Ferradi, Houda; **Géraud, Rémi**; **Naccache, David**

Human public-key encryption. (English) Zbl 1410.94066

Phan, Raphael C.-W. (ed.) et al., Paradigms in cryptology – Mycrypt 2016. Malicious and exploratory cryptology. Second international conference, Mycrypt 2016, Kuala Lumpur, Malaysia, December 1–2, 2016. Revised selected papers. Cham: Springer. Lect. Notes Comput. Sci. 10311, 494-505 (2017).

Summary: This paper proposes a public-key cryptosystem and a short password encryption mode, where traditional hardness assumptions are replaced by specific refinements of the CAPTCHA concept called decisional and existential CAPTCHAs.

The public-key encryption method, achieving 128-bit security, typically requires from the sender to solve one CAPTCHA. The receiver does not need to resort to any human aid.

A second symmetric encryption method allows to encrypt messages using very short passwords shared between the sender and the receiver. Here, a simple 5-character alphanumeric password provides sufficient security for all practical purposes.

We conjecture that the automatic construction of decisional and existential CAPTCHAs is possible and provide candidate ideas for their implementation.

For the entire collection see [Zbl 1369.94005].

MSC:

94A60 Cryptography

Full Text: DOI