IEICE TRANS. INF. & SYST., VOL.E99–D, NO.8 AUGUST 2016

INVITED PAPER *Special Section on Security, Privacy and Anonymity of Internet of Things*

Challenges of Fully Homomorphic Encryptions for the Internet of Things

Licheng WANG[†a)], ***Member***, **Jing LI**[†b)], ***and*** **Haseeb AHMAD**[†c)], ***Nonmembers***

SUMMARY With the flourish of applications based on the Internet of Things (IoT), privacy issues have been attracting a lot of attentions. Although the concept of privacy homomorphism was proposed along with the birth of the well-known RSA cryptosystems, cryptographers over the world have spent about three decades for finding the first implementation of the so-called fully homomorphic encryption (FHE). Despite of, currently known FHE schemes, including the original Gentry's scheme and many subsequent improvements as well as the other alternatives, are not appropriate for IoT-oriented applications because most of them suffer from the problems of inefficient key size and noisy restraining. In addition, for providing fully support to IoT-oriented applications, symmetric fully homomorphic encryptions are also highly desirable. This survey presents an analysis on the challenges of designing secure and practical FHE for IoT, from the perspectives of lightweight requirements as well as the security requirements. In particular, some issues about designing noise-free FHE schemes would be addressed.

key words: *Internet of Things (IoT), fully homomorphic encryption (FHE), challenges, cloud*

1. Introduction

We are witnessing the mutual promotion and rapid development of the Internet of Things (IoT) and cloud computing [19], [29], [34], [43], [51], [52], [56]. Let us consider a futuristic scenario of intensive care units (ICUs)* where patients' real-time health information is continuously collected by *a life-supporting system*, and streamed to some *cloud servers* that for computing the required statistics over these measurements and presumably decide on the course of treatments (e.g., changing the dosage of medicine) [30]. Towards this scenario, we further remind that

- A life-supporting system is generally comprised of a set of wired or wireless devices that could be big (such as respirator and ECG Monitor), small or even tiny (such as RFIDs, sensors, or smart capsules), and work in a collaborative and intelligent manner.
- The involved cloud servers must be *private* and accessible to those who work in the hospital, *or public* and the access should be granted to legitimate users via the Internet. Thus, the collected health information and the treatment instructions are highly sensitive and vital, and hence, these must be regarded as patients' top secrecy and privacy.
- The volume of the collected data could be so large, therefore, it might be troublesome for the patients and even the hospitals to store and manage all real-time data locally. Instead, they may prefer to outsource the storage and computation to some national/international leveled service providers.

The core requirement sighted by the aforementioned scenario is to answer that how to enjoy the convenient services provided by the IoT and the cloud, but meantime without suffering from the menace of privacy leakage. At present, concerning over loss of privacy is an overwhelming barrier towards the adoption of IoT and cloud services [30]. An *ideal* solution of towards this problem is to store all data in the encrypted form and perform computations on encrypted data, without fully decrypting the data on the cloud [33]. To this end, we need an encryption scheme that allows meaningful computation on encrypted data, namely a *homomorphic encryption (HE)* scheme.

The cryptographic primitive of homomorphic encryption is embedded in the concept of *privacy homomorphism* that was first proposed by Rivest, Adleman and Dertouzos in 1978 when they conceived the idea of data bank [41]. In fact, fully privacy supportive homomorphism requires a *fully homomorphic encryption (FHE)* scheme that was kept unavailable until 2009. At STOC 2009, Gentry [20] made the breakthrough for constructing the first FHE scheme. Since then, a lot of subsequent developments and improvements were proposed [6], [15], [45], [47]. Meanwhile, there has been much discussion in the industry as to whether FHE is implementable and practical. This is also the main concern of this paper, in particular, taking into account of the IoT scenario.

The rest of contents are organized as follows. Basic concepts and taxonomy of (fully) homomorphic encryption are given in Sect. 2; A quick review on partial homomorphic encryption schemes are given in Sect. 3; In Sect. 4, recent constructions of somewhat homomorphic encryption and fully homomorphic encryption, as well as the main technique – bootstrapping are analyzed; In Sect. 5, we pay attention to continuous optimizations on existing fully homo-

Manuscript received December 14, 2015.
Manuscript revised April 24, 2016.
Manuscript publicized May 31, 2016.

[†]The authors are with State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, P.R. China.
a) E-mail: wanglc@bupt.edu.cn
b) E-mail: lijingbeiyou@163.com
c) E-mail: haseeb_ad@hotmail.com

DOI: 10.1587/transinf.2015INI0003

*In a modern hospital, ICUs have already become one of the standard configurations by which serious patients are taken intensively cares.

morphic encryption schemes; In Sect. 6, challenges for using fully homomorphic encryptions in the IoT, and recent attempts for designing the IoT-friendly noise-free symmetric homomorphic encryption schemes are explored; Finally, concluding remarks are given in Sect. 7.

2. Homomorphic Encryptions and Taxonomy

Originally, the adjunct "fully" in FHE means to support all operations with respect to a given circuit set. But now, it always means to support universal and logical-complete set of operations, such as

- addition and multiplication towards arithmetic operations, or
- AND/OR and NOT gates towards Boolean logical operations.

However, before Gentry's breakthrough, we have merely known some homomorphic encryption schemes that support *a single kind of* homomorphic operations over encrypted data. For instances, both the RSA scheme [42] and the ElGamal scheme [18] (ElG for abbr.) merely support multiplicative homomorphism over ciphertexts in the sense that

$$\mathcal{D}(\mathcal{E}(m_1)\cdot\mathcal{E}(m_2) \bmod N) \equiv m_1\cdot m_2 \pmod N \tag{1}$$

(for RSA) and

$$\mathcal{D}(\mathcal{E}(m_1)\odot\mathcal{E}(m_2) \bmod p) \equiv m_1\cdot m_2 \pmod p \tag{2}$$

(for ElG), where the operator $\odot$ denotes the componentwise multiplication modulo p, while $\mathcal{D}: C\to\mathcal{M}$ and $\mathcal{E}:\mathcal{M}\to C$ are decryption and encryption algorithms with respect to the message space $\mathcal{M}$ and ciphertext space C, respectively. Similarly, the Paillier scheme [38] (Pai for abbr.) merely supports additive homomorphism over ciphertexts in the sense that

$$\mathcal{D}(\mathcal{E}(m_1)\cdot\mathcal{E}(m_2) \bmod N^2) \equiv m_1+m_2 \pmod N, \tag{3}$$

while the Goldwasser-Micali scheme [23] (GM for abbr.) merely supports bit-wise XOR (i.e. addition modulo 2) homomorphism over ciphertexts in the sense that

$$\mathcal{D}(\mathcal{E}(m_1)\cdot\mathcal{E}(m_2) \bmod N) \equiv m_1+m_2 \pmod 2. \tag{4}$$

Remark 1: Note that when we say that a cryptographic operation is a homomorphism, we do not mean that it is an exact homomorphic map according to mathematical definition. As for first reason, for example, a mathematical definition of a homomorphic encryption map $\mathcal{E}:\mathcal{M}\to C$ requires that either

$$\mathcal{E}(m_1)\odot\mathcal{E}(m_2) = \mathcal{E}(m_1\cdot m_2), (\forall m_1, m_2\in\mathcal{M}) \tag{5}$$

holds, or

$$\mathcal{E}(m_1)\odot\mathcal{E}(m_2) = \mathcal{E}(m_1+m_2), (\forall m_1, m_2\in\mathcal{M}) \tag{6}$$

holds, where $\odot: C\times C\to C$ is a well-defined ciphertext composition algorithm, which supports or accepts different instantiations with respect to different homomorphic encryption schemes. However, many encryption algorithms are probabilistic, two times encryptions towards a same message will lead to two different ciphertexts with overwhelming probability. In other words, the equalities in formula (5) and (6) do not hold in general, except for negligible probability. The second reason is that, implicitly suggested by (1), (2), (3) and (4), the homomorphic property of encryption algorithm is in fact specified by the mutual action between the decryption algorithm $D: C\to\mathcal{M}$ and the corresponding ciphertext composition operation $\odot: C\times C\to C$. The third reason lies in that for the homomorphic property of cryptographic operations, exceptions with negligible proportions are admissible. That is, a $\star$-homomorphic encryption algorithm $\mathcal{E}:\mathcal{M}\to C$ requires that for some well-defined message composition algorithm $\star:\mathcal{M}\to\mathcal{M}$ and some well-defined ciphertext composition algorithm $\odot: C\times C\to C$, the following probability

$$\Pr_{c_1,c_2\in C}[\mathcal{D}(c_1\odot c_2)\neq\mathcal{D}(c_1)\star\mathcal{D}(c_2)] \tag{7}$$

is negligible with respect to some system parameters, say $\log|\mathcal{M}|$ or $\log|C|$, and so on [†]. It is worth to note that the expression (7) cannot be replaced by

$$\Pr_{m_1,m_2\in\mathcal{M}}[\mathcal{D}(\mathcal{E}(m_1)\odot\mathcal{E}(m_2))\neq m_1\star m_2], \tag{8}$$

although the later seems *even closer* to our intuition about the concept of homomorphic encryption. In fact, the formula (8) merely captures the meaning of one layer homomorphic composition over encrypted messages, while the formula (7) requires that the homomorphic composition over ciphertexts should be performed without any limitations [††]. Therefore, to some extent, we can say that the true meaning of homomorphic encryption is *homomorphic decryption*.

Now, suppose that $\mathtt{OP}=\{\star_1,\cdots,\star_n\}$ is an operation set over the message space $\mathcal{M}$. Then, if there are n well-defined ciphertext composition algorithms $\odot_j: C\times C\to C, (j=1,\cdots,n)$, such that all the following probabilities

$$\Pr_{c_1,c_2\in C}[\mathcal{D}(c_1\odot_j c_2)\neq\mathcal{D}(c_1)\star_j\mathcal{D}(c_2)] \tag{9}$$

are negligible with respect to some system parameters, we say that $\mathcal{E}:\mathcal{M}\to C$ is a *homomorphic encryption (HE)* with respect to the operation set $\mathtt{OP}$. Furthermore, if $\mathtt{OP}$ is universal and logical-complete, i.e., all possible operations over $\mathcal{M}$ can be represented as a finite composition sequence of operations in $\mathtt{OP}$, we say that $\mathcal{E}$ is a *fully homomorphic encryption (FHE)* over message space $\mathcal{M}$. For an HE algorithm $\mathcal{E}$, the failure of achieving fully homomorphism over ciphertext space might due to the following two reasons:

[†]Here, we need a further agreement: If for some $c\in C$, $\mathcal{D}(c)=\perp$, i.e., c is not a valid ciphertext, then we define that $\mathcal{D}(c)\star\mathcal{D}(c')=\perp$ for $\forall c'\in C$.

[††]Further exploration on the difference between the formula (7) and (8) will also lead to the so-called concept of somewhat homomorphic encryption (SHE).

- $\mathtt{OP}$ is not a universal and logical-complete operation set. For instances, as for the aforementioned homomorphic encryption schemes, the $\mathtt{OP}$s are defined as $\mathtt{OP}_{RSA} = \langle\cdot\rangle_N$, $\mathtt{OP}_{ElG} = \langle\cdot\rangle_p$, $\mathtt{OP}_{Pai} = \langle+\rangle_N$, and $\mathtt{OP}_{GM} = \langle+\rangle_2 = XOR$, respectively, where $\langle\star\rangle_m$ indicates taking the remainder with respect to modulo m after performing the operation $\star$. We refer this category of HE algorithms as *partially homomorphic encryption (PHE)* algorithms.
- $\mathtt{OP}$ is universal and logical-complete, but for some operation $\star_j \in \mathtt{OP}$, the corresponding ciphertext composition algorithm $\odot_j$ is merely allowed nesting a limited layers. For instances, all currently known somewhat homomorphic encryption algorithms [6], [15], [20]–[22], [45], [47] lie in this category. In addition, the well-known pairing-based BGN scheme [3] also lies in this category since it supports arbitrary layers additive composition and only one layer multiplicative composition. Let us refer this category HE algorithms as *somewhat homomorphic encryption (SHE)* algorithms.

The taxonomy of HE algorithms is depicted as Fig. 1.

Another property related to (homomorphic) encryption is the so-called *compactness*, or *ciphertext expansion ratio*. A (homomorphic) encryption scheme is said to be ρ-*compact* if the length of a ciphertext is *no larger than* ρ times of the length of the corresponding message. That is,

$$\rho \triangleq \max_{m\in\mathcal{M}} \frac{|\mathcal{E}(m)|}{|m|}, \tag{10}$$

where $|x|$ indicates the length of x, and in general, it always means the bit-length, if without further specification. Here, we adopt the phrase of "no larger than" in definition of ρ-compactness with the purpose to obtain the following compatibility: On one hand, a ρ-compact encryption scheme is also ρ'-compact for any $\rho' > \rho$; on the other hand, if we further employ complexity symbols such as O and $\tilde{O}$ in discussing the rough magnitude of ρ, we have that for any constant c, a c-compact encryption scheme is also $O(1)$-compact, and similarly, a $O(n^k)$-compact encryption is also $\tilde{O}(n^k)$-compact, considering that by using $\tilde{O}$, we omit some polylogarithmic factors (i.e., $O(\log^c n)$ for some constant c). Without doubt, this property is in particular important for the IoT-oriented applications because that large ciphertext expansion factor means large bandwidth, storage and energy consumption in most cases.

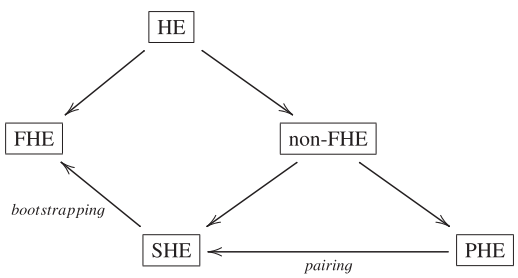

Fig. 1 Taxonomy of HE

3. Partial Homomorphic Encryptions

Although a PHE scheme fails to support homomorphism over a universal and logical-complete operation set, it is still very useful in practice. During the past three decades, we have not only worked out many mature FHE schemes, but also successfully engaged them into variety applications. For instances, both the GM scheme [23] and the Pai scheme [38] found numerous applications such as encrypted data aggregation, privacy-preserving distributed data mining [25], biometric authentications [7], etc.

During the past decades, an observable achievement in cryptography community is the continuous improvements, especially in compactness, towards the aforementioned PHE schemes. The RSA scheme is indeed an elegant design in the sense that it is 1-compact, we expect the optimal compactness for a cryptosystem that fully supports the entire message recovery. However, the compactness of the original GM scheme is as large as $\log N$. At Eurocrypt 1998, Okamoto and Uchiyama [37] made a remarkable progress by achieving a 3-compact additive HE scheme. This record was quickly renovated by Paillier one year late [38]: The compactness of the Paillier's scheme achieves 2. At PKC 2001, Damgård and Jurik [14] proposed an additive HE scheme that is almost 1-compact at the expense of enlarge the ciphertext space from N to N^k for sufficient large k. More recently, Joye and Libert [24] improved the Naccache-Stern cryptosystem by setting $k = 2^\alpha$, leading to an additive HE scheme with about 4-compactness.

In brief, the main PHE schemes, as well as their features, are listed in Table 1.

4. Somewhat/Fully Homomorphic Encryptions and Bootstrapping

Although BGN05 [3] lies in the category of somewhat homomorphic encryption (SHE) according to the taxonomy given in the previous section, the first formal appearance of the concept of SHE was in fact put forward by Gentry

Table 1 Partially homomorphic encryption schemes

Year	Contributors	Hom. Operations	ρ
1978	Rivest, Shamir and Adleman [42]	$\langle\cdot\rangle_N$	1
1982	Goldwasser and Micali [23]	$\langle+\rangle_2$ (i.e. XOR)	$O(\log N)$
1984	ElGamal [18]	$\langle\cdot\rangle_p$	2
1985	Cohen and Fischer [9]	$\langle+\rangle_p$ (for small prime p)	$O(\frac{\log N}{\log p})$
1994	Benaloh [2]	$\langle+\rangle_p$ (for small prime p)	$O(\frac{\log N}{\log p})$
1998	Naccache and Stern [35]	$\langle+\rangle_{\prod p_i}$ (for small primes p_i)	$O(\frac{\log N}{\log \prod p_i})$
1998	Okamoto and Uchiyama [37]	$\langle+\rangle_p$	3
1999	Paillier [38]	$\langle+\rangle_N$	2
2001	Damgård and Jurik [14]	$\langle+\rangle_{N^{k-1}}$	$1+\frac{k-1}{k}$
2005	BGN [3]	$\langle+\rangle_p$	$O(\frac{\log n}{\log T})$
		$\langle\cdot\rangle_p$ (only 1 time)	$(T < \sqrt{n})$
2013	Joye and Libert [24]	$\langle+\rangle_{2^\alpha}$	≈ 4

in 2009 [20]. Gentry's SHE scheme is capable of evaluating "low-degree" polynomials homomorphically [5]. More precisely, it supports arbitrary layers addition modulo 2 (i.e., XOR) and limited layers multiplication modulo 2 (i.e., AND) over encrypted bits. Similar to all known lattice-based cryptosystems, Gentry's SHE scheme, based on ideal lattice, also introduces noise as its footstone of the security. However, the magnitude of noise increases instantly with the homomorphic operations: The resultant noise increases linearly with the number of layers of homomorphic additions, while it increases exponentially with the number of layers of homomorphic multiplications. Whenever the magnitude of the noise in a ciphertext exceeds certain threshold, the ciphertext cannot be decrypted correctly. Therefore, Gentry's SHE scheme can only support logarithmic depth homomorphic multiplications.

To transform an SHE scheme to an FHE scheme, Gentry invented the so-called *bootstrapping* technique [20] (captured by the following theorem) is now the main blueprint for designing FHE schemes.

Theorem 1 (Bootstrapping Theorem, [20]): If an SHE scheme $\mathcal{E}$ has the self-referential property of being able to handle its own decryption function (augmented by a single gate), we say that it is *bootstrappable*. Furthermore, if $\mathcal{E}$ is bootstrappable, then one can use $\mathcal{E}$ to construct a fully homomorphic encryption scheme $\mathcal{E}^+$.

In principle, bootstrapping "refreshes" a ciphertext that contains big noise by running the decryption algorithm homomorphically, using an encrypted secret key — this can be added as a part of public key, resulting a new ciphertext for the same message but with a reduced noise [5]. Then, if the depth of the decryption circuit is small enough, say logarithmic, we can obtain an FHE by coupling the SHE scheme along with this kind of bootstrapping process. Unfortunately, many SHE schemes tend to be incapable of evaluating their own decryption circuits without significant modifications [5]. Therefore, Gentry's final blow is to *squash the decryption circuit* of the SHE scheme. That is, we need to transform the SHE scheme into one with a decryption circuit that is simple enough to allow bootstrapping, of course without discounting its homomorphic capacity. Gentry's core idea for doing this is to introduce a "hint" information into the public key: a large set with a secret sparse subset that sums to the original secret key [5].

Another famous FHE scheme, due to Dijk et al. [15] is based on integers, i.e., without relying on lattice theory. This scheme also follows Gentry's blueprint in the sense that it is comprised of the following two components: an SHE scheme that supports arbitrary additive homomorphism and limited multiplicative homomorphism over encrypted data, and a bootstrapping algorithm based on Gentry's squashing decryption method.

At FOCS 2011, Gentry [21] and Brakerski [6] proposed new methods for constructing FHE *without using the squashing step, respectively*. Moreover, the security of the Brakerski-Vaikuntanathan scheme is based on LWE assumption, without reliance on ideal lattices. But both of the schemes still follow Gentry's blueprint, namely, an SHE scheme plus a bootstrapping mechanism.

Based on the new technical tool for noise management – *modulus switching* that was developed by Brakerski and Vaikuntanathan [6], a radically new approach for building FHE *without using the bootstrapping procedure* was found in 2011 [5]. Shortly afterwards, even the modulus switching process was removed for building FHE scheme [4].

5. Continuous Optimizations on Fully Homomorphic Encryptions

Since Gentry's discovery of the first FHE scheme, a lot of optimizations have been made, either for basing the security of FHE on more standard and well understood assumptions, or for improving the efficiency of Gentry's initial scheme [17].

At PKC 2010, Smart and Vercauteren [46] proposed an FHE scheme, which offers the both relatively small key and ciphertext size. At a high level, the scheme is described using the elementary theory of algebraic number fields, hence, we do not require to understand lattice theory for its encryption and decryption operations [46]. In addition, the public and private keys consist of two large integers and the ciphertext consists of only one large integer. Therefore, this scheme has smaller message expansion and key size than Gentry's original scheme. However, the expected multiplicative depth of the underlying SHE scheme is in a *log-logarithmic* scale. Thus, to obtain a real FHE scheme, the related parameters must be large enough. In addition, just like the situation of the NTRU cryptosystem, the Smart-Vercauteren scheme falls into the category of schemes whose best known attack is based on lattices. Then, with the purpose to maintain the capability of bootstrapping and the security, the dimension of the relation lattices should be no less than 2^{27}. This leads towards a difficulty for key generation in practice [46]. At Asiacrypt 2010, Stehlé and Steinfeld [48] introduced an optimization by using a probabilistic decryption algorithm that can be implemented by a multiplicative algebraic circuit with low orders. Comparing with Gentry's original FHE scheme, this scheme performs faster: the per-gate circuit complexity[†] is reduced from $\tilde{O}(\lambda^6)$ to $\tilde{O}(\lambda^{3.5})$, where λ is the security parameter. At Eurocrypt 2011, Gentry and Halevi [21] presented two major optimizations towards the Smart-Vercauteren scheme: an efficient key generation procedure based on the Fast Fourier Transform, and a simpler decryption circuit. Along with some other minor improvements, Gentry and Halevi put forward an actual implementation of their FHE scheme while testing it on different settings. According to their reports [21], with the settings of lattice dimensions 512, 2048,

[†]Here, the term "per-gate circuit complexity" (or "per-gate complexity" in simplicity) means the average bit-complexity for homomorphically combining encrypted bits according to basic logic-gates (say AND, OR and NOT) or arithmetic gates (say ADD and MUL).

8192, and 32768, the public key size ranges in size from 70MB to 2.3GB, respectively; and accordingly, the time for bootstrapping ranges from 30 seconds to 30 minutes. Apparently, this performance is unacceptable for most applications, needless to say for lightweight ones such as IoT environments. At Crypto 2014, Halevi and Shoup reported their implementation of FHE library, HElib[†]: the bootstrapping procedure took around 6 minutes. Very recently, this record is drastically renovated by Ducas and Micciancio [17]: Their implementation of bootstrapping runs on a personal computer in just about half a second!

Parallelization is another typical mechanism for enhancing the performance of computational tasks. In 2011, Smart and Vercauteren [47] pointed out that the key generation method of [21] appears to exclude the SIMD (i.e., Single Instruction Multiple Data) style operation alluded to by [46]. Then, they showed how to select parameters to enable such SIMD operations, and meantime maintaining the practicality of the key generation technique of [21]. As a result, they obtain an SHE scheme that supports both SIMD operations and operations over large finite fields of characteristic two. This enables the new SHE scheme to be made fully homomorphic by recrypting all data elements seperately. In other words, the SIMD operations can be used to perform the recrypting procedure in a parallel manner, resulting in a substantial speed-up [47].

Considering one of the main criticism towards Gentry's FHE scheme that is the costly bootstrapping process in which the step of squashing the decryption circuit takes a large proposition, Gentry and Halevi [21] proposed another new technique for building FHE without using the squashing step. Their core idea is to combine an SHE scheme with a "compatible" multiplicative HE scheme (MFE for abbr.) such as ElGamal in a surprising way: First, the decryption circuit of the SHE scheme is represented as a $\sum\prod\sum$-like arithmetic circuit with depth 3; then, the $\prod$-part can be homomorphically evaluated by the MHE scheme, and during the bootstrapping process, the entire leveled FHE ciphertext consists of a single ElGamal ciphertext; Finally, the MHE scheme is replaced by an additive HE scheme (AHE for abbr.) that encrypts discrete logarithms. As a result, this method enables the SHE scheme having the capability to evaluate the decryption circuit of the MHE scheme, irrespective of evaluating the decryption circuit of the SHE scheme itself. Based on these optimizations, the Gentry-Halevi scheme has the following features: (1) replacing the sparse subset sum problem assumption with a more simple and standard assumption – the well-known decisional Diffie-Hellman (DDH) assumption; and (2) avoiding the circularity that necessitates squashing in Gentry's original blueprint.

Perhaps, the most radical progress towards Gentry's blueprint, at least in theoretical aspect, is the so-called *modulus switching* technique due to Brakerski and Vaikuntanathan [6]. The essence of the modulus-switching technique is captured in the following lemma.

[†]See https://github.com/shaih/HElib

Lemma 1 (Modulus Switching, [5]): For given two odd moduli p and q, and an integer vector $\vec{c}$, we define $\vec{c}'$ as the vector closest to $(p/q)\cdot\vec{c}$ such that $\vec{c}' = \vec{c} \bmod 2$. Then, for any vector $\vec{s}$ with

$$\left|[\langle\vec{c},\vec{s}\rangle]_q\right| < \frac{q}{2} - \frac{q}{p}\ell_1(\vec{s}), \tag{11}$$

we have

$$\left[[\langle\vec{c}',\vec{s}\rangle]_p\right]_2 = \left[[\langle\vec{c},\vec{s}\rangle]_q\right]_2, \tag{12}$$

and

$$\left|[\langle\vec{c}',\vec{s}\rangle]_p\right| < \frac{p}{q}\left|[\langle\vec{c},\vec{s}\rangle]_q\right| + \ell_1(\vec{s}), \tag{13}$$

where $\ell_1(\vec{s})$ is the ℓ_1-norm of $\vec{s}$, while $[\cdot]_q$, $[\cdot]_p$ and $[\cdot]_2$ indicates taking modulo q, p and 2, respectively.

In brief, the lemma states that one can, without knowing a secret key $\vec{s}$, instead only knowing a bound on its length, can transform a ciphertext $\vec{c}$ modulo q into another ciphertext $\vec{c}'$ modulo p while preserving correctness (in the sense of (12)). Moreover, if $\vec{s}$ is short and p is sufficient smaller than q, then the "noise" in the transformed ciphertext actually decreases (in the sense of (13)). Apparently, this lemma enable us to reduce the magnitude of the noise without knowing the secret key, and without relying on a bootstrapping process. To some extent, modulus switching is a *lightweight* way for managing noise in FHEs. By using this method, Brakerski, Gentry and Vaikuntanathan [5] derived two leveled FHE schemes based on ring-LWE (RLWE) assumption: one can evaluate L-level arithmetic circuits with per-gate complexity $\tilde{O}(\lambda\cdot L^3)$, i.e., *quasi-linear* in the security parameter λ, while the other, still using bootstrapping as an optimization, can reduce the per-gate complexity to $\tilde{O}(\lambda^2)$, i.e., *quadratic in* λ *but independent of* L. This is indeed a remarkable progress, considering that the per-gate complexities of all previous FHE schemes are no lower than $\tilde{O}(\lambda^{3.5})$.

Besides the continuous improvements towards lattice-based FHEs, cryptographers have also made a lot of optimizations towards integer-based FHEs. The first integer-based FHE scheme (DGHV for abbr.) [15], has $\tilde{O}(\lambda^8)$ overhead (mainly in encrypting and bootstrapping) with respect to the security parameter λ, and also suffers from an inefficient in key size – about $\tilde{O}(\lambda^{10})$. Note that, the corresponding SHE scheme of DGHV has overhead $\tilde{O}(\lambda^4)$. At Crypto 2011, Coron et al. [11] reduced the key size to $\tilde{O}(\lambda^7)$. Their core idea is to store only a smaller subset of the public key and then let the full public key can be generated on the fly by multiplicatively combining the elements in the small subset [11]. According to their reports, for achieving 72-bits security, the size of the corresponding public key was about 800MB, the encryption and the bootstrapping (i.e., recrypting) took 3 minutes and 14 minutes, respectively, while the decryption was reported close to instantaneous [11]. Shortly afterwards, Coron et al. [12] introduced the so-called modulus switching technique into integer-based FHE designing, and then reduced the complexity of key size from $\tilde{O}(\lambda^7)$ to

$\tilde{O}(\lambda^5)$.

All above improvements towards integer-based FHEs are mainly focused on reducing the key size. However, the messages in these schemes are encrypted bit-by-bit, resulting not only the very large ciphertext expansion ratios, but also the huge overheads. At Eurocrypt 2013, Coron et al. [10] extended the DGHV scheme to a batch FHE scheme that supports encrypting and homomorphically processes a vector of plaintext bits as a single ciphertext. The authors showed that the batch DGHV scheme [15] can encrypt $\ell = \tilde{O}(\lambda^2)$ bits in a single ciphertext, and hence the ciphertext expansion ratio reduces up to $\tilde{O}(\lambda^3)$, instead of $\tilde{O}(\lambda^5)$ in the original scheme. In the same year, Kim et al. [27] proposed a CRT-based FHE scheme over integers, in which the message space is extended from $\mathbb{Z}_2$ to $\mathbb{Z}_2^k$ with $k = \tilde{O}(\lambda^3)$. By doing so, the overheads of the corresponding SHE scheme and FHE are reduced to $\tilde{O}(\lambda)$ and $\tilde{O}(\lambda^5)$, respectively. Recently, Nuida and Kurosawa [36] proposed a new (batch) FHE scheme over integers. Their core contributions include two aspects: (1) extending the message space for $\mathbb{Z}_q$ (for any constant prime q) to $\mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_k}$ where $q_1, \cdots, q_k$ may be different; and (2) reducing the multiplicative degree of decryption circuit from $O(\lambda \log^2 \lambda)$ in [15], [27] to $O(\lambda)$.

In spite of having many desirable potentials and many theoretical and software oriented efforts in improving the performances, currently available SHE and FHE schemes are still not efficient enough for IoT and other real-time applications [33]. Recently, the development of optimized FHE architectures by using GPU technology or FPGA technology are being explored [33]. We deter more detailed discussions on this issue in the next section.

6. Challenges for Using Fully Homomorphic Encryptions in the IoT

The IoT paradigm envisions the pervasive interconnection and cooperation of smart things over the current and future Internet infrastructure [56]. In the IoT, the increasingly invisible and pervasive collection, aggregation and dissemination of data about people's private lives brings forth some serious security and privacy problems [56]. But in this survey, we mainly focus on the challenges of designing and using fully homomorphic encryption schemes in the IoT-oriented applications.[†] As far as we know, there is no such a comprehensive exploration.

Fully homomorphic encryption is viewed as one of the *holy grails* of modern cryptography [6]. In particular, it is highly expected to be a golden key for the security and privacy issues in cloud services. Considering that the technology of cloud computation and the technology of the IoT have already deeply interweaved and mutually promoted, it is an inevitable question to investigate the feasibility of FHEs in the IoT. From a pure functionality perspective, instead of practical aspects, there is no doubt that both the cloud technology and the IoT technology would embrace the FHE technology: FHEs enable us to publicly and even blindly handle encrypted sensitive information in clouds and the IoT infrastructure, and only legit users having authorized credentials can access the true contents.

However, whenever we mention the IoT, another term, *lightweight*, comes to mind. It is no doubt that all aforementioned constructions of FHE are *heavylight*, or even *ultra-heavylight*. Therefore, the major challenge of using FHEs in the IoT is this apparent mismatch between the "small rooms" left for cryptography[††] and the "huge trunks" of existing FHE schemes. To overcome this mismatch, very skillful and talented designs are optimizations as well as the highly expected.

6.1 Lightweight Requirements and "Rooms" Left for Cryptography in the IoT

No matter how many devices will be involved in the IoT infrastructure, RFID (abbr. of radio frequency identification) tags are the first class smart things. The major challenge for security protection and privacy preservation for RFID tags are their very limited computational capabilities (storage, circuitry and power consumption). López [32] addressed that before designing a new cryptographic algorithm/protocol, the requirements and restrictions of the target RFID system should be analyzed, and the security level of an RFID tag used for an e-passport should not be as the same as that of a low-cost tag employed in a supply chains [32]. Then, he presented a good specifications for low-cost and high-cost RFID tags, some of information we related to our concern is presented in Table 2, where circuitry merely indicates the "rooms" left for security functions, instead of the whole scale of the RFID tags.

From an even fine perspective of capability in supporting security/privacy functions, RFID tags[†††] can be further divided into four classess [8]:

- Full-fledged (F), having support of conventional cryptographic functions like symmetric encryption, cryptographic one-way function, or even the public key algorithms.

Table 2 Specifications for RFID tags [32]

	Low-cost RFID Tag	High-cost RFID Tag
Standards	EPC Class-1, Gen-2 ISO/IEC 18006-C	ISO/IEC 14443 A/B
Power Source	Passively powered	Passively powered
Storage	32–1K bits	32K – 70K Bytes
Circuitry	250–4K gates	Mircoproscessor
Reading Distance	Up to 3m	About 10 cm

[†]Interested readers are suggested to refer to [56] for good surveys on security and privacy issues in the IoT.

[††]This never means that the "rooms" in the IoT are small.

[†††]The true meaning of this classification in [8] is taken towards RFID authentication protocols, instead of RFID tags. But we think that from the perspective of capability in supporting security/privacy functions, this classification can be referred as a classification on RFID tags.

- Simple (S), having support of random number generators and one-way hash functions on tags.
- Lightweight (L), having support of random number generators and simple functions like CRC checksum, but not hash functions.
- Ultralightweight (U), only involving simple bit-wise operations (like XOR, AND, OR, etc.) on tags.

Of course, with the the progress and revolution in microelectronics industry, the above classification should not be viewed as firm lines. For instances, at present, many cryptographers are making efforts towards developing the so-called lightweight and even lightweight cryptographic components with the purpose to support RFID tags on full scale [40]. For instance, a typical lightweight implementation of Advanced Encryption Standard (AES) requires merely 3400 equivalent gates, and one time full-scale encryption requires only 1032 clock cycles [40].

Finally, we would like to mention that as the second class of smart things in the IoT – wireless sensors, to which the energy efficiency is a more critical problem [16]†. Wander et al. [50] suggested that in the wireless sensor network (WSN) domain, only 5% to 10% of a WSN's energy budget is available for handshakes, and they found that typical weak public-key cryptosystems (such as 160-bit ECC and 1024-bit RSA) took approximately 70% of the energy alloted for communication handshaking [50]. Moreover, Wander et al.'s work provided a good understanding on the energy cost for communication and cryptographic operations in typical WSN domains [50]. For example, as for the Mica2dot platform, the power required to transmit 1 bit is roughly equivalent to 2090 clock cycles of execution on the microcontroller alone; the cost of receiving one byte is about $28.6\mu J$, roughly half of that required to transmit a byte (i.e., $59.2\mu J$). For an assembly-optimized AES-128 implementation and a C-implementation of SHA-1, the average energy costs for per byte are $5.9\mu J$ (for SHA-1), $1.62\mu J$ (for AES-128 encryption), and $2.49\mu J$ (for AES-128 decryption), respectively [50]. Further, they tested the energy cost for executing RSA and ECC algorithms in signatures, key exchanges and authentications in typical settings. The results are re-collected and re-organized in Table 3.

Table 3 Mica2dot energy cost (μJ) for cryptographic primitive [50]

Primitive	Signature		Key Exchange		Authentication	
Alg/End	sign	verify	client	server	client	server
RSA-1024	304	11.9	15.4	304	397.7	390.3
ECC-160	22.82	45.09	22.3	22.3	93.7	93.9
RSA-2048	2302.7	53.7	57.2	2302.7	–	–
ECC-224	61.54	121.98	60.4	60.4	–	–

†For RFID tags, since most of them are designed to passively harvests energy from readers, it is difficult and less significant to quantify their energy budgets.

6.2 Noise-Free Symmetric Fully Homomorphic Encryptions

On one hand, although researchers have made a lot of improvements for restraining the noise during homomorphic compositions, however, the progress is still not satisfactory. The cost of these noise restraining processes such as bootstrapping and squashing is still very high. This urges us to think about another problem: Is it a necessary mechanism to introduce noise in building FHE schemes? At least, there is no such explicit suggestion. In fact, currently known FHE schemes are mostly based on noise-based intractability assumptions. In other words, noise is essential to the related underlying security assumptions, instead of to the property of homomorphism over ciphertexts. Therefore, it is interesting to seek noise-free designs of FHE schemes. On the other hand, at present, all formally published FHE schemes lie in the scope of public key cryptosystems, however, in order to fully support the IoT oriented applications, fully homomorphic symmetric encryption schemes are also highly expected.

In 2012, Kipnis and Hibshoosh proposed two noise-free symmetric FHEs in which the first FHE utilizes conjugate operations for 2×2 matrices over $\mathbb{Z}_q$ and the other one is based on the factorization problem of large integer, hence, introduces a new twist multiplication homomorphic technique [28]. Recently, Liu [31] proposed a novel symmetric FHE scheme that consists two layers: The lower layer encryption that can only be used at most $n-1$ times for hiding components of keys, while the upper layer encryption can be used arbitrary times for encrypting messages [31]. Besides, Yagisawa also presented three octonion-based FHEs without bootstrapping [53]–[55], where the message is encoded in an octonion number. In particular, octonion is neither commutative nor associative.

Interestingly, all of these noise-free symmetric FHE schemes are efficient both in storage cost and computational cost. The key sizes (in bits), compactness ρ (i.e. ciphertext expansion ratios), and encryption/decryption costs are depicted in Table 4, where the computational cost is given based on the number of $\langle\cdot\rangle_q$, i.e. the multiplication operations over the finite field $GF(q)$, while n, l, t are constants for the corresponding FHEs. Considering that the bit complexity of $\langle\cdot\rangle_q$ is bounded by $O(\log^2 q)$††, Table 4 suggests

Table 4 Performance analysis on noise-free symmetric FHEs

Schemes	key size (in bits)	ρ	Number of $\langle\cdot\rangle_q$	
			Enc	Dec
KH12-1 [28]	$4 \cdot \log q$	4	12	16
KH12-2 [28]	$2 \cdot \log q$	2	3	1
Liu15 [31]	$(n+1) \cdot \log q$	$n+1$	$l^3 + l^2$	l
Yag15-1 [53]	$8t \cdot \log q$	8	$128t$	$128t$
Yag15-2 [54]	$8 \cdot \log q$	8	1024	1024

††If the FFT technology is employed, this bound could be further reduced to $O(\log q \log\log q)$.

that these noise-free FHE schemes are so smart even to outperform most existing public key cryptosystems.

Unfortunately, all above constructions of noise-free symmetric FHE schemes are insecure [49]. Although these designs are very skillful, a common weakness lies in that the decryption algorithms can be represented as linear equations, where unknowns are the encrypted messages and the decryption keys, while the coefficients are specified by the given ciphertexts. Thus, all of these schemes are so weak to resist against even the chosen plaintext attacks.

7. Conclusions

There is no doubt that practical FHE schemes, if there would exist, will be very useful in the IoT and cloud computation. But it seems that the current IoT technology does not left sufficient "rooms" for currently known FHE schemes. Alive or Dead? The problem Hamlet once faced is now comes to the front of the primitive of FHE. Indeed, to use FHEs in the IoT is to organize a mandala in a spiral shell. It is difficult but might not be impossible. At least, it is interesting to explore new methods for rendering those noise-free and efficient FHE schemes to be secure.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (NSFC) (Nos. 61370194, 61411146001, 61502048).

References

[1] M. Ajtai and C. Dwork, "A public-key cryptosystem with worstcase/averagecase equivalence," Proc. twenty-ninth annual ACM symposium on Theory of computing, ACM, pp.284–293, 1997.
[2] J. Benaloh, "Dense Probabilistic Encryption," First Annual Workshop on Selected Areas in Cryptography, pp.120–128, 1994.
[3] D. Boneh, E. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," Theory of Cryptography-TCC'05, LNCS, pp.325–341, 2005.
[4] Z. Brakerski, "Fully homomorphic encryption without modulus switching from classical gapSVP," Advances in Cryptology-CRYPTO 2012, Springer, pp.868–886, 2012.
[5] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "Fully homomorphic encryption without bootstrapping," Proc. 3rd Innovations in Theoretical Computer Science Conference, ACM, pp.309–325, 2012.
[6] Z. Brakerski and V. Vaikuntanathan, "Fully Homomorphic Encryption from Ring-LWE and security for Key Dependent Messages," Advances in Cryptology-CRYPTO 2011, Springer, pp.505–524, 2011.
[7] J. Bringer, H. Chabanne, M. Izabach'ene, D. Pointcheval, Q. Tang, and S. Zimmer, "An Application of the Goldwasser-Micali Cryptosystem to Biometric Authentication," Information Security and Privacy, Springer, pp.96–106, 2007.
[8] H.-Y. Chien, "SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity," IEEE Trans. Dependable and Secure Computing, vol.4, no.4, pp.337–340, 2007.
[9] J. Cohen and M.J. Fischer, "A robust and verifiable cryptographically secure election scheme (extended abstract)," In FOCS, IEEE Computer Society, pp.372–382, 1985.
[10] J.H. Cheon, J.-S. Coron, J. Kim, M.S. Lee, T. Lepoint, M. Tibouchi, and A. Yun, "Batch fully homomorphic encryption over the integers," Advances in Cryptology-EUROCRYPT 2013, Springer, pp.315–335, 2013.
[11] J. Coron, A. Mandal, D. Naccache, and M. Tibouchi, "Fully homomorphic encryption over the integers with shorter public keys," Advances in Cryptology-CRYPTO 2011, Springer, pp.487–504, 2011.
[12] J. Coron, D. Naccache, and M. Tibouchi, "Public key compression and modulus switching for fully homomorphic encryption over the integers," Advances in Cryptology-EUROCRYPT 2012, Springer, pp.446–464, 2012.
[13] R. Cramer and V. Shoup, "A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack," Advances in Cryptology-CRYPTO'98, Springer, pp.13–25, 1998.
[14] I. Damgård and M. Jurik, "A generalisation, simplification and some applications of Paillier's probabilistic public-key system," Public Key Cryptography-PKC 2011, Springer, pp.119–136, 2001.
[15] M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, "Fully homomorphic encryption over the integers," Advances in cryptology-EUROCRYPT 2010, Springer, pp.24–43, 2010.
[16] M. Dong, K. Ota, L.T. Yang, S. Chang, H. Zhu, and Z. Zhou, "Mobile agent-based energy-aware and user-centric data collection in wireless sensor networks," Comput. Netw. 74, pp.58–70, 2014.
[17] L. Ducas and D. Micciancio, "FHEW: Bootstrapping homomorphic encryption in less than a second," Advances in Cryptology-EUROCRYPT 2015, Springer, pp.617–640, 2015.
[18] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms," Advances in cryptology, Springer, pp.10–18, 1984.
[19] Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving Efficient Cloud Search Services: Multi-keyword Ranked Search over Encrypted Cloud Data Supporting Parallel Computing," IEICE Trans. Commun., vol.98, no.1, pp.190–200, 2015.
[20] C. Gentry, "Fully homomorphic encryption using ideal lattices," STOC, pp.168–179, 2009.
[21] C. Gentry and Shai Halevi, "Fully homomorphic encryption without squashing using depth-3 arithmetic circuits," Foundations of Computer Science (FOCS), pp.107–109, 2011.
[22] C. Gentry, S. Halevi, and N.P. Smart, "Better bootstrapping in fully homomorphic encryption," Public Key Cryptography-PKC 2012, Springer, pp.1–16, 2012.
[23] S. Goldwasser and S. Micali, "Probabilistic encryption," J. Computer and System Sciences, vol.28, no.2, pp.270–299, 1984.
[24] M. Joye and B. Libert, "Efficient cryptosystems from 2^k-th power residue symbols," Advances in Cryptology-EUROCRYPT 2013, Springer, pp.76–92, 2013.
[25] M. Kantarcioglu, Privacy-preserving distributed data mining and processing on horizontally partitioned data. ETD Collection for Purdue University, 2005, AAI3191494.
[26] A. Kawachi, K. Tanaka, and K. Xagawa, "Multi-bit cryptosystems based on lattice problems," Public Key Cryptography-PKC 2007, Springer, pp.315–329, 2007.
[27] J. Kim, M.S. Lee, A. Yun, and J.H. Cheon, CRT-based fully homomorphic encryption over the integers, IACR Cryptology ePrint Archive 2013; 2013: 57. URL http://eprint.iacr.org/2013/057.
[28] A. Kipnis and E. Hibshoosh, Efficient methods for practical fully homomorphic symmetric-key encrypton, randomization and verification, IACR Cryptology ePrint Archive 2012; 2012: 637. URL http://eprint.iacr.org/2012/637.
[29] H. Li, M. Dong, and K. Ota, "Radio Access Network Virtualization for the Social Internet of Things," IEEE Cloud Computing, vol.2, no.6, pp.42–50, 2015.
[30] M. Naehrig, K. Lauter, and V. Vaikunthnathan, "Can homomorphic encryption be practical?" Proc. 3rd ACM workshop on Cloud computing security workshop, ACM, pp.113–124, 2011.
[31] D. Liu, Practical fully homomorphic encryption without noise reduction, IACR Cryptology ePrint Archive 2015; 2015: 468. URL

http://eprint.iacr.org/2015/468.
[32] A. López-Alt, E. Tromer, and V. Vaikuntanathan, Cloud-assisted multiparty computation from fully homomorphic encryption, IACR Cryptology ePrint Archive 2011; 2011: 663. URL http://eprint.iacr.org/2011/663.
[33] C. Moore, M. O'Neill, E. O'Sullivan, Y. Doröz, and B. Sunar, "Practical homomorphic encryption: A survey," Circuits and Systems (ISCAS), 2014 IEEE International Symposium on. IEEE, pp.2792–2795, 2014.
[34] T. Ma, J. Zhou, M. Tang, Y. Tian, A. Al-Dhelaan, M. Al-Rodhaan, and S. Lee, "Social network and tag sources based augmenting collaborative recommender system," IEICE Trans. Inf. & Syst., vol.E98-D, no.4, pp.902–910, 2015.
[35] D. Naccache and J. Stern, "A New Public Key Cryptosystem Based on Higher Residues," Proc. 5th ACM CCS, pp.59–66, 1998.
[36] K. Nuida and K. Kurosawa, "(Batch) Fully Homomorphic Encryption over Integers for Non-Binary Message Spaces," Advances in Cryptology-EUROCRYPT 2015, Springer, pp.537–555, 2015.
[37] T. Okamoto and S. Uchiyama, "A new public-key cryptosystemas secure as factoring," Advances in Cryptology-EUROCRYPT 1998, Springer, pp.308–318, 1998.
[38] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," Advances in cryptology-EUROCRYPT 1999, Springer, pp.223–238, 1999.
[39] C. Peikert and B. Waters, "Lossy Trapdoor Functions and Their Applications," SIAM J. Computing, vol.40, no.6, pp.1803–1844, 2011.
[40] A. Poschmann, Lightweight Cryptography from an Engineers Perspective, Workshop on Elliptic Curve Cryptography (ECC 2007). 2007.
[41] R.L. Rivest, L.M. Adleman, and M.L. Dertouzos, "On data banks and privacy homomorphisms," Foundations of Secure Computation, vol.4, no.11, pp.169–180, 1978.
[42] R.L. Rivest, A. Shamir, and L.M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol.21, no.2, pp.120–126, 1978.
[43] S. Sowe, T. Kimata, M. Dong, and K. Zettsu, "Managing Heterogeneous Sensor Data on a Big Data Platform: IoT Services for Data-Intensive Science," Computer Software and Applications Conference Workshops (COMPSACW), 2014 IEEE 38th International. IEEE, pp.295–300, 2014.
[44] T. Sander, A. Young, and M. Yung, "Non-interactive cryptocomputing for NC^1," Foundations of Computer Science (FOCS), pp.554–567, 1999.
[45] P. Scholl and N. Smart, "Improved key generation for Gentry's fully homomorphic encryption scheme," Cryptography and Coding, Springer, pp.10–22, 2011.
[46] N. Smart and F. Vercauteren, "Fully homomorphic encryption with relatively small key and ciphertext sizes," Public Key Cryptography-PKC 2010, Springer, pp.420–443, 2010.
[47] N. Smart and F. Vercauteren, "Fully homomorphic SIMD operations," Designs, codes and cryptography, vol.71, no.1, pp.57–81, 2014.
[48] D. Stehlé and R. Steinfeld, "Faster fully homomorphic encryption," Advances in Cryptology-ASIACRYPT 2010, Springer, pp.377–394, 2010.
[49] Y. Wang, Notes on two fully homomorphic encryption schemes without bootstrapping, IACR Cryptology ePrint Archive 2015; 2015: 519. URL http://eprint.iacr.org/2015/519.
[50] A.S. Wander, N. Gura, H. Eberle, V. Gupta, and S.C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on. IEEE, pp.324–328, 2005.
[51] J. Wu, M. Dong, K. Ota, L. Liang, and Z. Zhou, "Securing distributed storage for Social Internet of Things using regenerating code and Blom key agreement," Peer-to-Peer Networking and Applications, vol.8, no.6, pp.1133–1142, 2015.
[52] Z. Xia, X. Wang, X. Sun, and Q. Wang, A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data, IEEE Trans. Parallel Distrib. Syst., (DOI: 10.1109/TPDS.2015.2401003), 2015.
[53] M. Yagisawa, Fully homomorphic encryption with composite number modulus, IACR Cryptology ePrint Archive 2015; 2015: 474. URL http://eprint.iacr.org/2015/474.
[54] M. Yagisawa, Fully homomorphic encryption without bootstrapping, IACR Cryptology ePrint Archive 2015; 2015: 1040. URL http://eprint.iacr.org/2015/1040.
[55] M. Yagisawa, Fully homomorphic encryption on octonion ring, IACR Cryptology ePrint Archive 2015; 2015: 733. URL http://eprint.iacr.org/2015/733.
[56] J.H. Ziegeldorf, O.G. Morchon, and K. Wehrle, "Privacy in the internet of things: threats and challenges," Security and Communication Networks, vol.7, no.12, pp.2728–2742, 2014.

Licheng Wang received the B.S. degree from Northwest Normal University in 1995, the M.S. degree from Nanjing University in 2001, and the Ph.D. degree from Shanghai Jiao Tong University in 2007. His current research interests include modern cryptography, network security, trust management, etc. He is an associate professor in Beijing University of Posts and Telecommunications.

Jing Li received the B.S. degree from Inner Mongol Normal University in 2010 and the M.S. degree from Shanxi Normal University in 2013. Her current research interests include modern cryptography, network security, finite field and its applications, etc. She is a now a Ph.D. candidate studying in Beijing University of Posts and Telecommunications.

Haseeb Ahmad received the BS degree in Mathematics from G.C. University, Faisalabad, Pakistan in 2010 and the Masters degree in Computer Science from Virtual University of Pakistan in 2012. He is currently a PhD student in School of Computer Science at Beijing University of Posts and Telecommunications, Beijing, China. His current research interest includes Information security.