Privacy Preserving (Outsourced) Data Share and Search

Dr. Kaitai Liang

Surrey Centre for Cyber Security,
Department of Computer Science, University of Surrey.

December 13, 2017

Outline

About Me - Study Background

- Post-doc & PhD: Computer Science - applied cryptography; City U
- M.Sc.: Computer Applied Technology; SCAU
- B.Eng.: Software Engineering; SCAU

About Me - Research Background

Figure : Research Interests

About Me - Research Background

Government/Industrial projects as key member (past 3 years):

- Privacy-aware retrieval and modelling of genomic data (Academy of Finland).
- Secure data sharing in cloud computing environment (A*STAR, Singapore).
- Practical unified framework for secure E-consent mechanism for health records (Australian Research Council Linkage Project).
- On the theory and application of attribute-based cryptography (Research Grants Council of Hong Kong).

About Me - Research Background

Research Collaborations

- Europe: University College London; Sapienza University of Rome; COSIC, KU LEUVEN; University of Padua,
- Australia: Monash University; University of South Australia; Deakin University; University of Wollongong,
- Singapore: Institute for Infocomm Research; Nanyang Technological University; Singapore Management University; Huawei Singapore Research,
- Japan: Japan Advanced Institute of Science and Technology; Osaka University,

About SCCS

Personal Data - out of physical control

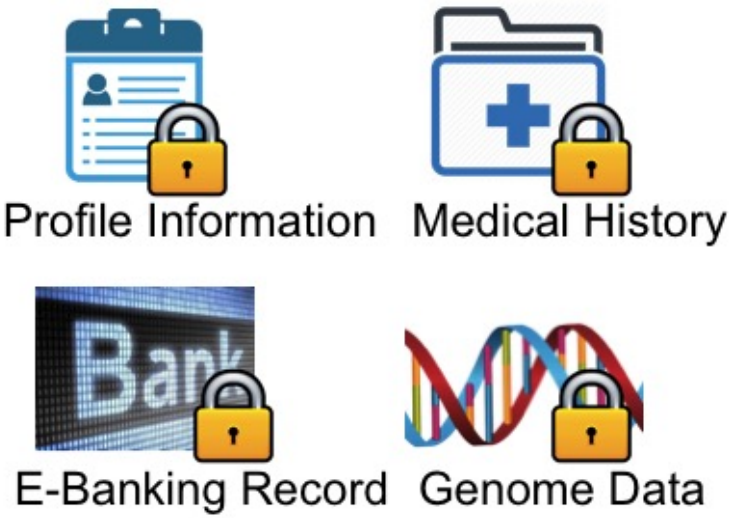

Figure : Encrypted Personal Data

A great amount of personal data is flooding in the Internet. To protect the confidentiality of the personal data, we may need encryption technology.

Encryption $\stackrel{?}{=}$ Practical

Figure : Encryption may Hinder Some Further Operations

Encryption technique, however, may yield some inconvenience.

Share Encrypted Outsourced Data

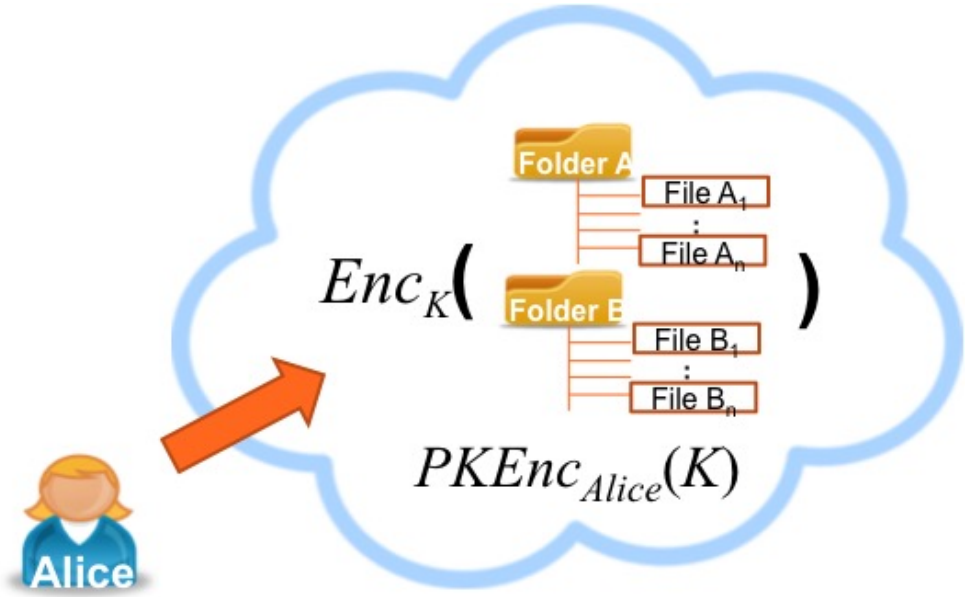

Figure : Outsource Encrypted Personal Data

Suppose Alice outsources her encrypted local data and the encrypted encryption/decryption key K to a cloud, and only stores her secret key sk in local.

Share Encrypted Outsourced Data

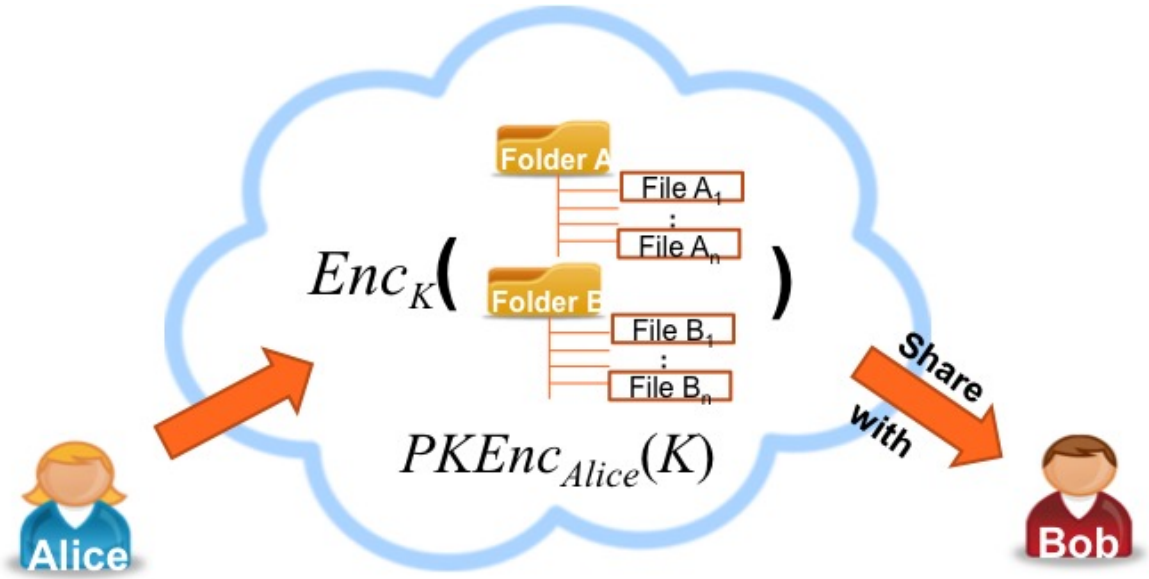

Figure : Share Encrypted Personal Data

Alice would like to share some of her files (stored in the cloud) with Bob.

Share Encrypted Outsourced Data - Naive solutions.

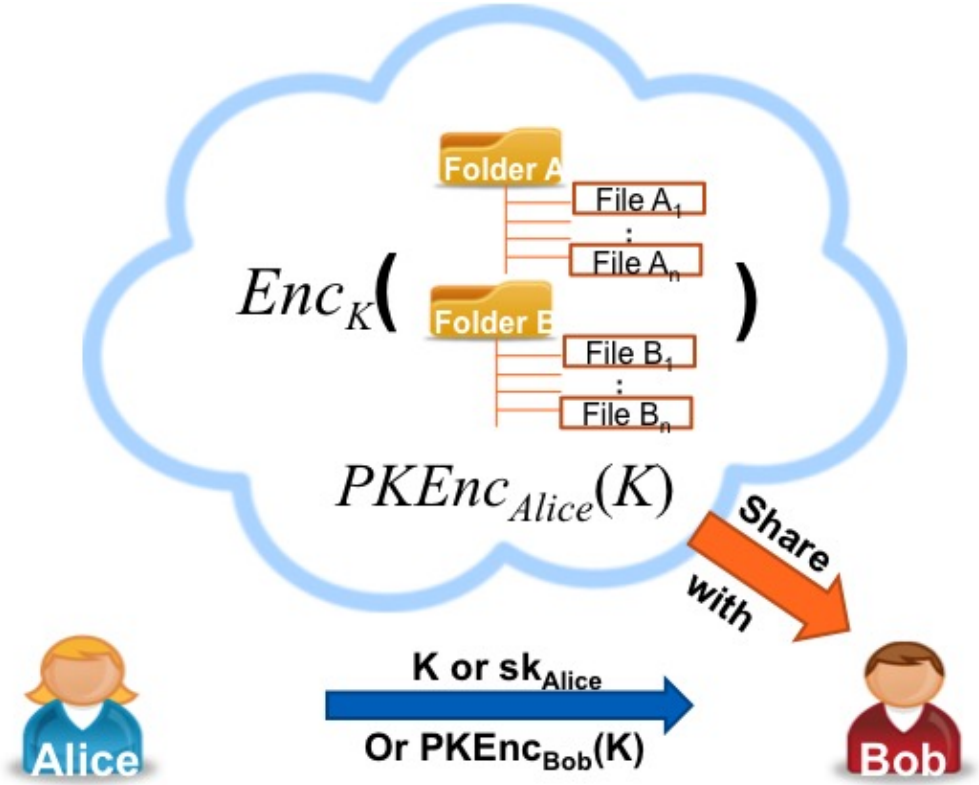

Figure : Share Encrypted Personal Data

Proxy Re-Encryption - Brief

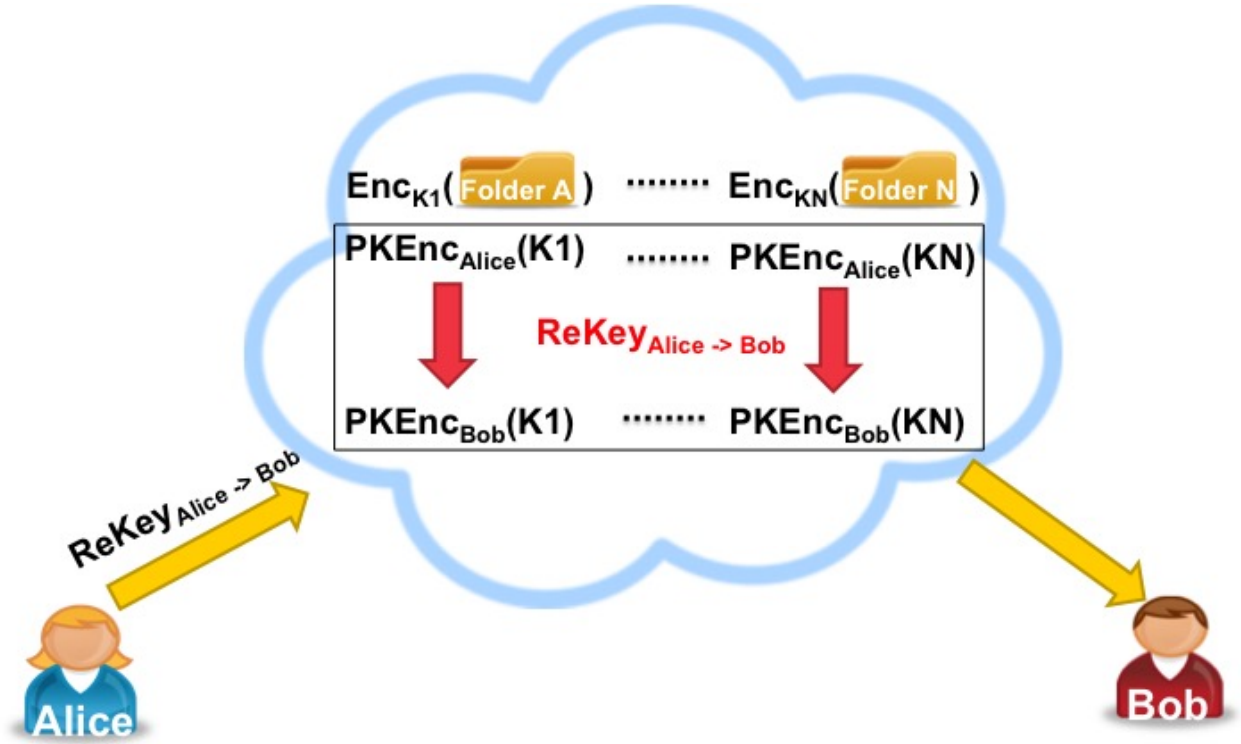

Figure : Proxy Re-Encryption

An effective and efficient technique.

Proxy Re-Encryption - History

Nearly two decades study:

- 1998 - M. Blaze, G. Bleumer and M. Strauss, "Divertible Protocols and Atomic Proxy Cryptography" (EUROCRYPT 98).
- 1999 - Markus Jakobsson, "On Quorum Controlled Asymmetric Proxy Re-encryption" (PKC 99).
- 2000 - 2010: variants of Proxy Re-encryption: Identity-based, broadcast-based, properties.
- 2010 - 2016: attribute-based, function-based.

Note that there is a proxy re-encryption library, JHU-MIT Proxy Re-encryption Library ("http://spar.isi.jhu.edu/ mgreen/prl/").

Proxy Re-Encryption - A Closer Look - Main Technique

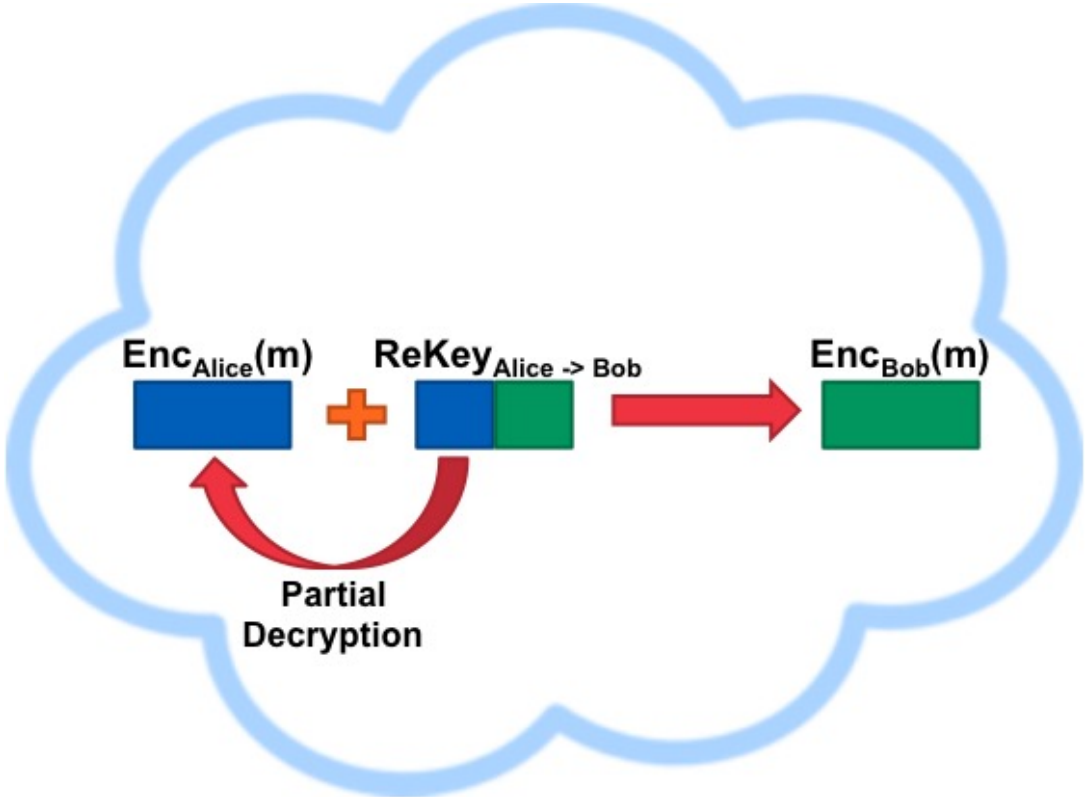

Figure : Proxy Re-Encryption Main Technique

Proxy Re-Encryption - A Closer Look - Properties

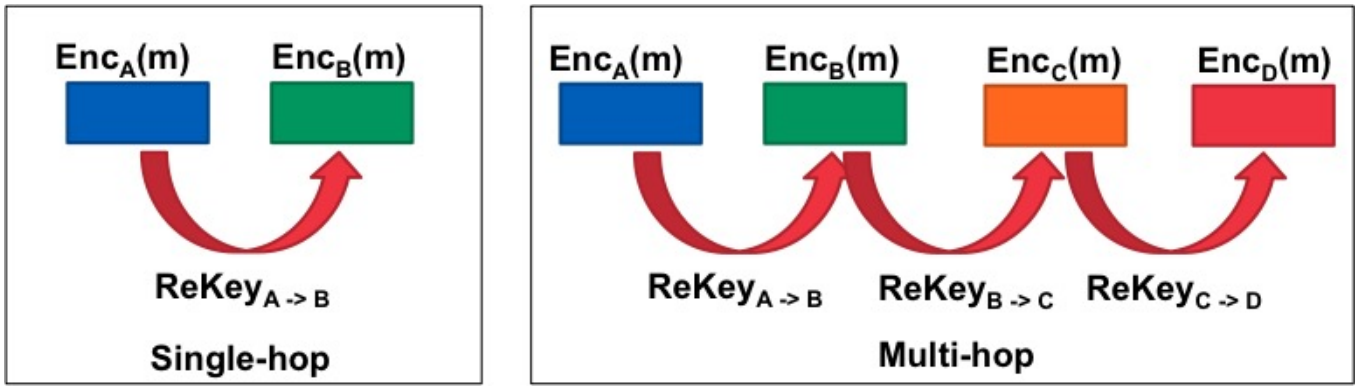

Figure : Proxy Re-Encryption Properties

Proxy Re-Encryption - A Closer Look - Properties

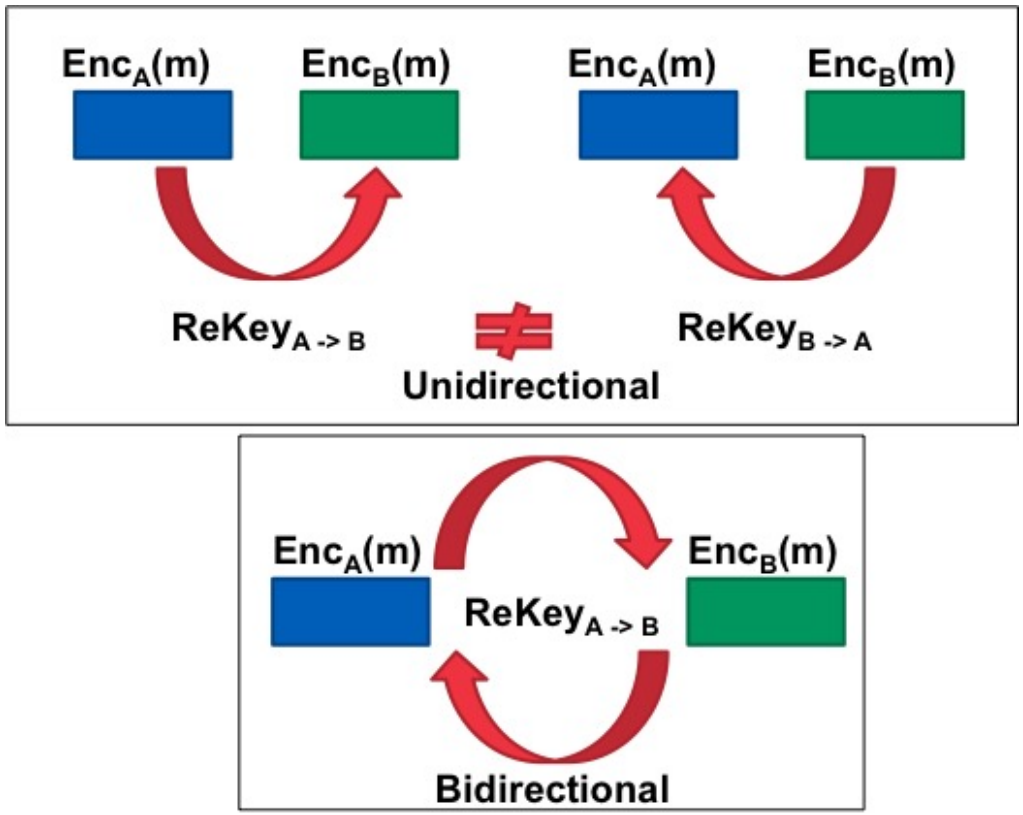

Figure : Proxy Re-Encryption Properties

Proxy Re-Encryption - A Closer Look - Security

- Security for original ciphertext
- Security for re-encrypted ciphertext
- Security for master secret key/collusion attacks

Proxy Re-Encryption - What I've Done

- PKE-PRE[1]
- IBE-PRE[2]
- ABE-PRE[3]
- FE-PRE[4]

[1] e.g., Jun Shao, Rongxing Lu, Xiaodong Lin, Kaitai Liang:Secure bidirectional proxy re-encryption for cryptographic cloud storage. Pervasive and Mobile Computing 28: 113-121 (2016)

[2] e.g., Kaitai Liang, Joseph K. Liu, Duncan S. Wong, Willy Susilo:An Efficient Cloud-Based Revocable Identity-Based Proxy Re-encryption Scheme for Public Clouds Data Sharing. ESORICS (1) 2014: 257-272

[3] e.g., Kaitai Liang, Man Ho Au, Joseph K. Liu, Willy Susilo, Duncan S. Wong, Guomin Yang, Yong Yu, Anjia Yang: A secure and efficient Ciphertext-Policy Attribute-Based Proxy Re-Encryption for cloud data sharing. Future Generation Comp. Syst. 52: 95-108 (2015)

[4] e.g., Kaitai Liang, Man Ho Au, Joseph K. Liu, Willy Susilo, Duncan S. Wong, Guomin Yang, Tran Viet Xuan Phuong, Qi Xie: A DFA-Based Functional Proxy Re-Encryption Scheme for Secure Public Cloud Data Sharing. IEEE Trans. Information Forensics and Security 9(10): 1667-1680 (2014)

Search Encrypted Outsourced Data - Naive Solutions

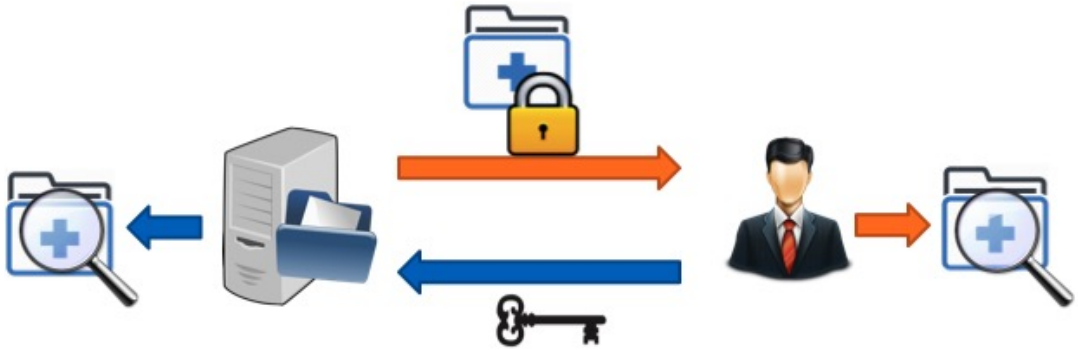

Figure : Search Encrypted Data

Searchable Encryption - Brief

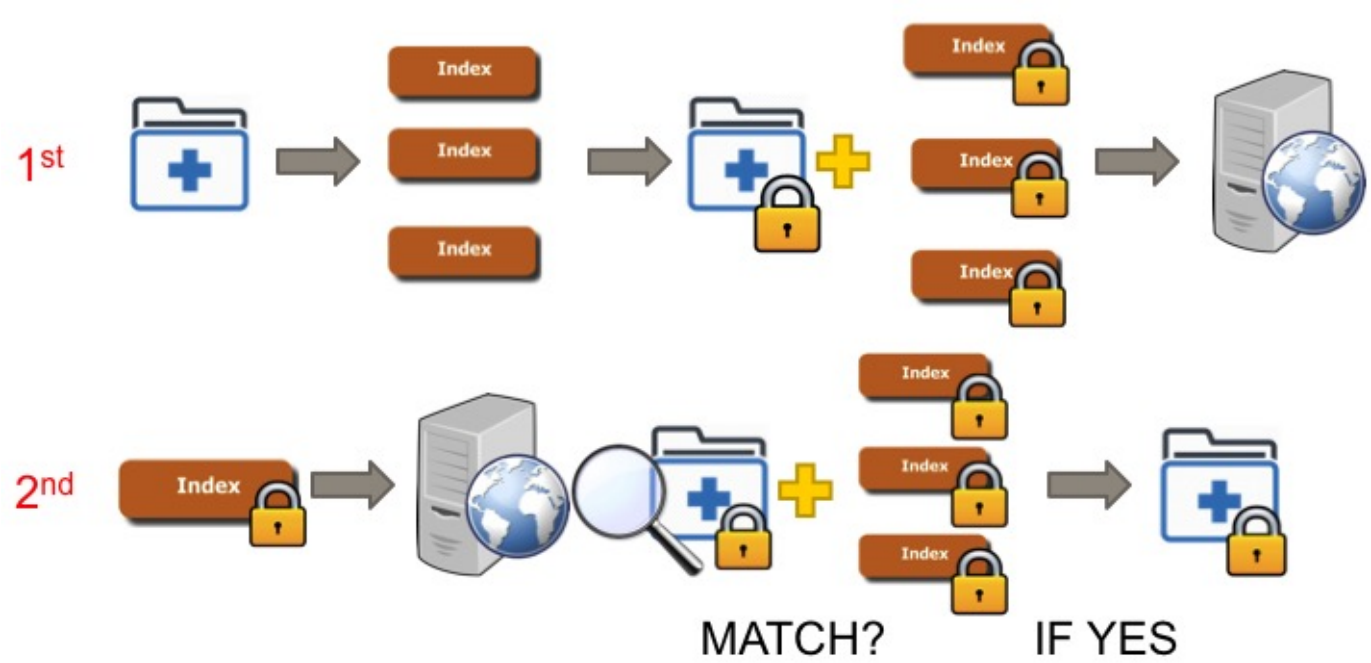

Figure : Searchable Encryption

Searchable Encryption - Branches

- Symmetric searchable encryption: [Goh03], [CM05], [CGKO06], [LSD+10], [CJJ+13]..
- Asymmetric searchable encryption: [BCOP04], [Abdalla+08], [BNS06], [Khader07], [ZI09], [BW07],[ZXA14]

Searchable Encryption - Main Technique

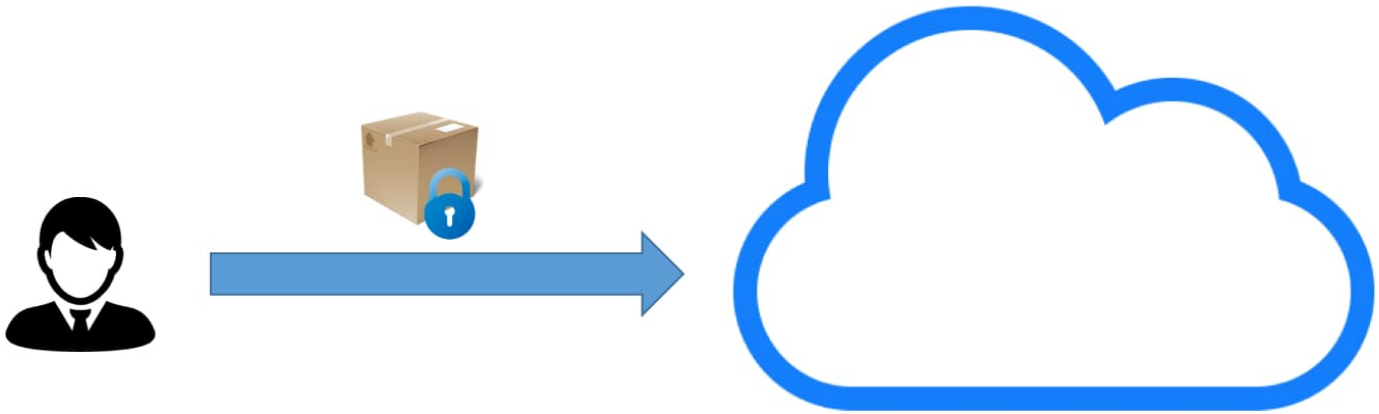

Figure : Searchable Encryption

Searchable Encryption - Main Technique

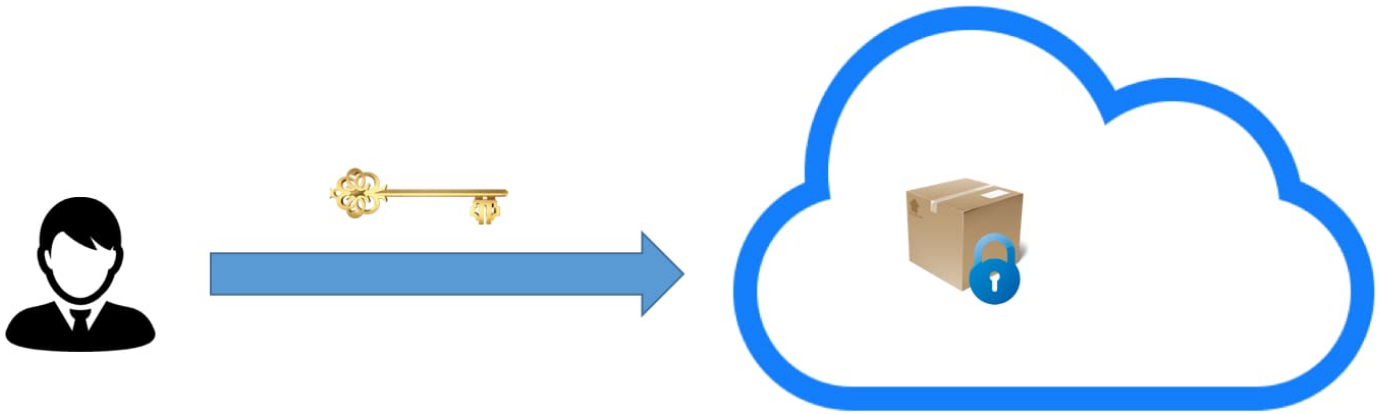

Figure : Searchable Encryption

Searchable Encryption - Main Technique

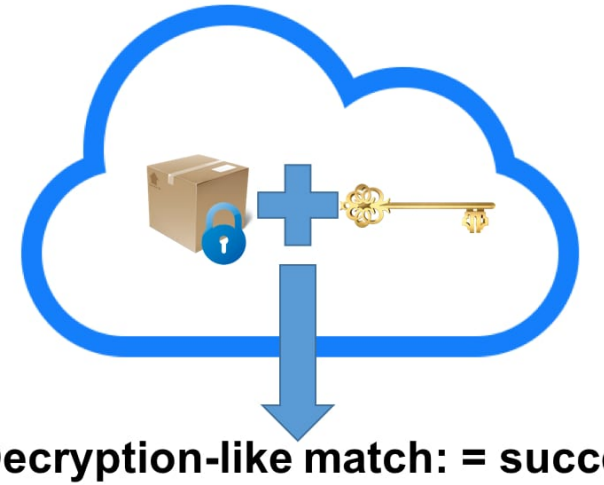

Figure : Searchable Encryption

Searchable Encryption - Main Technique

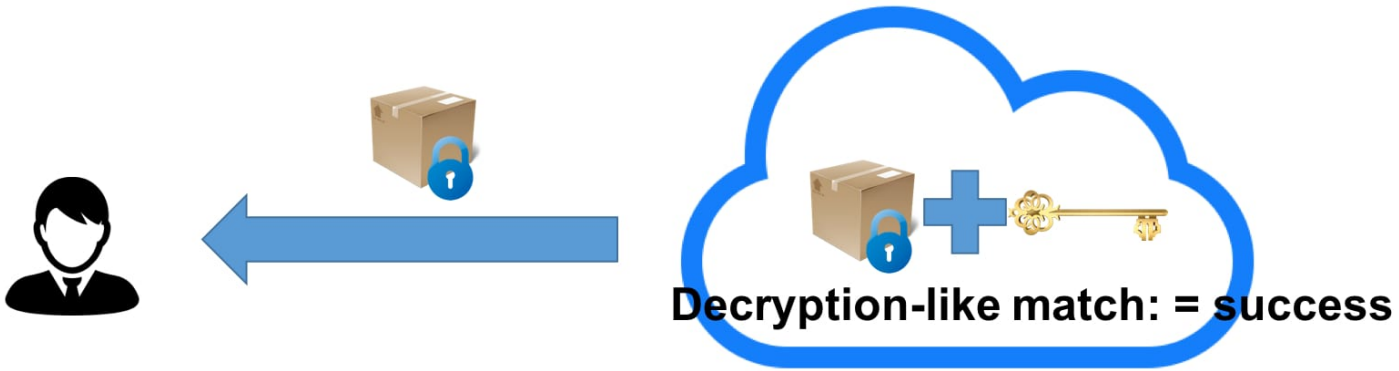

Figure : Searchable Encryption

Searchable Encryption - Security

- Keyword privacy.
- Search pattern.
- Access pattern.

Searchable Encryption - What I've Done

- SE-PRE[5]
- SE-ABE[6]
- Expressive SE[7]
- Attacks on SE[8]

[5] e.g., Joseph K. Liu, Man Ho Au, Willy Susilo, Kaitai Liang, Rongxing Lu, Bala Srinivasan:Secure sharing and searching for real-time video data in mobile cloud. IEEE Network 29(2): 46-50 (2015)

[6] e.g., Kaitai Liang, Willy Susilo: Searchable Attribute-Based Mechanism With Efficient Data Sharing for Secure Cloud Storage. IEEE Trans. Information Forensics and Security 10(9): 1981-1992 (2015)

[7] e.g., Kaitai Liang, Xinyi Huang, Fuchun Guo, Joseph K. Liu: Privacy-Preserving and Regular Language Search Over Encrypted Cloud Data. IEEE Trans. Information Forensics and Security 11(10): 2365-2376 (2016)

[8] e.g., ongoing works

Potential Topics

1. Build bridges among encryptions.
2. Post-quantum crypto in trusted computing and blockchain.
3. Machine learning + cybersecurity.
4. Side channel SSE attacks.

Thank you: Q&A

Contact Email: k.liang@surrey.ac.uk

References

bdalla+08 Michel Abdalla, Mihir Bellare, Dario Catalano, Eike Kiltz, Tadayoshi Kohno, Tanja Lange, John Malone-Lee, Gregory Neven, Pascal Paillier, and Haixia Shi. Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions. Journal of Cryptology 21, 3 (2008), 350391.

BCOP04 Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public key encryption with keyword search. In EUROCRYPT (LNCS), Vol. 3027. 506522.

BW07 Dan Boneh and Brent Waters. Conjunctive, subset, and range queries on encrypted data. In TCC (LNCS), Vol. 4392. Springer, 535554.

Goh03 Eu-Jin Goh. 2003. Secure Indexes. Cryptology ePrint Archive, Report 2003/216. (2003). http://eprint.iacr.org/2003/216/.

References

CM05 Yan-Cheng Chang and Michael Mitzenmacher. Privacy preserving keyword searches on remote encrypted data. In (ACNS). 442455.

CGKO06 Reza Curtmola, Juan Garay, Seny Kamara, and Rafail Ostrovsky. 2006. Searchable symmetric encryption: Improved definitions and efficient constructions. In CCS. ACM, New York, NY, 7988. DOI:http://dx.doi.org/10.1145/1180405.1180417

LSD+10 Peter van Liesdonk, Saeed Sedghi, Jeroen Doumen, Pieter H. Hartel, and Willem Jonker. Computationally efficient searchable symmetric encryption. In SDM (LNCS), Vol. 6358. Springer, 87100.

CJJ+13 David Cash, Stanislaw Jarecki, Charanjit S. Jutla, Hugo Krawczyk, Marcel Rosu, and Michael Steiner. 2013. Highly-Scalable searchable symmetric encryption with support

References

Khader07 Dalia Khader. Public key encryption with keyword search based on k-resilient IBE. In ICCSA (LNCS), Vol. 4707. Springer, 10861095.

ZI09 Rui Zhang and Hideki Imai. Combining public key encryption with keyword search and public key encryption. IEICE Transactions 92-D, 5 (2009), 888896.

ZXA14 Q. Zheng, S. Xu, and G. Ateniese. VABKS: verifiable attribute-based keyword search over outsourced encrypted data. In INFOCOM, pp. 522530.