Cryptology ePrint Archive: Report 2011/659

Formally Assessing Cryptographic Entropy

Daniel R. L. Brown

Abstract: Cryptography relies on the secrecy of keys. Measures of information, and thus secrecy, are called entropy. Previous work does not formally assess the cryptographically appropriate entropy of secret keys. This report defines several new forms of entropy appropriate for cryptographic situations. This report defines statistical inference methods appropriate for assessing cryptographic entropy.

Category / Keywords: foundations / Entropy Assessment, Key Generation

Date: received 6 Dec 2011, last revised 2 Jan 2013

Contact author: dbrown at certicom com

Available formats: PDF | BibTeX Citation

Note: Cited Bonneau and Boztas for a previous version of working entropy.

Version: 20130102:185223 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]