Re-encryption - perspectives in cryptography

Gyöngyvér MÁRTON

Department of Mathematics-Informatics, Sapientia Hungarian University of Transylvania

mgyongyi@ms.sapientia.ro

Re-encryption is a relatively new cryptography primitive that enables re-encryption of ciphertexts from one secret key to another without relying on trusted parties. Trough this process cannot learn anything about the original plaintext. In this lecture firstly we shall present the necessary theory which contribute to re-encryption, secondly we shall show our results.

References

[1] Video Surveillance: A Distributed Approach to protect Privacy. Martin Schaffer, Peter Schartner. Proceedings of the 9th IFIP TC-6 TC-11 international conference on Communications and Multimedia Security. (2005)

[2] Key-Private Proxy Re-Encryption. Giuseppe Ateniese, Karyn Benson, Susan Hohenberger. Proceedings of the The Cryptographers' Track at the RSA Conference (2009)

[3] Efficient Unidirectional Proxy Re-Encryption. Sherman S.M. Chow, Jian Weng, Yanjiang Yang, Robert H. Deng. Proceedings of the Third international conference on Cryptology in Africa (2010)