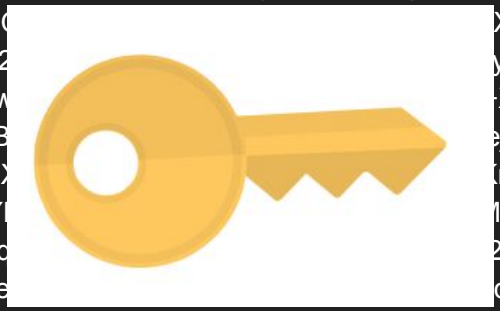
- What is Encryption?
- Why we can’t always Encrypt?
- Homomorphic Encryption
- Demo (IBM FHE toolkit)

Symmetric Encryption

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard when an unknown mbled it to make a t only five centuries ypesetting, remaining ularised in the 196 containing Lorem I th desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum.



Symmetric Encryption



A38b8q1TmcKDXmDOzwoyEbS2JNailCX89Dgx25yspz7l
Kp/REHIFHFx6MA72SjZ9n+LiEK0kSnHd9jj9aDFyisVF5
Q/vU4XcVamhZI1wqPY9/sZIuFF6a51N4QRRZ9jL54YUr
uLN4GhmkabD12Gv2Jr1RwjXJ9ZB/J1ogdr5Jk8+InPIlDJf
Wvrxs3 XyRQKxa
zu7vuh yXwA4VF
ApR+4w X0jZbSP
LeZ+DB ejITRYqFV
GLDuH nccEUoL
4+boxY NcAdBV
90MWIc 2/Nvq//ghf
xa7/Ene q8k/oD0r
WL6kQ3oGcrEzt2GLxKj1TeXfgMg56fVLVGlY/oCW+ky2/
92t4Dv6CpIIgbUGenCK+DlzH/b+Ekhjb2QoC5S+p9BG1V
I1dWLRionc0e9Bui60iz8na3gJYcunyb95qqBG8P7Jb5dr
Dc5w1d7+mLnE0yfUGvX70bg2Et+sC4vJ9Wk65B/UdLy2
nhyhqdqhHWy4qjt4VggpsbLliQStQJ7UCQssOU0iZBtdk1
wFOVyatCUQw

Symmetric Encryption

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum.

Why we can’t always encrypt

- Database Queries can only be performed on plain text
- Analysis, Indexing, tuning
- Applications must read data to process it
- TLS Termination Layer 7 Reverse Proxies and Load Balancing

Meet Homomorphic Encryption!

- Ability to perform arithmetic operations on encrypted data
- No need to decrypt!
- You can query a database that is encrypted!
- Layer 7 Reverse Proxies don’t have to terminate TLS, can route traffic based on rules without decrypting traffic
- Databases can index and optimize without decrypting data

Fully Homomorphic Encryption toolkit by IBM

- Download & run the source code
- Search an encrypted database (countries/capital)