**Claims**

1. A system for verifying a trusted execution environment programmed as a collection of abstract objects, comprising:

    a verifier for sequential programs for verifying annotated application programming interface (API) functions of each abstract object and for verifying annotated CASM functions of each abstract object;

    wherein the verifies outputs verified API functions and verified CASM functions;

    a verified compiler for compiling the verified API functions into verified assembly code; and

    an assembly code generator to generate verified assembly code from the verified CASM functions.

2. The system of claim 1 wherein the annotations of the API functions and the annotations of the CASM functions direct the verifier to check relevant properties of the API functions and the CASM functions that guarantee the trusted execution environment.

3. The system of claim 2 wherein assembly code in the object is written in CASM.

4. The system of claim 3 wherein CASM provides pseudofunctions corresponding to the assembly language of the object.

5. The system of claim 4 wherein the verifier replaces the CASM pseudofunctions with source code from a hardware model.

6. The system of claim 1 wherein each object comprises:

    an identifier;

an indication of the language in which the object is implemented;

a lock that ensures that the object run on only one core at a time;

an exclusive region of memory;

an initialization API that sets initializes the object;

a public API;

a set of CASM functions; and

a set of internal function declarations.

7. The system of claim 6 wherein the CASM functions are assembly code for a target hardware architecture.

8. The system of claim 6 wherein the object guarantees that, for any method in the public API, if a pre-condition is met upon invoking a public method, a post-condition is guaranteed to hold upon return from the public method.

9. The system of claim 6 wherein method of the public API of concurrent objects can be invoked in parallel on multiple CPU cores.

10. The system of claim 6 wherein the exclusive region of memory includes exclusive access to one or more control registers.