Compact Key Encoding of Data for Public Exposure Such As Cloud Storage

Tech ID: 33440 / UC Case 2018-391-0

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 improved cryptographic approaches to reduce decryption complexity while providing a substantially higher level of security for distributed cloud storage system and other applications. This new UCSC modality moves beyond conventional frameworks using substantially smaller keys than in previous UCSC approaches (or some combination) and achieves perfect security in some embodiments.

In the primary method embodiment, the method includes extracting first digital data comprising a number n of portions called chunks, each chunk containing a number Q of bits, wherein n=2(Q+1). The method also includes determining a first random value for mapping each chunk to only one batch of M numbered batches of two or more chunks of the n chunks, and storing securely second digital data that indicates the mapping. Furthermore, the method includes determining a second independent random value for a key containing Q+1 bits. The method further includes combining a bit based on a bit from the key with each chunk of a next batch of chunks to produce a next batch of enhanced chunks. Each enhanced chunk contains Q+1 bits and each enhanced chunk of the next batch of enhanced chunks has a bit based on the bit from the key at a location based on a number of the next chunk. The method still further includes repeating said combining step with each non-overlapping batch of chunks to produce non-overlapping enhanced chunks. Each enhanced chunk of the non-overlapping batch of enhanced chunks has a bit based on a different bit from the key. The method yet further includes combining a unique set of the enhanced chunks with a bit by bit exclusive OR operation to produce an encoded chunk so that every bit of the encoded chunk is

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, cloud, cloud security

CATEGORIZED AS

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

RELATED CASES

2018-391-0

based at least in part on a bit from the key. Still further, the method includes storing securely third data that indicates an encoding vector b that indicates the unique set of enhanced chunks combined. Even further still, the method includes causing the encoded chunk to be exposed publicly.

APPLICATIONS

- Digital data security

FEATURES/BENEFITS

- Perfect secrecy in clouds can be achieved with much smaller key size than the file size.
- Size of the compact key is much less than the size of the plaintext data being encoded as chunks.
- Techniques focus on perfect secrecy instead of merely asymptotic perfect secrecy (achieving perfect secrecy asymptotically as the key size increases).

INTELLECTUAL PROPERTY INFORMATION

Country	Type	Number	Dated	Case
United States Of America	Issued Patent	11,334,676	05/17/2022	2018-391

RELATED MATERIALS

- 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
- Mohsen Karimzadeh Kiskani and Hamid R Sadjadpour. Secure coded caching in wireless ad hoc networks. In Computing, Networking and Communications (ICNC), 2017 International Conference on, pages 387-391. IEEE, 2017. - 03/13/2017
- Mohsen Karimzadeh Kiskani and Hamid R Sadjadpour. Throughput analysis of decentralized coded content caching in cellular networks. IEEE Transactions on Wireless Communications, 16(1):663-672, 2017. - 11/11/2016

ADDITIONAL TECHNOLOGIES BY THESE INVENTORS

- Compact Key with Reusable Common Key for Encryption
- Extra-Compact Key with Reusable Common Key for Encryption
- Interference Management for Concurrent Transmission in Downlink Wireless Communications

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