Privacy-Preserving GWAS is Practical

Charlotte Bonte, Eleftheria Makri, Amin Ardeshirdavani, Jaak Simm, Yves Moreau, Frederik Vercauteren

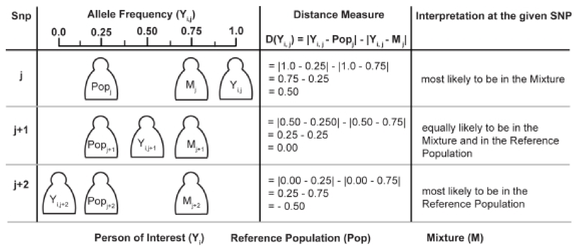
Dept. of Electrical Engineering, KU Leuven

Problem Statement

Design an *efficient* privacy-preserving system for GWAS, which can withstand attacks resolving individuals.

Motivation

Possibility to detect the presence of individuals in aggregated data

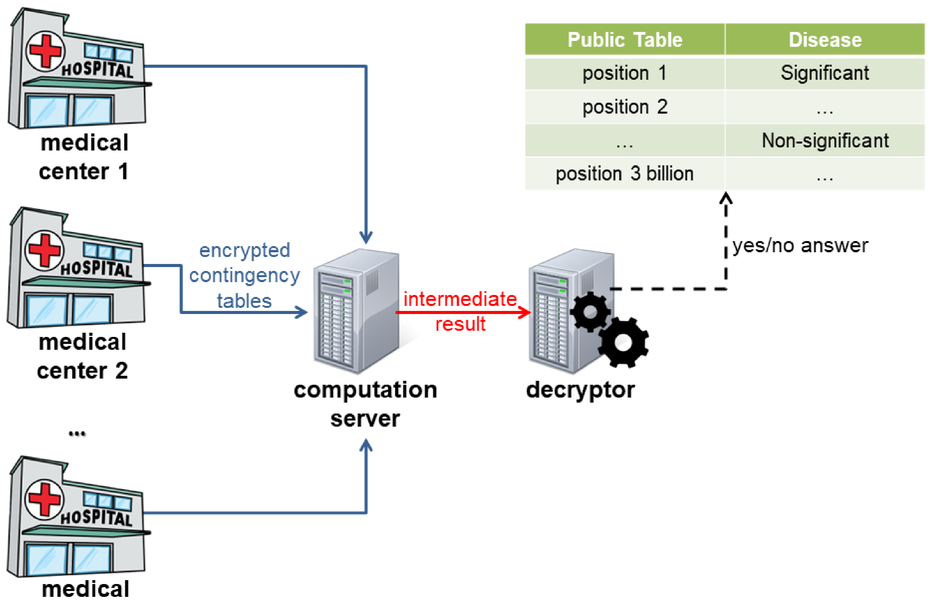


Homer, N., Szelinger, S., Redman, M., Duggan, D., Tembe, W., Muehling, J. Pearson J. V., Stephan D. A., Nelson S. F., Craig, D. W. (2008). *Resolving Individuals Contributing Trace Amounts of DNA to Highly Complex Mixtures Using High-Density SNP Genotyping Microarrays.* PLoS Genetics, 4(8), e1000167.
http://doi.org/10.1371/journal.pgen.1000167

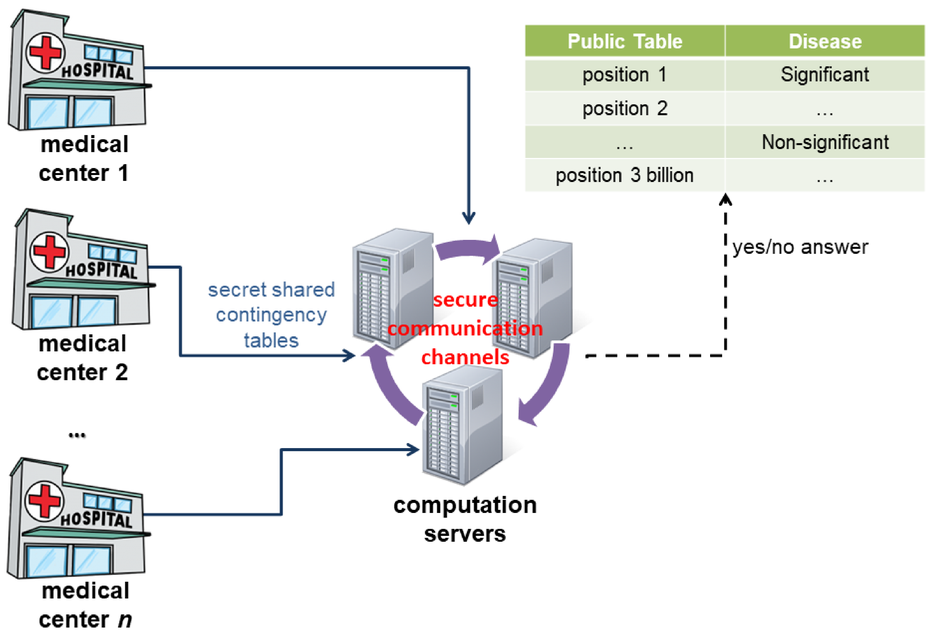
Contribution

- We propose a *somewhat homomorphic encryption* solution for GWAS.
- We develop an efficient *multiparty computation* solution for GWAS.
- The security and efficiency of both approaches are compared using a real-life application.
- We propose a new masking technique to allow efficient secure comparisons.
- Their short running times make our solutions practical.
- Our solution scales logarithmically in the number of subjets.

HE Scenario



MPC Scenario



Efficient Masking-Based Comparison

We check the inequality $[\![x]\!] \overset{?}{\geq} [\![y]\!]$ by computing $\widehat{[\![x-y]\!]} = [\![r]\!] \cdot [\![x-y]\!] + [\![r']\!]$, with r and r' random numbers satisfying the following condition: r has to be a positive integer number (bounded properly), and $r' < r$. If $r \cdot (\widehat{x-y}) + r' > 0$ then $x > y$.

HE Performance

Centers	Patients	CPU Time
20	200000	1.48 s
40	400000	1.52 s
60	600000	1.53 s
80	800000	1.56 s
100	100000	1.57 s

MPC Performance

	Server 1		Server i, $i \neq 1$
Centers	CPU Time	DataSent	CPU Time
20	1.7 ms	7.6 kB	1.4 ms
40	1.7 ms	12.7 kB	1.5 ms
60	1.9 ms	17.9 kB	1.7 ms
80	2.1 ms	23.0 kB	1.8 ms
100	2.2 ms	28.1 kB	1.9 ms

Conclusion

Both approaches are efficient for full-scale privacy-preserving GWAS, but the MPC is recommended:

- It offers active security.
- It is significantly more efficient.

Contact Information

Charlotte Bonte: cbonte@esat.kuleuven.be
Eleftheria Makri: emakri@esat.kuleuven.be