Literature Study: A survey on using Identity Based Encryption for Online Social Networks

Stijn Meul, ir. Filipe Beato, *Supervisor* Prof. dr. ir. Bart Preneel, *Promotor* Prof. dr. ir. Vincent Rijmen, *Promotor*

***Abstract*—In this paper the possibilities of realising user defined privacy in online social networks (with Facebook in particular) based on identity-based encryption and anonymous broadcast encryption are explored. The final goal is to propose a practical useable implementation of increased user defined privacy on Facebook.**

I. Introduction

ONLINE Social Networks (*OSNs*) are increasingly being used to share sensitive data with a limited circle of online connections. Users therefore have to count on the privacy infrastructure of the social network itself. Social networks like Google Plus or Facebook realise these security settings by defining groups of connections who are allowed to see certain profile updates. At first sight the user seems protected from the general public as it does not have access to these shielded updates. The OSN itself however still has access to this data and gratefully uses it for comercial purposes like targeted advertising or behavior analysis. All this data forms the basis of the OSN's economical existence. As recent events have shown, this user data is not only used for the sake of the OSN's financial survival but the data is leaked to third parties and agencies like NSA as well. One can wonder if a company non-transparently passes this data to any government agency for the argument of security, what other purposes this data will be used for.

Because the OSN has access to all users' data, it can be shared with external parties. This takes the users' full control over their data completely out of their hands. Additionally OSNs might offer API's to expose the users' information to other services like external applications. Finally, OSNs intentionally change security policies to maintain the balance between usability and the commercial value of their databases thereby leaving their users privacy behind. [1]

One could argue that if one wants to stay anonymous, he should not use an OSN. As the increasing popularity of OSNs has shown however, there is a market demand for OSNs because of their wide range of useful applications. It would therefore still be meaningful to make use of the infrastructure of a Social Network without its inherent data leakage.

The goal of this literature study is to research if an elegant architecture exists that allows to keep using OSN infrastructure without having to rely on the willingness of OSNs to keep the user's data private. The study is done with particularly Facebook in mind as this social network is amongst the most popular ones in the world. In the end the user should be able to define his own privacy instead of privacy policies being dictated by the social network.

The structure of this paper is the following. First existing architectures achieving similar privacy goals on social networks are discussed in section II. Next an introduction to identity-based encryption is given in section III and which appealing properties make IBE useful for increasing user defined privacy on Online Social Networks. In section IV different forms of broadcasting schemes are considered for implementing IBE for Online Social Networks. Finally, in section **??** a conclusion is given.

II. Existing Architectures [1]

Lots of fundamental work has been done on applications trying to enforce access control rules on OSNs. A grasp of all available applications is listed and analysed in the following section.

a) flyByNight: is a Facebook application that protects user data by storing it in encrypted form in Facebook. It relies on Facebook servers for its key management and is therefore not secure against active attacks by Facebook itself.

b) NOYB (None Of Your Business): replaces the details of user A with those of random users B and C thereby making this process only reversible by friends who are allowed to see the profile of user A. However this can not be applied to user messages or status updates that are the most frequently used features on Facebook.

c) FaceCloak: stores published Facebook data on its servers in encrypted form and replaces the data on Facebook with random text fetched from Wikipedia. This could be a useful mechanism to prevent OSNs from blocking security aware users because they are scared to see their advertising revenues shrink. However, this approach has the disadvantage that other users could take this data to be genuine user content. Furthermore FaceCloaks architecture leads to an inefficient key distribution system.

d) Persona: is a scheme that can be used as a Firefox extension to let users of an OSN determine their own privacy by supporting the ability to encrypt messages to a group of earlier defined friends based on *attribute-based encryption (ABE)*[2]. The scheme supports lots of useful use cases such as sending messages to all friends that are related to a certain attribute or even encrypting messages to friends of friends.

The major drawback of this system however is that every new friend has to exchange a public key before he is able to interact in the privacy preserving architecture consequently requiring an infrastructure for broadcasting and storing public keys. Furthermore, to support the encryption of messages to friends of friends, user defined groups should be made available publicly thereby making the public key distribution system even more complicated. Finally the proposed ABE encryption scheme is 100 to 1000 times slower than a standard RSA operation. [3]

e) Scramble: is a Firefox extension that allows defining groups of friends that are given access to certain social network updates. The tool uses public key encryption based on OpenPGP [4] to broadcast encrypted messages on almost any platform. Furthermore Scramble provides the implementation of a tiny link server such that OSN policies not allowing to post encrypted data are bypassed. However, as indicated by usability studies [5] OpenPGP has a higher usage threshold because an average user does not manage to understand OpenPGP properly. Additionally Scramble has to rely on the security decisions of the web of thrust. It therefore inherits the upleasant property of OpenPGP that the user can not be sure that the used PGP key actually belongs to the intended Facebook profile.[1]

The most unattractive property of all the above applications is that they have to rely on a rather complex infrastructure. Persona has to support an extended public key distribution system and Scramble relies on the leap-of-faith PGP web of thrust. Would it not be pleasant to use an infrastructure that inherently ensures that a Facebook update can only be read by the profiles the user inteded to? Would it not be a desirable approach that Facebook would require users to publish a public key on their Facebook profile such that communication with external providers is limited to a minimum? As the most important part of an OSNs' revenues lies in the data analysis of their users, the chances of Facebook implementing a required public key option are rather low to unexisting. To circumvent the requirement of such a public key attribute, it would be user friendly if any unique public string could be used as a public key. This is where identity based cryptography comes in.

III. Identity Based Encryption

Shamir proposed a concept of identity-based cryptography in 1984 [6]. The basic idea behind identity-based cryptography is that any string can be a valid public key for encryption or signature verification thereby eliminating the need for digital certificates. As a consequence identity-based cryptography reduces the system complexity and the cost for establishing and managing the Public Key Infrastructure (PKI). Identity-based cryptography proves to be particularly elegant if the public key is related to an attribute that uniquely identifies the identity of the user like an e-mail address, an IP address or a telephone number [7].

A. Working Principle [8]

IBE relies on a thrusted third party called the *Private Key Generator (PKG)*. During the initialisation of the architecture the PKG generates a public/private keypair called *the master public key* pk_{PKG} and *the master private key* sk_{PKG}. It is the master public key pk_{PKG} that is published publicly while the master private key sk_{PKG} is kept secret.

Once initialised, the secure exchange of packets takes place obeying the following steps as shown in Figure 1:

1) Alice uses Bob's identity ID_{Bob} and the master public key pk_{PKG} to encrypt a plaintext M to a ciphertext C.
2) Alice sends C and some plaintext instructions I over an insecure channel to Bob.
3) When Bob sees the ciphertext C, he uses the plaintext instructions I to connect to the PKG. Bob authenticates with the PKG by sending sufficient proof that ID_{Bob} belongs to him.
4) The PKG transmits Bob's private key sk_{Bob} to him over a secure channel.
5) Bob recovers the plaintext message M by decrypting it using his secret key sk_{Bob}.

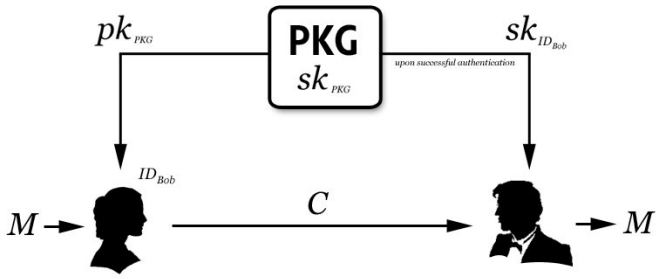

Fig. 1. Alice encrypting a message for Bob using Identity-Based Encryption

Please note that Alice does not require any prior actions from Bob to send him an encrypted message. This is one of the major motivations to use IBE in a practical setup. An attentive reader would remark however that this is realised at the expense of key escrow. The PKG namely knows the secret key of Bob thereby being able to decrypt every message that is sent to Bob. As the basic goal of this study is to limit the omniscience of the social network this property is very undesirable because the party to thrust has just shifted from the social network to a third party PKG. Possible workarounds solving this issue are discussed in Section III-F.

B. Pairings

Although Shamir easily constructed an *identity-based signature (IBS)* scheme based on RSA in 1984, the use case of *identity-based encryption (IBE)* remained an open problem for many years. It was by the introduction of *bilinear maps* (also known as *pairings*) that in 2001 Boneh and Franklin[9] were able to implement the first secure and truly practical IBE system [7].

An IBE scheme can be built from any bilinear map

$e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ between two groups $\mathbb{G}_1$, $\mathbb{G}_2$ as long as a variant of the Computational Diffie-Hellman problem in $\mathbb{G}_1$ is hard. Where $\mathbb{G}_1$ and $\mathbb{G}_2$ are two groups of order q for some large prime q. The bilinear map should satisfy the following properties:

1) Bilinear: A map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is *bilinear* if $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ for all $P, Q \in \mathbb{G}_1$
2) Non degenerate: The map does not send all pairs in $e : \mathbb{G}_1 \times \mathbb{G}_1$ to the identity in $\mathbb{G}_2$ such that if P is a generator of $\mathbb{G}_1$ then $\hat{e}(P, P)$ is a generator of $\mathbb{G}_2$.
3) Computable: There exists an efficient algorithm to compute $\hat{e}(P, Q)$ for any $P, Q \in \mathbb{G}_1$

A bilinear map satisfying the above properties is called an *admissible* bilinear map. In other words it can be stated that an admissible bilinear map is a function pairing elements from one cyclic group to another of the same prime order, where the discrete log problem is hard in the first group [8]. The group $\mathbb{G}_1$ is a subgroup of the additive group of points on an elliptic curve $E/\mathbb{F}$. The group $\mathbb{G}_2$ is a subgroup of the multiplicative group of points of a finite field $\mathbb{F}^*_{p^2}$. Consequently $\mathbb{G}_1$ can be seen as an additive group and $\mathbb{G}_2$ as a multiplicative group. [9]

The security of IBE is based on the *Bilinear Diffie-Hellman Assumption (BDH assumption)*. This assumption states that given:

- $\mathbb{G}_1$ and $\mathbb{G}_2$ groups of prime order q
- $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ an admissible bilinear map
- P a generator of $\mathbb{G}_1$
- $\langle P, aP, bP, cP \rangle$ for some ungiven $a, b, c \in \mathbb{Z}^*_q$

it is computationally hard to calculate $W = \hat{e}(P, P)^{abc}$ although calculating $\langle P, aP, bP, cP \rangle$ for some given $a, b, c \in \mathbb{Z}^*_q$ and $W = \hat{e}(P, P)^{abc}$ is fairly easy once a, b and c are known [9]. The admissible pairing thus functions as a one-way function as it can be shown that solving the BDH assumption is reducible to solving the discrete-log problem for these bilinear maps [8].

Both modified Weil and Tate pairings suffice the required properties for admissable bilinear maps and are used in practice. Tate pairings however have the advantage of being computationally more efficient then Weil pairings [10].

Please further note that:

$$\hat{e}(aX, bY) = \hat{e}(X, Y)^{ab} = \hat{e}(bX, aY) \tag{1}$$

where aX represents a multiplication of a point on an elliptic curve by integers. Although the multiplication operation aX is easy, finding a given aX will be computationally infeasible [8].

C. A Concrete IBE Scheme

Pairings as dicussed in Section III-B allow to implement a concrete IBE scheme based on the following 4 steps:

1) *Setup*: the PKG picks an elliptic curve, a random secret s and a point P on the curve. P and sP are made public such that $pk_{PKG} = \langle P, sP \rangle$ in Figure 1.
2) *Encryption*: As Alice knows pk_{PKG} and ID_{Bob}, she can pick a random r and calculate a key k to encrypt her plaintext message M by $k = \hat{e}(rID_{Bob}, pk_{PKG}) = \hat{e}(rID_{Bob}, sP)$. Alice then sends $\langle Encrypt_k(M), rP \rangle$ to Bob.
3) *Extract:* If Bob has never received a message before, he still needs to receive its private key from the PKG. Bob authenticates with the PKG after which the PKG calculates $sk_{Bob} = sID_{Bob}$ and returns this to Bob over a secure channel.
4) *Decryption:* Bob can now calculate the key k to decrypt $\langle Encrypt_k(M)$ by $k = \hat{e}(sID_{Bob}, rP)$.

Note that the key k calculated by Bob and the key k calculated by Alice is the same because of the property illustrated in Formula 1. Furthermore Bob and the PKG are the only ones able to decrypt $Encrypt_k(M)$ as nobody else knows sID_{Bob}.

D. Security Definitions

In all research concerning IBE, whether it is pure pairing based IBE or more complex broadcasting schemes, some definitions about an algorithm's level of security are always considered. Although most of these security definitions change depending on the considered algorithm, there are some general concepts that are similar.

The security level of an algorihm is mostly defined based on an attackers game. The more actions an attacker is allowed to perform in this game without gaining any advantage in trying to decrypt messages, the safer the algorithm. Although this is very roughly stated, it is a concept that is encountered frequently in literature.

In IBE there are mainly two accepted definitions of security:

1) *Full security* which means the attacker can choose adaptively the identity he wants to attack after having seen the parameters of the algorithm.
2) *Selective-ID security* which means that the attacker must choose the identity he wants to attack at the beginning, before seeing the paramters.

As the attacker is more restricted in its actions in Selective-ID security it is considered less secure. [11]

Another notion that frequently appears in literature covering IBE is the concept of *random oracles*. A random oracle is a black box that responds to every unique query with a (truly) random response chosen uniformly from its output domain, except that for any specific query, it responds the same way every time it receives that query. Very often, random oracles are used in security proofs to model true randomness. In reality these oracles are often implemented by hash functions. Therefore proving security based on true random oracles is easier than proving the actual implementation of an algorithm to be secure. However, an application that does not require random oracle heuristics is considered to be safer. [12]

E. Advantages of IBE

As already mentioned in Section III one of the most attractive properties of IBE is the recipient that does not have to have taken any action before being able to start receiving messages. Certainly in an OSN this would be a compelling feature as the user does not have to upload its public key to a key ring neither to a public server. For the public key, any string that uniquely identifies a user can be used. If a string is chosen that is inherently part of the OSN's architecture, the user does not have to perform actions that are incromprehensible to him. The ideal case is that once the user has signed up for the service of the OSN, he is ready to receive encrypted messages without taking any additional decisions concerning key lengths or algorithmic properties.

Moreover, an IBE architecture reduces the complexity of the system as there is no further need for public key certificates. The user only has to receive his secret key once from the PKG over a secure channel. After he knows his private key, the user theoretically never has to contact the PKG again unless he loses his private key. The contrast in complexity with a CA hierarchy and security certificates being issued periodically is immense.

Finally, IBE has less restrictions on scaling because PKGs can be distributed independently and geographically without the need to synchronise data. This property enables quick and easy key management all over the world. [13]

F. Disadvantages of IBE

One of the major drawbacks of IBE is its inherent key escrow property. If one does not want to trust his data to a provider of an OSN, he probably does not want any other unintended third party to have access to this data either. A possible countermeasure for the above key escrow problem would be to use Shamir's secret sharing technique to distribute the PKG's master secret key sk_{PKG} over a number of different PKGs [9]. But as this method requires users to authenticate themselves to multiple PKGs, this workaround increases the total communication and computational cost of the system [7].

Another disadvantage of IBE is that *Certificate Revocation Lists (CRLs)* are no longer supported as there are no security certificates to revoke. At first sight this seems a good thing as supporting CRLs is cumbersome and puts heavy demands on the individual users of a PKI. However, this also implies that public keys can not be revoked in case their coresponding private keys are compromised. Such a scenario would imply that the user could no longer make use of certain strings that are immediately linked to his identity. To get around this issue a validity timestamp could be concatenated to the ID component thereby limiting the period during which a public key would be valid. By doing so, restrictions would be placed on the duration the compromised secret key. Remark that such a workaround would imply a higher computational and communication cost as well because all users have to reconnect over the secure channel to the PKG asking for a new secret key every time their timestamp expires [8].

IV. Implementing IBE for Online Social Networks

As Scrambe [1] already has a user friendly interface that supports all required actions to implement encryption on Online Social Networks, it would be useful to alter the existing Scramble code that it can implement IBE as well. The most important trigger to modify the existing Scamble code is because Scramble is open source, lightweight and developed at KU Leuven. Certainly the latter argument eases the process of altering the existing code and therefore is an asset.

A. User Public Key

The most important design decision is which profile attribute to use as a public key string of the user. The desired properties for such a user public key (denoted ID_{Bob} in Figure 1) are the following:

1) The public key should uniquely identify the user
2) The public key should be mandatory for every user of the social network
3) The public key should not change frequently over time
4) The public key should be an inherent part of the infrastructure of the social network thereby meaning that the previous three properties are already ensured by the provider of the social network.

Please note that the decision of which string to use as a public key, is highly dependent on the targeted social network. Every OSN will namely have other profile attributes satisfying the earlier mentioned properties. Scramble would therefore become platform dependent. However, this is an offer the writers of this paper are willing to make for the sake of an increased ease of use.

As already mentioned in Section I the focus of this paper will be on Facebook although other OSNs could make use of the concepts mentioned in this paper. In Facebook there is a very obvious and readable string satisfying the earlier mentioned properties namely the Facebook username.

A Facebook username is an unique identifier that serves as an URL of someone's profile. For example `http://www.facebook.com/user.name` refers to the Facebook profile of the user with Facebook username `user.name`.

Using the username as an identifier ensures that all the above properties are satisfied as an URL can only refer to one page. Because every Facebook page is reachable using an URL, every user has such a username. Furthermore, the public key does not change frequently over time as Facebook limits changing this string only once [14]. Finally, Facebook has the responsibility to check all these properties as URL collisions would occur if they did not take care of this.

Additional pleasant properties are that user names are:

1) mostly closely related to the identity of the user.

2) mostly readable as users choose them to make their profile easier to reach using an URL. This property also makes them easier to remember.

B. IBE Broadcasting

Broadcast Encryption (BE) techniques ensure confidentiality when sending a message to an arbitrary subset drawn from a universe of users. The universe of users is usually called U and the set of targeted users is denoted with S such that $S \subseteq U$. The concept of Broadcast Encryption was originally introduced by Fiat and Naor [15] in 1993 [16]. A BE scheme is said to be *fully collusion resistant* when, even if all users that are not in S collude, they can by no means infer information about the broadcast message. [11]

If one wants to encrypt the same message M for a large set of identities, one can simply encrypt M seperateley for each individual identity and then transmit these encrypted messages separately. If the cardinality of the set of targeted identities is $|S|$, then one has to perform $|S|$ independent encryptions. Of course such a solution would be too expensive in terms of bandwidth requirement as well as pairing computation. Baek, Safavi-Naini and Susilo in [17] addressed this problem for the first time in literature. They call their protocol *Multi Receiver Identity-Based Encryption (MR-IBE)* and base it on the Boneh-Franklin IBE using bilinear pairings. In their paper, Baek et al. prove MR-IBE to be secure in the selective-ID model using the random oracle heuristic. Independent of this work, Barbosa and Farshim [18] proposed an identity-based key encapsulation scheme for multiple parties which is an extension of *mKEM* as proposed by Smart [19] 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. In this way only the encapsulation of the key uses computation intensive public key encryption [19]. Barbosa and Farshim prove their algorithm to be secure under random oracle assumptions. Later constructions based on the Boneh-Boyen (H)IBE [20] even show security without using the random oracle heurstic. [21]

The first proposals for these indentity-based broadcasting schemes had some undesirable properties like public key lengths being determined by the total number of possible users $|U|$. Lots of research optimising identity-based broadcasting schemes has been done since then to improve on the efficiency and usability of the original proposals. Delerablée introduces an Identity Based Broadcast Encryption scheme with constant sized ciphertext and private keys and a public key that is linear in the maximal number of receivers $|S|$. This is an improvement on earlier defined architectures as the maximum number of users is no longer fixed by the public key length. These improvements are realised by using broadcast KEM-DEM techniques. However, it is required in this architecture that the targeted set of receivers S is broadcasted to all users as well thereby leaking a lot of information. [11]

C. Anonymous Broadcast Encryption

It is maybe useful to take one step back and think about the consequences of all intended receivers being published in plain text together with the encrypted message on a Social Network. If for example Bob's girlfriend celebrates her birthday in a few weeks and he spreads an encrypted message to all her friends without including her as a recipient, she will probably know Bob is up to something. This is just one example of possible many that illustrates the negative impact on security broadcasting of S can have in real life situations. Depending on the context, information can be deduced about a status update without decrypting the update to plain text.

Broadcast encryption schemes that do not leak information about the intended recipients are called *Anonymous Broadcasting Encryption (ANOBE)* schemes. [16] As these systems do not profit from S being known to every user upfront they are less efficient than non-anonymous BE schemes. Thus there clearly is a tradeoff between secrecy and efficiency in ID-based Broadcasting architectures although this tradeoff can be partially cancelled by letting the sender precompute certain parameters [22].

Fan et al. [22] are the first to consider the anonymity of the receivers in an ID-based broadcasting encryption architecture. They propose a protocol based on Lagrange interpolating polynomials such that anonymity is preserved for every receiver against any other receiver. All users of the system U can analyse whether they are an intended receiver or not while only the sender knows who the other receivers in S are. Wang et al. show in [23] that the original architecture as proposed in [22] does not provide the level of anonymity as originally intended because everyone is able to deduce the set of authorised identities. In [23] protocol changes fixing these weaknesses are suggested and prove is given that the improved scheme satisfies the confidentiality and receiver anonymity under random oracle assumptions. Also Chien [24] proposes similar improvements on the original architecture by Fan et al. [22] Zhang et al. [25] point out that the scheme of Wang et al. is not safe either as all authorised users in S can deduce which other users are in S. In their paper a solution is presented to this issue as well as some computational improvements compared to Wang et al.'s scheme.

Note however that although receivers being secret to unintended other users is desirable, it might be useful on a social network that the members of the set S know each other. Suppose for example that Alice posts a Facebook update on her profile page intended to Bob and Dylan. This means that $Bob, Dylan \in S$. As a reaction to Alice's Facebook update, Bob wants to write a reply to start a discussion. However, as Bob does not know which other users are allowed to see Alice's update, he can now only encrypt his reply to Alice thereby preventing Dylan from joining the discussion.

However, this discussion could have been useful to Dylan as well because otherwise Alice would not have included Dylan as a recipient in S in the first place. A workaround for this issue could be to concatenate S to the plaintext message M such that $M||S$ is encrypted instead of M. Currently possible algorithms taking a computational advantage of the broadcasting of S in an encrypted form, are not known to the writers of this paper.

V. Conclusion

Identity-Based Encryption (IBE) seems to have desirable properties for implementations increasing user defined privacy in OSNs. Mainly the minimal additional architectural support and the increased ease of use, are major motivations to implement IBE in Online Social Network (OSN) environments. Some disadvantages like a lack of key revocation and implicit key escrow are unpleasant but can be solved at the expense of increasing the complete system's complexity.

Broadcast Encryption (BE) techniques can be used to optimise the required bandwidth and computational cost. Anonymous Broadcast Encryption (ANOBE) techniques even protect the identity of the authorised receivers. Anonymous Identity-Based Broadcast Encryption combines all desirable properties to a prefered architecture for IBE in OSNs although this still is a fast changing research domain.

For a practical implementation of IBE on an OSN, Scramble could be rewritten that it supports Anonymous Identity-Based Broadcast Encryption on Facebook by using Facebook usernames as public keys. The key escrow property of IBE could be circumvented using a threshold secret sharing setup. The inability to revoke public keys could be compensated by appending a validity period to each public key in a standardised fashion such that the architecture implicitly knows when to issue new private/public key pairs.[26] t [27] s [28] e [29] f [26]

References

[1] F. Beato, M. Kohlweiss, and K. Wouters, "Scramble! your social network data," in *PETS*, ser. Lecture Notes in Computer Science, S. Fischer-Hübner and N. Hopper, Eds., vol. 6794. Springer, 2011, pp. 211–225.

[2] A. Sahai and B. Waters, "Fuzzy identity based encryption," *IACR Cryptology ePrint Archive*, vol. 2004, p. 86, 2004.

[3] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin, "Persona: an online social network with user-defined privacy," *SIGCOMM Comput. Commun. Rev.*, vol. 39, no. 4, pp. 135–146, Aug. 2009. [Online]. Available: \url{http://doi.acm.org/10.1145/1594977.1592585}

[4] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, and R. Thayer, "OpenPGP Message Format," RFC 4880 (Proposed Standard), Internet Engineering Task Force, November 2007, updated by RFC 5581. [Online]. Available: http://www.ietf.org/rfc/rfc4880.txt

[5] A. Whitten and J. D. Tygar, "Why johnny can't encrypt: a usability evaluation of PGP 5.0," in *Proceedings of the 8th conference on USENIX Security Symposium - Volume 8*, ser. SSYM'99. Berkeley, CA, USA: USENIX Association, 1999, pp. 14–14. [Online]. Available: http://dl.acm.org/citation.cfm?id=1251421.1251435

[6] A. Shamir, "Identity-based cryptosystems and signature schemes," in *CRYPTO*, ser. Lecture Notes in Computer Science, G. R. Blakley and D. Chaum, Eds., vol. 196. Springer, 1984, pp. 47–53.

[7] J. Baek, J. Newmarch, R. Safavi-naini, and W. Susilo, "A survey of identity-based cryptography," in *Proc. of Australian Unix Users Group Annual Conference*, 2004, pp. 95–102.

[8] C. Youngblood, "An introduction to identity-based cryptography," 2005. [Online]. Available: http://courses.cs.washington.edu/courses/csep590/06wi/finalprojects/youngblood_csep590tu_final_paper.pdf

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

[10] Y. Yacobi, "A note on the bilinear diffie-hellman assumption," 2002, identity Based Encryption; Weil pairing yacov@microsoft.com 11909 received 7 Aug 2002, last revised 9 Aug 2002. [Online]. Available: http://eprint.iacr.org/2002/113

[11] C. Delerablée, "Identity-based broadcast encryption with constant size ciphertexts and private keys," in *ASIACRYPT*, ser. Lecture Notes in Computer Science, K. Kurosawa, Ed., vol. 4833. Springer, 2007, pp. 200–215.

[12] Wikipedia, "Random oracle," 2013. [Online]. Available: http://en.wikipedia.org/wiki/Random_oracle

[13] V. Security, "Identity based encryption," 2013. [Online]. Available: www.voltage.com/technology/identity-based-encryption/

[14] Facebook, "What are the guidelines around creating a custom username?" 2013. [Online]. Available: https://www.facebook.com/help/105399436216001\#What-are-the-guidelines-around-creating-a-custom-username?

[15] A. Fiat and M. Naor, "Broadcast encryption," in *CRYPTO*, ser. Lecture Notes in Computer Science, D. R. Stinson, Ed., vol. 773. Springer, 1993, pp. 480–491.

[16] B. Libert, K. G. Paterson, and E. A. Quaglia, "Anonymous broadcast encryption: Adaptive security and efficient constructions in the standard model," in *Public Key Cryptography*, ser. Lecture Notes in Computer Science, M. Fischlin, J. Buchmann, and M. Manulis, Eds., vol. 7293. Springer, 2012, pp. 206–224.

[17] J. Baek, R. Safavi-Naini, and W. Susilo, "Efficient multi-receiver identity-based encryption and its application to broadcast encryption," in *Public Key Cryptography*, ser. Lecture Notes in Computer Science, S. Vaudenay, Ed., vol. 3386. Springer, 2005, pp. 380–397.

[18] M. Barbosa and P. Farshim, "Efficient identity-based key encapsulation to multiple parties," in *IMA Int. Conf.*, ser. Lecture Notes in Computer Science, N. P. Smart, Ed., vol. 3796. Springer, 2005, pp. 428–441.

[19] N. P. Smart, "Efficient key encapsulation to multiple parties," in *SCN*, ser. Lecture Notes in Computer Science, C. Blundo and S. Cimato, Eds., vol. 3352. Springer, 2004, pp. 208–219.

[20] S. Chatterjee and P. Sarkar, "Generalization of the selective-id security model for hibe protocols," in *Public Key Cryptography*, ser. Lecture Notes in Computer Science, M. Yung, Y. Dodis, A. Kiayias, and T. Malkin, Eds., vol. 3958. Springer, 2006, pp. 241–256.

[21] ——, "Multi-receiver identity-based key encapsulation with shortened ciphertext," in *INDOCRYPT*, ser. Lecture Notes in Computer Science, R. Barua and T. Lange, Eds., vol. 4329. Springer, 2006, pp. 394–408.

[22] C.-I. Fan, L.-Y. Huang, and P.-H. Ho, "Anonymous multireceiver identity-based encryption," *IEEE Trans. Comput.*, vol. 59, no. 9, pp. 1239–1249, Sep. 2010. [Online]. Available: http://dx.doi.org/10.1109/TC.2010.23

[23] H. Wang, Y.-C. Zhang, H. Xiong, and B. Qin, "Cryptanalysis and improvements of an anonymous multi-receiver identity-based encryption scheme," *IET Information Security*, vol. 6, no. 1, pp. 20–27, 2012.

[24] H.-Y. Chien, "Improved anonymous multi-receiver identity-based encryption," *The Computer Journal*, vol. 55, no. 4, pp. 439–446, 2012. [Online]. Available: http://comjnl.oxfordjournals.org/content/55/4/439.abstract

[25] J. Zhang and Y. Xu, "Comment on anonymous multi-receiver identity-based encryption scheme," in *INCoS*, F. Xhafa, L. Barolli, F. Pop, X. Chen, and V. Cristea, Eds. IEEE, 2012, pp. 473–476.

[26] C. Gentry, "Practical identity-based encryption without random oracles," in *Advances in Cryptology - EUROCRYPT 2006*, ser. Lecture Notes in Computer Science, S. Vaudenay, Ed. Springer Berlin Heidelberg, 2006, vol. 4004, pp. 445–464. [Online]. Available: \url{http://dx.doi.org/10.1007/11761679_27}

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

[28] A. Barth, D. Boneh, and B. Waters, "Privacy in encrypted content distribution using private broadcast encryption," in *Financial Cryptography*, ser. Lecture Notes in Computer Science, G. D. Crescenzo and A. D. Rubin, Eds., vol. 4107. Springer, 2006, pp. 52–64.

[29] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," *IACR Cryptology ePrint Archive*, vol. 2012, p. 52, 2012.