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

References

[AGVW12] Shweta Agrawal, Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Functional encryption: New perspectives and lower bounds. *IACR Cryptology ePrint Archive*, 2012:468, 2012.

[BGI$^+$01] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil P. Vadhan, and Ke Yang. On the (im)possibility of obfuscating programs. In Joe Kilian, editor, *CRYPTO*, volume 2139 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2001.

[BSW11] Dan Boneh, Amit Sahai, and Brent Waters. Functional encryption: Definitions and challenges. In *TCC*, pages 253–273, 2011.

[BV11a] Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. In *FOCS'11*. IEEE Computer Society, 2011.

[BV11b] Zvika Brakerski and Vinod Vaikuntanathan. Fully homomorphic encryption from ring-LWE and security for key dependent messages. In *Advances in Cryptology - CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 505–524. Springer, 2011.

[DGHV10] Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. Fully homomorphic encryption over the integers. In *Advances in Cryptology - EUROCRYPT'10*, volume 6110 of *Lecture Notes in Computer Science*, pages 24–43. Springer, 2010. Full version available on-line from http://eprint.iacr.org/2009/616.

[Gen09] Craig Gentry. Fully homomorphic encryption using ideal lattices. In Michael Mitzenmacher, editor, *STOC*, pages 169–178. ACM, 2009.

[GGH12a] Sanjam Garg, Craig Gentry, and Shai Halevi. Attribute based encryption for general circuits. Manuscript, 2012.

[GGH12b] Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate multilinear maps from ideal lattices and applications. Cryptology ePrint Archive, Report 2012/610, 2012. http://eprint.iacr.org/.

[GGSW12] Sanjam Garg, Craig Gentry, Amit Sahai, and Brent Waters. Witness encryption and its applications. Manuscript, 2012.

[GH11] Craig Gentry and Shai Halevi. Implementing gentry's fully-homomorphic encryption scheme. In Kenneth G. Paterson, editor, *EUROCRYPT*, volume 6632 of *Lecture Notes in Computer Science*, pages 129–148. Springer, 2011.

[RAD78] Ron Rivest, Leonard Adleman, and Michael L. Dertouzos. On data banks and privacy homomorphisms. In *Foundations of Secure Computation*, pages 169–180, 1978.

[SW12] Amit Sahai and Brent Waters. Attribute-based encryption for circuits from multilinear maps. Cryptology ePrint Archive, Report 2012/592, 2012. http://eprint.iacr.org/.

[vDJ10] Marten van Dijk and Ari Juels. On the impossibility of cryptography alone for privacy-preserving cloud computing. *IACR Cryptology ePrint Archive*, 2010:305, 2010.