Secure Signal Processing for Genomic Privacy Protection

Mina Namazi

Advisors: Juan Ramón Troncoso-Pastoriza* and Fernando Pérez-González

*juan.troncoso-pastoriza@epfl.ch, {fperez,mnamazi}@gts.uvigo.es

Universidad de Vigo
Signal Theory and Communications Department
University of Vigo
Spain

Workshop on Monitoring PhD Student Progress. June 14-15, 2018

1. Motivation of the Work

Growth of privacy-aware signal processing applications due to unprecedented advances and needs of outsourced processing benefits studies of genomic data in advancing medicine research, however, information leakage may put patients' privacy in peril.

Sensitive nature of genome entails severs privacy risks when the sequences are outsourced to an untrustworthy environment, like a Cloud service and makes them vulnerable to attacks and accesses violating patient's privacy.

Pairing privacy protection of patients with the execution of genomic analysis on their data and the management of access policies over them is a challenging problem. Therefore, encryption techniques under the paradigm of **Secure Signal Processing** (SSP) is a crucial aspect for protecting individuals' privacy while processing genomic information in outsourced environments.

2. Thesis Objectives

The main objective during the development of this PhD thesis is to **advance the state of the art in secure signal processing cryptographic methods for secure outsourcing of privacy aware applications in the e-Health area**.
Specifically, the three main objectives are the following:

A. Analyzing existing schemes and techniques for secure signal processing e-Health applications from a privacy and security point of view.

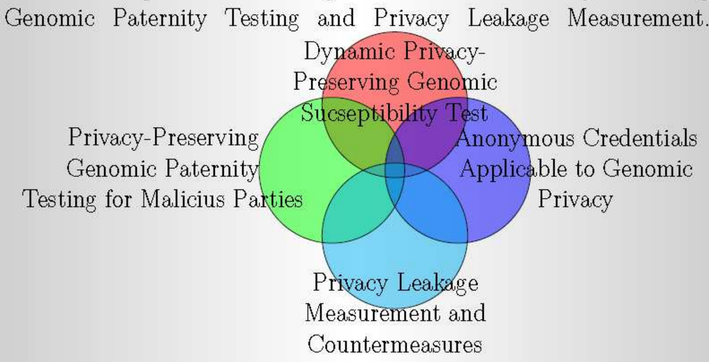
B. Developing novel secure signal processing methods for privacy-preserving e-health applications enhancing efficiency and privacy.

C. Devising new information-theoretic metrics to quantify the information leakage on genomic data when it is partially protected or when the results of several subsequent processes are disclosed.

3. Research Plan

The research plan for the next year is focused on Privacy-Preserving Genomic Paternity Testing and Privacy Leakage Measurement.

The research plan for the next year is focused on Privacy-Preserving Genomic Paternity Testing and Privacy Leakage Measurement.



And the **Methodology** to achieving this goals is:

- Leverage homomorphic authentication and encryptions schemes.
- Model security for malicious parties.
- Apply verification methods.
- Evaluate and compare efficiency with the existing methods.

⇓

- Investigate delegatable anonymous credentials applicable to genomic privacy.
- Gather a survey on delegatable anonymous credentials.
- Apply to fully anonymize genomic sharing/testing methods.

⇓

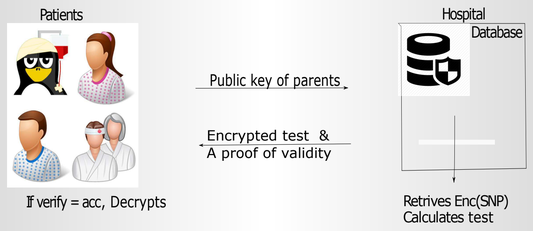
- Leverage entropy of DNA to define a new information-leakage metric.
- Matlab coding of entropy-based metric.
- Evaluate the privacy in releasing genomic data with the new metric.

4. Results and Discussions

We developed a method for **Dynamic Privacy-Preserving Genomic Susceptibility Testing**.
We proposed a novel protocol where a server calculates the susceptibility test function without having access to the clear-text genomic data of patients.
This work has been presented at an international conference [5].
Our contributions are:

- Reduce the Patient's and medical centers' involving.
- Leave the computation workload to $\mathcal{SPU}$.
- Somewhat Homomorphic Encryption enables multiplications by know values and encrypted values.
- More Efficiency and less rounds the rounds, more privacy.

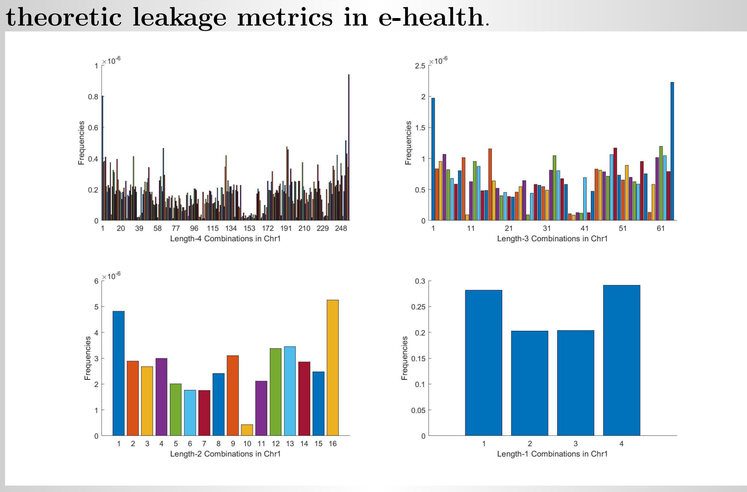
This paper is accepted in IH&MMSEC conference: http://ihmmsec.org/program/.
We developed a method for **Paternity Genomic Testing with Malicious Parties**, which leverage homomorphic properties and features of a message authentication on top of a verifiable computation scheme to resist against malicious parties running active attacks.



Our contributions with respect to prior approaches are:

- We investigate possible cryptographic constructions to enhance an paternity testing scheme with malicious users.
- We guarantee privacy of the patient with malicious server without threshold decryption of multi-party computation setting.
- We extend our protocol to other testing methods such as ancestry, compatibility testing.
- We achieved a higher security level due to applying highly secure cryptographic constructions as a core protocol.

We are developing an "entropy-based" analysis for **information-theoretic leakage metrics in e-health**.



5. Temporal Planning

There are three lines of work which will be followed during the next year:

Verifiable genomic privacy-preserving processing protocols with malicious security model

The following points will be addressed:

- Finalizing privacy-enhanced methods for genomic testing for malicious security model
- Evaluating the results and comparing with existing methods

Quantification of data leakage in privacy-preserving genomic processing

The following points will be addressed:

- Formalizing entropy-based data leakage measurement for genomic information
- Evaluating the results and comparing with existing methods

Investigation in delegatable anonymous credentials for genomic access control

The following points will be addressed:

- Research on delegatable anonymous credential schemes applicable to genomic data
- Investigate how delegatable anonymous credential is applied to genomic share consent
- Finalize the reserach in a survey platform.

6. References

[1] M. Naveed, E. Ayday, E. W. Clayton, J. Fellay, C. A. Gunter, J.-P. Hubaux, B. A. Malin, and X. Wang. Privacy in the genomic era. ACM Computing Surveys (CSUR), 48(1):6, 2015.
[2] Z. Brakerski, C. Gentry, and V. Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. In 3rd Innovations in Theoretical Computer Science Conference, pages 309-325. ACM, 2012.
[3] Marina Blanton and Fattaneh Bayatbabolghani. Efficient server-aided secure two-party function evaluation with applications to genomic computation. Proceedings on Privacy Enhancing Technologies, 4:1-22, 2016.
[4] C. Gentry, A. Sahai, and B. Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In Advances in Cryptology-CRYPTO 2013, pages 75-92. Springer, 2013.
[5] M. Namazi, J. Troncoso-Pastoriza, F Pérez-González. Dynamic Privacy Preserving Susceptibilty Testing. In Information Hiding & Multimedia Security, 2016
[6] Dario Fiore, Rosario Gennaro, and Valerio Pastro. Efficiently verifiable computation on encrypted data. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, pages 844-855. ACM, 2014.
[7] Mathias Humbert, Erman Ayday, Jean-Pierre Hubaux, and Amalio Telenti. Quantifying interdependent risks in genomic privacy. ACM Transactions on Privacy and Security (TOPS), 20(1):3, 2017.