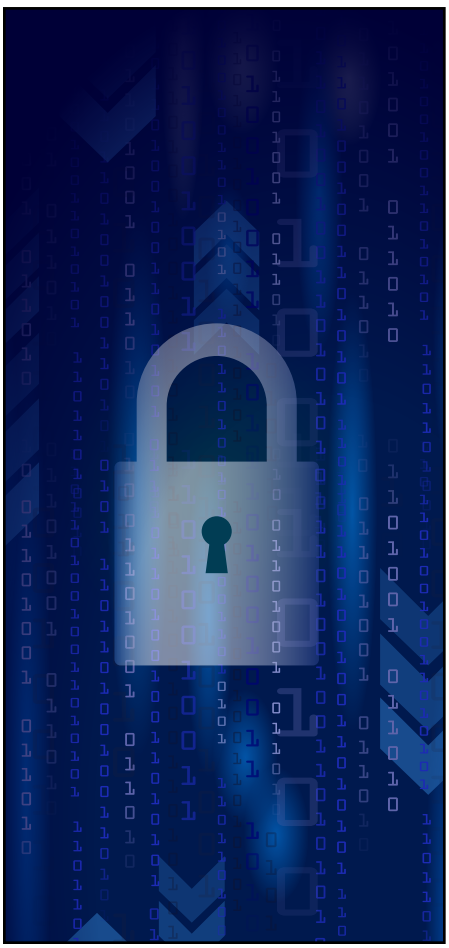
Solution Brief

Intel® Xeon® Scalable Processors
Financial Services Industry

Protect Data Privacy with Homomorphic Encryption on 3rd Gen Intel Xeon Scalable Processors

Extract the value of confidential data in its encrypted state.



Financial institutions (FIs) benefit from sharing data to improve their customers' experiences and to help manage risk. But they must also ensure compliance with data-management and privacy regulations. FIs must secure their data to protect both sensitive customer information and critical intellectual property (IP). This can create potential challenges because securing data throughout its lifecycle, including encryption and decryption, can be complex and computationally intensive.

Enterprises such as banks and insurance companies in the financial sector have recently begun adopting homomorphic encryption (HE) to combat these challenges. HE allows FIs to perform computations on encrypted data without decrypting it. This technology enables FIs to share data without revealing sensitive information, and to accelerate their overall system performance. With this capability, these institutions can collaborate on sensitive datasets using emerging artificial intelligence (AI) or hybrid cloud technologies without compromising privacy.

To help FIs get more from their data with HE, Intel has taken a holistic approach to support industry-wide HE adoption. Intel is helping organizations deploy HE through hardware-enabled acceleration, software toolkits, and ecosystem optimizations with key partners. Intel's portfolio of built-in accelerators—including Intel® Advanced Vector Extensions 512 (Intel AVX-512), Intel Software Guard Extensions (Intel SGX), and more—on high-performing Intel platforms has enabled well-known FIs to realize the benefits from HE today.

Bringing HE to financial services

HE is a cryptographic technique that enables computation and collaboration on data while preserving confidentiality. Computing advances in the last decade have set the stage for HE to become more widely adopted. HE is now at the inflection point where its overall performance is already suitable for a variety of use scenarios. In particular, those in regulated industries stand to benefit greatly, such as in finance, where preserving the privacy and confidentiality of data is paramount.

Traditional vs. homomorphic encryption

Objective	Traditional encryption	Homomorphic encryption
Data protected at rest	Yes	Yes
Data protected in flight	Yes	Yes
Data protected while in use	No	Yes
Data can be used in encrypted state	No	Yes

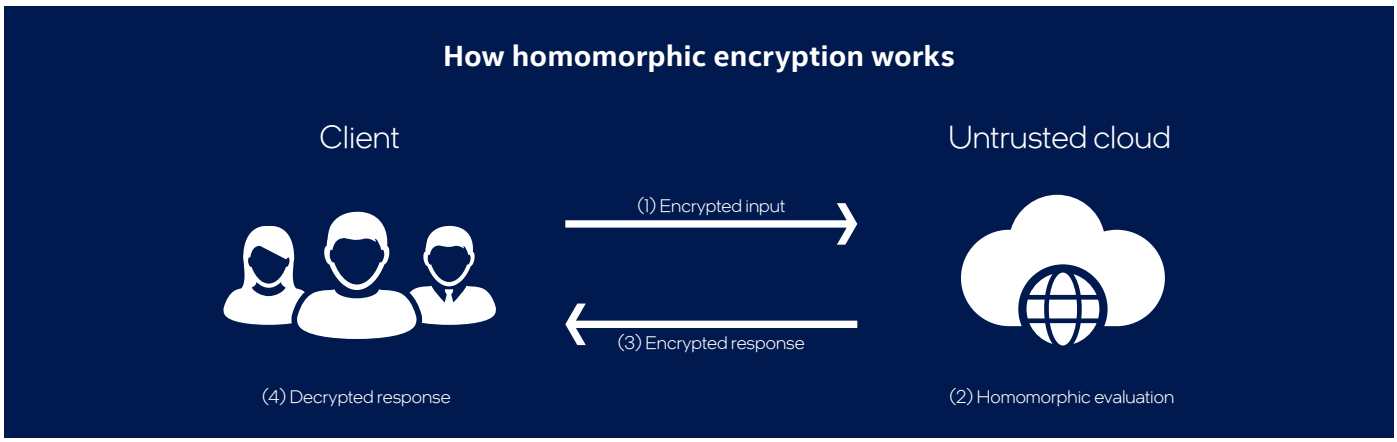


Figure 1. Fully homomorphic encryption operations in a nutshell

Fighting crime and managing risk

HE can help FIs address longstanding challenges, such as fraud. FIs must follow a complex set of laws and programs that are designed to deter or uncover the financing of criminal activities. But compliance is expensive, and regulations have mixed results in preventing crime. Legacy hardware used by FIs often lacks the ability to scale to combat threats across business units.

HE also helps FIs gain deeper insight for areas such as risk assessment. After the U.S. housing crisis of 2008, global regulators established new compliance measures that require FIs to calculate the valuation and risk associated with housing investments. HE can be used to significantly increase the speed at which risk-management analysis is conducted while keeping data private.

Intel has been working closely with financial organizations to help them integrate HE and benefit in these and other ways. The following sections provide two examples.

> "The performance improvements achieved with Intel's latest Xeon platform will support our efforts in wider adoption of HE, particularly in improving data analysis and insights, as well as product innovation around areas such as anti-financial crime."
>
> — Nikolai Larbalestier, Senior Vice President, Enterprise Architecture, Nasdaq

Nasdaq: Fighting fraud with detection technology

Nasdaq, the American stock exchange based in New York City, makes use of the crypto-acceleration instructions in 3rd Gen Intel Xeon Scalable processors to speed up computation for its HE applications. Nasdaq uses HE to enable AI and machine learning (ML) on large datasets. The stock exchange has been experimenting with HE in strengthening technology solutions that detect financial crimes, such as money laundering and fraud, while also complying with data-privacy regulations.

3rd Gen Intel Xeon Scalable processors support the organization's efforts to apply HE widely. Unlocking proprietary data without exposing the data itself allows for a stronger collective effort to consolidate unique datasets to analyze and identify potential financial crime activity.

WeBank: Accelerating federated learning

WeBank, the first digital bank in China, strives to provide more convenient financial services to micro-sized, small, and medium-sized enterprises and the public. WeBank is an active explorer and participant in federated learning, which is a type of ML in which a set of client computers collaboratively trains a model on local data. Everything is orchestrated by a central server without sharing the raw data.[1] Federated learning can be applied by those in the financial industry to manage credit risks through AI-based risk-control models to reduce the rate of non-performing loans. This technique requires an abundant and rich source of data.

WeBank has led the way in federated learning by releasing an industrial open source framework, called Federated AI Technology Enabler (FATE), to help improve the convenience and efficiency of building a federated learning solution. WeBank partnered with Intel to accelerate HE on FATE-based solutions built on 3rd Gen Intel Xeon Scalable processors with the integrated Intel AVX-512 instruction set, which has helped improve the company's overall operating efficiencies by up to 4.7x.[2]

The Intel platform for HE

Intel has been on the forefront of building a software and hardware platform for HE computation. 3rd Gen Intel Xeon Scalable processors include built-in accelerators that can deliver optimized performance across heavy workloads such as HE. These built-in accelerators mean that there is no need to add more CPU cores or discrete accelerator hardware to meet the performance requirements for HE and a wide variety of other workloads and use cases.

Built-in accelerators on 3rd Gen Intel Xeon Scalable processors

Need	Intel accelerator	Benefits
Faster insights into decision making for risk-management and portfolio optimization	Intel AVX-512	Accelerates performance for workloads and use cases such as scientific simulations, financial analytics, AI/deep learning (DL), cryptography, and data compression.
Preventing financial crimes and meeting compliance requirements	Intel SGX	Allows applications to encrypt small regions of memory, called enclaves, for use only by the application. Intel SGX enclaves are available in sizes of up to 512 GB per socket.
Unlocking the value of proprietary datasets without exposing data	Intel Crypto Acceleration	Increases the performance of encryption-intensive workloads (Secure Sockets Layer [SSL]/Transport Layer Security [TLS], 5G, and VPNs/firewalls).
Increased performance and better user experience (UX) when using encryption	Intel QuickAssist Technology (Intel QAT)	Works with Intel Crypto Acceleration to improve the performance of encryption-intensive workloads by accelerating data offload from Intel Xeon Scalable processors.

Intel software optimizations for HE

The Intel platform for HE is a modular design that allows new components to be incorporated or updated as they become available.

The accelerated math libraries layer includes the open source Intel Homomorphic Encryption Acceleration Library (Intel HEXL), which implements CPU-based acceleration of mathematical operations, capable of delivering up to 7.2x speedup in calculations compared to a native C++ implementation.[3] Above this layer are the HE libraries that use Intel HEXL for acceleration, including HElib, Microsoft SEAL, and PALISADE.

The Intel Homomorphic Encryption Toolkit (Intel HE Toolkit) is designed to make it easier for new HE users to get started evaluating and deploying HE on Intel platforms. Like Intel HEXL, the Intel HE Toolkit takes advantage of the latest Intel AVX-512 instructions to accelerate encryption on shared datasets. The Intel HE Toolkit also offers numerous kernel examples of how HE libraries can be used to implement mathematical operations.

Support from a large partner ecosystem

Intel has been collaborating with the largest cloud service providers (CSPs) and a wide variety of commercial software vendors, including SAP and VMware, to optimize HE solutions for customer-specific use cases. In addition, Intel continues to participate actively in the open source community, including the Linux Foundation and FINOS, to support open source innovation in HE. These efforts have resulted in a broad array of solutions that help FIs accelerate performance and improve their time to business value.

Increase opportunities to use data—while protecting it

Intel has been on the forefront of constructing a software and hardware platform for HE computations. These advancements are helping the financial services industry tap into rich stores of data without compromising privacy. This capability will help lead to faster business insights, faster fraud detection, and new products and services that can improve customer experiences.

Learn more about Intel solutions supporting the financial services industry.

intel XEON

[1] Emily Glanz, Nova Fallen. "What Is Federated Learning?" *O'Reilly*. Accessed June 2022. oreilly.com/library/view/what-is-federated/9781098107253/ch01.html.

[2] Intel. "WeBank Accelerates Secure Computing." April 2022. intel.com/content/www/us/en/customer-spotlight/stories/webank-customer-story.html.

[3] Fabian Boemer, Sejun Kim, Gelila Seifu, Fillipe D. M. de Souza, and Vinodh Gopal. "Intel HEXL: Accelerating Homomorphic Encryption with Intel AVX512-IFMA52." *Cryptology ePrint Archive*. April 2021. https://eprint.iacr.org/2021/420.

Printed in USA 0722/EH/PRW/PDF Please Recycle 351932-001US