Homomorphic Encryption: A Practitioner's Guide to Utilizing Breakthroughs in Advanced Cryptography to Meet Mission Needs

Ryan Carr, Ph.D.
Chief Technology Officer and VP of Engineering
Enveil

Recent advances in homomorphic encryption (HE), a pillar of the increasingly important technology category known as Privacy Enhancing Technologies (PETs), are changing the paradigm of secure data usage for mission use cases. HE protects data while it's being used or processed by allowing computations to occur in the encrypted or ciphertext domain, and most of the primitives that are currently used for HE are resistant to hypothesized quantum computing attacks. These powerful capabilities have led to HE being referred to as the "holy grail" of cryptography and are why it has been the subject of research and academic pursuit for nearly four decades. Once computationally impractical for use at scale, recent performance and utilization breakthroughs are redefining how and where organizations can leverage data to unlock value.

HE is transformative because the mission-enabling capabilities it delivers are not making something better; they are making something entirely new possible. By enabling users to encrypt the content of their search, analytic, or machine learning model as well as the associated results, organizations can securely leverage publicly available, open-source, and/or low-side, government-curated data sources while protecting their interests and intent. DoD users can perform secure searches, watchlisting, and analytics using sensitive/classified indicators against Publicly Available Information (PAI) or other less sensitive data on untrusted systems without moving/replicating data or compromising mission objectives.

HE significantly expands the way in which external and lower-trust data sources can be effectively leveraged and is serving as an important component of a Zero Trust architecture. These capabilities have far-reaching implications across the USG mission space in applications including high-to-high and high-to-low secure search as well as tactical edge use cases.

In this presentation, Dr. Ryan Carr will:

- Provide a brief history of homomorphic encryption and the attributes that make the technology stand out.
- Demystify the HE market landscape, highlighting the distinctions between HE researchers, libraries, and solution providers.
- Outline the security and intelligence challenges HE is uniquely positioned to overcome, and how those capabilities can significantly reduce operational risk and accelerate the timeline for turning raw data into actionable intelligence.
- Discuss how HE can power mission-enabling capabilities for the future, including the technology's role in a Zero Trust architecture.