Feng-he Wang, Chun-xiao Wang, Zhen-hua Liu, 2016. Efficient hierarchical identity based encryption scheme in the standard model over lattices. *Frontiers of Information Technology & Electronic Engineering*, **17**(8):781-791. http://dx.doi.org/10.1631/FITEE.1500219

Efficient hierarchical identity based encryption scheme in the standard model over lattices

Key words: Hierarchical identity based encryption scheme, Lattice-based cryptography, Standard model, Learning with errors problem, Gaussian

Corresponding author: Feng-he Wang
E-mail: fenghe2166@163.com
ORCID: http://orcid.org/0000-0002-5510-3133

Motivation

- Hierarchical identity based encryption (HIBE) is an important cryptographic notation. Security and efficiency are two important characters for HIBE.
- Most of HIBE schemes are not secure under the quantum attack (Boneh *et al*., 2005; Boyen and Waters, 2006; Gentry and Halevi, 2009; Waters, 2009).
- Lattice-based HIBE can achieve the quantum security, while the efficiency is low. For example: large public key size, large message-ciphertext expanse factor (M-C factor) (Agrawal *et al*.,2010a; 2010b; Cash *et al*., 2010).
- How to improve the efficiency of the lattice-based HIBE?

Main idea

- The known public key assignment rule leads to large public key size and even large M-C factor, though it is important for the design of the lattice-based HIBE.
- We would make lattice-based HIBE scheme more efficient by designing a more efficient public key assignment rule.

Method

1. Propose a public key assignment rule for the design of the lattice-based HIBE scheme.
2. Give an embedded technology by which the proposed public key assignment rule can be combined with lattice-based delegation.
3. The security proof technology in the standard model.

Major results

- The proposed public key assignment rule:

Algorithm 3 Assignment rule

Input: $R_1, R_2, \ldots, R_d$; $\mathbf{id}_{|d} = (\mathrm{id}_1, \mathrm{id}_2, \ldots, \mathrm{id}_d)$

Output: $\{R_{i_1}, R_{i_2}, \ldots, R_{i_{d^*}}\}$

// return R_{i_j} for $\mathrm{id}_{i_j} = 1$

```
1: for i = 1 to d do
2:     if id_i=1 then
3:         return R_i
4:     else
5:         Output nothing
6:     end if
7: end for
```


- Efficient HIBE scheme over lattice in the standard model by the proposed public key assignment rule.

Major results (Cont'd)

- Security: security against the selective identities and chosen message attacks in the standard model
- Efficiency:

Table 1 Comparison of space efficiency

Scheme	Public key length (bit)	Message-ciphertext expansion factor
Agrawal *et al.* (2010b)	$(2dm^2+mn+n)\log q$	$m\log q+1$
Singh *et al.* (2012)	$(dl''+2)mn\log q$	$[(l+1)m+1]\log q$
Singh *et al.* (2014)	$(l''+2)mn\log q$	$[(l+1)m+1]\log q$
Our scheme	$(dm^2+mn)\log q$	$\log q$

Table 2 Comparison of computation efficiency for each bit message

Scheme	Gaussian sampling		Modular multiplication	
	Encrypt	Decrypt	Encrypt	Decrypt
Agrawal *et al.* (2010b)	2	1	$(l-1)m^2+2mn+n$	m
Singh *et al.* (2012)	1	1	$(l''+l+1)mn+m$	$(l+1)m$
Singh *et al.* (2014)	1	1	$(ll'')mn+m^2+(l''+1)mn^2$	$(l+1)m$
Our scheme	$1/m$	0	$n+j^*-1$	2

Conclusions

- We proposed a public key assignment rule for lattice-based HIBE scheme.
- We designed a lattice-based HIBE scheme in the standard model by the proposed public key assignment rule.
- We proved that the proposed HIBE scheme is secure under the hardness of the LWE problem. It is also efficient compared with known HIBE schemes over lattice.
- The proposed public key assignment rule also can be used to further improve the efficiency of lattice-based HIBE by combining with other technologies. (e.g., Singh *et al*., 2014)