Homomorphic encryption

Rob Slade

rslade@vcn.bc.ca
rslade@gmail.com

https://is.gd/RotlWB

Ebo Fynqr znl or na vasbezngvba frphevgl naq znantrzrag pbafhygnag sebz Abegu Inapbhire, Oevgvfu Pbyhzovn, Pnanqn, be ur znl or na negvsvpvny vagryyvtrapr cebtenz tbar ubeevoyl jebat, naq ubbxrq hc gb inevbhf rznvy nqqerffrf. Ur vf gur ynfg fheivivat aba-nyvtarq znyjner erfrnepure va pncgvivgl. Zber vasbezngvba guna nalbar jbhyq jnag gb xabj nobhg uvz vf ninvynoyr ng uggc://ra.jvxvcrqvn.bet/jvxv/Eboreg_Fynqr

https://cryptii.com/pipes/rot13

Homomorphic encryption

- Encrypt data
- Still be able to use it for something without decrypting it

Canadian Centre for Cyber Security

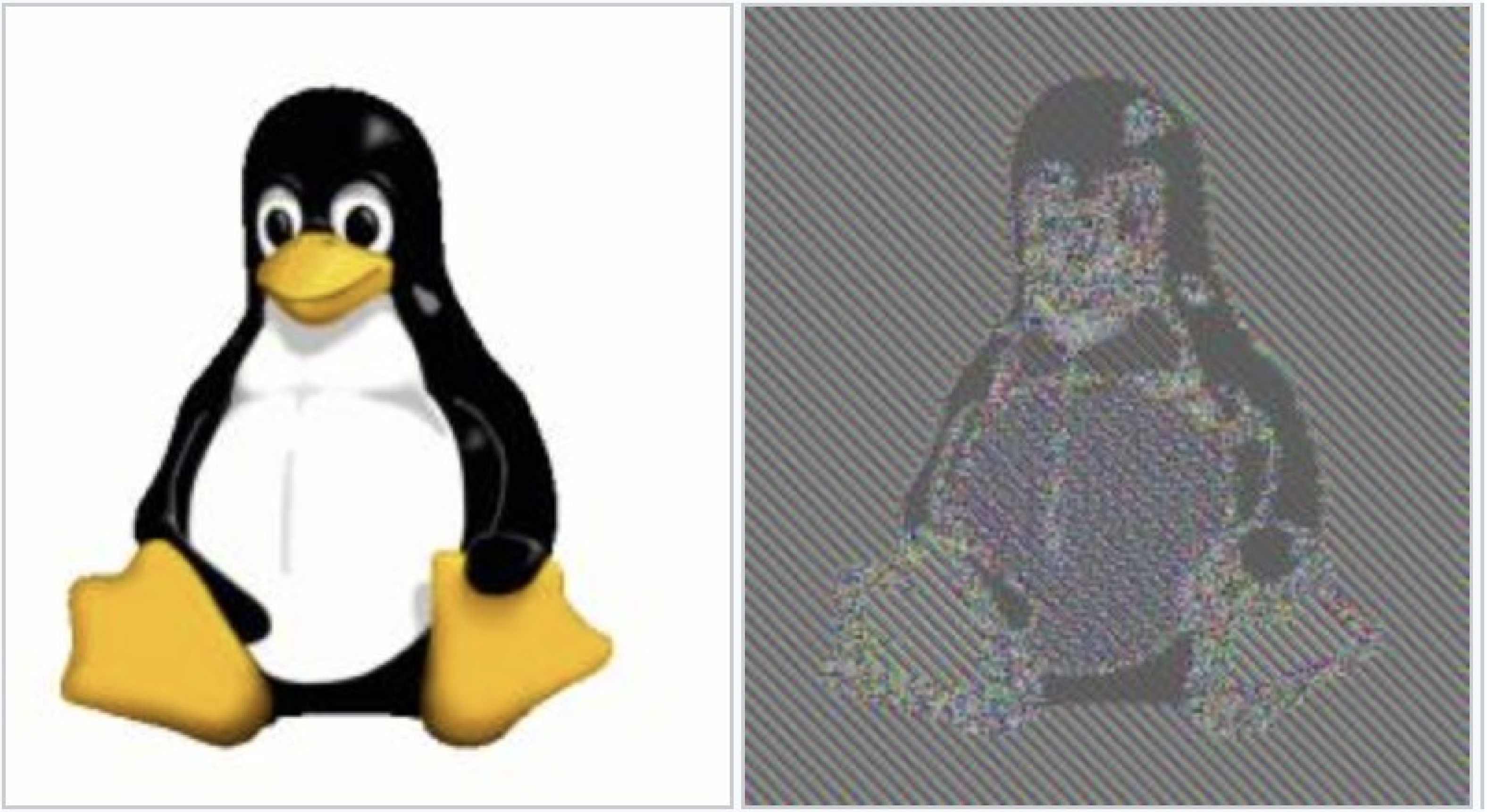
- Canada's cyber intelligence agency working on 'Holy Grail' of encryption
    - https://www.cbc.ca/news/politics/cse-homomorphic-encryption-1.5468400
  - “Jones said the CSE has teamed up with industry players and academics to work out how homomorphic encryption could function in a Canadian setting.”

Not new!

Password hashing

Bad examples

- Exact search
  - Electronic code book mode of block cipher



Original image

Encrypted using ECB mode

Bad examples (cont’d)

- Exact search
  - Electronic code book mode of block cipher
  - Block size matches record size
- Sort
  - Caesar cipher
  - (or mod functions)

Bad examples (cont’d)

- CoVID-19 contact tracing (DP-3T, etc.)
  - Random data “beacon”
  - “beacon” contains no PII

Better example

- Rivest Three-Ballot Voting
- https://en.wikipedia.org/wiki/ThreeBallot
  - Microsoft ElectionGuard?
- Anonymous
- Non-repudiation of voting
- Verifiable to voter
- Ballots counted without being decrypted
- Can be implemented on paper or digitally

More recent example

- Addition and multiplication
- $3x(4+5) = (3x4)+(3x5)$
- So any $f(a+b) = (fa)+(fb)$ might be basis for solution

More recent examples

- IBM (BGV) addition and multiplication
  - https://github.com/shaih/HElib
- Microsoft (SEAL) addition and multiplication
  - https://github.com/Microsoft/SEAL
- Google - comparison and limited addition
  - https://github.com/Google/private-join-and-compute

- https://homomorphicencryption.org/introduction/

This isn't the mask you wore to school this morning.

No, this one is way cooler. I traded mine to Taylor who traded with Hunter.

ifunny.co

What it isn’t

- A “thing”
  - Various functions and implementations
  - (shades of “blockchain”?)
- Universal
  - Choose your function

Digression to crypto

- Symmetric vs asymmetric
- Strength vs key management
- Hybrid
  - Asymmetric for key management only
- Can’t do that with homomorphic encryption
  - Working directly with encrypted data
- Going to require lots of compute cycles ...

Weaknesses

- Limited algorithms
- Restricted functions
- If combining functions, algorithms even more limited
  - Recall bad examples
    - Caesar cipher weak address space
    - Block mode weakest mode for block ciphers

Sample Question

17. Which of the following is NOT an effective deterrent against a database inference attack?

- a. Partitioning
- b. Small query sets
- c. Noise and perturbation
- d. Cell suppression

Weaknesses

- Accuracy
  - Fully Homomorphic Encryption, Gentry?

Microsoft is using homomorphic encryption!

- https://www.microsoft.com/en-us/research/blog/password-monitor-safeguarding-passwords-in-microsoft-edge/
- Well, no it isn’t
  - That’s just hashing again
- Besides, Google Chrome has been doing that for years

Homomorphic encryption

Rob Slade

rslade@vcn.bc.ca
rslade@gmail.com

https://is.gd/RotlWB