Anonymous Lattice-Based Broadcast Encryption

Adela Georgescu

Anonymous Lattice-Based Broadcast Encryption

Adela Georgescu*

Faculty of Mathematics and Computer Science, University of Bucharest,
Academiei Street 14, Bucharest 010014, Romania
adela@fmi.unibuc.ro

Abstract. In this paper we propose a lattice-based anonymous broadcast encryption scheme obtained by translating the broadcast encryption scheme of Paterson et al. [7] into the lattices environment. We use two essential cryptographic primitives for our construction: tag-based hint systems secure under Ring-LWE hardness and IND-CCA secure cryptosystem under LWE-hardness. We show that it is feasible to construct anonymous tag-based hint systems from Ring-LWE problem for which we use a variant with "small" secrets known to be as hard as regular Ring-LWE. We employ an IND-CCA-secure public key encryption scheme from LWE [12] for the PKE component of the anonymous broadcast encryption scheme.

Key words: broadcast encryption, anonymity, Learning With Errors, Lattices

1 Introduction

In this paper, we translate the anonymous broadcast encryption scheme from [7] into the lattices environment. Lattices are more and more studied recently and lattices environment is becoming wider and more populated with different cryptographic primitives. They offer certain undeniable advantages over traditional cryptography based on number theory: hard problems which form the security basis of many cryptographic primitives, great simplicity involving linear operations on small numbers and increasingly efficient implementations. A very important issue is that they are believed to be secure against quantum attacks in an era where quantum computers are a great promise for the near future. It is not surprising that lately we are witnessing a great development of cryptographic constructions secure under lattice-based assumptions. This is the main motivation for our current work: we want to propose a lattice-based variant of this cryptographic primitive (i.e. anonymous broadcast encryption) existent in classical cryptography.

Authors from [7] use two cryptographic primitives in order to achieve anonymous broadcast encryption: IND-CCA public key encryption scheme and anonymous tag-based hint system. We employ variants of both these primitives derived from the Ring-Learning With Errors problem (RLWE) introduced recently

* This work was sponsored by the European Social Fund, under doctoral and postdoctoral grant POSDRU/88/1.5/S/56668.

in [10]. This problem is the ring-based variant of Regev's Learning With Errors problem [13]. Lyubashevsky et al. [10] show that their problem can be reduced to the worst-case hardness of short-vector problems in ideal lattices. The advantage of RLWE based cryptographic primitives over LWE-based cryptographic primitives is that they achieve more compact ciphertext and smaller key sizes by a factor of n, thus adding more efficiency.

The RLWE problem has already been used as underlying hardness assumption for many cryptographic constructions, starting with the original cryptosystem from [10] and continuing with efficient signature schemes [9], [12], pseudorandom functions [2], fully homomorphic encryption [3] and also NTRU cryptosystem [14]. So it is a natural question to ask if we can achieve anonymous broadcast encryption from lattices. As one can see in the rest of the paper, we found it is not hard to construct this kind of primitive. IND-CCA cryptosystem based on LWE problem (and also RLWE) were already introduced in the literature (see section 6.3 [12] for LWE-based IND-CCA cryptosystem). We also prove that it is feasible to construct tag-based hint anonymous systems from RLWE following the model of DDH hint system from [7]. For this specific task, we deal with the Hermite Normal Form variant of RLWE and with an equivalent version of DDH problem based on RLWE introduced in [5].

1.1 Related work

There is another candidate in the literature for lattice-based broadcast encryption scheme introduced in [15]. Anyway, there are some important differences between our scheme and this one: the latter does not offer anonymity but it is an identity-based scheme. Our scheme can also be transformed into identity-based broadcast encryption by replacing the LWE-based IND-CCA secure PKE with identity-based encryption (IBE) from LWE as the one from [4]. On the other hand, the CCA-secure PKE scheme from [12] we employ in our construction has better efficiency and simplicity due to the simple structure of the new trapdoor they introduce, thus also making our construction more efficient.

2 Preliminaries

2.1 Lattices

Let $\mathbf{B} = \{\mathbf{b_1}, ...\mathbf{b_n}\} \in \mathbb{R}^{n \times k}$ be linearly independent vectors in $\mathbb{R}^n$. The lattice generated by $\mathbf{B}$ is the set of all *integer* linear combinations of vectors from $\mathbf{B}$

$$\mathcal{L}(\mathbf{B}) = \{\sum_{i=1}^{n} x_i \cdot \mathbf{b_i} \ : \ x_i \in \mathbb{Z}\}.$$

Matrix $\mathbf{B}$ constitutes a basis of the lattice. Any lattice admits multiple bases, some bases are better than others.

We introduce here a function that we'll apply in section 3.1, the $round(\cdot)$ function. This function was first used with its basic variant in [13] for decryption, and later on to almost all the lattice-based cryptosystems :

$$round(x) = \begin{cases} 1, x \in [0, \lfloor q/2 \rfloor] \\ 0, \text{ otherwise} \end{cases}$$

In our construction, we use the extended variant of the function which rounds to smaller intervals, namely $round(x) = a$ if $x \in [a \cdot q/A, (a+1) \cdot q/A]$ where A is the total number of intervals. We suggest setting A = 4.

We employ this function in order to derive the same value from numbers that are separated only by a small difference (Gaussian noise).

2.2 The Learning With Errors problem

The learning with errors problem (LWE) is a recently introduced (2005, [13]) but very famous problem in the field of lattice-based cryptography. Even if it is not related directly to lattices, the security of many cryptographic primitives in this field rely on its hardness believed to be the same as worst-case lattice problems.

Informally, the problem can be described very easily: given n linear equations on $s \in \mathbb{Z}_q^n$ which have been perturbed by a small amount of noise, recover the secret s.

We present here the original definition from [13].

Definition 1 *(The Learning With Errors Problem [13])*
Fix the parameters of the problem: $n \geq 1$, modulus $q \geq 2$ and Gaussian error probability distribution χ on $\mathbb{Z}_q$ (more precisely, it is chosen to be the normal distribution rounded to the nearest integer, modulo q with standard deviation αq where $\alpha > 0$ is taken to be $1/(poly(n))$). Given an arbitrary number of pairs $(\mathbf{a}, \mathbf{a^T s} + e)$ where s is a secret vector from $\mathbb{Z}_q^n$, vector $\mathbf{a}$ is chosen uniformly at random from $\mathbb{Z}_q^n$ and e is chosen according to χ, output $\mathbf{s}$ with high probability.

Proposition 1 *[13] Let $\alpha = \alpha(n) \in (0,1)$ and let $q = q(n)$ be a prime such that $\alpha q > 2\sqrt{n}$. If there exists an efficient (possibly quantum) algorithm that solves $LWE_{q,\chi}$, then there exists an efficient quantum algorithm for approximating SIVP in the worst-case to within $O(n/\alpha)$ factors.*

2.3 The Ring-Learning With Errors problem

The *ring learning with errors* assumption introduced by Lyubashevsky et al. [10] is the translation of the LWE into the ring setting. More precisely, the group $\mathbb{Z}_q^n$ from the LWE samples is replaced with the ring $R_q = \mathbb{Z}_q[x]/\langle x^n + 1 \rangle$, where n is a power of 2 and q is a prime modulus satisfying $q = 1 \bmod 2n$. This is in fact a particularization of the ring-LWE problem introduced in the original paper, but for our construction, as for many others, it is enough. The ring $\mathbb{Z}_q[x]/\langle x^n + 1 \rangle$

contains all integer polynomials of degree $n-1$ and coefficients in $\mathbb{Z}_q$. Addition and multiplication in this ring are defined modulo x^n+1 and q.

In ring-LWE [10], the parameter setting is as follows: $s \in R_q$ is a fixed secret, a is chosen uniformly from R_q and e is an error term chosen independently from some error distribution χ concentrated on "small" elements from R_q. The ring-LWE (RLWE) assumption is that it is hard to distinguish samples of the form $(a, b = a \cdot s + e) \in R_q \times R_q$ from samples (a, b) where a, b are chosen uniformly in R_q. A hardness result based on the worst-case hardness of short-vector problems on ideal lattices is given in [10]. An important remark is that the assumption still holds if the secret s is sampled from the noise distribution χ rather than the uniform distribution; this is the "Hermite Normal Form (HNF)" of the assumption (HNF-ring-LWE). The advantage of the RLWE problem is that it represents a step forward in making the lattice-based cryptography practical. In most applications, a sample $(a, b) \in R_q \times R_q$ from RLWE distribution can replace n samples $(\mathbf{a}, b) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ from the standard LWE distribution, thus reducing the key size by a factor of n.

We note that in our construction of the broadcast encryption scheme, we will make use of the HNF form of the RLWE problem.

We present in the following the correspondent of the Decisional Diffie-Hellman based on the Ring-LWE problem, which was first introduced in [5] and which is derived from the ring-LWE cryptosystem from [8], section 3.1. The security of this cryptosystem is proven conditioned by the fact that an adversary cannot solve the below problem, which is essentially its view from the cryptosystem.

DDH-RLWE Problem. [5] Given a tuple $(s, y_1 = s \cdot x + e_x, y_2 = s \cdot y + e_y, z)$ where s is chosen uniformly at random from R_q, x, y, e_x, e_y are sampled from χ distribution, one has to distinguish between the tuple where $z = y_1 \cdot y + e_3$, with e_3 sampled independently from χ and the same tuple where z is chosen uniformly and independently from anything else in R_q.

We present a hardness result for the above problem but, due to lack of space, we defer a complete proof to [5].

Proposition 2 *[5]*
The DDH-RLWE problem is hard if the RLWE problem in its "Hermite normal form" (HNF) is hard.

3 Anonymous Broadcast Encryption

In this section we recall a general Broadcast Encryption model from [7] which allows anonymity.

Definition 2 *A broadcast encryption scheme with security parameter λ and $U = \{1, ..., n\}$ the universe of users consists of the following algorithms.*

`Setup`(λ, n) *takes as input security parameter λ and the number of users and outputs a master public key MPK and master secret key MSK.*

`KeyGen`(MPK, MSK, i) *takes as input MPK, MSK and* $i \in U$ *and outputs the private key* sk_i *corresponding to user* i.

`Enc`(MPK, m, S) *takes as input MPK and a message* m *to be broadcasted to a set of users* $S \subseteq U$ *and it outputs a cipheretxt* c.

`Dec`(MPK, sk_i, c) *takes as input MPK, a private key* sk_i *and a ciphertext* c *and outputs either the message* m *or a failure symbol.*

We provide the same security model as in [7] for the anonymous broadcast encryption scheme we'll describe later.

Definition 3 *We define the ANO-IND-CCA security game (against adaptive adversaries) for broadcast encryption scheme as follows.*

Setup *The challenger runs the Setup to generate the public key MPK and the corresponding private key MSK and gives MPK to the adversary* $\mathcal{A}$.

Phase 1. $\mathcal{A}$ *can issues two types of queries:*

- *private key extraction queries to an oracle for any index* $i \in U$*; the oracle will respond by returning the private key* $sk_i = KeyGen(MPK, MSK, i)$ *corresponding to* i*;*
- *decryption queries* (c, i) *to an oracle for any index* $i \in U$*; the oracle will respond by returning the* $Dec(MPK, sk_i, c)$.

Challenge. *The adversary selects two equal length messages* m_0 *and* m_1 *and two distinct sets* S_0 *and* $S_1 \subseteq U$ *of users. We impose the same requirements as in [7]: sets* S_0 *and* S_1 *should be of equal size and A has not issued any query to any* $i \in (S_0 \setminus S_1) \cup (S_1 \setminus S_0)$*. Further, if there exists an* $i \in S_0 \cap S_1$ *for which A has issued a query, then we require that* $m_0 = m_1$*. The adversary gives* m_0*,* m_1 *and* S_0*,* S_1 *to the challenger. The latter picks a random bit* $b \in \{0, 1\}$*, computes* $c^* = Enc(MPK, m_b, S_b)$ *and returns it to A.*

Phase 2. $\mathcal{A}$ *continues to issue private key extraction queries with the restriction that* $i \notin (S_0 \setminus S_1) \cup (S_1 \setminus S_0)$*; otherwise it is necessary that* $m_0 = m_1$*.* $\mathcal{A}$ *continues to issue decryption queries* (c, i) *with the restriction that if* $c = c^*$ *then either* $i \notin (S_0 \setminus S_1) \cup (S_1 \setminus S_0)$ *or* $i \in S_0 \cap S_1$ *and* $m_0 = m_1$.

Guess. *The adversary A outputs a guess* $b' \in \{0, 1\}$ *and wins the game if* $b = b'$.

We denote $\mathcal{A}'s$ advantage by $Adv_{A,KT}^{ANO-IND-CPA}(\lambda) = |Pr[b' = b] - \frac{1}{2}|$ where λ is the security parameter of the scheme.

Generic constructions for anonymous broadcast encryption can be obtained exactly as in Section 3 and 4 from [7], but they require linear time decryption. Thus, we follow the idea of introducing tag-based anonymous hint system as in [7], but we construct it from the ring-LWE problem. The construction has the advantage of achieving constant time decryption.

3.1 Tag-Based Anonymous Hint Systems

A tag-based anonymous hint system (TAHS) [7] is a sort of encryption under a tag t and a public key pk. The output is a pair (U, H) where H is a hint. This

pair should be hard to distinguish when using two different public keys. Such a system consists of the following algorithms:

$\texttt{KeyGen}(\lambda)$ on input security parameter λ, outputs a key pair (sk, pk).
$\texttt{Hint}(t, pk, r)$ takes as input a public key pk and a tag t; outputs a pair (U, H) consisting of a value U and a hint H. It is required that U depends only on random r and not on pk.
$\texttt{Invert}(sk, t, U)$ takes as input a value U, a tag t and a private key sk. It outputs either a hint H or $\perp$ if U is not in the appropriate domain.

Correctness implies that for any pair $(sk, pk) \leftarrow \texttt{KeyGen}(\lambda)$ and any random r, if $(U, H) \leftarrow \texttt{Hint}(t, pk, r)$, then $\texttt{Invert}(sk, t, U) = H$.

Definition 4 *[7]*
A tag-based hint system as defined above is anonymous if there is no polynomial time adversary which has non-negligible advantage in the following game:

1. *Adversary $\mathcal{A}$ chooses a tag t' and sends it to the challenger.*
2. *The challenger generates two pairs $(sk_0, pk_0), (sk_1, pk_1) \leftarrow \texttt{KeyGen}(\lambda)$ and gives pk_0, pk_1 to the adversary.*
3. *The following phase is repeated polynomially many times: $\mathcal{A}$ invokes a verification oracle on a value-hint-tag triple (U, H, t) such that $t \neq t'$. In reply, the challenger returns bits $d_0, d_1 \in \{0, 1\}$ where $d_0 = 1$ if and only if $H = \texttt{Invert}(sk_0, t, U)$ and $d_1 = 1$ if and only if $H = \texttt{Invert}(sk_1, t, U)$.*
4. *In the challenge phase, the challenger chooses random bit $b \leftarrow \{0, 1\}$ and random $r' \leftarrow R_q$ and outputs $(U', H') = \texttt{Hint}(t', pk_b, r')$.*
5. *$\mathcal{A}$ is allowed to make any further query but not involving target t'.*
6. *$\mathcal{A}$ outputs a bit $b' \in \{0, 1\}$ and wins the game if $b' = b$.*

To show that this primitive can be constructed in the lattice-based environment, we give an example of an anonymous hint system based on the DDH-RLWE assumption. This is the equivalent of the hint system based on the classical DDH assumption from [7].

Let R_q be the ring of polynomial integers as described in section 2.3 i.e. $R_q = \mathbb{Z}_q^n / \langle x^n + 1 \rangle$ where n is a power of 2 and q is a prime modulus such that $q = 1 \bmod 2n$. Remember that χ is the noise distribution concentrated on "small" elements from R_q; s is a fixed element from R_q.

We draw attention to the fact that, unlike in the tag-based hint system from [7], the `Hint` algorithm outputs a value H_1 which is slightly different from the value H_2 recovered by `Invert` algorithm (by a small quantity from χ as shown below) and only the holder of the secret key sk can derive a value H from both H_1 and H_2. We stress that the final value H is the same for every use of the tag-based hint scheme, just that is somehow hidden by the output of `Hint` algorithm.

$\texttt{KeyGen}(\lambda)$ take random $x_1, x_2, y_1, y_2, e_1, e_2, e_1', e_2' \leftarrow \chi$ and compute $X_i = s \cdot x_i + e_i$ and $Y_i = s \cdot y_i + e_i'$. The public key is $pk = (X_1, X_2, Y_1, Y_2)$ and the private key is $sk = (x_1, x_2, y_1, y_2)$.

$\texttt{Hint}(t, pk, r)$ choose e, e_x, e_y from χ distribution and compute (U, H_1) as

$$U = s \cdot r + e; \quad H_1 = (V, W) = ((X_1 \cdot t + e_x + X_2)r, (Y_1 \cdot t + e_y + Y_2)r)$$

$\texttt{Invert}(sk, t, U)$ parse sk as (x_1, x_2, y_1, y_2), compute

$$H_2 = (V, W) = (U(t \cdot x_1 + x_2), U(t \cdot y_1 + y_2))$$

and then check if the difference $H_2 - H_1$ is small (i.e. from χ distribution). If this is true, then output
$round(H_2) = (round(U(t \cdot x_1 + x_2)), round(U(t \cdot y_1 + y_2))) = round(H_1) = H$

Let us now check the correctness of the scheme. We note that the output of $\texttt{Hint}$ algorithm is the pair (U, H_1) where $U = s \cdot r + e$. After some simplifications, we obtain

$H_1 = (s \cdot r \cdot (t \cdot x_1 + x_2) + (e_1 \cdot t + e_x + e_2) \cdot r, s \cdot r \cdot (t \cdot y_1 + y_2) + (e'_1 \cdot t + e_y + e'_2) \cdot r)$

where $(e_1 \cdot t + e_x + e_2) \cdot r$ and $(e'_1 \cdot t + e_y + e'_2) \cdot r$ are "small" since they both belong to the χ distribution.

On the other hand, H_2 will be computed as

$H_2 = (s \cdot r \cdot (t \cdot x_1 + x_2) + (t \cdot x_1 + x_2) \cdot e, s \cdot r \cdot (t \cdot y_1 + y_2) + (t \cdot y_1 + y_2) \cdot e)$

again with $(t \cdot x_1 + x_2) \cdot e$ and $(t \cdot y_1 + y_2) \cdot e$ both small from χ.

Therefore, the difference $H_2 - H_1$ is small and belongs to χ. Thus, by computing both $round(H_1)$ and $round(H_2)$, one gets exactly the same value, which is in fact hidden in the output of $\texttt{Hint}$ algorithm.

Lemma 1 *The above tag-based hint system is anonymous if the DDH-RLWE assumption holds in the ring R_q.*

Proof. The proof of this lemma follows closely that of Lemma 1 from [7] adapted to the LWE environment. We will give a sketch of it in the following.

The proof is modeled by a sequence of games, starting with the first game which is the real game.

Game 0 is the real attack game.

Game 1 differs from Game 0 in the following two issues: the challenger's bit b is chosen at the beginning of the game and in the adversary's challenge $(U^*, (V^*, W^*))$, W^* is replaced by a random element of R_q.

We show that a computationally bounded adversary cannot distinguish the adversary's challenge $(U^*, (V^*, W^*))$ from the one where W^* is replaced by a random element from R_q, under the DDH-RLWE assumption.

We construct a DDH-RLWE distinguisher B for Game 0 and Game 1 which takes as input $(s, X = s \cdot x + e_x, Y = s \cdot y + e_y, Z)$ where x, y, e_x, e_y are from χ and aims at distinguishing whether $Z = X \cdot y + e_z$ or Z is random in R_q. At the beginning of the game, B chooses θ_1 and θ_2 from χ and defines $X' = s \cdot \theta_1 + X \cdot \theta_2$. When the challenge bit b is chosen, B generates pk_{1-b} by choosing $x_{1-b,1}, x_{1-b,2}, y_{1-b,1}, y_{1-b,2}, e_{1-b,1}, e_{1-b,2}, e_{1-b,1}, e_{1-b,2} \leftarrow \chi$ and setting $X_{1-b,i} = s \cdot x_{1-b,i} + e_{1-b,i}$, for $i \in \{1, 2\}$. For pk_b, B chooses

$\alpha, \beta_1, \beta_2 \leftarrow \chi$ and computes $X_{b,1} = X', X_{b,2} = X' \cdot (-t^*) + s \cdot \beta_1, Y_{b,1} = s \cdot \beta_2 + X \cdot \alpha$ and $Y_{b,2} = s \cdot (-\beta_2) \cdot t^*$. The adversary is given the public keys $(X_{0,1}, X_{0,2}, Y_{0,1}, Y_{0,1})$ and $(X_{1,1}, X_{1,2}, Y_{1,1}, Y_{1,1})$.
To answer a verification query $(U, (V, W), t)$ with $t \neq t^*$ coming from adversary A, B can run algorithm $\texttt{Invert}(sk_{1-b}, t, U)$ since he knows sk_{1-b}. As for $\texttt{Invert}(sk_b, t, U)$, he computes
$Z_1 = (V - U \cdot \beta_1) \cdot 1/(t - t^*)$ $Z_2 = (w - U \cdot \beta_2(t - t^*)) \cdot 1/\alpha t$
and answers that $d_b = 1$ if and only if $round(Z_1) = round(U \cdot \theta_1 \cdot Z_2 \cdot \theta_2)$.
First of all, we note that we are working in the ring $\mathbb{Z}_q^n / \langle x^n + 1 \rangle$ which is a field , since q is prime and $x^n + 1$ is irreducible. Therefore, the multiplicative inverse is defined and we can compute $(1/(t - t^*))$ for example.
Finally, in the challenge phase, B constructs the challenge pair $(U^*, (V^*, W^*))$ as $U^* = Y,\ V^* = Y \cdot \beta_1,\ W^* = T \cdot \alpha t^*$. If $T = X \cdot y + e_{xy}$ with $e_{xy} \leftarrow R_q$, then A's view is the same as in Game 0 (except with small probability) while if T is random in R_q A's view is the same as in Game 1. Therefore, we have $|Pr[S_1] - Pr[S_0]| \leq Adv^{DDH}(B) + "small"$.

Game 2 is identical to Game 1 but in the challenge phase both V^* and W^* are chosen uniformly in R_q and independent of U^*. We argue that adversary A cannot see the difference as long as the DDH-RLWE assumption holds. In this game, the challenge is just a sequence of random ring elements and we have $Pr[S_2] = 1/2$.
By combing the above informations, we obtain

$$Adv^{anon-hint}(A) \leq 2Adv^{DDH}(B) + 2q/p.$$

3.2 Anonymous Broadcast Encryption

In this subsection we construct the anonymous broadcast encryption scheme from anonymous hint system $S_{hint} = (\texttt{KeyGen}, \texttt{Hint}, \texttt{Invert})$ based on LWE and LWE-based public key encryption scheme $S_{pke} = (\texttt{Gen}, \texttt{KeyGen}, \texttt{Encrypt}, \texttt{Decrypt})$. We also need a LWE-based signature scheme $\Sigma = (\mathcal{G}, \mathcal{S}, \mathcal{V})$. We remark that this is precisely the construction from [7], since in this stage of description, we don't have any contribution to it. Our contribution was mainly to translate the TAHS scheme in the lattice-based environment.

$\texttt{Setup}(\lambda, n)$: Obtain $par \leftarrow \texttt{Gen}(\lambda)$ and, for $i = 1$ to n generate encryption key pairs $(sk_i^e, pk_i^e) \leftarrow S^{pke}.\texttt{KeyGen}(par)$ and hint key pairs $(sk_i^h, pk_i^h) \leftarrow S^{hint}.\texttt{KeyGen}(\lambda)$; the master public key consists of

$$MPK = (par, \{pk_i^e, pk_i^h\}_{i=1}^n, \Sigma)$$

and the master secret key is $MSK = \{sk_i^e, sk_i^h\}_{i=1}^n$
$\texttt{KeyGen}(MPK, MSK, i)$: parse $MSK = \{sk_i^e, sk_i^h\}_{i=1}^n$ and output $sk_i = (sk_i^e, sk_i^h)$.
$\texttt{Enc}(MPK, M, S)$: to encrypt a message M for a set of users $S = \{i_1, ..., i_l\} \subseteq \{1, ..., n\}$, generate a signature key pair $(SK, VK) = \mathcal{G}(\lambda)$. Then choose random $r, e \leftarrow \chi$ and compute $(U, H_j) = S^{hint}.\texttt{Hint}(VK, pk_{i_j}^h, r)$ for $j = 1$

to l. Then, for each user index $j \in \{1, ..., l\}$ compute a ciphertext $C_j = S^{pke}.\texttt{Encrypt}(pk^e_{i_j}, M||VK)$. Choose a random permutation $\pi : \{1, ..., l\} \to \{1, ..., l\}$ and output the final ciphertext as

$$C = (VK, U, (H_{\pi(1)}, C_{\pi(1)}), ..., (H_{\pi(l)}, C_{\pi(l)}), \sigma)$$

where $\sigma = \mathcal{S}(SK, U, (H_{\pi(1)}, C_{\pi(1)}), ..., (H_{\pi(l)}, C_{\pi(l)}))$

$\texttt{Dec}(MPK, sk_i, C)$: for $sk_i = (sk^e_i, sk^h_i)$ and $C = (VK, U, (H_{\pi(1)}, C_{\pi(1)}), ..., (H_{\pi(l)}, C_{\pi(l)}), \sigma)$, return $\perp$ if $\mathcal{V}(VK, U, (H_{\pi(1)}, C_{\pi(1)}), ..., (H_{\pi(l)}, C_{\pi(l)}), \sigma) = 0$ or if U is not in the appropriate space. Otherwise, compute $H = S^{hint}.\texttt{Invert}(sk^h_i, VK, U)$. If $H \neq H_j$ for all $j \in \{1, ..., l\}$, return $\perp$. Otherwise, let j be the smallest index such that $H = H_j$ and compute $M' = S^{pke}.\texttt{Decrypt}(sk^e_i, C_j)$. If M' can be parsed as $M' = M||VK$, return M. Otherwise, return $\perp$.

We already presented an anonymous tag-based hint system secure under Ring-LWE problem. As for the PKE component of the above scheme, we suggest using the IND-CCA secure scheme described in [12]. As the authors claim, it is more efficient and compact than previous lattice-based cryptosystems since it uses a new trapdoor which is simpler, efficient and easy to implement. Under the same reasons, we suggest also employing a lattice-based signature scheme from [12], section 6.2.

Due to lack of space, we can not present any of these two suggested cryptographic primitives here but we refer the reader to [12] for more details. We just mention that they were proven to be secure under LWE-assumption. We note that the tag-based hint system and the PKE cryptosystem employed are independent in our lattice broadcast encryption scheme. Therefore, the fact that the components of the ciphertext are elements from different algebraic structures is not prohibitive. In order to apply the signature scheme, one needs to first apply a hash function on the input with the aim of "smoothing" it.

Theorem 1 *The above broadcast encryption scheme is ANO-IND-CCA secure assuming that S^{hint} scheme is anonymous, the S^{pke} scheme is IND-CCA secure and the signature scheme Σ is strongly unforgeable.*

We remark that the proof of Theorem 4 from [7] is also valid for our theorem since it deals with general IND-CCA encryption scheme and tag-based hint systems, and not with some specific constructions in a certain environment (like traditional cryptography or lattice-based cryptography).

4 Conclusions

We introduced a lattice-based variant of the anonymous broadcast encryption scheme from [7]. We showed that it is feasible to construct anonymous tag-based hint scheme from the RLWE assumption in order to achieve anonymity of the scheme. We used a variant of RLWE assumption with "small" secrets and proved

that the hint scheme is anonymous based on a RLWE-based DDH assumption. For public key encryption, we suggested the use of the IND-CCA secure LWE-based encryption scheme and digital signature scheme from [12] as they gain in efficiency and simplicity over the previous similar constructions from lattices.

References

1. Ajtai, M. : Generating hard instances of the short basis problem, In: Wiedermann, J., Van Emde Boas, P., Nielsen, M. (eds.) ICALP 1999. LNCS, vol. 1644, pp. 1-9. Springer, Heidelberg (1999).
2. Banerjee, A., Peikert, P., Rosen, A.: Pseudorandom functions and lattices, In: Pointcheval, D., Johansson, T. (eds.) Advances in Cryptology - EUROCRYPT 2012. LNCS, vol. 7237, pp. 719-737, Springer, Heidelberg (2012).
3. Brakerski, Z., Vaikuntanathan, V.: Fully homomorphic encryption from ring-lwe and security for key dependent messages, In: Rogaway, P. (ed.) Advances in Cryptology - CRYPTO 2011. LNCS, vol. 6841, pp. 505-524. Springer, Heidelberg (2011).
4. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions, In 40th Annual ACM Symposium on Theory of Computing, pp. 197–206, ACM, New York (2008).
5. Georgescu, A., Steinfeld, R.: Lattice-based key agreement protocols, 2013. In preparation.
6. Gentry, C., Waters, B.: Adaptive Security in Broadcast Encryption Systems, In: Joux, A. (ed.), Advances in Cryptology - EUROCRYPT 2009. LNCS, vol. 5479, pp. 171-188, Springer, Heidelberg (2009).
7. Libert, B., Paterson, K., Quaglia, E.: Anonymous Broadcast Encryption: Adaptive Security and Efficient Constructions in the Standard Model, In: Fischlin, M., Buchmann, J., Manulis, M. (eds.), Public Key cryptography - PKC 2012, LNCS, vol. 7293, pp. 206-224, Springer, Heidelberg (2012).
8. Lindner, R., Peikert, C.: Better Key Sizes (and Attacks) for LWE-Based Encryption. In: 11th international conference on Topics in cryptology: CT-RSA 2011, pp. 319-339, Springer-Verlag Berlin, Heidelberg (2011).
9. Lyubashesky, V.: Lattice Signatures Without Trapdoors, In: Pointcheval, D., Johansson, T. (eds.), Advances in Cryptology – EUROCRYPT 2012, vol. 7237, pp. 738-755, Springer, Heidelberg (2012).
10. Lyubashevsky, V., Peikert, C., Regev, O.: On Ideal Lattices and Learning with Errors Over Rings, In: Gilbert, H. (ed), Advances in Cryptology – EUROCRYPT 2010, vol. 6110, pp 1-23, Springer, Heidelberg (2010).
11. Micciancio, D., Goldwasser, S.: Complexity of Lattice Problems: a cryptographic perspective, Kluwer Academic Publishers, Boston, 2002.
12. Micciancio, D., Peikert, C.: Trapdoors for lattices: Simpler,tighter, faster, smaller, In: Pointcheval, D., Johansson, T. (eds.), Advances in Cryptology – EUROCRYPT 2012, vol. 7237, pp. 700-718, Springer, Heidelberg (2012).
13. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography, In 37th Annual ACM Symposium on Theory of Computing, pp. 84–93, ACM, New York (2005).
14. Stehlé, D., Steinfeld, R.: Making NTRU as secure as worst-case problems over ideal lattices, In: Paterson, K.G. (ed.), Advances in Cryptology - EUROCRYPT 2011. LNCS, vol. 6632, pp. 27-47, Springer, Heidelberg (2011).
15. Wang, J. Bi, J.: Lattice-based Identity-Based Broadcast Encryption, Cryptology ePrint Archive, Report 2010/288, 2010.