Security in Personal Genomics: Lest We Forget

Gene Tsudik
Computer Science Department
University of California, Irvine
gene.tsudik@uci.edu

ABSTRACT

Genomic privacy has attracted much attention from the research community, mainly since its risks are unique and breaches can lead to terrifying leakage of most personal and sensitive information. The much less explored topic of genomic security needs to mitigate threats of the digitized genome being altered by its owner or an outside party, which can have dire consequences, especially, in medical or legal settings. At the same time, many anticipated genomic applications (with varying degrees of trust) require only small amounts of genomic data. Supporting such applications requires a careful balance between security and privacy. Furthermore, genome's size raises performance concerns.

We argue that genomic security must be taken seriously and explored as a research topic in its own right. To this end, we discuss the problem space, identify the stakeholders, discuss assumptions about them, and outline several simple approaches based on common cryptographic techniques, including signature variants and authenticated data structures. We also present some extensions and identify opportunities for future research. The main goal of this paper is to highlight the importance of genomic security as a research topic in its own right.

CCS Concepts/ACM Classifiers

• Security and privacy → Authentication; Security and privacy → Management and querying of encrypted data

Author Keywords

Genomic Security; Authenticity; Integrity; Authenticated Data Structures; Digital Signature Chaining

BIOGRAPHY

Gene Tsudik is a Chancellor's Professor of Computer Science at the University of California, Irvine (UCI). He obtained his PhD in Computer Science from USC in 1991. Before coming to UCI in 2000, he was at IBM Zurich Research Laboratory (1991-1996) and USC/ISI (1996-2000). Over the years, his research interests included numerous topics in security and applied cryptography.. Gene Tsudik is a Fulbright Scholar, a Fubright Specialist, a fellow of ACM, IEEE and AAAS, as well as a member of Academia Europaea. From 2009 to 2015 he was the Editor-in-Chief of ACM Transactions on Information and Systems Security (TISSEC).

ASIA CCS'17, April 2–6, 2017, Abu Dhabi, United Arab Emirates.
ACM ISBN 978-1-4503-4944-4/17/04.
DOI: http://dx.doi.org/10.1145/3052973.3056128