SOFTWARE

LINK COLLECTION HOMOMORPHIC ENCRYPTION ALGORITHM

19.04.2016

... is a form of encryption that allows computations to be carried out on ciphertext, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext...

First publication: acm.org
Introduction: technologyreview.com
Details: en.wikipedia.org
Use in genomics: nature.com
R package: www.louisaslett.com

```
install.packages(c("Rcpp", "RcppParallel", "gmp"))
install.packages("http://www.louisaslett.com/HomomorphicEncryption/dl/
HomomorphicEncryption_0.2.tgz", repos=NULL)
library("HomomorphicEncryption")
p <- pars("FandV")
k <- keygen(p)
c1 <- enc(k$pk, c(42,34))
c2 <- enc(k$pk, c(7,5))
cres1 <- c1 + c2
cres2 <- c1 * c2
cres3 <- c1 %*% c2
dec(k$sk, cres1)
dec(k$sk, cres2)
dec(k$sk, cres3)
```