Cryptology ePrint Archive: Report 2011/172

The weak password problem: chaos, criticality, and encrypted p-CAPTCHAs

T.V. Laptyeva and S. Flach and K. Kladko

Abstract: Vulnerabilities related to weak passwords are a pressing global economic and security issue. We report a novel, simple, and effective approach to address the weak password problem. Building upon chaotic dynamics, criticality at phase transitions, CAPTCHA recognition, and computational round-off errors we design an algorithm that strengthens security of passwords. The core idea of our method is to split a long and secure password into two components. The first component is memorized by the user. The second component is transformed into a CAPTCHA image and then protected using evolution of a two-dimensional dynamical system close to a phase transition, in such a way that standard brute-force attacks become ineffective. We expect our approach to have wide applications for authentication and encryption technologies.

Category / Keywords: foundations / applications complexity theory foundations key management

Date: received 3 Apr 2011

Contact author: kladko at axiomaresearch com