UNIVERSITY OF CALIFORNIA SANTA CRUZ OFFICE OF RESEARCH

Extra-Compact Key with Reusable Common Key for Encryption

Tech ID: 33357 / UC Case 2020-289-0

CONTACT

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

INVENTORS

- Sadjadpour, Hamid R.

OTHER INFORMATION

KEYWORDS

cryptographic, cryptography, cryptosystem, security, internet security, digital security, symmetric, asymmetric, encryption, encrypt

CATEGORIZED AS

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

RELATED CASES

2020-289-0

BACKGROUND

A major aim of the field of cryptography is to design cryptosystems that is both provably secure and practical. Symmetric-key (private-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. One-time pad (OTP) is a symmetric-type encryption technique that cannot be cracked, but requires the use of a single-use pre-shared key that is larger than or equal to the size of the message being sent. In this technique, a plaintext is paired with a random secret key (also referred to as OTP).

Asymmetric-type (public-key, asymptotic) frameworks use pairs of keys consisting of a public and private key, and these models depend heavily on the privacy of the non-public key. Asymmetric-based protocols are generally much slower than symmetric approaches in practice. Hypertext Transfer Protocol Secure (HTTPS) protocol which is the backbone of internet security uses the Transport Layer Security (TLS) protocol stack in Transmission Control Protocol / Internet Protocol (TCP/IP) for secure and private data transfer. TLS is a protocol suite that uses a myriad of other protocols to guarantee security. Many of these subprotocols consume a lot of CPU power and are complex processes which are not optimized for big data applications. TLS uses public-key cryptography paradigms to exchange the keys between the communicating parties through the TLS handshake protocol.

Unfortunately, traditional cryptographic algorithms and protocols (including schemes above and incorporating TLS, RSA, and AES) are not well suited in big data applications, as they need to perform a significant number of computations in practice. In turn, cloud providers face increasing CPU processing times and power usage to appropriately maintain services. In the modern computing era with quantum architecture and increased access to network and cloud resources, the speed and integrity of such outmoded cryptographic models will be put to the test.

TECHNOLOGY DESCRIPTION

To overcome these challenges, researchers at UC Santa Cruz (UCSC) have developed a new cryptographic approach with primary aims to reduce decryption complexity. UCSC’s new security paradigm for archival data targets perfect secrecy while featuring an extra-compact key for encryption of data for public exposure, such as cloud storage. In the primary method embodiment, digital data is extracted comprising one or more batches. Each batch includes no more than a number T of packets (T>1) and, each packet contains a number n of bits (n>1). The method generated a random binary matrix common key (CK) consisting of T rows and n columns. For a first batch, a first random n-bit temporary key is generated and positions of the nT elements of matrix CK are randomized to produce randomized matrix CK(RP). Further, the method includes for each digital data packet in the first batch, generating a packet vector key based on non-overlapping pairs of bit positions for both the temporary key and for a row of randomized matrix CK(RP) which corresponds to the number of the packet in the batch. Still further, the method includes generating an encrypted packet for the packet based on the packet and the packet vector key. This modality moves beyond conventional frameworks by providing a substantially higher level of security, including perfect security in some embodiments, with substantially smaller keys than in previous UCSC approaches.

APPLICATIONS

- Digital data security

FEATURES/BENEFITS

- Reduces decryption complexity for big public data/cloud applications.
- As compared to previous work, efficient encryption is achieved without encoding data with an additional bit.
- Does not require any restriction on an eavesdropper storage size or computational capability (both a user and an eavesdropper are assumed to have unlimited storage and computational complexity capabilities).

INTELLECTUAL PROPERTY INFORMATION

Country	Type	Number	Dated	Case
United States Of America	Issued Patent	11,741,268	08/29/2023	2020-289
Patent Cooperation Treaty	Published Application	WO 2021/258109	12/23/2021	2020-289

RELATED MATERIALS

- ▶ Mohsen Karimzadeh Kiskani, Hamid R Sadjadpour, Mohammad Reza Rahimi, and Fred Etemadieh. Low complexity secure code (LCSC) design for big data in cloud storage systems. In Communications (ICC), 2018 International Conference on. IEEE, 2018. - 07/30/2018
- ▶ Mohsen Karimzadeh Kiskani and Hamid R Sadjadpour. Secure and private cloud storage systems with random linear fountain codes. In Cloud and Big Data Computing (CBDCOM), 2017 International Conference on. IEEE, 2017. - 06/28/2018

ADDITIONAL TECHNOLOGIES BY THESE INVENTORS

- ▶ Compact Key with Reusable Common Key for Encryption
- ▶ Interference Management for Concurrent Transmission in Downlink Wireless Communications
- ▶ Compact Key Encoding of Data for Public Exposure Such As Cloud Storage

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

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