Bos, Joppe W.; Özen, Onur; Hubaux, Jean-Pierre
Analysis and optimization of cryptographically generated addresses. (English) Zbl 1307.94039

Summary: The need for nodes to be able to generate their own address and verify those from others, without relying on a global trusted authority, is a well-known problem in networking. One popular technique for solving this problem is to use self-certifying addresses that are widely used and standardized; a prime example is cryptographically generated addresses (CGA). We re-investigate the attack models that can occur in practice and analyze the security of CGA-like schemes. As a result, an alternative protocol to CGA, called CGA++, is presented. This protocol eliminates several attacks applicable to CGA and increases the overall security. In many ways, CGA++ offers a nice alternative to CGA and can be used notably for future developments of the Internet Protocol version 6.

For the entire collection see [Zbl 1172.68310].

MSC:
94A60 Cryptography

Software:
eBACS; eBASH; OpenSSL

Full Text: DOI

References:

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.