Functional Encryption: Origins and Recent Developments

Brent Waters[1] *

The University of Texas at Austin
bwaters@cs.utexas.edu

Abstract. In this talk, we will present the notion of functional encryption and recent progress in the area. We will begin by describing the concept and origins of functional encryption. Next, we will describe intuitively why current bilinear map based constructions appear to be "stuck" with boolean formula type functionality even in the public index setting. Finally, we will see some very recent work that uses multilinear forms to move beyond these barriers and achieve functionality for any circuit.

Overview

Encryption is a method to encode data such that it can only be understood by a recipient that holds a certain private key object. The traditional notion of public key encryption [10, 11, 21, 13] is that a data owner will encrypt data to the public key of a specific targeted user to create a ciphertext. Later, a user possessing the corresponding private key can decrypt the ciphertext to obtain the original data. Ingrained in this notion is that: (1) *Encryption is a method to target to a specific user.* (2) *Decryption is an all or nothing operation; either a ciphertext is fully decrypted and the original data is recovered or else it fails and nothing is learned.*

Functional encryption is a new vision of encryption that moves pass these barriers. In a Functional Encryption system what a user learns from decryption is determined by a function of the encrypted data and the user's secret key descriptor (as issued by some authority). Briefly, in a functional encryption system with functionality $F(\cdot, \cdot)$ a user is issued a secret key sk_k for value k by some authority. Suppose that a ciphertext ct is the encryption of data x. The user can apply their secret key to learn $F(k, x)$.

Functional encryption for expressive functionalities open up a wide variety of applications. For instance, one might determine access to encrypted data based on an arbitrary policy over a user's credentials. Another possibility is that encrypted data could consist of images and a user's private key of their headshot.

* Supported by NSF CNS-0915361 and CNS-0952692, CNS-1228599 DARPA through the U.S. Office of Naval Research under Contract N00014-11-1-0382, DARPA N11AP20006, Google Faculty Research award, the Alfred P. Sloan Fellowship, and Microsoft Faculty Fellowship, and Packard Foundation Fellowship.

The user would be able to view the image only if their face appeared in it as determined by some vision recognition algorithm. Moreover, the functionality could blur out parts of the image not immediately surrounding the user's body. In a medical research environment, one could consider encrypting a large database containing medical histories of patients coupled with DNA sequencing. Later, if a researcher is granted permission to test a correlation between a certain type of cancer and genotype they could be given a secret key that divulges the correlation and nothing else.

Origins of Functional Encryption

The origins of functional encryption can be traced to the concept of Attribute-Based Encryption (ABE) [23] proposed by Sahai and Waters. In a (Key-Policy) ABE scheme a ciphertext contains a hidden message as well as (unhidden) metadata or attributes. A user's private key is associated with a formula ϕ. A user can decrypt a given ciphertext and recover the hidden message if and only if the formula is satisfied when its values are assigned according to the metadata. A technical lynchpin was the concept that any secure system must be *collusion resistant*. Suppose an attacker obtains multiple secret keys, e.g., $\mathrm{sk}_k, \mathrm{sk}_{k'}$. In particular, the attacker should not be able to combine two private keys to decrypt ciphertexts that neither private key was authorized for.

While Attribute-Based Encryption moves beyond the notion of encrypting to a particular user, decryption is still an all or nothing proposition. In subsequent works [6, 16] the concept evolved to hide the metadata. The notion of Functional Encryption first appeared in presentation slides prepared by Sahai and Waters in 2008 [24] and was described during talks given by both authors. Significant conceptual work was done while both Sahai and Waters were researchers at IPAM for the 2006 Securing Cyberspace program. The term functional encryption first appeared in a published research paper by Lewko et. al. [17]. Finally, a definitional framework for functional encryption was put forward by Boneh, Sahai, and Waters [5] where they put forward both simulation and indistinguishability definitions.[1] The above work was influenced by concepts such as Identity-Based Encryption (IBE) [26, 4, 9] and Anonymous IBE [3, 1].

Achieving Stronger Functionality

Over the past several years there has been significant research activity on a variety directions in functional encryption including proofs of adaptive security [17, 19], revocation of secret keys [2, 22], policies across multiple authorities [7, 8, 18], and investigation of definitions [5, 20]. *Arguably, the most important question is what functionality can we achieve.* For several years the strongest form of expression we had was boolean formulas[2] in ABE cryptosystems. While boolean

[1] Concurrently, with [5] and subsequent to discussions stemming from [24], O'Neill [20] also put forward general definitions for functional encryption.

[2] Technically, one can obtain span programs.

formula ABE systems give rise to several interesting applications, they are still a far cry from being able to express access control in the form of any program or circuit.

In this talk we will first explore the techniques that give rise to ABE systems for boolean formulas. Our starting point will be the "Key-Policy" ABE system of Goyal et. al. [15]. We will see how they use bilinear maps as the primary mechanism for decryption blended with interpolation in the exponent techniques. Together these give the boolean formula functionality and the needed protection against collusion attacks. We also give insight into the difficulty of obtaining stronger functionality using bilinear maps by arguing why such constructions are "stuck" at the level of boolean formulas. Intuitively, the bilinear map mechanism is "used up" in pairing the ciphertext with the secret key to prevent collusions between different users. However, this leaves natural larger fanout generalizations of GPSW to so called backtracking attacks.

We will next describe some very recent progress [25] that obtains Attribute-Based Encryption for circuits. Obtaining ABE for circuits is a major jump in that circuits can express any program of fixed running time. The new result is obtained by applying the recent work of Garg, Gentry, and Halevi [12] which describes some approximation of groups with multilinear maps. The new ABE crypto leverages these multilinear forms to create a new "move forward and shift" technique for decryption that replaces and subsumes the prior methods. Independently, Gorbunov, Vaikuntanathan and Wee [14] obtained the same result under the Learning with Error (LWE) assumption. They create a set of novel and elegant techniques to combat the backtracking issue. We refer the reader to the introduction of [25] for further discussion of backtracking attacks and how these are circumvented by new techniques.

References

1. 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. *J. Cryptology*, 21(3):350–391, 2008.
2. Alexandra Boldyreva, Vipul Goyal, and Virendra Kumar. Identity-based encryption with efficient revocation. In *ACM Conference on Computer and Communications Security*, pages 417–426, 2008.
3. Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public key encryption with keyword search. In *EUROCRYPT*, pages 506–522, 2004.
4. Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. *SIAM J. Comput.*, 32(3):586–615, 2003. extended abstract in Crypto 2001.
5. Dan Boneh, Amit Sahai, and Brent Waters. Functional encryption: Definitions and challenges. In *TCC*, pages 253–273, 2011.
6. Dan Boneh and Brent Waters. Conjunctive, subset, and range queries on encrypted data. In *TCC*, pages 535–554, 2007.

7. Melissa Chase. Multi-authority attribute based encryption. In *TCC*, pages 515–534, 2007.
8. Melissa Chase and Sherman S. M. Chow. Improving privacy and security in multi-authority attribute-based encryption. In *ACM Conference on Computer and Communications Security*, pages 121–130, 2009.
9. Clifford Cocks. An identity based encryption scheme based on quadratic residues. In *IMA Int. Conf.*, pages 360–363, 2001.
10. Whitfield Diffie and Martin E. Hellman. Multiuser cryptographic techniques. In *AFIPS National Computer Conference*, pages 109–112, 1976.
11. Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976.
12. 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/`.
13. S. Goldwasser and S. Micali. Probabilistic encryption. *Jour. of Computer and System Science*, 28(2):270–299, 1984.
14. Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Personal Communication, 2012.
15. Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *ACM Conference on Computer and Communications Security*, pages 89–98, 2006.
16. Jonathan Katz, Amit Sahai, and Brent Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In *EUROCRYPT*, pages 146–162, 2008.
17. Allison B. Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In *EUROCRYPT*, pages 62–91, 2010.
18. Allison B. Lewko and Brent Waters. Decentralizing attribute-based encryption. In *EUROCRYPT*, pages 568–588, 2011.
19. Tatsuaki Okamoto and Katsuyuki Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In *CRYPTO*, pages 191–208, 2010.
20. Adam O'Neill. Definitional issues in functional encryption. Cryptology ePrint Archive, Report 2010/556, 2010. `http://eprint.iacr.org/2010/556`.
21. Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978.
22. Amit Sahai, Hakan Seyalioglu, and Brent Waters. Dynamic credentials and ciphertext delegation for attribute-based encryption. In *CRYPTO*, pages 199–217, 2012.
23. Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In *EUROCRYPT*, pages 457–473, 2005.
24. Amit Sahai and Brent Waters. Slides on functional encryption. PowerPoint presentation, 2008. `http://www.cs.utexas.edu/~bwaters/presentations/files/functional.ppt`.
25. Amit Sahai and Brent Waters. Attribute-based encryption for circuits from multilinear maps. Cryptology ePrint Archive, Report 2012/592, 2012. `http://eprint.iacr.org/`.
26. Adi Shamir. Identity-based cryptosystems and signature schemes. In *CRYPTO*, pages 47–53, 1984.