New Results on Identity-based Encryption from Quadratic Residuosity *

Ferucio Laurenţiu Ţiplea[1] and Emil Simion[2]

[1] Department of Computer Science, "Al.I.Cuza" University of Iaşi
700506 Iaşi, Romania, e-mail: fltiplea@info.uaic.ro
[2] Advanced Technologies Institute
Bucharest, Romania, e-mail: ati@dcti.ro

Abstract. This invited talk surveys the results obtained so far in designing identity-based encryption (IBE) schemes based on the quadratic residuosity assumption (QRA). We begin by describing the first such scheme due to Cocks, and then we advance to the novel idea of Boneh, Gentry and Hamburg. Major improvements of the Boneh-Gentry-Hamburg scheme are then recalled. The recently revealed algebraic torus structures of the Cocks scheme allows for a better understanding of this scheme, as well as for new applications of it such as homomorphic and anonymous variants of it.

Identity-based encryption (IBE) was proposed in 1984 by Adi Shamir [10] who formulated its basic principles but he was unable to provide a solution to it, except for an identity-based signature scheme. Sakai, Ohgishi, and Kasahara [9] have proposed in 2000 an identity-based key agreement scheme and, one year later, Cocks [4] and Boneh and Franklin [1] have proposed the first IBE schemes. Cocks' solution is based on quadratic residues. It encrypts a message bit by bit and requires $2\log n$ bits of cipher-text per bit of plain-text. The scheme is quite fast but its main disadvantage is the ciphertext expansion. Boneh and Franklin's solution is based on bilinear maps. Moreover, Boneh and Franklin also proposed a formal security model for IBE, and proved that their scheme is secure under the Bilinear Diffie-Hellman (BDH) assumption.

The Cocks scheme [4] is very elegant and per se revolutionary. It is based on the standard QRA modulo an RSA composite. The scheme encrypts one bit at a time. The bits are considered to be exactly the two values (i.e., -1 and 1) of the Jacobi symbol modulo an RSA modulus n, when applied to an integer non-divisible by n. Thus, if Alice wants to send a bit $b \in \{-1, 1\}$ to Bob, she randomly generates an integer t with the Jacobi symbol b modulo n, hides t into a new message $s = t + at^{-1} \bmod n$ obtained by means of Bob's identity a, and sends s to Bob. The decryption depends on whether a is a quadratic residue or not modulo n. As neither Alice nor Bob knows whether a is a quadratic residue or not, Alice repeats the procedure above with another integer t' whose Jacobi

* Work partially supported by the Romanian National Authority for Scientific Research (CNCS-UEFISCDI) under the project PN-II-PT-PCCA-2013-4-1651.

symbol modulo n is b, and sends $s' = t' - at'^{-1} \bmod n$ as well. Now, Bob can easily decrypt by using a private key obtained from the key generator, because either a or $-a$ is a quadratic residue modulo n. It can be shown that the Cocks IBE scheme is IND-ID-CPA secure in the random oracle model under the QRA.

The main disadvantage regarding the efficiency of the Cocks scheme consists of the fact that it encrypts one bit by $2\log n$ bits. A very interesting idea proposed by Boneh, Gentry and Hamburg [2] is to encrypts a stream of bits by multiplying each of them by an Jacobi symbol randomly generated. The generation of these new Jacobi symbols are based on the equation $ax^2+Sy^2 \equiv 1 \bmod n$. Any solution to this congruential equation leads to two polynomials f and g with the property that $g(s)$ and $f(r)$ have the same Jacobi symbol modulo n, for any square root s of S and any square root r of a. Therefore, g can be used to encrypt one bit, while f can be used to decrypt it. If the solutions of the above congruential equation can be obtained by a deterministic algorithm, then the decryptor knows how to decryt the ciphertext. Therefore, in order to send an ℓ-bit message to Bob, Alice has to solve 2ℓ equations as above (two equations for each bit, one for Bob's identity a and the other one for $-a$), while the decryptor needs to solve only ℓ equations. The ciphertext size is $2\ell + \log n$ bits. Some improvements at the sender side reduces the number of equations to be solved by the encryptor to $\ell + 1$.

An important improvement of the Boneh-Gentry-Hamburg (BGH) scheme was proposed later by Jhanwar and Barua [7]. The improvement works in two directions: improve the time complexity of the algorithm to solve equations $ax^2 + Sy^2 \equiv 1 \bmod n$, and reduce the number of equations to be solved. The first improvement is based on a careful analysis of the solutions of the equation $ax^2 + Sy^2 \equiv 1 \bmod n$. Thus, an efficient probabilist algorithm is developed to randomly generate solutions of such an equation. The second improvement is based on a composition formula according to which two solutions can be combined in some way to obtain a new solution. Therefore, to encrypt an ℓ-bit message, only $2\sqrt{\ell}$ equations need to be solved. Unfortunately, the probabilistic nature of the algorithm by which solutions are obtained leads to a ciphertext larger than in the case of the BGH scheme, namely $2\ell + 2\sqrt{\ell}\log n$ bits. The Jhanwar-Barua (JB) scheme was revisited in [6], where some errors were corrected; unfortunately, the security was not sufficiently argued as it was later remarked in [5]. Moreover, [5] also proposes an improvement by which the number of equations needed to be solved by Alice is reduced to $2\log \ell$. The ciphertext size is also reduced to $2\ell + 2(\log \ell)(\log n)$ bits.

It is well-known that the Cocks scheme is not anonymous [2]. Several researchers tried to extend this scheme to offer identity anonymity; usually, such extensions are based on creating lists of ciphertext so that the identity becomes hidden in the lists. This approach gives rise to very large ciphertexts. It was also a believe that the Cocks scheme does not have homomorphic properties. A very recent result [8] rehabilitates the Cocks scheme with respect to these two weaknesses. Joye [8] identified the algebraic structure of the Cocks ciphertexts: he proved that these are squares in a torus like structure, and form a quasi-

group. The underlying group law is the operation needed on ciphertexts to show that the Cocks scheme is homomorphic when the operation on clear messages is the multiplication. Therefore, the Cocks scheme offer homomorphic properties. Another important consequence obtained in [8] is about the anonymity of the Cocks scheme. It was shown that a different way of computing the ciphertext, without expansion, leads to identity anonymity.

A very interesting question is whether high order Jacobi symbols can be used in the Cocks scheme in order to encrypt more than one bit at a time. A first attempt to do that is the one in [3]. Unfortunately, the only secure scheme proposed in [3] suffers from massive ciphertext expansion.

References

1. Boneh, D., Franklin, M.K.: Identity-based encryption from the Weil pairing. In: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology. pp. 213–229. CRYPTO '01, Springer-Verlag, London, UK, UK (Aug 2001)
2. Boneh, D., Gentry, C., Hamburg, M.: Space-efficient identity based encryption without pairings. In: Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science. pp. 647–657. FOCS '07, IEEE Computer Society, Washington, DC, USA (2007)
3. Boneh, D., LaVigne, R., Sabin, M.: Identity-based encryption with e^{th} residuosity and its incompressibility. In: Autumn 2013 TRUST Conference. Washington DC (oct 2013), poster presentation
4. Cocks, C.: An identity based encryption scheme based on quadratic residues. In: Proceedings of the 8th IMA International Conference on Cryptography and Coding. pp. 360–363. Springer-Verlag, London, UK, UK (Dec 2001)
5. Ţiplea, F.L., Simion, E., Teşeleanu, G.: An improvement of Jhanwar-Barua's identity-based encryption scheme. Tech. rep. (2015)
6. Elashry, I., Mu, Y., Susilo, W.: Jhanwar-Barua's identity-based encryption revisited. In: Au, M., Carminati, B., Kuo, C.C. (eds.) Network and System Security, Lecture Notes in Computer Science, vol. 8792, pp. 271–284. Springer International Publishing (2014)
7. Jhanwar, M.P., Barua, R.: A variant of Boneh-Gentry-Hamburg's pairing-free identity-based encryption scheme. In: Inscrypt. pp. 314–331 (2008)
8. Joye, M.: On identity-based cryptosystems from quadratic residuosity (2015)
9. Sakai, R., Ohgishi, K., Kasahara, M.: Cryptosystems based on pairing. In: Symposium on Cryptography and Information Security (SCIS2000) (January 2000)
10. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Proceedings of CRYPTO 84 on Advances in cryptology. pp. 47–53. Springer-Verlag New York, New York, NY, USA (1985)