

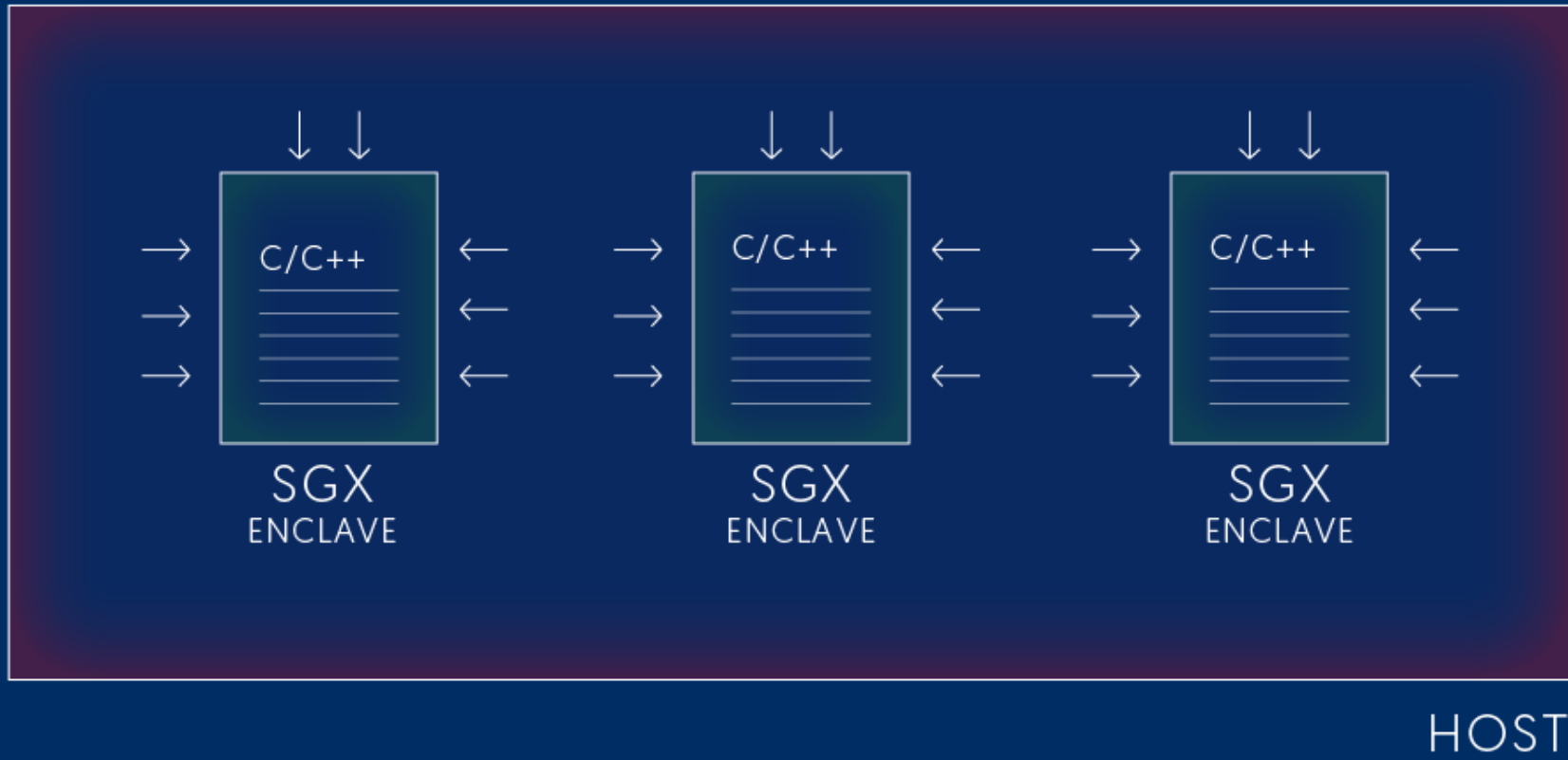
The background is a solid dark blue. Overlaid on this are numerous circles of varying sizes, some of which are connected by thin, light blue lines, creating a network-like or molecular structure. The circles and lines are semi-transparent, allowing the dark blue background to show through.

golem

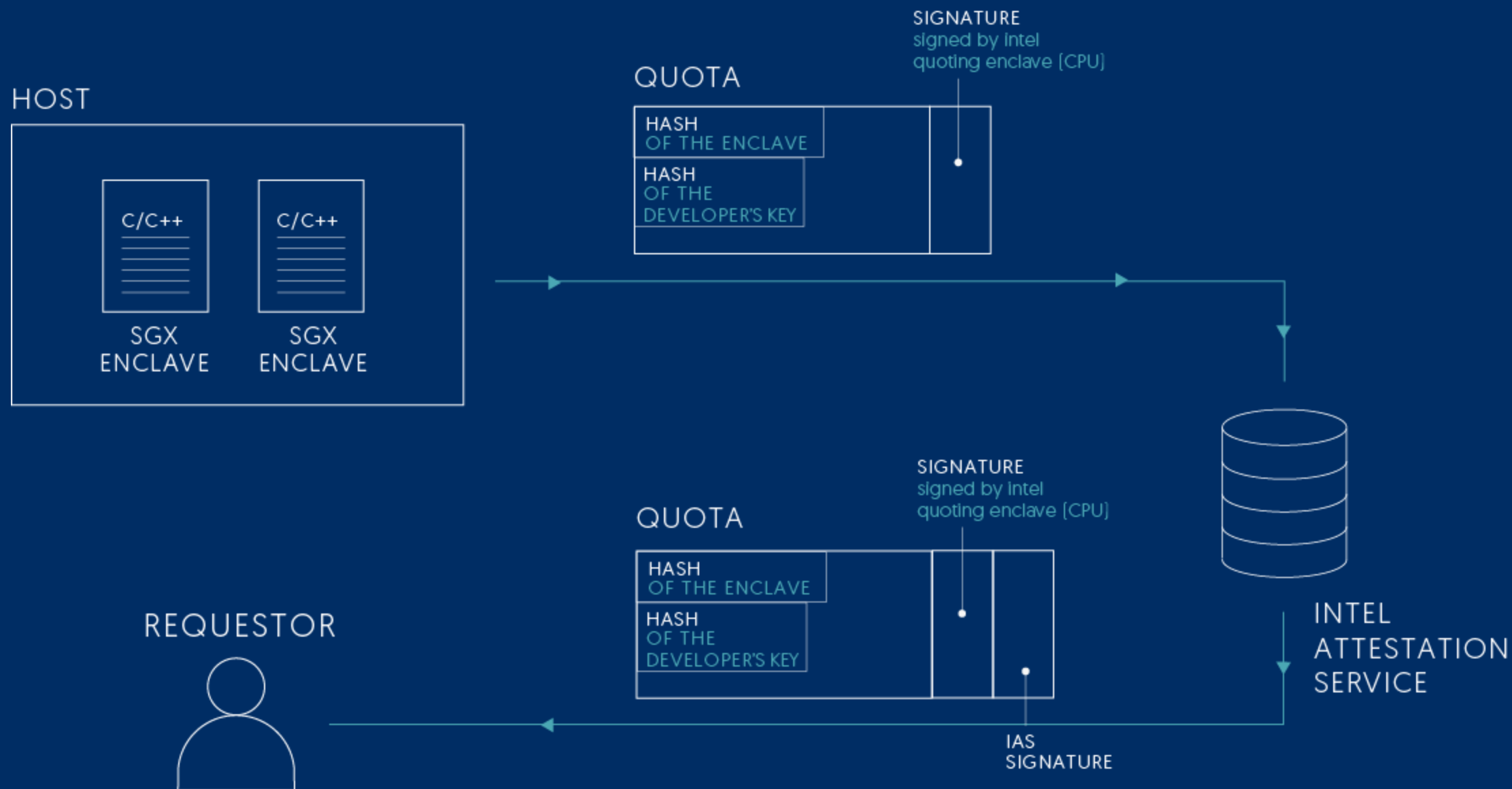
ARBITRARY COMPUTATIONS WITH SGX IN GOLEM

SGX

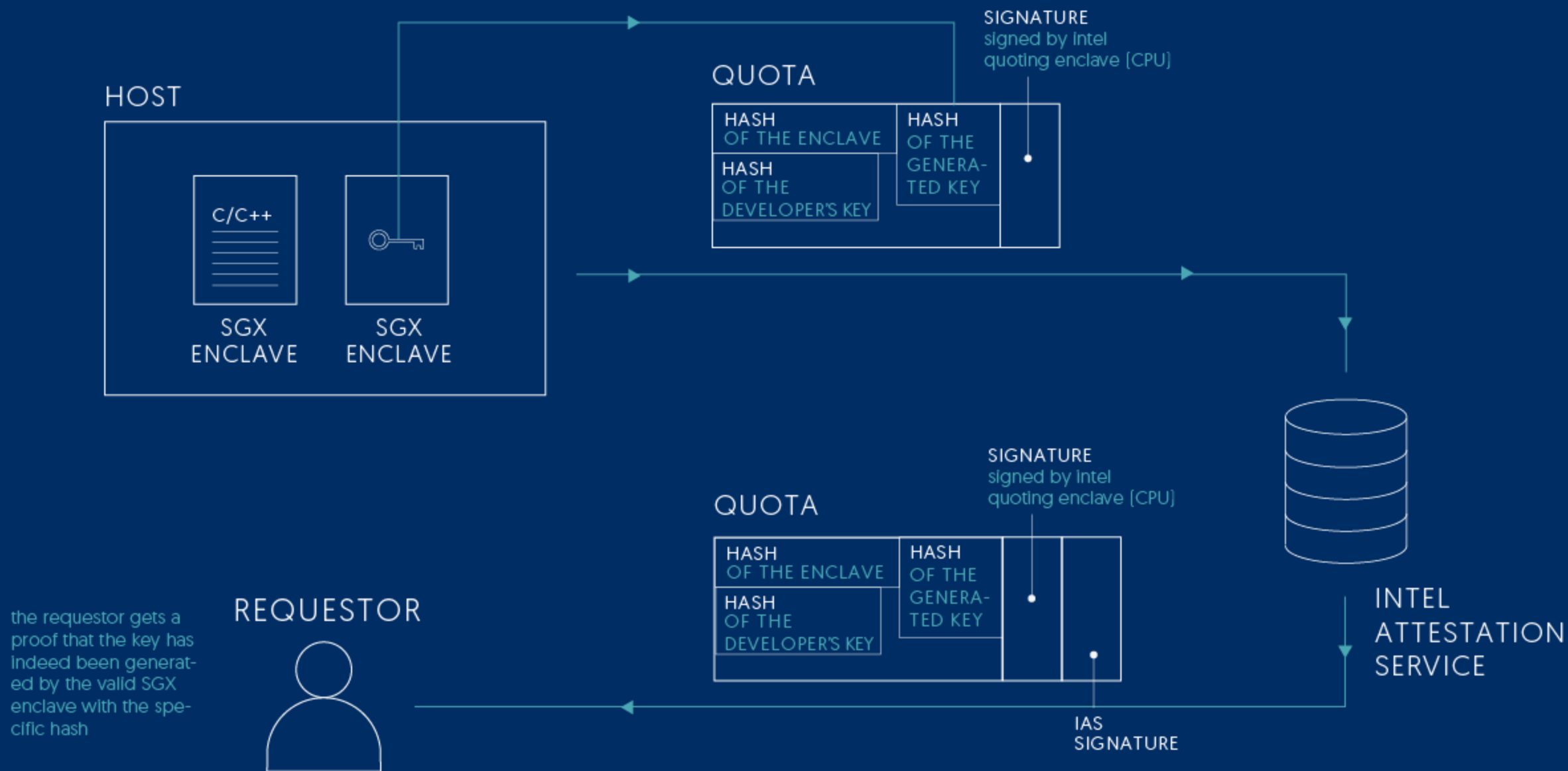
— Intel Software Guard Extensions



REMOTE ATTESTATION

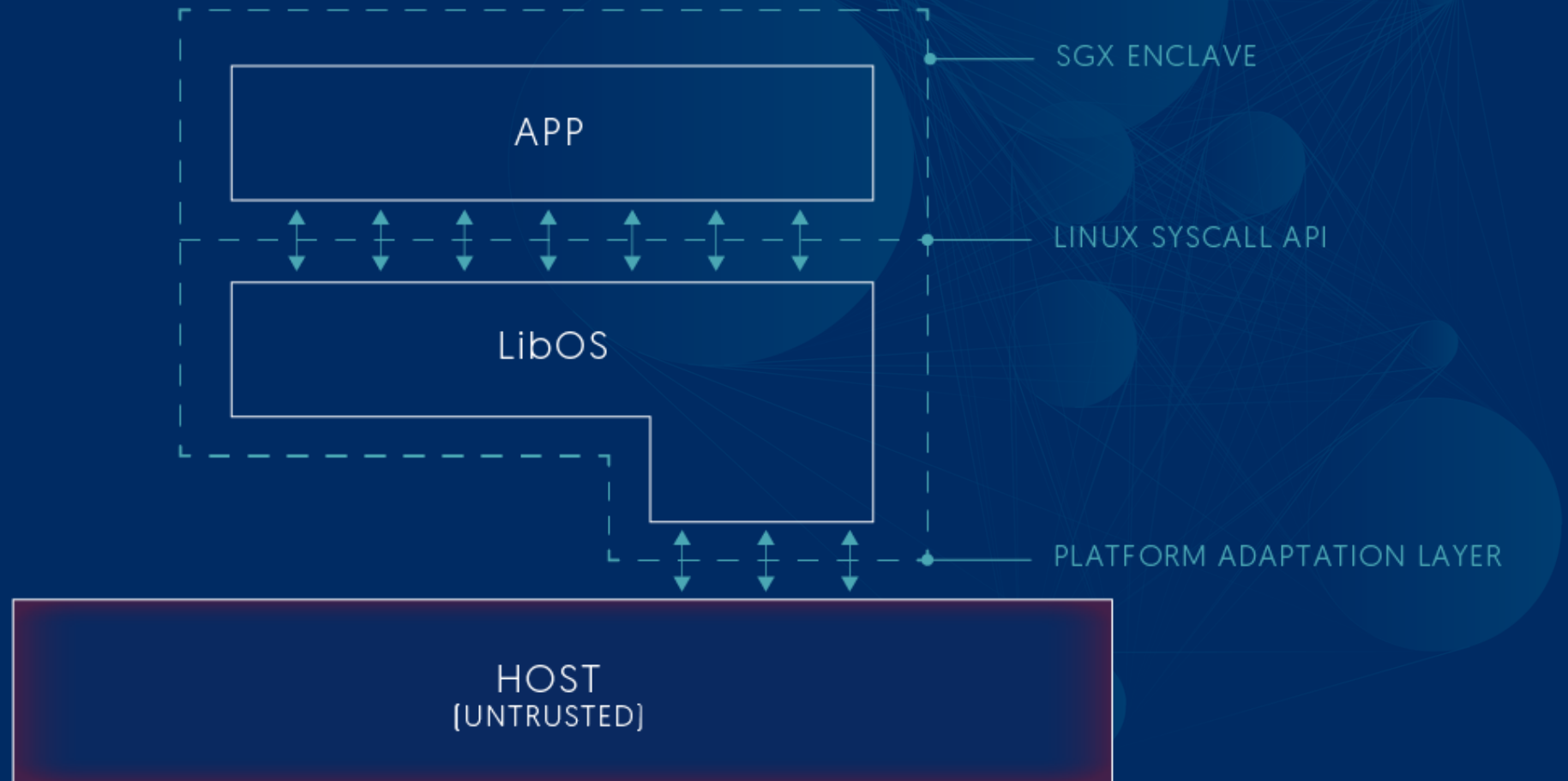


REMOTE ATTESTATION



GRAPHENE

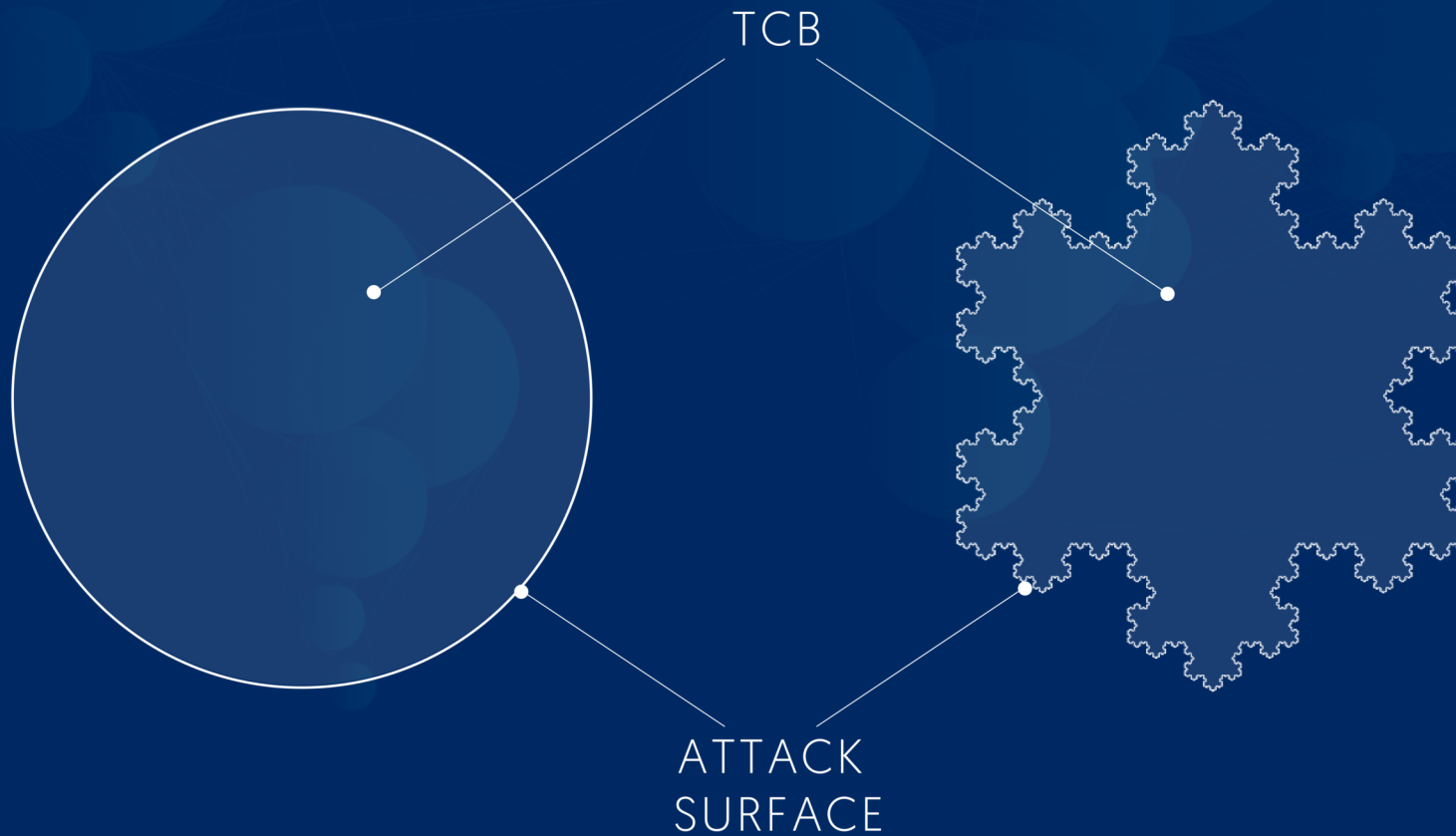
— A library OS for Linux multi-process applications, with Intel SGX support



TCB VS ATTACK SURFACE

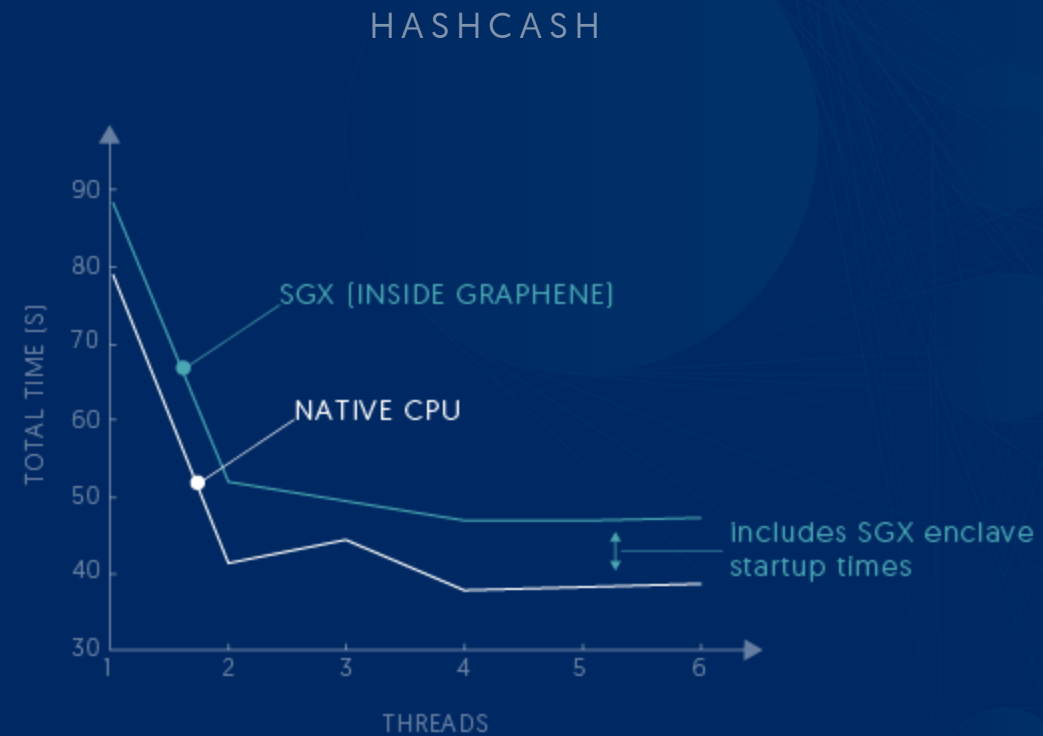
- Trusted computing base
 - The set of all hardware, firmware, and/or software components that are critical to the security of a computer system
- Attack surface of a software environment
 - The sum of the different points [the 'attack vectors'] where an unauthorized user [the 'attacker'] can try to enter data to or extract data from the environment

-WIKIPEDIA



EFFICIENCY

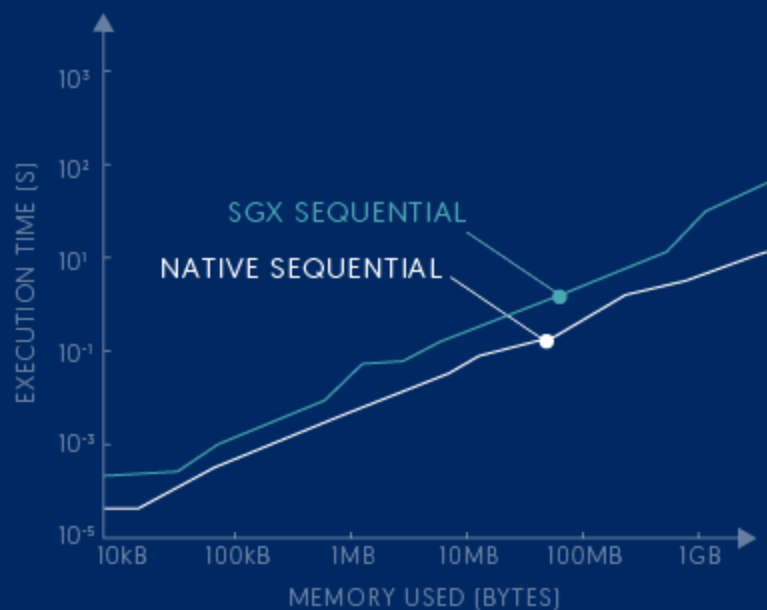
— Compute-intensive algorithm



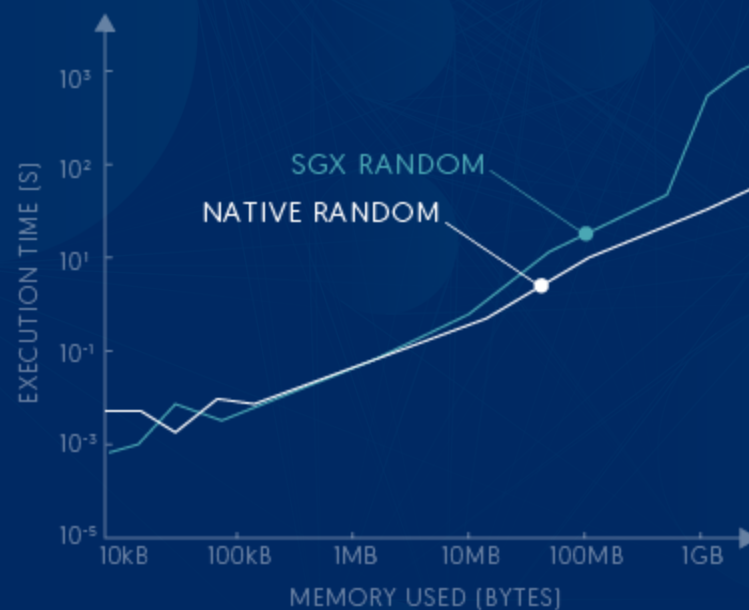
EFFICIENCY

— Memory-intensive algorithms

SEQUENTIAL ACCESS PATTERN

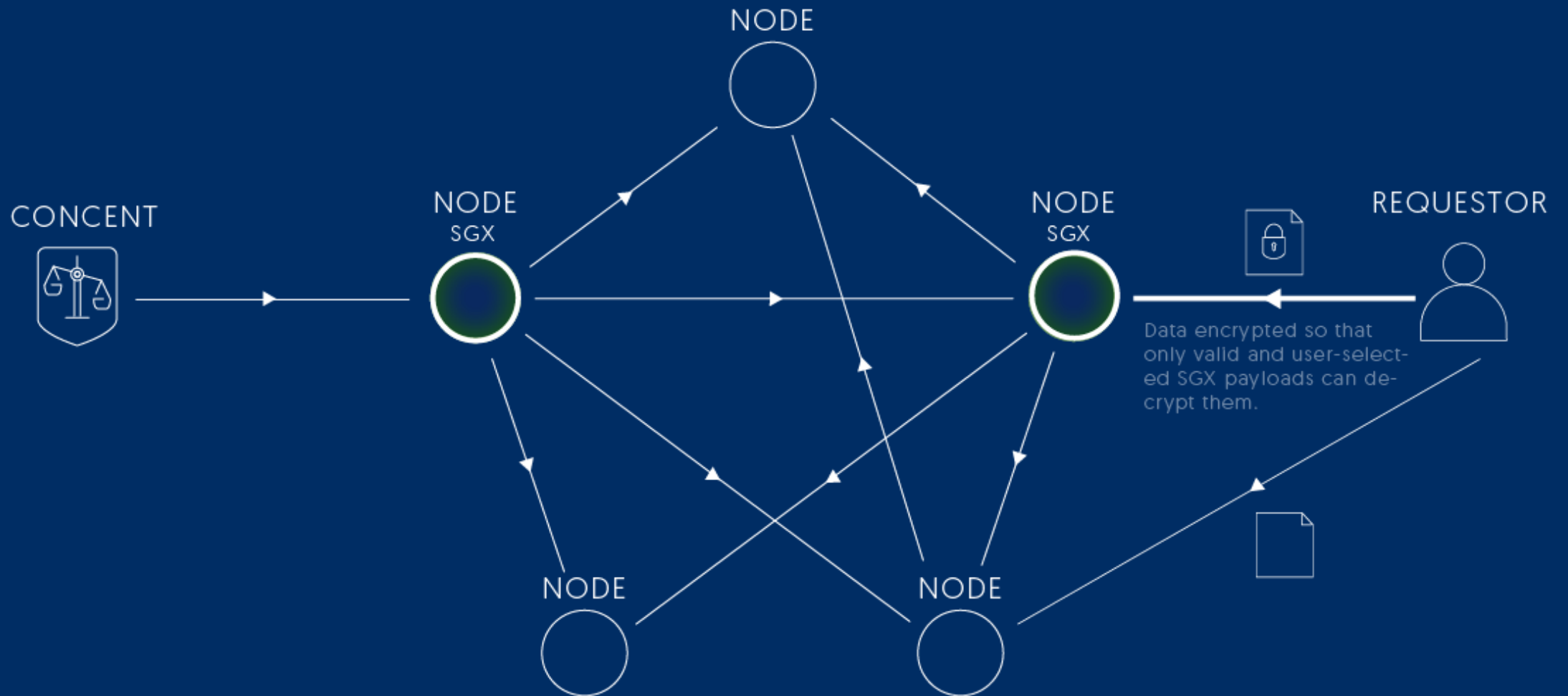


RANDOM ACCESS PATTERN



GRAPHENE NODES IN GOLEM

- Providers with SGX nodes
- Consent using SGX backends



FUTURE IDEAS

—— 01 Launch Enclave Liberation

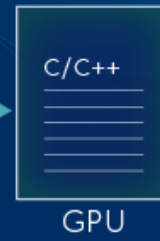
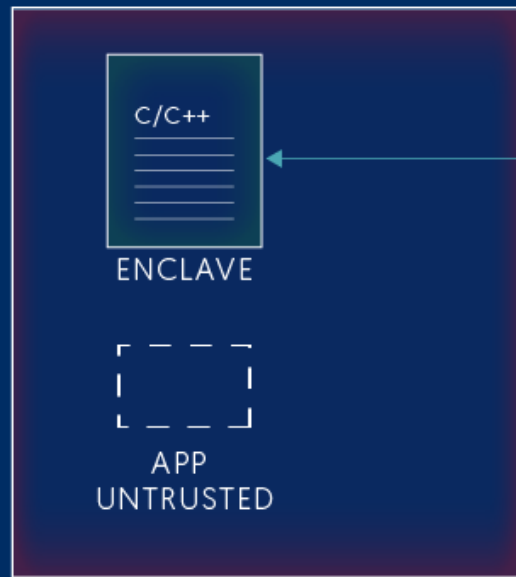
—— 02 IAS Liberation



FUTURE IDEAS

- 01 Launch Enclave Liberation
- 02 IAS Liberation
- 03 Secure GPU for enclaves

HOST



The background is a solid dark blue. It features an abstract pattern of various-sized circles in a lighter shade of blue, connected by thin, light blue lines, creating a network-like or molecular structure. The circles and lines are more concentrated on the left and right sides, leaving the center relatively clear for the text.

THANK YOU

golem

For the help with this presentation thanks to:

Substantial knowledge: Joanna Rutkowska, Michał Kowalczyk, Aleksandra Skrzypczak

Design: Natalia Mroszczyk

GOLEM.NETWORK