Techniques for Encryption based on Perfect Secrecy for Bounded Storage

Tech ID: 32975 / UC Case 2022-823-0

BACKGROUND

A major aim of the field of cryptography is to design cryptosystems that are provably secure and practical. Factors such as integrity, confidentiality and authentication are important. Symmetric-key methods have traditionally been viewed as practical in terms of typically a smaller key size, which means less storage requirements, and also faster processing. This, however, opens the protocols up to certain vulnerabilities, such as brute-force attacks. To reduce risk, the cryptographic keys are made longer, which in turn adds overhead burden and makes the scheme less practical. Asymmetric-type frameworks use pairs of keys consisting of a public and private key, and these models depends heavily on the privacy of the non-public key. Asymmetric-based protocols are generally much slower than symmetric approaches. Symmetric-Asymmetric hybrid models have attempted to blend the speed and convenience of the public asymmetric encryption schemes with the effectiveness of a private symmetric encryption schemes. Examples of hybrids include GNU Privacy Guard, Advanced Encryption Standard-RSA, and Elliptical Curve Cryptography-RSA. In the modern computing era with quantum architecture and access to network and cloud resources on the rise, the integrity and confidentiality of such modern cryptographic models will increasingly be under pressure.

TECHNOLOGY DESCRIPTION

To overcome these challenges, researchers at UC Santa Cruz (UCSC) have developed a new cryptographic modality which moves beyond conventional frameworks. By designing a system and methods based on a bounded storage model and while using both short constant-length secret keys and public random bit strings, UCSC's protocol bridges the cryptographic approaches of old and new. In this novel model, a large random string *a*, which is publicly available, is used, and the adversary can compute any function on a but can only store *B* bits of the output due to storage bound. This in effect limits the storage capacity of the adversary during protocol. For encryption and decryption between two allies, a secret key of certain length and random string of certain length are stipulated, and they need to store a certain number of bits of the random string for performing plaintext-ciphertext functions. Both the secret key length and public random string are independent of the size of the message.

APPLICATIONS

Digital security

ADVANTAGES

- Can be implemented using only finite group arithmetic and additive cipher.
- Secure even if key is revealed to an adversary after message is transferred.
- Potentially applicable to both communications/data in transit and memory/data at rest.

INTELLECTUAL PROPERTY INFORMATION

Country	Type	Number	Dated	Case
Patent Cooperation Treaty	Published Application	WO 2023/108037	06/15/2023	2022-823

Additional Patent Pending

RELATED MATERIALS

CONTACT

Marc Oettinger
marc.oettinger@ucsc.edu
tel: 831-502-0253.

OTHER INFORMATION

KEYWORDS

cryptographic, cryptography, cryptosystem, Bounded Storage Model, security, internet security, digital security, symmetric, asymmetric, quantum, encryption

CATEGORIZED AS

- **Communications**
  - Internet
  - Networking
- **Computer**
  - Security
  - Software

RELATED CASES

2022-823-0

▶ D. Bhardwaj and H. R. Sadjadpour, "Perfect Secrecy in the Bounded Storage Model," 2021 IEEE Global Communications Conference (GLOBECOM), 2021, pp. 1-6, doi: 10.1109/GLOBECOM46510.2021.9685688. - 02/02/2022

University of California, Santa Cruz
Industry Alliances & Technology Commercialization
Kerr 413 / IATC,
Santa Cruz,CA 95064

Tel: 831.459.5415
innovation@ucsc.edu
officeofresearch.ucsc.edu/
Fax: 831.459.1658