

Functional Randomness In Security Tokens

Disclosure Number

201102576

Technology Summary

The Functional Randomness in Security Tokens method and system improves the security of two-factor authentication hardware tokens by improving on the algorithms used to securely generate random data. Instead, this system allows one to configure the security of the token based on storage cost and computational security. The limit of this approach enables us to build a system where its security will no longer be based on one time pads generated from a cryptographic function (e.g., SHA-256). The ability to have secure randomness from physical security (rather than computational security) is a much stronger security guarantee.

Inventor

PAUL, NATHANAEL R

Computational Sciences & Engineering Div

Licensing Contact

SIMS, DAVID L

UT-Battelle, LLC

Oak Ridge National Laboratory

Rm 124C, Bldg 4500N, MS: 6196

1 Bethel Valley Road

Oak Ridge, TN 37831

Office Phone: (865) 241-3808

E-mail: SIMSDL@ORNL.GOV

Note: The technology described above is an early stage opportunity. Licensing rights to this intellectual property may be limited or unavailable. Patent applications directed towards this invention may not have been filed with any patent office.