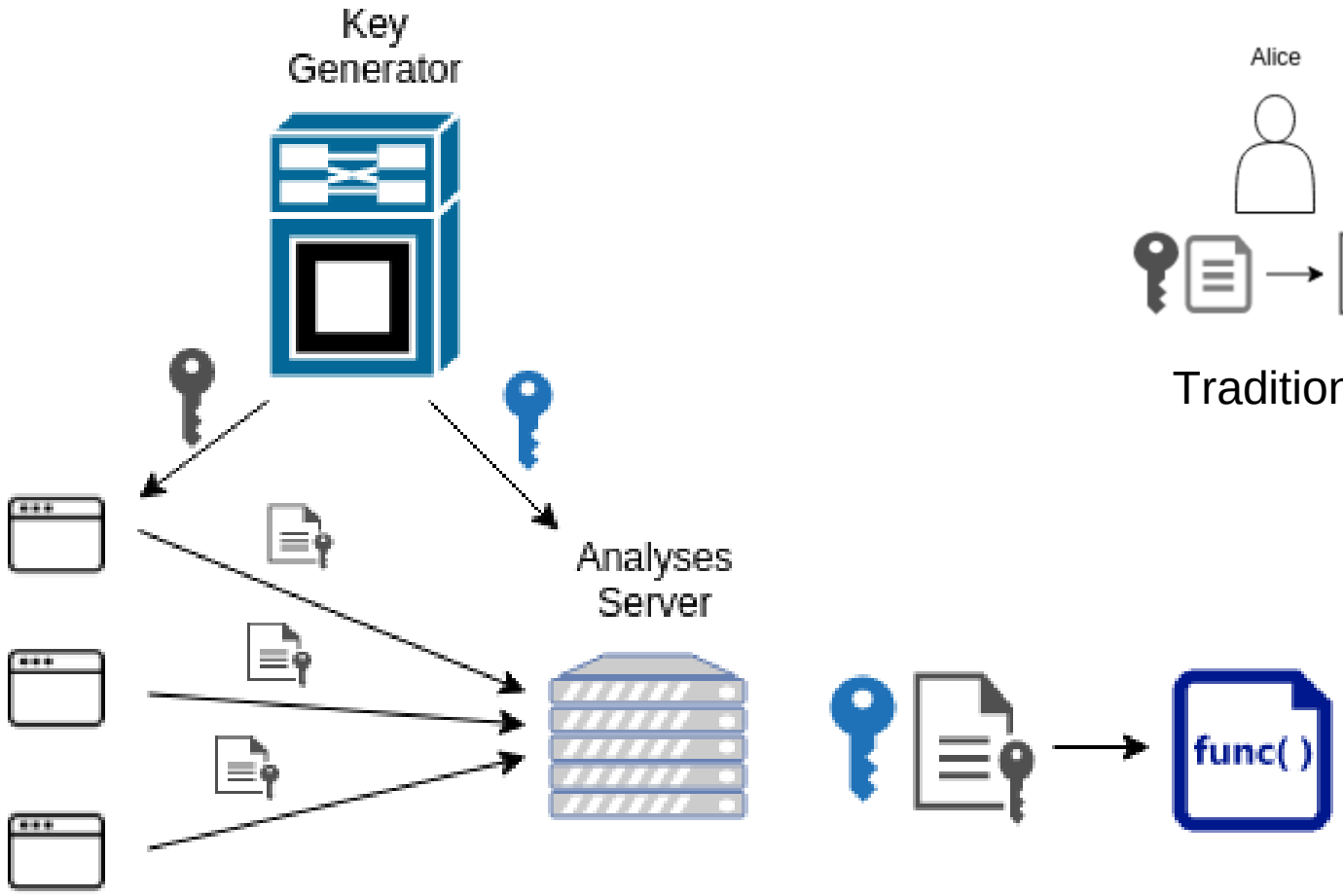
Functional Encryption - fentec.eu

Miha Stopar

Functional Encryption (FE)



Traditional public-key encryption

Prediction of cardiovascular disease (CDV)

CDV risk can be calculated using Framingham* algorithms by using parameters: age, sex, total and high-density lipoprotein cholesterol, systolic blood pressure, treatment for hypertension, smoking, and diabetes status:

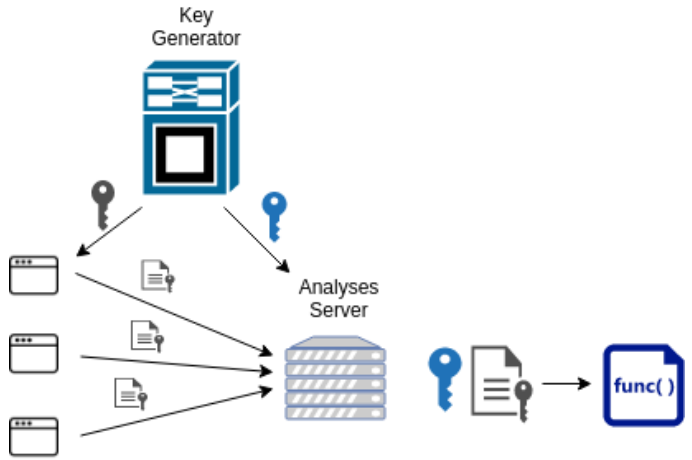
```
risk = framingham_algo(age, sex, cholesterol, pressure,
treatment, smoking, diabetes)
```

*Framingham heart study: https://www.framinghamheartstudy.org/

Prediction of cardiovascular disease (CDV)

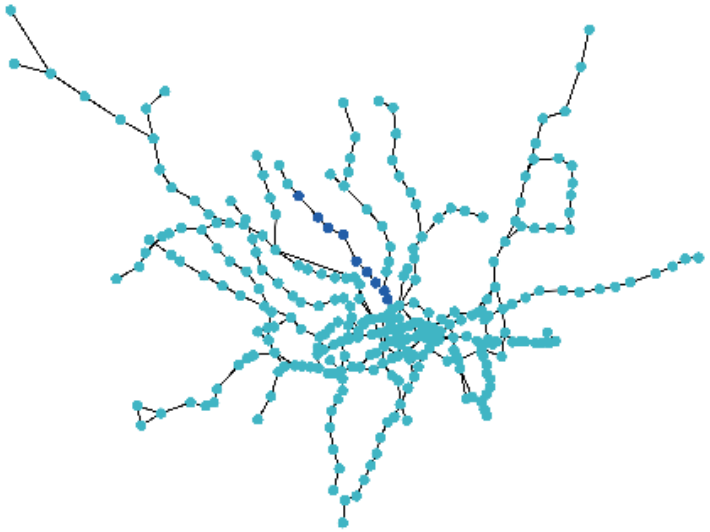
But how to compute the risk of general cardiovascular disease without exposing your data?

- c = encrypt(age, sex, cholesterol, pressure, treatment, smoking, diabetes)
- send ciphertext c to the Analyses Server
- Analyses Server computes risk solely using ciphertext c and returns it to the user

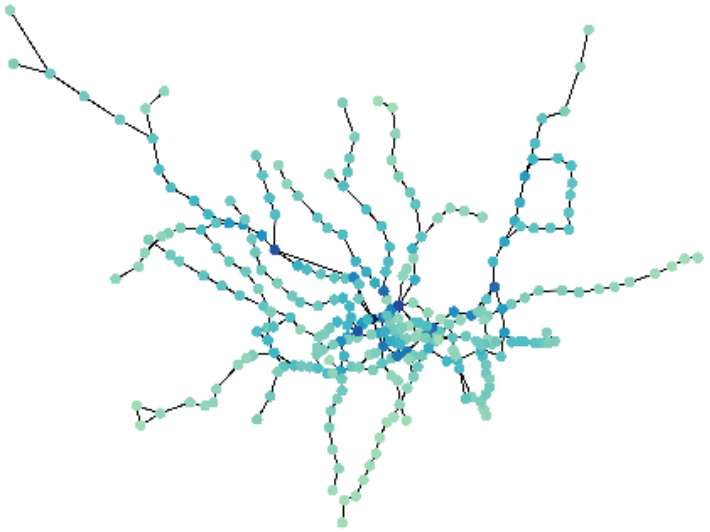


Anonymous heatmap of the London underground

Given the encrypted information about users, Analyses Server can measure the traffic density at each station.



(a) Path of one user



(b) Heatmap

Open-source FENTEC libraries

- Go: https://github.com/fentec-project/gofe
- C: https://github.com/fentec-project/CiFEr
- Privacy-friendly analyses: https://github.com/fentec-project/privacy-friendly-analyses
- Anonymous heatmap: https://github.com/fentec-project/FE-anonymous-heatmap
- Neural-networks on encrypted data: https://github.com/fentec-project/neural-network-on-encrypted-data

Get IT done.