Public Key Cryptography without Certificates for Beyond 5G Mobile Small Cells

Marcus de Ree*,†, Georgios Mantas*,‡, James Gao‡, Jonathan Rodriguez*,†, and Ifiok E. Otung†
*Instituto de Telecomunicações, Aveiro, Portugal
Email: {mderee, gimantas, jonathan}@av.it.pt
†University of South Wales, Pontypridd, UK
Email: {marcus.deree, jonathan.rodriguez, ifiok.otung}@southwales.ac.uk
‡University of Greenwich, London, UK
Email: {g.mantas, j.gao}@greenwich.ac.uk

***Abstract*—The 5G network takes advantage of the small cells technology. The next logical step is to cover the urban landscape with mobile small cells, to optimize network services. However, the introduction of mobile small cells raises various security challenges. Cryptographic solutions are capable of solving these as long as they are supported by appropriate key management schemes. The threshold-tolerant identity-based cryptosystem forms a solid basis for key management schemes for mobile small cells. However, this approach is unable to sustain security over time. Therefore, we introduce two extensions, proactive secret sharing and private key cloaking, to address this challenge.**

***Index Terms*—Ad Hoc Network, Beyond 5G, Cryptography, Decentralized Systems, D2D Communication, Key Management, Mobile Small Cell, Security**

I. Introduction

The mobile network has seen immense growth over the last decade, both the number of connected mobile devices and the amount of mobile data that a mobile device requests has seen a massive increase. This immense growth does not seem to slow down as more and more Internet-of-Things (IoT) devices become available on the global market. The network infrastructure is limited in its data processing and forwarding capabilities, even with novel 5G technologies such as the small cells technology. Many network users have experienced these limitations during events in which large amounts of data are simultaneously transmitted, such as New Year's Eve [1].

The densely populated areas will be the first to notice network delays. To this end, the EU funded H2020-MSCA project "SECRET" [2] introduced a networking scenario which allows for network offloading. In their scenario, an urban environment is covered by so-called "mobile small cells". These are small cells which are entirely made up of existing mobile devices, connected through device-to-device (D2D) communication and infrastructureless by nature. Network users within relative close proximity could rely on the concept of mobile small cells to communicate instead of having to rely on the network infrastructure to transmit all their data. Additional advantages include an increase in data rates and energy efficiency while reducing latency and interference.

However, mobile small cells networking raises significant challenges in terms of security [3]. Cryptographic security solutions (e.g., encryption schemes, signature schemes) are capable of solving these as long as they are supported by a key management scheme. Generally, key management schemes rely on some form of a trusted third party (TTP) to provide security. This TTP is an entity which every user inside the network believes to be trustworthy and secure against compromise. However, it is assumed that the network infrastructure and mobile devices from the network users are physically vulnerable to being compromised and are therefore unable to act as the TTP to establish security. Security must therefore be guaranteed by means of a key management scheme which decentralizes trust.

In this paper, we look into the threshold-tolerant identity-based cryptosystem [4] as a basis to design a key management scheme to secure beyond 5G mobile small cells. This cryptosystem is unique in the way that it is the only one (to the authors' knowledge) which does not rely on an online TTP during network operation. During network operation, a threshold number of network users can collectively provide access to new users. This system therefore decentralizes trust and does not suffer from a single point of attack from which the network can be taken down. However, the cryptosystem is only secure as long as the threshold remains intact. We investigate whether we can utilize this public key cryptosystem and design a key management scheme to secure beyond 5G mobile small cells. This investigation explores two extensions, (i) proactive secret sharing [5], [6] and (ii) private key cloaking.

This paper is organized as follows. Section II describes the related works. Section III covers some important preliminaries. Section IV covers the two proposed extensions to design a secure key management scheme based on the threshold-tolerant identity-based cryptosystem. Section V describes the planned future work and Section VI concludes the paper.

II. Related Works

In the last two decades, a variety of key management schemes have been designed for distributed environments. Depending on the deployment scenario, a key management design has its own unique set of requirements. For our deployment scenario, a fully distributed trusted third party (FD-TTP)-based key management approach has been evaluated to be the most suitable [3].

The FD-TTP-based key management approach was first proposed by Luo et al. [7], [8] and is based on the traditional

The research work leading to this publication has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement H2020-MSCA-ITN-2016-SECRET-722424.

public key infrastructure (PKI). In traditional PKI, the centralized TTP is in possession of a master key pair and uses this to provide key management services, such as creating signed certificates for participating network users. In their FD-TTP-based scheme, the master private key is broken up into pieces (or shares) using threshold secret sharing techniques [9]. These shares are distributed among the network users, such that a threshold amount of these can collaboratively provide the key management service. Deng and Agrawal [10] designed a FD-TTP-based key management scheme based on identity-based public key cryptography and Zhang et al. [11] and de Ree et al. [12] designed FD-TTP-based key management schemes based on certificateless public key cryptography. To emphasize, the secret shares in these schemes are merely used as a tool to establish verifiable keys at network users.

Feldman proposed verifiable secret sharing [13] as an extension to ordinary threshold secret sharing. Consider the following scenario: a master secret has been distributed among a number of users and a threshold amount of these wishes to reconstruct the master secret. Among their midst is a dishonest user which discloses a false share instead, making it impossible for the honest users to reconstruct the master secret. Furthermore, the honest users are unable to verify whether the disclosed shares are correct, so there is no way of knowing which user(s) has been dishonest. In Feldman's verifiable secret sharing scheme, additional public information (related to the master secret) is made available to every user which allows them to verify whether the disclosed shares are correct. Luo et al. [7], [8] incorporated this extension into their FD-TTP-based key management scheme to make it more robust against malicious adversaries. However, Saxena [4] proposed an alternative interpretation of the verifiable secret sharing scheme entirely.

Saxena [4] proposed a threshold-tolerant identity-based cryptosystem which is particularly suitable for ad hoc networks. He proposed that the secret shares should be used directly as private keys and that the associated public shares would be used as public keys. The secret shares are therefore no longer used as a tool to create additional keying material, reducing the memory storage overhead and computational overhead. Also, users can compute the public key of other network users from their identities and the publicly available information (also called commitment values or witness values, depending on the literature) in a non-interactive manner, minimizing the communication overhead. Finally, new users can join the network using the standard threshold secret sharing techniques. The design of a FD-TTP-based key management scheme for beyond 5G mobile small cells which is constructed from the threshold-tolerant identity-based cryptosystem seems to have efficiency benefits. However, such a key management scheme will only be secure as long as a malicious user is incapable of obtaining a threshold amount of private keys during the entire lifetime of the network [14], [15].

III. Preliminaries

A. Network Model

The incorporation of mobile small cells into the network infrastructure can provide major benefits. The mobile small cells, making use of D2D communications, are particularly suitable in the urban environment as the high density of mobile devices translates to many data requests but also provides many pathways between arbitrary users. This network infrastructure is capable of increasing data rates and energy efficiency while reducing latency and interference. However, many of these advantages should be credited to ordinary small cells. The strength of a radio signal diminishes with the square of the distance, therefore replacing the large transmissions to and from the base station (BS) by numerous shorter transmissions provide significant energy savings. The shorter and less power signals will also reduce interference and allows for increased data rates. Latency is reduced by providing a more direct route between a source node (SN) and a destination node (DN). Nevertheless, mobile small cells provide additional benefits. They can be set up on-the-fly, based on demand, at any place, at any time, using existing mobile devices. This wireless ad hoc network can therefore function at a low cost since network operators are not required to install and maintain additional network infrastructure. Furthermore, mobile small cells support time and space varying traffic [16].

The H2020-MSCA project "SECRET" [2] introduced this scenario architecture for the next generation cellular network as it provides opportunities for both network operators and network users. This scenario architecture is illustrated in Figure 1.

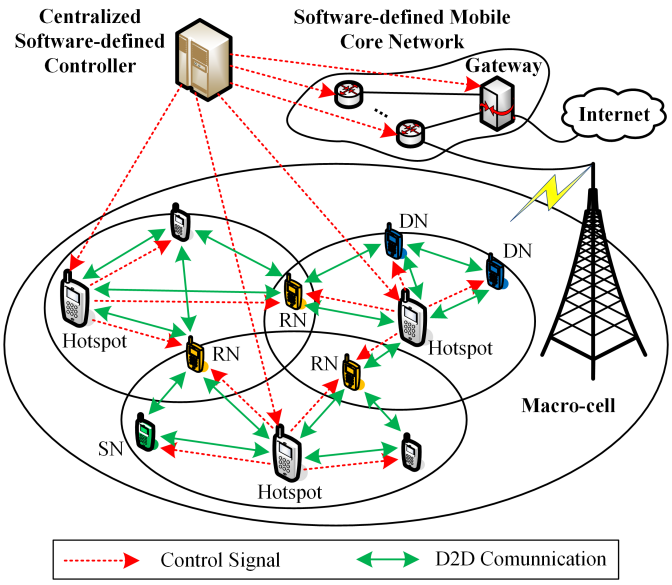

Fig. 1. The scenario architecture as introduced by project "SECRET" [3].

The cellular network, consisting of macro cells, is partitioned into a network of mobile small cells. Each mobile small cell is controlled and maintained by a hotspot. This is a mobile device that is selected to become the local radio manager. In addition, each hotspot is controlled by a centralized software-defined controller. Through cooperation, these hotspots form a wireless network that has several gateways to the mobile network using intelligent high-speed connections. Data traffic between the mobile devices is established through D2D communications and the use of relay nodes (RNs). Use cases include (i) a group of friends playing a multiplayer

game on their devices and (ii) the exchange of multimedia (i.e. pictures and videos) between devices. Using multi-hop D2D communications, data can be exchanged between a source node (SN) and a destination node (DN).

B. Adversarial Model

To provide security in a network of mobile small cells, we require an efficient and secure key management scheme which is able to function without requiring access to a centralized TTP. The utilization of threshold secret sharing to create a distributed TTP causes the key management scheme to be susceptible against the following secret sharing-related attacks.

- *Mobile Adversary*: A mobile adversary [14] dynamically moves through the network and compromises devices, one at a time, with the goal to collect a threshold amount of unique secret shares. A successful attack enables the adversary to reconstruct the master key and use it to compute the private keys of other users, eavesdrop on their private conversations, or launch identity impersonation attacks.
- *Sybil Attack*: In the Sybil attack [15], an adversary creates a large amount of unique identities and wishes to join the network with each one in order to be provided with a large set of secret shares. Collecting a threshold amount of secret shares enables the adversary to reconstruct the master key and use it to compute the private keys of other users, eavesdrop on their private conversations, or launch identity impersonation attacks.

C. Feldman's Verifiable Secret Sharing (VSS)

In Feldman's verifiable secret sharing scheme [13], a network administrator initializes a network of n users. The network administrator chooses two large primes p and q, such that q is a factor of $p-1$. The network administrator then chooses a generator g of cyclic subgroup $\mathbb{G} \subset \mathbb{Z}_p^*$ which has order q. All these values are then made public. The network administrator selects a security parameter t and a random polynomial $f(x)$ of degree $t-1$ with coefficients $a_i \in \mathbb{Z}_q^*$:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \tag{1}$$

Based on the polynomial coefficients, the network administrator computes the commitment values as:

$$c_i \equiv g^{a_i} \pmod{p} \mid 0 \leq i \leq t-1 \tag{2}$$

For every participating user j in the network, the network administrator provides a network identifier ID_j and secret share s_j:

$$s_j \equiv f(ID_j) \pmod{q} \tag{3}$$

The user j can use the public commitment values c_i to verify that its secret share s_j is correct using the following equation:

$$g^{s_j} \equiv \prod_{i=0}^{t-1} {c_i}^{{ID_j}^i} \pmod{p} \tag{4}$$

D. The Threshold-Tolerant Identity-based Cryptosystem

The verifiable secret sharing scheme by Feldman [13] can be translated into an identity-based cryptosystem. The distributed secret shares s_j would instead be used as private keys sk_j, the corresponding public shares then become public keys pk_j, and the commitment values c_i and the users' personal identifiers ID_j are publicly available information. This allows any user to non-interactively compute the public key of any other user (using equation 4). Saxena [4] proposed a threshold-tolerant identity-based cryptosystem for ad hoc networks which is based on this translation. The structure of key generation in the threshold-tolerant identity-based cryptosystem is illustrated in Figure 2.

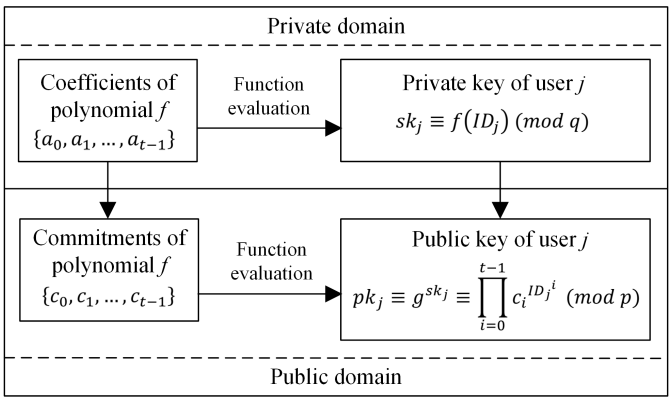

Fig. 2. Key generation in the threshold-tolerant identity-based cryptosystem.

Additionally, Saxena proposed three cryptographic procedures and named these the secret sharing-based pairwise key establishment procedure, the secret sharing-based signature procedure and the secret sharing-based encryption procedure. Each of these procedures rely on the discrete logarithm problem for security. To be exact, the pairwise key establishment procedure is based on the Diffie-Hellman key agreement technique, the signature procedure is based on Schnorr's signature scheme and the encryption procedure is based on ElGamal encryption.

IV. Our Proposals

In this section, we introduce two techniques to design a secure key management scheme for beyond 5G mobile small cells based on the threshold-tolerant identity-based cryptosystem.

A. Proactive Secret Sharing (PSS)

The popular method to prevent a mobile adversary from collecting a threshold number of shares over an extended period of time is by incorporating proactive secret sharing [5], [6]. In proactive secret sharing, the secret shares of every network user is periodically updated such that their updated shares are independent from the previous shares. A mobile adversary which managed to collect a number of shares below the threshold is unable to combine these with updated shares to reconstruct the master secret and break the security of the entire system (i.e. compute every user's private key). The mobile adversary therefore has to start over from scratch.

It is important to mention that the original description of proactive secret sharing wishes to update the shares while keeping the master secret the same. Keeping the master secret unchanged is an important requirement in other FD-TTP-based key management schemes since they are required to reconstruct the master secret to perform some kind of key management operation (e.g. signing a certificate). However, a key management scheme that is based on the threshold-tolerant identity-based cryptosystem does not require honest users to reconstruct the master secret and could therefore allow the master secret to change as well. A successful mobile adversary attack in other FD-TTP-based key management schemes therefore leads to a compromised network for its entire lifetime, whereas the threshold-tolerant identity-based cryptosystem key management scheme will only be compromised during that particular period in between updating phases. This additional layer of security may allow updating phases to be less frequent, leading to a futher reduction of the communication overhead compared to other FD-TTP-based key management schemes.

Proactive secret sharing effectively updates every user's private key, its corresponding public key and the public commitment values. This key updating procedure is equivalent to the two updating procedures which are necessary in the other FD-TTP-based key management schemes (e.g., the key updating procedure and the share updating procedure). Furthermore, periodic key updating also provides benefits in terms of key revocation. By limiting the amount of time between key compromise and key expiration (through updating), key revocation may become redundant [17], [18]. These consequences allow for a more elegant and simplistic key management design.

However, proactive secret sharing is solely designed to prevent a mobile adversary attack and is incapable of preventing the Sybil attack. To prevent the Sybil attack, admission control would have to be organized in cooperation with the existing network infrastructure. Network operators have access to identifying information of their subscribers and thus have the ability to consider and authorize whether or not a user may participate and communicate through the network of mobile small cells. The network operators could provide their subscribers with some kind of token, acting as an indicator for network users that a requesting user can be safely added to the network.

B. Private Key Cloaking

An alternative solution would be to cloak the value of the private key by combining it with an additional public-private key pair. We name this technique "private key cloaking" and is similar to key generation in certificateless public key cryptography [19]. In certificateless public key cryptography, every user obtains a partial private key (the private key which corresponds to the user's identity) from the TTP and generates an additional partial key pair. Both partial private keys are combined into the user's private key while the public keys remain separated. The public key which corresponds to the user's identity can be estimated from publicly available information, whereas the additional public key has to be exchanged between users. The additional public key does not need to be certified, since a malicious adversary is unable to benefit from launching a key replacement attack (i.e. the malicious adversary does not have access to the partial private key corresponding to the user's identity). Key generation is similar in our proposal, except that we replace the identity-based public-private key pair for the secret sharing-based public-private key pair. The key generation structure is illustrated in Figure 3.

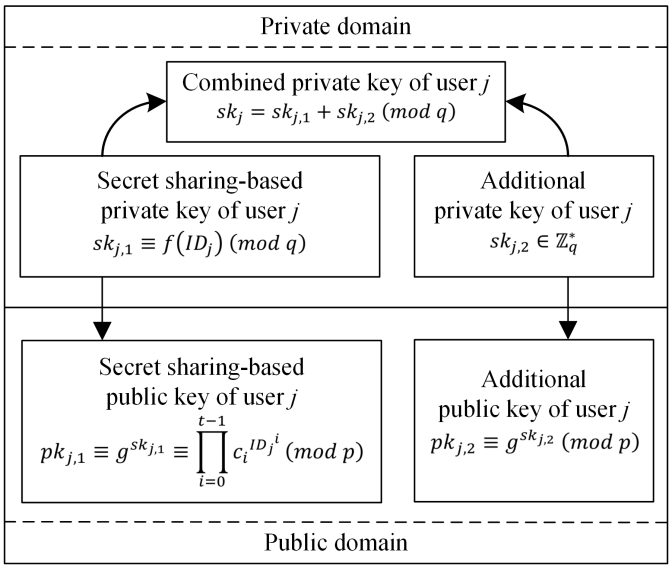

Fig. 3. Key generation with private key cloaking.

This key generation structure effectively cloaks the value of the secret share, preventing a mobile adversary from collecting a threshold amount of secret shares (or even a single one). An additional advantage to this solution is that the threshold t could be set to a reasonably low value. This means that users do not need to store as many public commitment values in the memory of their devices and thus reduces the memory storage overhead.

The reduced threshold also affects the user admittance process. New users can be admitted to the network by sending a request to a threshold number of network users for its private key. These network users would securely provide the joining user with a share of its private key (i.e. its cloaked secret share) and the joining user would combine these to establish its own private key. The reduced threshold means that it becomes easier for a new user to join the network since it is more likely that it has a threshold amount of network users within its transmission range. Furthermore, the communication overhead is reduced as fewer transmissions are required. A Sybil attack is also prevented with this technique since new users (or the same user with multiple identities) are unable to compute their secret sharing-based private key from the obtained private key.

However, there is also a downside to the private key cloaking technique. As is also the case in certificateless public key cryptography, only one of the two public keys can be computed non-interactively from the publicly available information (i.e. the user's identity and the commitment values). The additional public key must still be transmitted through the network before two users can establish a secure

channel. Similarly, this additional public key does not need to be certified as a malicious attacker would not benefit from launching a man-in-the-middle attack.

V. Future Work

In our future work, we will design a key management scheme for each proposed extension. This key management scheme is expected to include: (i) a network initialization phase with a master key creation and private key distribution protocol, and (ii) a network operational phase with a pairwise key establishment protocol, a key updating protocol and a threshold key distribution protocol to support joining users. These key management schemes will be evaluated and compared with related FD-TTP-based key management schemes.

VI. Conclusion

In this paper, we studied whether we can design an efficient and secure fully distributed key management scheme based on the threshold-tolerant identity-based cryptosystem for beyond 5G mobile small cells. To provide security in beyond 5G mobile small cells, we require resistance against mobile adversary and Sybil attacks. We proposed the incorporation of proactive secret sharing and found that such a key management scheme can reach a higher level of security, have a reduced overhead and will be more simplistic compared to related FD-TTP-based key management schemes. However, this extension is incapable of providing resistance against a Sybil attack. We also proposed the incorporation of private key cloaking and found that such a key management scheme can effectively prevent both the mobile adversary and the Sybil attack at the cost of an increased communication overhead.

References

[1] J. Carmody, "New Year's Texting Data Load to Surge as Clock Ticks over to 2018." ABC News. https://www.abc.net.au/news/2017-12-31/new-years-texting-data-load-to-surge-as-clock-strikes-midnight/9294372 (accessed Mar. 23, 2020).

[2] J. Rodriguez et al. "SECRET - Secure Network Coding for Reduced Energy Next Generation Mobile Small Cells: A European Training Network in Wireless Communications and Networking for 5G," in *Proc. 7th Int. Conf. Internet Technologies and Applications (ITA)*, Wrexham, UK, Sep. 2017, pp. 329-333.

[3] M. de Ree, G. Mantas, A. Radwan, S. Mumtaz, J. Rodriguez, and I. E. Otung, "Key Management for Beyond 5G Mobile Small Cells: A Survey," *IEEE Access*, vol. 7, pp. 59200-59236, May 2019.

[4] N. Saxena, "Public Key Cryptography sans Certificates in Ad Hoc Networks," in *Proc. 4th Int'l. Conf. Applied Cryptographhy and Network Security (ACNS)*, Singapore, Singapore, Jun. 2006, pp. 375-389.

[5] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung, "Proactive Secret Sharing OR: How to Cope with Perpetual Leakage," *Proc. CRYPTO*, Santa Barbara, CA, USA, Aug. 1995, pp. 339-352.

[6] S. Jarecki, "Proactive Secret Sharing Public Key Cryptosystems," M.S. thesis, Dept. Elect. Eng. Comput. Sci., Massachusetts Inst. Technol., Cambridge, MA, USA, 1995.

[7] H. Luo and S. Lu, "Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks," Dept. Comp. Sci., Univ. California, Los Angeles, CA, USA, Tech. Rep. UCLA-CSD-TR-200030, Oct. 2000.

[8] H. Luo, J. Kong, P. Zerfos, S. Lu and L. Zhang, "URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks," *IEEE/ACM Trans. Netw.*, vol. 12, no. 6, pp. 1049-1063, Dec. 2004.

[9] A. Shamir, "How to Share a Secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, Nov. 1979.

[10] H. Deng and D. P. Agrawal, "TIDS: Threshold and Identity-based Security Scheme for Wireless Ad Hoc Networks," *Ad Hoc Networks*, vol. 2, no. 3, pp. 291-307, Jul. 2004.

[11] Z. Zhang, W. Susilo and R. Raad, "Mobile Ad-Hoc Network Key Management with Certificateless Cryptography" *Proc. 2nd Int. Conf. Signal Process. Commun. Syst. (ICSPCS)*, Gold Coast, QLD, Australia, Dec. 2008, pp. 1-10.

[12] M. de Ree, G. Mantas, J. Rodriguez and I. E. Otung, "Distributed Trusted Authority-based Key Management for Beyond 5G Network Coding-enabled Mobile Small Cells," *Proc. 2nd IEEE 5G World Forum (5GWF)*, Dresden, Germany, Sep. 2019, pp. 80-86.

[13] P. Feldman, "A Practical Scheme for Non-Interactive Verifiable Secret Sharing," in *Proc. 28th Ann. Symp. Foundations of Computer Science (SFCS)*, Los Angeles, CA, USA, Oct. 1987, pp. 427-437.

[14] R. Ostrovsky and M. Yung, "How to Withstand Mobile Virus Attacks," in *Proc. 10th ACM Symp. Principles of Distributed Compututing (PODC)*, Montreal, QC, Canada, Aug. 1991, pp. 51-59.

[15] J. R. Douceur, "The Sybil Attack," in *Proc. Int. Workshop Peer-to-Peer Systems (IPTPS)*, Cambridge, MA, USA, Mar. 2002, pp. 251-260.

[16] S.-F. Chou, T.-C. Chiu, Y.-J. Yu and A.-C. Pang, "Mobile Small Cell Deployment for Next Generation Cellular Networks," *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Austin, TX, USA, Dec. 2014, pp. 4852-4857.

[17] K. Hoeper and G. Gong, "Bootstrapping Security in Mobile Ad Hoc Networks using Identity-based Schemes," in *Security in Distributed and Networking Systems*, Y. Xiao and Y. Pan, Eds., World Scientific, 2007, pp. 313-337.

[18] J. Lai, W. Kou and K. Chen, "Self-Generated-Certificate Public Key Encryption without Pairing and its Application," *Information Sciences*, vol. 181, no. 11, pp. 2422-2435, Jun. 2011.

[19] S. S. Al-Riyami and K. G. Paterson, "Certificateless Public Key Cryptography," *Proc. ASIACRYPT*, Taipei, Taiwan, Nov. 2003, pp. 452-473.