Related Work

Identity Based Encryption The first concept of Identity-Based Encryption (IBE) was introduced by Shamir in 1984 [21]. Although Shamir easily constructed an identity-based signature scheme based on RSA, the use case of IBE remained an open problem until the introduction of bilinear maps. In [5] Boneh and Franklin propose the first practically usable IBE scheme based on the Weil pairing. However, the security proof in [5] still relies on the random oracle assumption. Canetti et al. [7] succeed in proposing a secure IBE scheme without having to rely on the random oracle model. However, the attacker model in [7] requires the adversary to declare which identity it will target, therefore the scheme in [4] is considered more secure as attackers can adaptively choose the targeted identity. Gentry [12] proposes a more efficient alternative to this scheme without random oracles while achieving shorter public parameters.

Broadcast Encryption Fiat and Naor introduced the first concept of Broadcast Encryption (BE) in [11]. The implementation in [11] requires a ciphertext of size $O\left(t \log^2 t \log n\right)$ to be secure against t colluding users. The first fully collusion resistant scheme was proposed in [19] by Naor et al. thereby making the ciphertext size independent of the number of colluding users. Halevy and Shamir further reduce the required ciphertext length for collusion resistant schemes in [15]. It is the first paper in a series of many ([9], [14] and [17]) that achieves a ciphertext size that is only dependent on the number of revoked users $O\left(r\right)$. Boneh, Gentry and Waters [6] consider using bilinear maps to achieve constant size ciphertexts and $O\left(n\right)$ public keys.

Identity Based Broadcast Encryption Sakai and Furukawa are the first to define a collusion resistant identity based broadcast encryption (IBBE) scheme in [20]. Independently from [20] Delerablée realises a similar identity based broadcast encryption scheme and claims to be the first as well in [8]. The size of the public key in both [20] and [8] is proportional to the maximum size of the intended set of recipients while realising short ciphertexts and private keys. Baek et al. [1] define an IBBE scheme that requires only one pairing computation. The scheme in [1] is proven secure under the random oracle assumption where the attacker ties himself to a selective-ID attack. Gentry and Waters achieve identity based broadcast encryption with sublinear ciphertexts in [13]. Their scheme is proven secure against a stronger notion of adaptive security where the attacker can adaptively alter its queries depending on earlier received information. Barbosa and Farshim [2] proposed an identity-based key encapsulation scheme for multiple parties which is an extension of *mKEM* as considered by Smart [22] to the identity-based setting. An mKEM is a Key Encapsulation Mechanism which takes multiple public keys as input. An encrypted message under mKEM consists of an encapsulated session key K and a symmetric encryption of the plaintext message M under K.

Recipient Anonymous Broadcast Encryption All earlier mentioned references describing BE require the intended set of recipients to be published to realise a higher efficiency. Barth, Boneh and Waters [3] are the first to design a BE scheme that takes the anonymity of the recipient into account. The proposed anonymous broadcast

encryption (ANOBE) scheme imposes a linear dependency of the ciphertext on the number of recipients and can only be proven secure in the random oracle model. In [18] Libert et al., propose an alternative ANOBE scheme that is proven secure in the standard model. Both [3] and [18] propose a tag based system that allows efficient decryption at the cost of making the public master key linear dependent on the total number of users. Krzywiekci et al. [16] propose a scheme that is proportional to the number of revoked users. In [23], Yu et al. design an architecture that even hides the number of users in the recipient set. Fazio and Perera introduce the notion of outsider anonymous broadcast encryption in [10]. The scheme relies on IBE to encode where a recipient is positioned in a publicly published tree to achieve sublinear ciphertexts. This construction allows sublinear ciphertexts while attaining recipient anonymity to all users that are outside the intended set of receivers.

References

[1] J. Baek, R. Safavi-Naini, and W. Susilo. Efficient multi-receiver identity-based encryption and its application to broadcast encryption. In S. Vaudenay, editor, *Public Key Cryptography*, volume 3386 of *Lecture Notes in Computer Science*, pages 380–397. Springer, 2005.

[2] M. Barbosa and P. Farshim. Efficient identity-based key encapsulation to multiple parties. In N. P. Smart, editor, *IMA Int. Conf.*, volume 3796 of *Lecture Notes in Computer Science*, pages 428–441. Springer, 2005.

[3] A. Barth, D. Boneh, and B. Waters. Privacy in encrypted content distribution using private broadcast encryption. In G. D. Crescenzo and A. D. Rubin, editors, *Financial Cryptography*, volume 4107 of *Lecture Notes in Computer Science*, pages 52–64. Springer, 2006.

[4] D. Boneh and X. Boyen. Secure identity based encryption without random oracles. *IACR Cryptology ePrint Archive*, 2004:173, 2004.

[5] D. Boneh and M. K. Franklin. Identity based encryption from the Weil pairing. *IACR Cryptology ePrint Archive*, 2001:90, 2001.

[6] D. Boneh, C. Gentry, and B. Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. *IACR Cryptology ePrint Archive*, 2005:18, 2005.

[7] R. Canetti, S. Halevi, and J. Katz. A forward-secure public-key encryption scheme. *IACR Cryptology ePrint Archive*, 2003:83, 2003.

[8] C. Delerablée. Identity-based broadcast encryption with constant size ciphertexts and private keys. In K. Kurosawa, editor, *ASIACRYPT*, volume 4833 of *Lecture Notes in Computer Science*, pages 200–215. Springer, 2007.

[9] Y. Dodis and N. Fazio. Public key broadcast encryption for stateless receivers. In J. Feigenbaum, editor, *Digital Rights Management Workshop*, volume 2696 of *Lecture Notes in Computer Science*, pages 61–80. Springer, 2002.

[10] N. Fazio and I. M. Perera. Outsider-anonymous broadcast encryption with sublinear ciphertexts. *IACR Cryptology ePrint Archive*, 2012:129, 2012.

[11] A. Fiat and M. Naor. Broadcast encryption. In D. R. Stinson, editor, *CRYPTO*, volume 773 of *Lecture Notes in Computer Science*, pages 480–491. Springer, 1993.

[12] C. Gentry. Practical identity-based encryption without random oracles. In S. Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 445–464. Springer Berlin Heidelberg, 2006.

[13] C. Gentry and B. Waters. Adaptive security in broadcast encryption systems. *IACR Cryptology ePrint Archive*, 2008:268, 2008.

[14] M. T. Goodrich, J. Z. Sun, and R. Tamassia. Efficient tree-based revocation in groups of low-state devices. In M. K. Franklin, editor, *CRYPTO*, volume 3152 of *Lecture Notes in Computer Science*, pages 511–527. Springer, 2004.

[15] D. Halevy and A. Shamir. The lsd broadcast encryption scheme. In M. Yung, editor, *CRYPTO*, volume 2442 of *Lecture Notes in Computer Science*, pages 47–60. Springer, 2002.

[16] L. Krzywiecki, P. Kubiak, and M. Kutylowski. A revocation scheme preserving privacy. In H. Lipmaa, M. Yung, and D. Lin, editors, *Inscrypt*, volume 4318 of *Lecture Notes in Computer Science*, pages 130–143. Springer, 2006.

[17] A. B. Lewko, A. Sahai, and B. Waters. Revocation systems with very small private keys. *IACR Cryptology ePrint Archive*, 2008:309, 2008.

[18] B. Libert, K. G. Paterson, and E. A. Quaglia. Anonymous broadcast encryption: Adaptive security and efficient constructions in the standard model. In M. Fischlin, J. Buchmann, and M. Manulis, editors, *Public Key Cryptography*, volume 7293 of *Lecture Notes in Computer Science*, pages 206–224. Springer, 2012.

[19] D. Naor, M. Naor, and J. B. Lotspiech. Revocation and tracing schemes for stateless receivers. *IACR Cryptology ePrint Archive*, 2001:59, 2001.

[20] R. Sakai and J. Furukawa. Identity-based broadcast encryption. *IACR Cryptology ePrint Archive*, 2007:217, 2007.

[21] A. Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and D. Chaum, editors, *CRYPTO*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer, 1984.

[22] N. P. Smart. Efficient key encapsulation to multiple parties. In C. Blundo and S. Cimato, editors, *SCN*, volume 3352 of *Lecture Notes in Computer Science*, pages 208–219. Springer, 2004.

[23] S. Yu, K. Ren, and W. Lou. Attribute-based on-demand multicast group setup with membership anonymity. *Computer Networks*, 54(3):377–386, 2010.