INCORPORATING SHARED RANDOMNESS INTO DISTRIBUTED CRYPTOGRAPHY

ABSTRACT

A method of distributed cryptography for high consequence security systems which employs shared randomness between operating parties. Shared randomness is accomplished by sharing cryptographic keys stored in secure hardware tokens by potentially less secure software or general purpose computing units that perform distributed cryptography. The shared randomness is based on shared keys (at the tokens) and unique context. Shared random values are incorporated into the computation of partial results used in the distributed cryptographic calculation. The incorporation of shared randomness provides a hand-shake among the hardware tokens. When the operation is successful, a result is computed with assurance that the correct parties have taken part in forming the result. The hand-shake assures binding of operating parties and added system security.

FIGURE 1

162162

G00002