Compact Key with Reusable Common Key for Encryption

Tech ID: 33371 / UC Case 2019-506-0

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, 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 also includes generating a random binary matrix A consisting of T rows and n columns. For a first batch, a secret first random n-bit temporary key is generated. Further, the method includes, for each packet in the first batch, generating a first packet vector key with each element j=1 to n of the first packet vector key equal to an element from the temporary key combined using an exclusive OR function with a corresponding element from a first packet-corresponding row of matrix A, generating a first encrypted packet based on the first packet and the first packet vector key, and causing the first encrypted packet to be exposed publicly.

APPLICATIONS

- Digital data security

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

2019-506-0

FEATURES/BENEFITS

- Perfect secrecy in clouds can be achieved with much smaller key size than the file size.
- 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	Published Application	20200320227	10/08/2020	2019-506

RELATED MATERIALS

- Kiskani, M. K., Sadjadpour, H. R., Rahimi, M. R., & Etemadieh, F. (2018, May). Low complexity secure code (LCSC) design for big data in cloud storage systems. In 2018 IEEE International Conference on Communications (ICC) (pp. 1-7). IEEE. - 07/30/2018
- Kiskani, M. K., & Sadjadpour, H. R. (2017, August). Secure and private cloud storage systems with random linear fountain codes. In 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI) (pp. 1-8). IEEE. - 06/28/2018

ADDITIONAL TECHNOLOGIES BY THESE INVENTORS

- Extra-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

© 2023, The Regents of the University of California
Terms of use
Privacy Notice