Genomic sequencing is hailed as the future of healthcare. Genomic sequences contain vast amounts of information that can improve our understanding of medical conditions, as well as revolutionize treatments and prevention of illnesses. However, genomes also carry highly sensitive information about individuals, including traits that uniquely identify a person. This raises serious concerns about the security and privacy protection provided by infrastructures used to store, share, and process genomic information[1].

Genomic sequences not only are extremely privacy sensitive but they are, generally, very large files (from 2 to 20Gb). Hence, it is difficult to share them in such a way that they are only available for sender and receiver, and not to third parties like service providers (email providers, cloud storage providers, etc).

In order to solve this pain point and reduce barriers that may limit advances in genomic research and diagnosis we present a tool that allows for privacy-preserving sharing and visualization of genomic sequences, keeping them encrypted while they traverse outsourced environments. This tool is an outcome of the SCAPE project dedicated to the development of privacy-preserving solutions based on processing in the encrypted domain. The SCAPE project is co-funded by the Fundación Barrié[2], and is carried out by Gradiant[3] in collaboration with the Signal Processing in Communications Group at the University of Vigo[4].

The tool comprises three main elements:

- A web service that allows users to upload and manage their public keys, encrypted genomic files, and decide with whom to share each of these files. Efficient upload and controlled sharing is implemented with access control mechanisms and adequately chosen proxy re-encryption techniques[5], which allow the proxy to alter a ciphertext which has been encrypted for one party, so that it may be decrypted by another without clear-text access by the proxy.
- A local service that allows users to create their own key pairs, encrypt and decrypt files.
- A modified version of the Integrative Genome Viewer[6] (IGV) that uses the functionalities offered by the local service to allow users to easily download and transparently view the encrypted genomic sequences stored in the web service.

The tool works as follows:

1) The owner of a genomic sequence encrypts the file and uploads it to the web service
2) When a geneticist wants to have access to the file, she uploads her public key to the server and asks the owner to provide permission
3) The owner creates a re-encryption key for the file and genetist
4) The geneticist can then visualize the file (whole or part) through the modified IGV.

[1] Erman Ayday, Emiliano De Cristofaro, Jean-Pierre Hubaux, Gene Tsudik. Whole Genome Sequencing: Revolutionary Medicine or Privacy Nightmare. IEEE Computer Magazine, Vol. 48, No. 2, February 2015 (accepted in August 2013).
[2] http://www.fundacionbarrie.org/en
[3] http://www.gradiant.org/
[4] http://gpsc.uvigo.es/
[5] https://en.wikipedia.org/wiki/Proxy_re-encryption
[6] https://www.broadinstitute.org/igv/