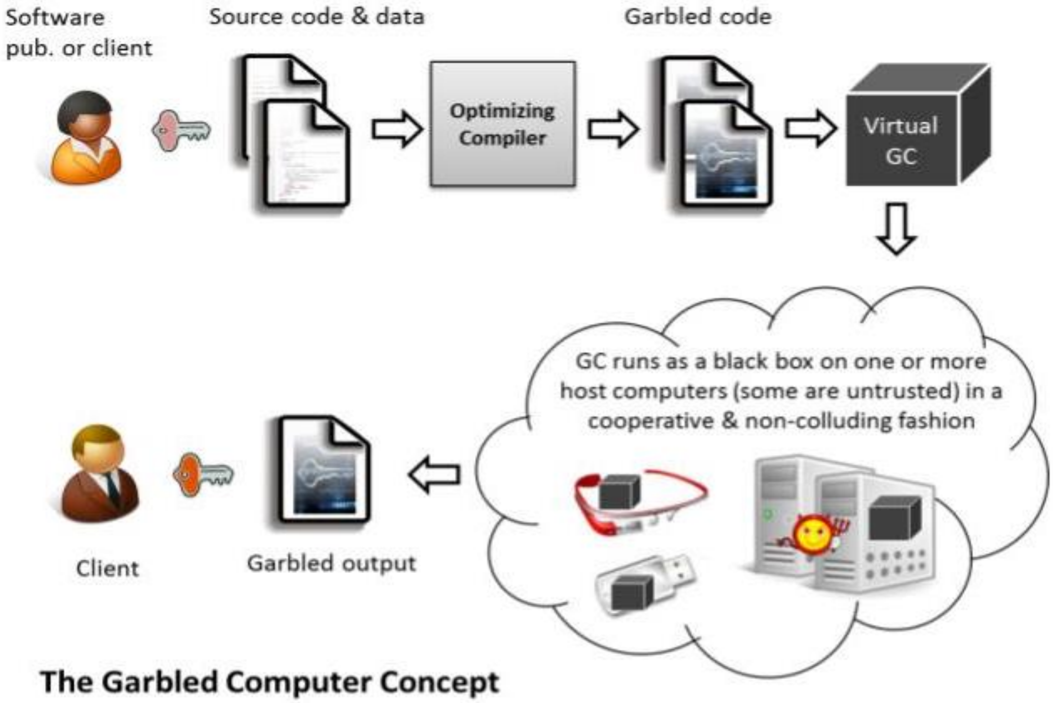
Research of the issue

An adversary observing the computations of a GC learns nothing about what it is doing, what data it is operating on (whether inputs or intermediate values), and the outputs it is producing. The GC enables execution on untrusted platforms, of trusted and confidential code whose inputs and outputs are sensitive. For example it can enable the utilization of Amazon cloud services without revealing to Amazon the nature of the computation or the data, and without requiring Amazon to change the operation of its cloud services (i.e., use standard off-the-shelf services).

Successful development of the GC would be a disruptive technology that would create substantial commercialization opportunities and significant scientific implications on the area of cyber security.

The project received initial support from the Qatar National Research Fund under the exceptional NPRP program. Several Qatar University researchers have been leading this research effort including Qutaibah Malluhi, Aiman Erbad, Khaled Khan, Ryan Riley and Abdullatif Shikfa. Researchers at Purdue University have been also collaborating on this project.


Software
pub. or client
Source code & data
Optimizing Compiler
Garbled code
Virtual GC
GC runs as a black box on one or more host computers (some are untrusted) in a cooperative & non-colluding fashion
Client
Garbled output

The Garbled Computer Concept