Encrypted Messages from the Heights of Cryptomania

Craig Gentry

IBM T.J. Watson Research Center,
Yorktown Heights, New York, USA

How flexible can encryption be? This question motivated the invention of public key encryption that began modern cryptography. A lot has happened since then. I will focus on two lines of research that I find especially interesting (mainly the second) and the mysterious gap between them.

The first line of research asks: how flexibly can encryption handle computation? The answer seems to be "very flexibly". We have fully homomorphic encryption (FHE) schemes [RAD78, Gen09, DGHV10, BV11b, GH11, BV11a] that allow a worker (non-interactively) to do arbitrary blind processing of encrypted data without obtaining access to the data. However, current FHE schemes do not handle access control flexibly; there is only one keyholder, and only it can decrypt.

The second line of research asks: how flexibly can encryption handle access control? Again, the answer seems to be "very flexibly". Building on Garg et al.'s [GGH12b] approximate multilinear maps, we now have attribute-based encryption (ABE) schemes for arbitrary circuits [SW12, GGH12a] that allow an encrypter (non-interactively) to embed an arbitrarily complex access policy into its ciphertext, such that only users whose keys are associated to a satisfying set of attributes can (non-interactively) decrypt. We can be even more flexible: Garg et al. [GGSW12] describe a "witness encryption" scheme where a user's decryption key is not really a key at all, but rather a witness for some arbitrary NP relation specified by the encrypter (the encrypter itself may not know a witness). However, current ABE and witness encryption schemes do not handle computation flexibly; the decrypter recovers the encrypter's message, unmodified.

In between, we have concepts like obfuscation and functional encryption that attempt to handle computation and access control simultaneously – in particular, by allowing the user to learn a prescribed function only of the user's input (similar to ABE), while hiding all intermediate values of the computation (similar to FHE). Here, it seems that we finally have reached the edge of Cryptomania, as we bump against impossibility results [BGI$^+$01, vDJ10, BSW11, AGVW12]. However, the precise contours of the boundary between possible and impossible remain unknown.

In this talk, I will focus mostly on the recent positive results in the second line of research, showing how a somewhat homomorphic variant of the NTRU encryption scheme leads quite naturally to Garg et al.'s approximate multilinear maps, and describing how to use multilinear maps to construct witness encryption.

A. Sahai (Ed.): TCC 2013, LNCS 7785, pp. 120–121, 2013.

Regarding obfuscation, functional encryption, and the boundary between possible and impossible, I only promise to leave you with intriguing questions.

References

[AGVW12] Agrawal, S., Gorbunov, S., Vaikuntanathan, V., Wee, H.: Functional encryption: New perspectives and lower bounds. IACR Cryptology ePrint Archive, 2012:468 (2012)

[BGI+01] Barak, B., Goldreich, O., Impagliazzo, R., Rudich, S., Sahai, A., Vadhan, S.P., Yang, K.: On the (Im)possibility of Obfuscating Programs. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 1–18. Springer, Heidelberg (2001)

[BSW11] Boneh, D., Sahai, A., Waters, B.: Functional Encryption: Definitions and Challenges. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 253–273. Springer, Heidelberg (2011)

[BV11a] Brakerski, Z., Vaikuntanathan, V.: Efficient fully homomorphic encryption from (standard) LWE. In: FOCS 2011. IEEE Computer Society (2011)

[BV11b] Brakerski, Z., Vaikuntanathan, V.: Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 505–524. Springer, Heidelberg (2011)

[DGHV10] van Dijk, M., Gentry, C., Halevi, S., Vaikuntanathan, V.: Fully Homomorphic Encryption over the Integers. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 24–43. Springer, Heidelberg (2010), Full version available online from `http://eprint.iacr.org/2009/616`

[Gen09] Gentry, C.: Fully homomorphic encryption using ideal lattices. In: Mitzenmacher, M. (ed.) STOC, pp. 169–178. ACM (2009)

[GGH12a] Garg, S., Gentry, C., Halevi, S.: Attribute based encryption for general circuits (2012) (manuscript)

[GGH12b] Garg, S., Gentry, C., Halevi, S.: Candidate multilinear maps from ideal lattices and applications. Cryptology ePrint Archive, Report 2012/610 (2012), `http://eprint.iacr.org/`

[GGSW12] Garg, S., Gentry, C., Sahai, A., Waters, B.: Witness encryption and its applications (2012) (manuscript)

[GH11] Gentry, C., Halevi, S.: Implementing Gentry's Fully-Homomorphic Encryption Scheme. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 129–148. Springer, Heidelberg (2011)

[RAD78] Rivest, R., Adleman, L., Dertouzos, M.L.: On data banks and privacy homomorphisms. In: Foundations of Secure Computation, pp. 169–180 (1978)

[SW12] Sahai, A., Waters, B.: Attribute-based encryption for circuits from multilinear maps. Cryptology ePrint Archive, Report 2012/592 (2012), `http://eprint.iacr.org/`

[vDJ10] van Dijk, M., Juels, A.: On the impossibility of cryptography alone for privacy-preserving cloud computing. IACR Cryptology ePrint Archive, 2010:305 (2010)