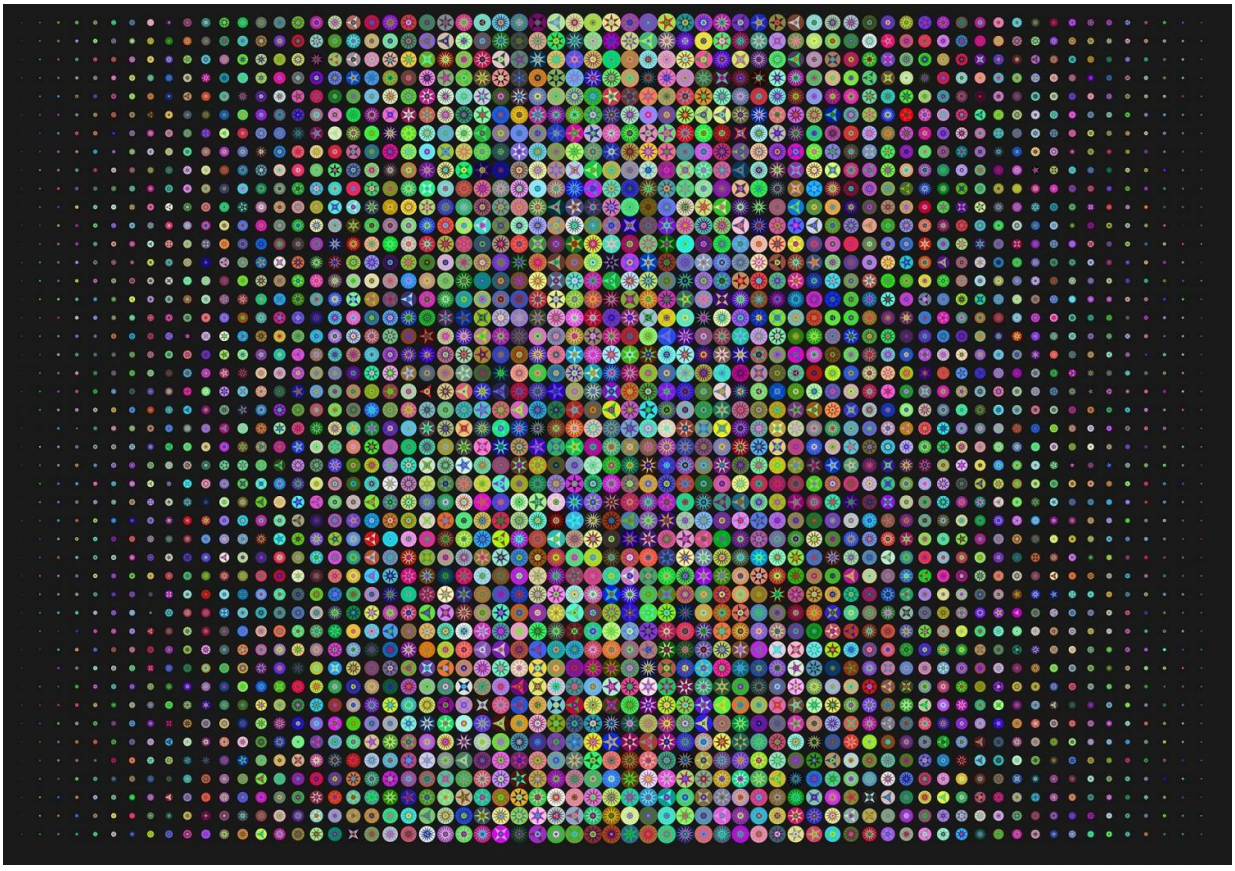
Recommendation for cryptographic key generation

March 8 2019



Credit: CC0 Public Domain

Cryptography is often used in information technology security environments to protect sensitive, high-value data that might be compromised during transmission or while in storage. It relies upon two

basic components: an algorithm (i.e., cryptographic methodology) and a cryptographic key. NIST has developed a wide variety of Federal Information Processing Standards (FIPS) and guidance to specify, approve, and manage cryptographic algorithms and keys for Federal Government use.

NIST invites comments on Draft Special Publication (SP) 800-133 Revision 1, Recommendation for Cryptographic Key Generation, which discusses the generation of keys to be managed and used by approved cryptographic algorithms. This revision adds the Edwards-curve Digital Signature Algorithm (EdDSA) to the original list of digital signature algorithms as well as KMAC as an algorithm for generating a Message Authentication Code (MAC). EdDSA will also be proposed as an additional signature algorithm in a forthcoming revision of Federal Information Processing Standard (FIPS) 186, Digital Signature Standard (DSS). KMAC is specified in SP 800-185, Recommendation for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters. Additional changes are listed in the final appendix of SP 800-133 Rev. 1.

A public comment period for this document is open until May 8, 2019.

A call for patent claims is included on page iv of this draft. For additional information, see the Information Technology Laboratory (ITL) Patent Policy—Inclusion of Patents in ITL Publications.

Provided by National Institute of Standards and Technology