

Cloud-assisted Asynchronous Key Transport with Post-Quantum Security

Gareth T. Davies¹, Herman Galteland², Kristian Gjøsteen², and Yao Jiang²

¹Bergische Universität Wuppertal, Germany.

`davies@uni-wuppertal.de`

²Norwegian University of Science and Technology, NTNU, Norway.

`{herman.galteland,kristian.gjosteen,yao.jiang}@ntnu.no`

Abstract

In cloud-based outsourced storage systems, many users wish to securely store their files for later retrieval, and additionally to share them with other users. These retrieving users may not be online at the point of the file upload, and in fact they may never come online at all. In this asynchronous environment, key transport appears to be at odds with any demands for forward secrecy. Recently, Boyd et al. (ISC 2018) presented a protocol that allows an initiator to use a modified key encapsulation primitive, denoted a blinded KEM (BKEM), to transport a file encryption key to potentially many recipients via the (untrusted) storage server, in a way that gives some guarantees of forward secrecy. Until now all known constructions of BKEMs are built using RSA and DDH, and thus are only secure in the classical setting.

We further the understanding of the use of blinding in post-quantum cryptography in two aspects. First, we show how to generically build blinded KEMs from homomorphic encryption schemes with certain properties. Second, we construct the first post-quantum secure blinded KEMs, and the security of our constructions are based on hard lattice problems.

Keywords: Lattice-based cryptography, NTRU, Group Key Exchange, Blinded Key Encapsulation, Forward Secrecy, Cloud Storage, Post-quantum cryptography.

1 Introduction

Consider the following scenario: a user of a cloud storage service wishes to encrypt and share a file with a number of recipients, who may come online to retrieve the file at some future time. In modern cloud storage environments, access control for files is normally done via the storage provider’s interface, and the user is usually tasked with performing any encryption and managing the resulting keys. However the users do not trust the server, and in particular may be concerned that key compromise may occur to any of the involved parties at some point in the future – they thus desire some forward secrecy guarantees. A number of approaches can be taken for transporting a (randomly chosen) file encryption key from the initiator to the recipients. The first option is public-key encryption – simply encrypting under each recipient’s public key. This approach does not provide any forward secrecy, however if the initiator were to use puncturable encryption then this would provide a (currently inefficient) solution for achieving forward secrecy. The users could also perform a (necessarily interactive) group key exchange protocol, however this requires all recipients to be online: a disqualifying criterion for many usage scenarios. The challenge of providing efficient key transport that allows asynchronous fetching by the recipients and simultaneously gives some forward secrecy guarantees appears to invoke trade-offs.

Recent work by Boyd et al. [BDGJ18] (hereafter BDGJ) provided a solution that utilized the high availability of the storage provider. The initiator essentially performs key encapsulation, using an (public) encapsulation key belonging to the server, and sends an encapsulated value

(out-of-band) to each recipient. Then, each recipient blinds this value in such a way that when it asks the server to decapsulate, the server does not learn anything about the underlying file encryption key, and the homomorphic properties of the scheme enable successful unblinding by the recipient. This encapsulation-and-blinding procedure was named by the authors as a *blinded KEM* (BKEM), and the complete protocol built from this was called offline assisted group key exchange (OAGKE). Forward secrecy is achieved if the recipients delete their ephemeral values after recovering the file encryption key, and if the server deletes its decapsulation key after all recipients have been online and recovered the file.

A conceptual overview of the construction, which can achieve all these security properties, is described in Figure 1, and we refer to BDGJ [BDGJ18] for full details. In the protocol, the server runs the key generation algorithm KG and the decapsulation algorithm Decap to help the initiator share file encryption key k . The blinding algorithm Blind , executed by the responder, should prohibit the server from learning any information about the file encryption key. After the server has decapsulated a blinded encapsulation, the responder can use the unblinding algorithm Unblind to retrieve the file encryption key.

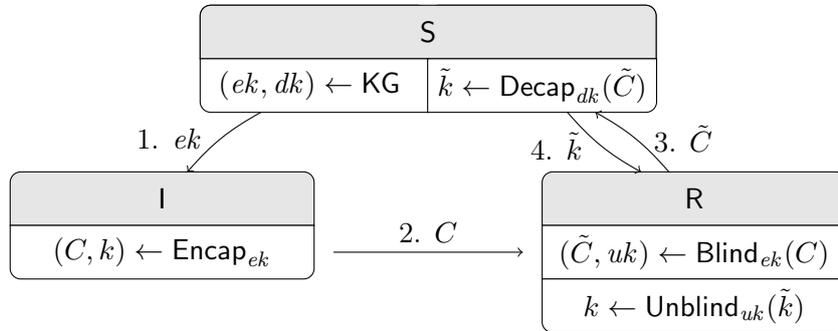


Figure 1: A simplified overview of an OAGKE protocol [BDGJ18] between an initiator I, server S and potentially many recipients R (one is given here for ease of exposition), built using a BKEM. File encryption key k is used by I to encrypt one or more files. The numbered arrows indicate the order in which operations occur.

While the approach appears promising, their two BKEM constructions built from DDH and RSA, are somewhat ad hoc, and further do not resist attacks in the presence of quantum computers. In this work we focus on one of the components of the OAGKE protocol, namely the BKEM scheme. Our wish is to achieve a post-quantum secure OAGKE protocol, where we need the individual components – a blinded KEM (parameterized by a homomorphic encryption scheme), a collision resistant hash function, a digital signature scheme, and a key derivation function – to all be post-quantum secure. Achieving post-quantum security of all components except for the BKEM has been covered extensively in prior work, and thus we focus on finding post-quantum constructions of BKEMs.

Much work has been done in the past on constructing regular key encapsulation mechanisms (KEMs) [CS01, CS03, Den03, KD04, HK07, AGKS05] that are post-quantum secure [LPR10, LPR13b, CHK⁺16, BCD⁺16, HRSS17] (the ongoing NIST standardization effort [NIS] specifically asks for KEMs), however BKEMs do not generalize KEMs, since decapsulation operates on blinded ciphertexts.

Providing post-quantum-secure BKEMs invokes a number of technical challenges. The Blind algorithm must modify the file encryption key by incorporating some randomness r , in such a way that after decapsulation (by the server) the recipient can strip off r to recover the file encryption key. In the DDH setting this is straightforward since the recipient can simply exponentiate the encapsulation, and apply the inverse on the received value from the server (the RSA setting is similarly straightforward), and, importantly, the encapsulation (with the underlying file encryption key) *and* multiple blinded samples (each with a value that is derived from the

file encryption key) will all look like random group elements. In the security game for BKEMs (as provided by BDGJ), the adversary receives: an encapsulation of a ‘real’ key, a number of blinded versions of this encapsulation (blinded encapsulations), a number of blinded versions of the ‘real’ key (blinded keys), and either this ‘real’ key or a random key, and must decide which it has been given. If the blinded key samples (the \tilde{k} s) leak information about the file encryption key then the adversary’s task in this game becomes much easier. For example, if the blinding algorithm alters the file encryption key such that the blinded keys are located close to it then exhaustive search becomes possible. We overcome this hurdle by using a large blinding value to hide the file encryption key. Similarly the blinded encapsulation samples (the \tilde{C} s) can leak information about the blinding value used to hide the file encryption key, which can be used to recover the file encryption key. For example, if the blinded encapsulation is a linear combination of the original encapsulation, the blinding value, and some small error then the distance between the blinded encapsulation and the original encapsulation could reveal the blinding value, or a small interval containing it, and therefore the file encryption key. By making sure blinded encapsulations look fresh then all blinded encapsulation samples and the encapsulation looks independent of each other. We use these techniques to provide secure BKEMs built from (a variant of) NTRU [HPS98, SS11] and ideas from Gentry’s FHE scheme [Gen09].

The second shortfall of the work of BDGJ lies in the non-generic nature of their constructions. The two provided schemes appear to have similar properties, yet do not immediately indicate how any further BKEM schemes could be constructed. We show how to generically build BKEMs from homomorphic encryption schemes with minimal properties. This allows us to more precisely cast the desirable properties of schemes used to build BKEMs, generalizing the way that the responder alters the content of an encapsulation (ciphertext) by adding an encrypted random value. Essentially, the resulting blinded ciphertext is an encryption of the sum of a file encryption key and the random value. The server can decrypt the blinded ciphertext to retrieve the blinded key, and then the responder can unblind by removing (subtracting) the random value.

1.1 Related work

Boyd et al. [BDGJ18] formalized OAGKE and BKEMs, and provided BKEM constructions based on Diffie-Hellman and RSA. To our knowledge these are the only BKEM constructions in the literature.

Recent works on secure messaging have shown how to perform secure key transport in the presence of pre-keys of the recipients [MP16, CCG⁺18, The]: we wish to avoid this assumption in our system architecture. Puncturable encryption has developed rapidly [GM15, GHJL17, DJSS18, AGJ19], however current constructions are still impractical or unsuitable for the cloud-based key transport scenario that we consider.

Gentry introduced the first fully homomorphic encryption (FHE) scheme, based on lattice problems, and gave a generic framework [Gen09]. Soon after, several FHE schemes followed this framework [BGV12, FV12, CKKS17, GSW13]: all of these schemes rely on the learning with errors (LWE) problem. Two FHE schemes based their security on an overstretched variant of the NTRU problem [LATV12, BLLN13], however, subfield lattice attacks against this variant was subsequently found [ABD16, CJL16], and consequently these schemes are no longer secure. As a side note, our NTRU based BKEM construction relies on the hardness of the LWE problem.

To make a BKEM from existing post-quantum secure KEM schemes we need, for each individual scheme, a method for altering the encapsulations in a predictable way. Most of the post-quantum secure KEM schemes submitted to NIST are built from a PKE scheme, where we can use our techniques to make a BKEM if the PKE scheme supports one homomorphic operation. FrodoKEM is the only submission that advertises its additive homomorphic properties of its FrodoPKE scheme [ABD⁺a]. Other submissions based on lattices [LLJ⁺], LWE [ABD⁺b, ADPS16, DKRV18], or NTRU [CDH⁺, BCLvV17] are potential candidates for a BKEM construction. Note that the NTRU submission of Chen et al. [CDH⁺] does not

use the Gaussian distribution to sample their polynomials, and NTRU Prime of Bernstein et al. [BCLvV17] uses a large Galois group to construct their polynomial field, instead of a cyclotomic polynomial. Furthermore, the NTRU construction of Stehlé and Steinfeld [SS11] chooses the distribution of the secret keys such that the public key looks uniformly random and they provide a security proof which relies on this.

1.2 Our contribution

Our aim in this work is to further the understanding of the use of blinding in cryptography attaining post-quantum security. In particular, we focus on blinded KEMs and their possible instantiations, in order to deliver secure key transport protocols in cloud storage environments. Specifically, we provide:

- a generic homomorphic-based BKEM construction, and show that it meets the expected indistinguishability-based security property for BKEMs, under feasible requirements.
- two instantiations of our homomorphic-based BKEM, built from primitives with post-quantum security. The proof chain is as follows.

$$\text{Hard problems} \xrightarrow[\text{or Lyubashevsky et al. [LPR13a]}]{\text{Quantum, Gentry [Gen09]}} \text{IND-CPA HE} \xrightarrow{\text{This work}} \text{IND-secure HE-BKEM}$$

As long as the underlying schemes HE (which rely on hard lattice problems) are post-quantum secure, then our HE-BKEM schemes are post-quantum secure.

1.3 Organization

In Section 2 we provide the necessary background of ideal lattices and the discrete Gaussian Distribution. In Section 3 we formally define BKEMs and their security. In Section 4 we construct a generic homomorphic BKEM schemes and analyze its security requirements. In Section 5 we provide two homomorphic-based BKEM constructions and prove that they are secure.

2 Preliminaries

This section introduces terminology and results from [Gen09, GPV08, MR07], and provides an introduction to our notation and building blocks for constructing post-quantum secure homomorphic encryption schemes. In Fig. 2 we given an overview of the notation used in the paper. Towards the end of this section we detail two specific constructions of post-quantum secure homomorphic encryption schemes [Gen09, SS11].

2.1 Notation

Given n linearly independent vectors $\{\mathbf{b}_1, \dots, \mathbf{b}_n\}$, $\mathbf{b}_i \in \mathbb{R}^m$, the m -dimensional *lattice* L generated by the vectors is $L = \{\sum_{i=1}^n x_i \mathbf{b}_i \mid x_i \in \mathbb{Z}\}$. If $n = m$ then L is a *full-rank n -dimensional lattice*, we always use full-rank lattices in this paper.

Suppose $\mathbf{B} = \{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\}$ is a basis of I , let $\mathcal{P}(\mathbf{B}) = \{\sum_{i=1}^n x_i \mathbf{b}_i \mid x_i \in [-1/2, 1/2)\}$, $\mathbf{b}_i \in \mathbf{B}$ be the half-open parallelepiped associated to the basis \mathbf{B} . Let $R = \mathbb{Z}[x]/(f(x))$ be a polynomial ring, where $f(x)$ is a monic polynomial of degree n . Any ideal $I \subseteq R$ yields a corresponding integer sublattice called *ideal lattice* of the polynomial ring. For convenience, we identify all ideals of R with its ideal lattice. Let $\|\mathbf{v}\|$ be the Euclidean norm of a vector \mathbf{v} . Define the *norm of a basis \mathbf{B}* to be the Euclidean norm of its longest column vector, that is, $\|\mathbf{B}\| = \max_{1 \leq i \leq n} (\|\mathbf{b}_i\|)$.

For a full-rank n -dimensional lattice L , let $L^* = \{\mathbf{x} \in \mathbb{R}^n \mid \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}, \forall \mathbf{y} \in L\}$ denote its *dual lattice*. If \mathbf{B} is a basis for the full-rank lattice L , then $(\mathbf{B}^{-1})^T$ is a basis of L^* . Let

| | |
|-------------------------------|--|
| L | a lattice |
| \mathbf{B} | a basis of ideal lattice I |
| $\mathcal{P}(\mathbf{B})$ | the half-open parallelepiped associated to the basis \mathbf{B} , where $\mathcal{P}(\mathbf{B}) = \{\sum_{i=1}^n x_i \mathbf{b}_i \mid x_i \in [-1/2, 1/2), \mathbf{b}_i \in \mathbf{B}\}$ |
| $R = \mathbb{Z}[x]/(f(x))$ | a polynomial ring, where $f(x)$ is a monic polynomial of degree n |
| $\ \mathbf{v}\ $ | Euclidean norm of a vector \mathbf{v} |
| $\ \mathbf{B}\ $ | norm of a basis \mathbf{B} , where $\ \mathbf{B}\ = \max_{1 \leq i \leq n} (\ \mathbf{b}_i\)$ |
| L^* | dual lattice of L |
| $\gamma_\times(R)$ | multiplicative expansion factor |
| $\mathbf{r} \bmod \mathbf{B}$ | the distinguished representative of the coset $\mathbf{r} + I$ |
| $R \bmod \mathbf{B}$ | set of all distinguished representatives in R |
| $\mathcal{B}_{\mathbf{c}}(r)$ | closed Euclidean ball centered at \mathbf{c} with radius r |
| $\mathcal{B}(r)$ | closed Euclidean ball centered at $\mathbf{0}$ with radius r |
| $\lambda_i(L)$ | the i th successive minimum |
| $\Delta(D_1, D_2)$ | statistical distance between two discrete distributions D_1 and D_2 |
| $D_{L,s,\mathbf{c}}$ | discrete Gaussian distribution over L centered at \mathbf{c} with standard deviation s |
| $\eta_\epsilon(L)$ | smoothing parameter for lattice L |

Figure 2: Summary of notation used in this paper.

$\gamma_\times(R) = \max_{\mathbf{x}, \mathbf{y} \in R} \frac{\|\mathbf{x} \cdot \mathbf{y}\|}{\|\mathbf{x}\| \cdot \|\mathbf{y}\|}$ be the *multiplicative expansion factor*. For $\mathbf{r} \in R$, define $\mathbf{r} \bmod \mathbf{B}$ to be the unique vector $\mathbf{r}' \in \mathcal{P}(\mathbf{B})$ such that $\mathbf{r} - \mathbf{r}' \in I$. We call $\mathbf{r} \bmod \mathbf{B}$ to be the *distinguished representative* of the coset $\mathbf{r} + I$. Denote $R \bmod \mathbf{B} = \{\mathbf{r} \bmod \mathbf{B} \mid \mathbf{r} \in R\}$ to be the set of all distinguished representatives in R , this set can be chosen to be the same as the half-open parallelepiped $\mathcal{P}(\mathbf{B})$ associated to the basis \mathbf{B} . For convenience we treat $R \bmod \mathbf{B}$ and $\mathcal{P}(\mathbf{B})$ as the same set. Let $\mathcal{B}_{\mathbf{c}}(r)$ denote the closed Euclidean ball centered at \mathbf{c} with radius r , for $\mathbf{c} = \mathbf{0}$ we write $\mathcal{B}(r)$. For any n -dimensional lattice L and $i = 1, \dots, n$, let the *i th successive minimum* $\lambda_i(L)$ be the smallest radius r such that $\mathcal{B}(r)$ contains i linearly independent lattice vectors.

The *statistical distance* between two discrete distributions D_1 and D_2 over a set S is $\Delta(D_1, D_2) = \frac{1}{2} \sum_{s \in S} |\Pr[D_1 = s] - \Pr[D_2 = s]|$.

2.2 Discrete Gaussian Distributions over Lattices

Definition 1 (Discrete Gaussian Distribution). Let $L \subseteq \mathbb{R}^n$ be a lattice, $s \in \mathbb{R}^+$, $\mathbf{c} \in \mathbb{R}^n$. For all $\mathbf{x} \in L$, let $\rho_{s,\mathbf{c}}(\mathbf{x}) = \exp(-\pi \|\mathbf{x} - \mathbf{c}\|^2 / s^2)$. For a set S let $\rho_{s,\mathbf{c}}(S) = \sum_{\mathbf{x} \in S} \exp(-\pi \|\mathbf{x} - \mathbf{c}\|^2 / s^2)$. Define the *discrete Gaussian distribution* over L centered at \mathbf{c} with standard deviation s to be the probability distribution

$$D_{L,s,\mathbf{c}}(\mathbf{x}) = \frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{\rho_{s,\mathbf{c}}(L)}.$$

If the standard deviation of a discrete Gaussian distribution is larger than the smoothing parameter, defined below, then there are known, useful, results of discrete Gaussian distributions that we will use in this paper.

Definition 2 (Smoothing parameter). For lattice L and real value $\epsilon > 0$, let the *smoothing parameter* $\eta_\epsilon(L)$ denote the smallest s : $\rho_{1/s}(L^* \setminus \{\mathbf{0}\}) \leq \epsilon$. We say that “ s exceeds the smoothing parameter” if $s \geq \eta_\epsilon(L)$ for negligible ϵ .

Below we show that the discrete Gaussian distribution is spherical if its standard deviation is larger than the smoothing parameter.

Lemma 1 (Micciancio and Regev [MR07]). Let L be any full-rank n -dimensional lattice. For any $\mathbf{c} \in \mathbb{R}^n$, real $\epsilon \in (0, 1)$, and $s \geq \eta_\epsilon(L)$, we have

$$\Pr[\|\mathbf{x} - \mathbf{c}\| > s \cdot \sqrt{n} \mid \mathbf{x} \leftarrow D_{L,s,\mathbf{c}}] \leq \frac{1 + \epsilon}{1 - \epsilon} \cdot 2^{-n}.$$

For a discrete Gaussian distribution over L centered at $\mathbf{0}$, with standard deviation s , $D_{L,s,\mathbf{0}}$ we let the translated discrete Gaussian distribution over L centered at any \mathbf{c} , with standard deviation s , be $D_{L,s,\mathbf{c}}$. Below we show that the statistical distance between the original discrete Gaussian distribution and its translated discrete Gaussian distribution is negligible when $\|\mathbf{c}\|$ is small.

Lemma 2 (Brakerski and Vaikuntanathan [BV11]). Let L be any full-rank n -dimensional lattice. For any $s \geq \eta_\epsilon(L)$, and any $\mathbf{c} \in \mathbb{R}^n$, we have then the statistical distance between $D_{L,s,\mathbf{0}}$ and $D_{L,s,\mathbf{c}}$ is at most $\|\mathbf{c}\|/s$.

2.3 Gentry's homomorphic encryption scheme

Let $\text{GHE} = (\text{KG}_{\text{GHE}}, \text{Enc}_{\text{GHE}}, \text{Dec}_{\text{GHE}}, \text{Add}_{\text{GHE}})$ be an (additively) Homomorphic encryption scheme derived from ideal lattices, with algorithms as defined in Figure 3. The scheme is similar to Gentry's somewhat-homomorphic scheme [Gen09]. The parameters of the GHE scheme are chosen as follows:

- Polynomial ring $R = \mathbb{Z}[x]/(f(x))$,
- Basis \mathbf{B}_I of the ideal $I \subseteq R$,
- **IdealGen** takes (R, \mathbf{B}_I) as input and outputs public and secret bases \mathbf{B}_J^{pk} and \mathbf{B}_J^{sk} of some ideal J , where I and J are relatively prime,
- **Samp** takes $(\mathbf{B}_I, \mathbf{x} \in R, s)$ as input and outputs a sample from the coset $\mathbf{x} + I$ according to a discrete Gaussian distribution with standard deviation s . In our construction we use the following two distributions.
 - $\text{Samp}_1(\mathbf{B}_I, \mathbf{x}, s) = \mathbf{x} + D_{I,s,-\mathbf{x}}$,
 - $\text{Samp}_2(\mathbf{B}_I, \mathbf{x}, s) = \mathbf{x} + D_{I,s,\mathbf{0}}$.
- Plaintext space $\mathcal{P} = R \bmod \mathbf{B}_I$ is the set of distinguished representatives of cosets of I with respect to the basis \mathbf{B}_I .

| | |
|---|---|
| $\text{KG}_{\text{GHE}}(R, \mathbf{B}_I) :$ $(\mathbf{B}_J^{pk}, \mathbf{B}_J^{sk}) \xleftarrow{\$} \text{IdealGen}(R, \mathbf{B}_I)$ $\text{pk} = (R, \mathbf{B}_I, \mathbf{B}_J^{pk}, \text{Samp}), \text{sk} = \mathbf{B}_J^{sk}$ return pk, sk | $\text{Enc}_{\text{GHE}}(\text{pk}, s, \pi \in \mathcal{P}) :$ $\psi' \leftarrow \text{Samp}(\mathbf{B}_I, \pi, s)$ $\psi \leftarrow \psi' \bmod \mathbf{B}_J^{pk}$ $\text{return } \psi$ |
| $\text{Dec}_{\text{GHE}}(\text{sk}, \psi) :$ $\pi \leftarrow (\psi \bmod \mathbf{B}_J^{sk}) \bmod \mathbf{B}_I$ $\text{return } \pi$ | $\text{Add}_{\text{GHE}}(\text{pk}, \psi_1, \psi_2) :$ $\psi \leftarrow \psi_1 + \psi_2 \bmod \mathbf{B}_J^{pk}$ $\text{return } \psi$ |

Figure 3: The algorithms of the GHE homomorphic encryption scheme, which is similar to Gentry's somewhat homomorphic encryption scheme [Gen09].

Correctness. Let X_{Enc} denote the image of Samp and X_{Dec} denote $R \bmod \mathbf{B}_f^{sk} = \mathcal{P}(\mathbf{B}_f^{sk})$. Notice that all ciphertexts are in $X_{\text{Enc}} + J$, because X_{Dec} is the set of distinguished representatives with respect to \mathbf{B}_f^{sk} . The correctness requirement of this encryption scheme is $X_{\text{Enc}} \subseteq X_{\text{Dec}}$. Furthermore, for the addition algorithm Add_{GHE} to output valid ciphertexts we require that $X_{\text{Enc}} + X_{\text{Enc}} \subseteq X_{\text{Dec}}$.

Let r_{Enc} be the smallest value such that $X_{\text{Enc}} \subseteq \mathcal{B}(r_{\text{Enc}})$ and let r_{Dec} be the largest value such that $X_{\text{Dec}} \supseteq \mathcal{B}(r_{\text{Dec}})$. By the spherical property of discrete Gaussian distribution (Lemma 1) we know that, for Samp_1 as above, X_{Enc} is located inside the ball $\mathcal{B}(s\sqrt{n})$ with high probability and $r_{\text{Enc}} = s\sqrt{n}$. For a general Samp algorithm, which is located in $\mathcal{B}(l_{\text{Samp}})$, we have that $r_{\text{Enc}} \leq (n + \sqrt{n}l_{\text{Samp}}) \|\mathbf{B}_f\|$ [Gen09]. For r_{Dec} we know that $r_{\text{Dec}} = 1/(2 \cdot \|((\mathbf{B}_f^{sk})^{-1})^T\|)$ [Gen09].

For GHE, if $\sqrt{2}r_{\text{Enc}} \leq r_{\text{Dec}}$, both ciphertexts and the sum of two ciphertexts decrypt to the correct message except for negligible probability.

2.4 The revised NTRU encryption scheme

The NTRU encryption scheme variant by Stehlé and Steinfeld [SS11], which relies on the LWE problem, has the similar structure as Gentry's homomorphic encryption scheme. We modify the NTRU scheme to use a discrete Gaussian distribution as the noise distribution instead of an elliptic Gaussian. The parameters of the scheme, given in Figure 4, are as follows:

- $R = \mathbb{Z}[x]/(x^n + 1)$, where $n \geq 8$ is a power of 2,
- q is a prime, $5 \leq q \leq \text{Poly}(n)$, $R_q = R/q$,
- $p \in R_q^\times$, $I = (p)$, the plaintext space $\mathcal{P} = R/p$,
- set the noise distribution to be $D_{\mathbb{Z}^n, s, \mathbf{0}}$.

| | |
|---|---|
| $\text{KG}_{\text{NTRU}}(n, q \in \mathbb{Z}, p \in R_q^\times, s > 0) :$ | $\text{Enc}_{\text{NTRU}}(\text{pk} = h, s, \pi \in \mathcal{P}) :$ |
| while $(f \bmod q) \notin R_q^\times$ do | $e_1, e_2 \leftarrow D_{\mathbb{Z}^n, s, \mathbf{0}}$ |
| $f' \leftarrow D_{\mathbb{Z}^n, s, \mathbf{0}}$ | $\psi \leftarrow \pi + pe_1 + he_2 \in R_q$ |
| $f = p \cdot f' + 1$ | return ψ |
| while $(g \bmod q) \notin R_q^\times$ do | $\text{Dec}_{\text{NTRU}}(\text{sk} = f, \psi) :$ |
| $g \leftarrow D_{\mathbb{Z}^n, s, \mathbf{0}}$ | $\psi' = f \cdot \psi \in R_q$ |
| $h = pg/f \in R_q$ | $\pi \leftarrow \psi' \bmod p$ |
| $(\text{pk}, \text{sk}) \leftarrow (h, f)$ | return π |
| return (pk, sk) | $\text{Add}_{\text{NTRU}}(\psi_1, \psi_2) :$ |
| | $\psi \leftarrow \psi_1 + \psi_2 \in R_q$ |
| | return ψ |

Figure 4: The algorithms of the revised NTRU encryption scheme [SS11].

Correctness Let $\psi' = f\pi + p(fe_1 + ge_2) \in R_q$ and $\psi'' = f\pi + p(fe_1 + ge_2) \in R$ (not modulo q), if $\|\psi''\|_\infty \leq q/2$ then the decryption algorithm will output π (see [SS11, Lemma 12]). We will perform a single homomorphic addition and want to find a bound on the sum of two ciphertexts. Discrete Gaussian samples are bounded by $s\sqrt{n}$ with high probability (Lemma 1) and the message space parameter p is a polynomial with small coefficients, where we let p_i denote the largest coefficient of p . We have

$$\begin{aligned} \|f(\psi_1 + \psi_2)\|_\infty &= \|f(\pi_1 + \pi_2) + p_i(f(e_1 + e'_1) + g(e_2 + e'_2))\|_\infty \\ &\leq 2(p_i^2(s\sqrt{n})^2) + p_i^2 s\sqrt{n} + p_i s\sqrt{n} + p_i + (s\sqrt{n})^2 \\ &\leq 8p_i^2 s^2 n. \end{aligned}$$

Standard deviation $s \geq \eta_\epsilon(\mathbb{Z}^n)$ and has to satisfy $\eta_\epsilon(\mathbb{Z}^n) \leq s$ and $8p_i^2 s^2 n < q/2$ for decryption to be correct with high probability. Then both ciphertexts and the sum of two ciphertexts, in the revised NTRU encryption scheme, decrypt to the correct message except for negligible probability.

2.5 Hard lattice problems

The following lattice problems, that are assumed to be hard, are used in the paper.

Definition 3 (Shortest Vector Problem (SVP)). Given a basis \mathbf{B} for a n -dimensional lattice L , output a nonzero vector $\mathbf{v} \in L$ of length at most $\lambda_1(L)$.

Definition 4 (Ideal Shortest Independent Vector Problem (SIVP)). Fix a polynomial ring R and positive real $\gamma \geq 1$. Let \mathbf{B}_I be a basis for an ideal lattice I of R . Given \mathbf{B}_I , and parameters, output a basis \mathbf{B}'_I of I with $\|\mathbf{B}'_I\| \leq \gamma \cdot \lambda_n(I)$.

Reduce Hard problems to the semantic security of Gentry's encryption scheme. The following two theorems describe Gentry's reduction from worst-case SIVP (believed to be a hard problem) to the semantic security of the encryption scheme GHE, via the ideal independent vector improvement problem (IVIP).

Theorem 1 (Gentry [Gen09, Corollary 14.7.1], reduce IVIP to semantic security). Suppose that $s_{\text{IVIP}} < (\sqrt{2}sc - 4n^2(\max\{\|\mathbf{B}_I\|\})^2)/(n^4\gamma_\times(R)\|f\|\max\{\|\mathbf{B}_I\|\})$, where s is the Gaussian deviation parameter in the encryption scheme GHE. Also suppose that $s/2$ exceeds the smoothing parameter of I , that `IdealGen` always outputs an ideal J with $s \cdot \sqrt{n} < \lambda_1(J)$, and that $[R : I]$ is prime. Finally, suppose that there is an algorithm \mathcal{A} that breaks the semantic security of GHE with advantage ϵ . Then there is a quantum algorithm that solves s_{IVIP} -IVIP for an $\epsilon/4$ (up to negligible factors) weight fraction of bases output by `IdealGen`.

Theorem 2 (Gentry [Gen09, Theorem 19.2.3 and Corollary 19.2.5], reduce SIVP to IVIP). Suppose $d_{\text{SIVP}} = (3 \cdot e)^{1/n} \cdot d_{\text{IVIP}}$, where e is Euler's constant. Suppose that there is an algorithm \mathcal{A} that solves s_{IVIP} -IVIP for parameter $s_{\text{IVIP}} > 16 \cdot \gamma_\times(R)^2 \cdot n^5 \cdot \|f\| \cdot g(n)$ for some $g(n)$ that is $\omega(\sqrt{\log n})$, whenever the given ideal has $\det(J) \in [a, b]$, where $[a, b] = [d_{\text{IVIP}}^n, 2 \cdot d_{\text{IVIP}}^n]$. Assume that invertible prime ideals with norms in $[a, b]$ are not negligibly sparse. Then, there is an algorithm \mathcal{B} that solves worst-case d_{SIVP} -SIVP.

In summary we have the following informal result, which we will use to prove that our GHE-BKEM (see Section 5.4) is post-quantum secure.

Theorem 3 (Gentry [Gen09]). If there exists an algorithm that breaks the semantic security of GHE with parameters chosen as in Theorem 1 and Theorem 2, then there exists a quantum algorithm that solves worst-case SIVP.

Reduce Hard problems to the semantic security of the revised NTRU encryption scheme We define the ring learning with error problem as follows. For $s \in R_q$ and error distribution D over R_q , let $A_{s,D}$ be a distribution that outputs tuples of the form $(a, as + e)$, where a is sampled uniformly at random from R_q and e is sampled from D . The problem is to distinguish between tuples sampled from $A_{s,D}$ and uniformly random ones.

We now introduce the tools necessary to analyze the NTRU construction.

Definition 5 (Ring-LWE). Let \mathcal{D} be a distribution over a family of distributions, each over R_q . The *Ring Learning With Errors Problem* with parameters q , and \mathcal{D} ($\text{R-LWE}_{q,\mathcal{D}}$) is as follows. Let D be sampled from \mathcal{D} and s be sampled uniformly at random from R_q . Given access to an oracle \mathcal{O} that produces samples in R_q^2 , distinguish whether \mathcal{O} outputs samples from the distribution $A_{s,D}$ or $U(R_q^2)$. The distinguishing advantage should be non-negligible.

Lyubashevsky et al. [LPR13a] proposed a reduction from SIVP or SVP (both are thought to be hard problems) to R-LWE.

Theorem 4 (Lyubashevsky et al. [LPR13a]). Let $\alpha < \sqrt{\log n/n}$ and $q = 1 \pmod{2n}$ be a $\text{poly}(n)$ -bounded prime such that $\alpha q \geq \omega(\sqrt{\log n})$. Then there is a polynomial-time quantum reduction from $O(\sqrt{n}/\alpha)$ -approximate SIVP (or SVP) on ideal lattices to $\text{R-LWE}_{q,D_s}$ given only $l(\geq 1)$ samples, where $s = \alpha \cdot (nl/\log(nl))^{1/4}$.

We consider a different variant of the R-LWE problem, namely $\text{R-LWE}_{\text{HNF}}^\times$, which is the same as $\text{R-LWE}_{q,D}$ except for the oracle \mathcal{O} that outputs samples from the distribution $A_{s,D}^\times$ or $U(R_q^2)$, where $A_{s,D}^\times$ outputs $(a, as + e)$ with $a \in R_q^\times, s \in D$. The analysis in the end of Section 2 of Stehlé and Steinfeld [SS11] shows that when $q = \Omega(n)$, $\text{R-LWE}_{\text{HNF}}^\times$ remains hard.

The security proof of NTRU encryption scheme is similar to the security proof of Lemma 3.8 of Stehlé and Steinfeld [SS11]. The proof relies on the uniformity of public key and $p \in R_q^\times$. We chose a slightly different error distribution for our construction in Section 5.4, but adaption to our setting is straightforward.

Lemma 3. Let $n \geq 8$ be a power of 2 such that $\Phi = x^n + 1$ splits into n irreducible factors modulo prime $q \geq 5$. Let $0 < \epsilon < 1/3$, $p \in R_q^\times$ and $s \geq 2n\sqrt{\ln(8nq)} \cdot q^{1/2+\epsilon}$. For any IND-CPA adversary \mathcal{A} against NTRU encryption scheme, there exists an adversary \mathcal{B} solving $\text{R-LWE}_{\text{HNF}}^\times$ such that

$$\text{Adv}_{\text{NTRU}}^{\text{IND-CPA}}(\mathcal{A}) \leq \text{Adv}_{\text{R-LWE}_{\text{HNF}}^\times}(\mathcal{B}) + q^{-\Omega(n)}.$$

3 Blinded KEM

The blinded KEM primitive is the most important building block that BDGJ used to construct their key transport protocol [BDGJ18] – also required are a signature scheme, a public-key encryption scheme, a hash function and a key derivation function. In this paper we only focus on blinded KEMs.

A *blinded KEM* scheme $\text{BKEM} = (\text{KG}, \text{Encap}, \text{Blind}, \text{Decap}, \text{Unblind})$ is parameterized by a key encapsulation mechanism $\text{KEM} = (\text{KG}, \text{Encap}, \text{Decap})$, a blinding algorithm Blind and an unblinding algorithm Unblind . The *key generation* algorithm KG outputs an encapsulation key $ek \in \mathcal{K}_E$ and a decapsulation key $dk \in \mathcal{K}_D$. The *encapsulation* algorithm Encap takes as input an encapsulation key and outputs a (file encryption) key $k \in \mathcal{K}_F$ together with an encapsulation $C \in \mathcal{C}$ of that key. The *blinding* algorithm takes as input an encapsulation key and an encapsulation and outputs a blinded encapsulation $\tilde{C} \in \mathcal{C}$ and an unblinding key $uk \in \mathcal{K}_U$. The *decapsulation* algorithm Decap takes a decapsulation key and a (blinded) encapsulation as input and outputs a (blinded) key $\tilde{k} \in \mathcal{K}_B$. The *unblinding* algorithm takes as input an unblinding key and a blinded key and outputs a key.

Definition 6 (Correctness of a BKEM). We say that a blinded KEM scheme BKEM has $(1 - \epsilon)$ -correctness if:

$$\Pr[\text{Unblind}_{uk}(\tilde{k}) = k] \geq 1 - \epsilon,$$

for $(ek, dk) \leftarrow \text{KG}$, $(C, k) \leftarrow \text{Encap}_{ek}$, $(\tilde{C}, uk) \leftarrow \text{Blind}_{ek}(C)$ and $\tilde{k} \leftarrow \text{Decap}_{dk}(\tilde{C})$.

(A KEM scheme KEM has $(1 - \epsilon)$ -correctness if

$$\Pr[\text{Decap}_{dk}(C) = k] \geq 1 - \epsilon,$$

where $(ek, dk) \leftarrow \text{KG}$ and $(C, k) \leftarrow \text{Encap}_{ek}$.)

We parameterize all BKEM schemes by a public key encryption scheme (PKE), since any PKE scheme can trivially be turned into a KEM. We modify the above definition to be a PKE-based BKEM, where the KEM algorithms are described in Figure 5.

Definition 7 (PKE-based BKEM). We call BKEM a *PKE-based BKEM* if the underlying scheme $\text{KEM} = (\text{KG}, \text{Encap}, \text{Decap})$ is parameterized by a PKE scheme $\text{PKE} = (\text{KG}_{\text{PKE}}, \text{Enc}, \text{Dec})$ as described in Figure 5.

| | | |
|---|---|--|
| $\begin{array}{l} \text{KG}(\lambda) : \\ \text{pk}, \text{sk} \leftarrow \text{KG}_{\text{PKE}}(\lambda) \\ (ek, dk) \leftarrow (\text{pk}, \text{sk}) \\ \text{return } ek, dk \end{array}$ | $\begin{array}{l} \text{Encap}_{ek} : \\ k \xleftarrow{\$} \mathcal{M} \\ C \leftarrow \text{Enc}_{ek}(k) \\ \text{return } C, k \end{array}$ | $\begin{array}{l} \text{Decap}_{dk}(\tilde{C}) : \\ \tilde{k} \leftarrow \text{Dec}_{dk}(\tilde{C}) \\ \text{return } \tilde{k} \end{array}$ |
|---|---|--|

Figure 5: KEM algorithms parameterized by a PKE scheme $\text{PKE} = (\text{KG}_{\text{PKE}}, \text{Enc}, \text{Dec})$.

3.1 Security

We define indistinguishability under chosen-plaintext attack (IND-CPA) for public key encryption and indistinguishability (IND) for blinded KEMs, respectively.

Definition 8. Let $\text{PKE} = (\text{KG}_{\text{PKE}}, \text{Enc}, \text{Dec})$ be a public key encryption scheme. The IND-CPA advantage of any adversary \mathcal{A} against PKE is

$$\text{Adv}_{\text{PKE}}^{\text{IND-CPA}}(\mathcal{A}) = 2 \left| \Pr[\text{Exp}_{\text{PKE}}^{\text{IND-CPA}}(\mathcal{A}) = 1] - 1/2 \right|,$$

where the experiment $\text{Exp}_{\text{PKE}}^{\text{IND-CPA}}(\mathcal{A})$ is given in Figure 6 (left).

Definition 9. Let $\text{BKEM} = (\text{KG}, \text{Encap}, \text{Blind}, \text{Decap}, \text{Unblind})$ be a blinded KEM. The *distinguishing advantage* of any adversary \mathcal{A} against BKEM getting r blinded encapsulations and their blinded decapsulation tuples is

$$\text{Adv}_{\text{BKEM}}^{\text{IND}}(\mathcal{A}, r) = 2 \left| \Pr[\text{Exp}_{\text{BKEM}}^{\text{IND}}(\mathcal{A}, r) = 1] - 1/2 \right|,$$

where the experiment $\text{Exp}_{\text{BKEM}}^{\text{IND}}(\mathcal{A}, r)$ is given in Figure 6 (right).

The value r represents the number of recipients in the OAGKE protocol of BDGJ – in practice this will often be fairly small, and certainly bounded by the number of users of the system.

| | |
|---|---|
| $\begin{array}{l} \text{Exp}_{\text{PKE}}^{\text{IND-CPA}}(\mathcal{A}) : \\ b \xleftarrow{\$} \{0, 1\} \\ (\text{pk}, \text{sk}) \leftarrow \text{KG}_{\text{PKE}} \\ (\text{m}_0, \text{m}_1, \text{state}) \xleftarrow{\$} \mathcal{A}(\text{pk}) \\ C_b \leftarrow \text{Enc}_{\text{pk}}(\text{m}_b) \\ b' \leftarrow \mathcal{A}(\text{state}, C_b) \\ \text{return } b' \stackrel{?}{=} b \end{array}$ | $\begin{array}{l} \text{Exp}_{\text{BKEM}}^{\text{IND}}(\mathcal{A}, r) : \\ b \xleftarrow{\$} \{0, 1\} \\ (ek, dk) \leftarrow \text{KG} \\ (C, k_1) \leftarrow \text{Encap}_{ek} \\ k_0 \xleftarrow{\$} \mathcal{K}_F \\ \text{for } j \in \{1, \dots, r\} \text{ do} \\ \quad (\tilde{C}_j, uk_j) \leftarrow \text{Blind}_{ek}(C) \\ \quad \tilde{k}_j \leftarrow \text{Decap}_{dk}(\tilde{C}_j) \\ b' \leftarrow \mathcal{A}(ek, C, k_b, \{(\tilde{C}_j, \tilde{k}_j)\}_{1 \leq j \leq r}) \\ \text{return } b' \stackrel{?}{=} b \end{array}$ |
|---|---|

Figure 6: IND-CPA experiment $\text{Exp}_{\text{PKE}}^{\text{IND-CPA}}(\mathcal{A})$ for a PKE scheme PKE (left). Indistinguishability experiment $\text{Exp}_{\text{BKEM}}^{\text{IND}}(\mathcal{A}, r)$ for a BKEM scheme BKEM (right).

4 Homomorphic-based BKEM

We now show how to turn a homomorphic encryption scheme with certain properties into a BKEM, and analyze the security requirements of such a BKEM. We eventually prove that the homomorphic-based BKEM is post-quantum secure as long as the underlying homomorphic encryption scheme is post-quantum secure.

4.1 Generic homomorphic-based BKEM

We look for PKE schemes with the following homomorphic property: suppose C and C' are two ciphertexts, then $\text{Dec}_{\text{sk}}(C \oplus_1 C') = \text{Dec}_{\text{sk}}(C) \oplus_2 \text{Dec}_{\text{sk}}(C')$, where \oplus_1 and \oplus_2 denote two group operations.

We construct blinding and unblinding algorithms using this homomorphic property. Suppose the underlying PKE scheme has $1 - \epsilon$ -correctness. To blind an encapsulation C (with corresponding file encryption key k) the **Blind** algorithm creates a fresh encapsulation C' (with corresponding blinding value k') using the Encap_{ek} algorithm, the blinded encapsulation \tilde{C} is computed as $\tilde{C} \leftarrow C \oplus_1 C'$. The unblinding key uk is the inverse element of k' with respect to \oplus_2 , that is, $uk \leftarrow k'^{-1}$. The blinding algorithm outputs \tilde{C} and uk . The decapsulation algorithm can evaluate the blinded encapsulation because of the homomorphic property. The blinded key \tilde{k} is the output of this decapsulation algorithm, that is, $\tilde{k} \leftarrow \text{Decap}_{dk}(\tilde{C})$. Hence, $\tilde{k} = k \oplus_2 k'$ with probability $1 - 2\epsilon + \epsilon^2$. To unblind \tilde{k} the unblinding algorithm outputs $\tilde{k} \oplus_2 uk$, which is k except for probability $2\epsilon - \epsilon^2$, and so the BKEM scheme has $(1 - 2\epsilon + \epsilon^2)$ -correctness. Formally, we define the BKEM scheme constructed above as follows.

Definition 10 (Homomorphic-based BKEM). Let BKEM be a PKE-based BKEM, as in Definition 7. Suppose the underlying public key encryption scheme is a homomorphic encryption scheme $\text{HE} = (\text{KG}_{\text{HE}}, \text{Enc}, \text{Dec})$ such that for any ciphertexts $C, C' \in \mathcal{C}$ and any key pair $(\text{sk}, \text{pk}) \xleftarrow{\$} \text{KG}_{\text{HE}}$ it holds that

$$\text{Dec}_{\text{sk}}(C \oplus_1 C') = \text{Dec}_{\text{sk}}(C) \oplus_2 \text{Dec}_{\text{sk}}(C'),$$

where (\mathcal{M}, \oplus_2) is the plaintext group and (\mathcal{C}, \oplus_1) is the ciphertext group. Furthermore, let the blinding and unblinding algorithms operate according to Figure 7. We call such a scheme BKEM a *homomorphic-based BKEM*.

| | |
|--|--|
| $\begin{array}{l} \text{Blind}_{ek}(C) : \\ \hline (C', k') \leftarrow \text{Encap}_{ek} \\ \tilde{C} \leftarrow C \oplus_1 C' \\ uk \leftarrow k'^{-1} \\ \text{return } \tilde{C}, uk \end{array}$ | $\begin{array}{l} \text{Unblind}_{uk}(\tilde{k}) : \\ \hline k \leftarrow \tilde{k} \oplus_2 uk \\ \text{return } k \end{array}$ |
|--|--|

Figure 7: Blinding and unblinding algorithms of the homomorphic based BKEM.

We stress that all BKEM schemes we consider in the rest of this paper are homomorphic-based BKEMs. The homomorphic encryption scheme HE does not need to be fully homomorphic, since we only need one operation in the blinding algorithm: a somewhat group homomorphic encryption scheme is sufficient.

4.2 Security requirements

In the indistinguishability game IND for BKEMs the adversary \mathcal{A} has r blinded samples. If the decryptions of blinded encapsulations output the correct blinded keys, then these r blinded

samples are the following two sets: $\{\tilde{C}_i = C \oplus_1 C'_i\}_{1,\dots,r}$ and $\{\tilde{k}_i = k \oplus_2 k'_i\}_{i=1\dots r}$, where the encapsulation is C and the real file encryption key is k . We want the blinded samples and the encapsulation to be random looking such that the combination of all these values does not reveal any information about the underlying file encryption key k that is being transported.

First, we show how to choose the blinding values k'_i to make the blinded keys \tilde{k}_i look random. Then, we show how to make the blinded encapsulations \tilde{C}_i look random, which is achievable when \tilde{C}_i looks like a fresh output of the encapsulation algorithm: this idea is similar to circuit privacy [Gen09]. Finally, we show how an IND-CPA-secure HE scheme ensures that the encapsulation does not reveal any information about the file encryption key. With these steps in place, we provide the main theorem in this paper stating how to achieve an IND secure BKEM scheme. In particular, if the underlying HE scheme is post-quantum IND-CPA secure then the corresponding homomorphic-based BKEM scheme is post-quantum IND secure.

Random-looking blinded keys. We want the blinded key to look like a random element of the space containing blinded keys. In the IND game the adversary is given several blinded keys of the form $\tilde{k} = k \oplus_2 k'$, where k is the file encryption key and k' is a blinding value, and wishes to gain information about k .

Let k be sampled uniformly at random from the file encryption key set, denoted \mathcal{K}_F , and let k' be sampled uniformly at random from the blinding value set, denoted \mathcal{K}_R . We would like that the size of \mathcal{K}_F is large enough to prevent a brute force attacker from guessing k , say $|\mathcal{K}_F| = 2^\lambda$ for some security parameter λ . If \mathcal{K}_R is a small set then the value of any blinded key $\tilde{k} = k \oplus_2 k'$ will be located within a short distance around k , so the adversary can successfully guess k with high probability. We always assume that \mathcal{K}_R is at least as large as \mathcal{K}_F .

If a given blinded key \tilde{k} can be expressed as a result of any file encryption key k and a blinding value k' , with respect to an operation, then our goal is to ensure that the adversary cannot get any information of the true file encryption key hidden in \tilde{k} : ideally we wish it to be indistinguishable from a random element.

Definition 11 (ϵ -blinded blinded key). Let BKEM be a blinded KEM with blinded key set \mathcal{K}_B . Let k be sampled uniformly random from the file encryption key set \mathcal{K}_F and let k' be sampled uniformly random from the blinding value set \mathcal{K}_R . We define a ϵ -blinded blinded key set $S := \{\tilde{k} \in \mathcal{K}_B \mid \forall k \in \mathcal{K}_F, \exists 1k' \in \mathcal{K}_R \text{ such that } \tilde{k} = k \oplus_2 k'\}$: we say that BKEM has ϵ -blinded blinded keys if

$$\Pr \left[\tilde{k} = k \oplus_2 k' \in S \mid k \xleftarrow{\$} \mathcal{K}_F, k' \xleftarrow{\$} \mathcal{K}_R \right] = 1 - \epsilon.$$

Suppose the adversary is given any number of ϵ -blinded blinded keys from S with the same underlying file encryption key k . By the definition of the ϵ -blinded blinded set the file encryption key k can be any value in \mathcal{K}_F and all values are equally probable. In other words, guessing k , given ϵ -blinded blinded keys, is the same as guessing a random value from \mathcal{K}_F . To prevent giving the adversary a better chance at guessing the key k we wish the blinded keys to be located inside the ϵ -blinded blinded key set S with high probability, which means we want ϵ to be small.

Fresh-looking blinded encapsulations. In the IND game for BKEMs the adversary \mathcal{A} gets r blinded samples and has knowledge of the set $\{\tilde{C}_i = C \oplus_1 C'_i\}_{1,\dots,r}$, where C is an encapsulation of a file encryption key k and C'_i is an encapsulation of a blinding value. We cannot guarantee that the set of the blinded encapsulations do not reveal any information about the encapsulation C . However, if each of these blinded encapsulations looks like a fresh output of the encapsulation algorithm then they are independent and random-looking compared to the encapsulation C . Therefore we want this set to be indistinguishable from the output set of the encapsulation algorithm.

Definition 12 (ϵ -blinded blinded encapsulation). Let HE-BKEM be a homomorphic based BKEM. Let ek be any encapsulation key and C_0 be an encapsulation with the underlying file encryption key k_0 . We say that HE-BKEM has ϵ -blinded blinded encapsulation if the statistical distance between the following distributions is at most ϵ :

$$\begin{aligned} X &= \{C_0 \oplus_1 C' \mid k' \xleftarrow{\$} \mathcal{K}_R, C' \leftarrow \text{Enc}_{ek}(k')\}, \\ Y &= \{C \mid k' \xleftarrow{\$} \mathcal{K}_R, C \leftarrow \text{Enc}_{ek}(k_0 \oplus_2 k')\}. \end{aligned}$$

This property ensures that the output of the blinding algorithm looks like a fresh encapsulation except for probability ϵ . Note that the BKEM constructions of Boyd et al. [BDGJ18], DH-BKEM [BDGJ18, Section 4.1] and RSA-BKEM [BDGJ18, Section 4.2], both have 0-blinded blinded encapsulation.

In most fully homomorphic encryption schemes the product of two ciphertexts is much larger in size compared to the sum of two ciphertexts, hence, it is easier to achieve ϵ -blinded blinded encapsulation for one addition compared to one multiplication. In our constructions we use addition.

Indistinguishability of BKEMs. Furthermore, if we want to achieve indistinguishability of blinded KEMs. We require the underlying homomorphic encryption scheme have some kind of semantic security to protect the message (the file encryption key) in the ciphertext (the encapsulation).

Theorem 5 (Main Theorem). For negligible ϵ_3 , let BKEM be a homomorphic based BKEM designed as in Definition 10 from a $(1 - \epsilon_3)$ -correct homomorphic encryption scheme HE. Let the file encryption key k and the blinding value k' be sampled uniformly random from the large sets \mathcal{K}_F and \mathcal{K}_R , respectively. Suppose BKEM has ϵ_1 -blinded blinded encapsulations and ϵ_2 -blinded blinded keys. For any adversary \mathcal{A} against BKEM getting r blinded encapsulations and their blinded decapsulation samples, there exists an IND-CPA adversary \mathcal{B} against HE such that

$$\text{Adv}_{\text{BKEM}}^{\text{IND}}(\mathcal{A}, r) \leq 2(r + 1)(\epsilon_1 + \epsilon_2 + \epsilon_3) + \text{Adv}_{\text{HE}}^{\text{IND-CPA}}(\mathcal{B})$$

Proof. The proof of the theorem consists of a sequence of games. □

Game 0

The first game is the experiment $\text{Exp}_{\text{BKEM}}^{\text{IND}}(\mathcal{A}, r)$, given in Figure 6 (right). Let E_0 be the event that the adversary's guess b' equals b (and let E_i be the corresponding event for Game i). From Definition 9 we have that

$$\text{Adv}_{\text{BKEM}}^{\text{IND}}(\mathcal{A}, r) = 2|\Pr[E_0] - 1/2|.$$

Game 1

We consider a modified game which is the same as Game 0 except that blinded key given to the adversary is the sum of the file encryption key and the blinding value instead of the decryption of the blinded encapsulation. More precisely, suppose C is the encapsulation with corresponding file encryption key k . For $1 \leq j \leq r$, let $C'_j + C$ is the blinded encapsulation where C'_j is a fresh encapsulation with corresponding blinding value k'_j . When \mathcal{A} queries for the blinded key of user j , the game outputs $k \oplus_2 k'_j$.

By the homomorphic property of PKE, if C and C'_1, \dots, C'_r all decrypt to the correct messages, then the output of blinded keys are the same in both Game 1 and Game 0. Hence the difference between Game 1 and Game 0 is upper bounded by the decryption error of PKE as follows.

$$\left| \Pr[E_1] - \Pr[E_0] \right| \leq 1 - (1 - \epsilon_3)^{r+1} \approx (r + 1)\epsilon_3.$$

Game 2

We consider a modified game which is the same as Game 1 except that blinded encapsulation and blinded key pairs given to the adversary are now independent and random compared to the file encryption key. More precisely, for $1 \leq j \leq r$:

- When \mathcal{A} queries the blinded encapsulation of user j , the game first chooses a random ϵ -blinded blinded key (Definition 11), $\tilde{k}_j \xleftarrow{\$} \mathbb{S}$, and computes an encapsulation of this random key, $\tilde{C}_j \leftarrow \text{Enc}_{ek}(\tilde{k}_j)$, which is given to \mathcal{A} .
- When \mathcal{A} queries for the blinded key of user j , the game outputs \tilde{k}_j .

Step 1. We first prove that a real pair of blinded key and blinded encapsulation in Game 1 is $(\epsilon_1 + \epsilon_2)$ -statistically close to the modified values in Game 2.

Suppose $k_0 \in \mathcal{K}_F$ is the file encryption key and $C_0 \leftarrow \text{Enc}_{ek}(k_0)$ is the encapsulation with k_0 , let $X = \{(k_0 \oplus_2 k', C_0 \oplus_1 C') \mid k' \xleftarrow{\$} \mathcal{K}_R, C' \leftarrow \text{Enc}_{ek}(k')\}$ be the statistical distribution of the real pair of blinded key and blinded encapsulation output in Game 1, and $Y = \{(\tilde{k}, \tilde{C}) \mid \tilde{k} \xleftarrow{\$} \mathbb{S}, \tilde{C} \leftarrow \text{Enc}_{ek}(\tilde{k})\}$ be the statistical distribution of the modified values output in Game 2. We define a middle distribution $Z = \{(k_0 \oplus_2 k', C) \mid k' \xleftarrow{\$} \mathcal{K}_R, C \leftarrow \text{Enc}_{ek}(k_0 \oplus_2 k')\}$. We compute the statistical distance between X and Y as follows.

$$\begin{aligned}
\Delta(X, Y) &\leq \Delta(X, Z) + \Delta(Z, Y) \\
&= \Delta(X, Z) + \frac{1}{2} \left(\sum_{\substack{\tilde{k} \in \mathcal{K}_B \\ \tilde{C} \in \mathcal{C}}} \left| \Pr[Z = (\tilde{k}, \tilde{C})] - \Pr[Y = (\tilde{k}, \tilde{C})] \right| \right) \\
&\leq \epsilon_1 + \frac{1}{2} \left(\sum_{\substack{\tilde{k} \in \mathcal{K}_B \\ \tilde{C} \in \mathcal{C}}} \left| \Pr[Z = (\tilde{k}, \tilde{C}) \mid \tilde{k} \in \mathbb{S}] \cdot \Pr[\tilde{k} \in \mathbb{S}] \right. \right. \\
&\quad \left. \left. + \Pr[Z = (\tilde{k}, \tilde{C}) \mid \tilde{k} \notin \mathbb{S}] \cdot \Pr[\tilde{k} \notin \mathbb{S}] - \Pr[Y = (\tilde{k}, \tilde{C})] \right| \right) \\
&= \epsilon_1 + \frac{1}{2} \left(\sum_{\substack{\tilde{k} \in \mathbb{S} \\ \tilde{C} \in \mathcal{C}}} \left| \Pr[Z = (\tilde{k}, \tilde{C}) \mid \tilde{k} \in \mathbb{S}] \cdot (1 - \epsilon_2) - \Pr[Y = (\tilde{k}, \tilde{C})] \right| \right. \\
&\quad \left. + \sum_{\substack{\tilde{k} \notin \mathbb{S} \\ \tilde{C} \in \mathcal{C}}} \left| \Pr[Z = (\tilde{k}, \tilde{C}) \mid \tilde{k} \notin \mathbb{S}] \cdot \epsilon_2 \right| \right) \tag{1} \\
&\leq \epsilon_1 + \frac{1}{2} \left(\sum_{\substack{\tilde{k} \in \mathbb{S} \\ \tilde{C} \in \mathcal{C}}} \left| \epsilon_2 \cdot \Pr[Y = (\tilde{k}, \tilde{C})] \right| + 1 \cdot \epsilon_2 \right) \tag{2} \\
&\leq \epsilon_1 + \epsilon_2
\end{aligned}$$

Note that in (1) we split the summation into two parts, namely $\tilde{k} \in \mathbb{S}$ and $\tilde{k} \notin \mathbb{S}$. For $\tilde{k} \in \mathbb{S}$ we have $\Pr[Z = (\tilde{k}, \tilde{C}) \mid \tilde{k} \notin \mathbb{S}] \cdot \Pr[\tilde{k} \notin \mathbb{S}] = 0$, and for $\tilde{k} \notin \mathbb{S}$ we have $\Pr[Z = (\tilde{k}, \tilde{C}) \mid \tilde{k} \in \mathbb{S}] \cdot \Pr[\tilde{k} \in \mathbb{S}] = 0$ and $\Pr[Y = (\tilde{k}, \tilde{C})] = 0$. Furthermore, (2) holds because distributions Z and Y over set \mathbb{S} are equal. For r samples:

$$\left| \Pr[E_2] - \Pr[E_1] \right| \leq r(\epsilon_1 + \epsilon_2).$$

Step 2. Next, we claim that there exists an adversary \mathcal{B} against IND-CPA security of HE such that

$$2 \left| \Pr[E_2] - \frac{1}{2} \right| = \mathbf{Adv}_{\text{HE}}^{\text{IND-CPA}}(\mathcal{B}).$$

We construct a reduction \mathcal{B} that plays the IND-CPA game by running \mathcal{A} , that simulates the responses of Game 2 to \mathcal{A} as follows.

1. \mathcal{B} flips a coin $b \xleftarrow{\$} \{0, 1\}$,
2. \mathcal{B} queries its IND-CPA challenger to get the public key of its IND-CPA game, and forwards this public key as the encapsulation key to \mathcal{A} ,
3. \mathcal{B} simulates the encapsulation by randomly choosing two group key k_0, k_1 , sends challenge query with input (k_0, k_1) to its IND-CPA challenger, and forwards the response C to \mathcal{A} ,
4. \mathcal{B} simulates the output of Blind and Decap by using the Encap algorithm. \mathcal{B} samples $\tilde{k} \xleftarrow{\$} \mathcal{S}$, computes $\tilde{C} \leftarrow \text{Enc}_{ek}(\tilde{k})$, and outputs \tilde{C} as the blinded encapsulation and \tilde{k} as the decapsulation of the blinded encapsulation,
5. When \mathcal{A} asks for a challenge, \mathcal{B} sends k_b to \mathcal{A} ,
6. After \mathcal{A} returns b' , \mathcal{B} sends $1 \oplus b \oplus b'$ to the challenger.

If the challenge ciphertext \mathcal{B} received in $\mathbf{Exp}_{\text{HE}}^{\text{IND-CPA}}(\mathcal{B})$ is C_b , then \mathcal{B} perfectly simulates the inputs of \mathcal{A} in Game 2 when the output of the key is a real key. Otherwise (the challenge ciphertext \mathcal{B} received in $\mathbf{Exp}_{\text{HE}}^{\text{IND-CPA}}(\mathcal{B})$ is C_{1-b}), k_b is a random key to \mathcal{A} and \mathcal{B} perfectly simulate the inputs of \mathcal{A} in Game 2 when the output of the key is a random key.

Remark 1. As a specific case of Theorem 5, the DH-BKEM construction of BDGJ has 0-blinded blinded encapsulations and 0-blinded blinded keys, and the indistinguishability of DH-BKEM is upper bounded by DDH advantage (defined in the real-or-random sense instead of left-or-right). That is

$$\mathbf{Adv}_{\text{DH-BKEM}}^{\text{IND}}(\mathcal{A}, r) \leq \mathbf{Adv}^{\text{DDH}}(\mathcal{B}).$$

This observation matches with the result of Boyd et al. [BDGJ18, Theorem 1].

5 Instantiating Homomorphic-based BKEMs

We provide two homomorphic-based BKEM constructions, based on Gentry's homomorphic encryption scheme (Section 2.3) and the NTRU variant by Stehlé and Steinfeld (Section 2.4). We show that (for some parameters) our BKEM schemes are post-quantum secure, by Theorem 5, as long as the underlying HE schemes are post-quantum secure [Gen09, LPR13a, SS11]. We only require the HE scheme to support one homomorphic operation, and we have chosen addition. Our HE schemes do not need to support bootstrapping or any multiplicative depth.

5.1 Two Homomorphic-based BKEM Schemes

Let $\text{HE} = (\text{KG}_{\text{HE}}, \text{Enc}_{\text{HE}}, \text{Dec}_{\text{HE}})$ be a homomorphic encryption scheme described in Section 2.3 or Section 2.4 with $(1-\epsilon_3)$ -correctness for negligible ϵ_3 . Let L be any full-rank n -dimensional lattice, for any $\epsilon \in (0, 1)$, $s \geq \eta_\epsilon(L)$, and $r \geq 2^{\omega(\log(n))} \cdot s$. The abstract construction of HE-BKEM is in Figure 8.

5.2 Constructions of random-looking blinded keys

We want the blinded keys to be in the ϵ -blinded blinded key set \mathcal{S} with high probability, and we analyze the requirements of the blinding values. We provide two constructions of the ϵ -blinded blinded keys set \mathcal{S} as follows.

| | | |
|---|---|---|
| $\begin{array}{l} \text{KG}(\lambda) : \\ \text{pk, sk} \leftarrow \text{KG}_{\text{HE}}(\lambda) \\ (ek, dk) \leftarrow (\text{pk}, \text{sk}) \\ \text{return } ek, dk \end{array}$ | $\begin{array}{l} \text{Blind}_{ek}(C) : \\ k' \xleftarrow{\$} \mathcal{K}_R \\ C' \leftarrow \text{Enc}_{\text{HE}}(ek, r, k') \\ \tilde{C} \leftarrow \text{Add}_{\text{HE}}(C, C') \\ uk \leftarrow -k' \pmod{\mathbf{B}} \\ \text{return } \tilde{C}, uk \end{array}$ | $\begin{array}{l} \text{Decap}_{dk}(\tilde{C}) : \\ \tilde{k} \leftarrow \text{Dec}_{\text{HE}}(dk, \tilde{C}) \\ \text{return } \tilde{k} \end{array}$ |
| $\begin{array}{l} \text{Encap}_{ek} : \\ k \xleftarrow{\$} \mathcal{K}_F \\ C \leftarrow \text{Enc}_{\text{HE}}(ek, s, k) \\ \text{return } C, k \end{array}$ | | $\begin{array}{l} \text{Unblind}_{uk}(\tilde{k}) : \\ k \leftarrow \tilde{k} + uk \pmod{\mathbf{B}} \\ \text{return } k \end{array}$ |

Figure 8: HE-BKEM, where \mathbf{B} is the basis of the plaintext space \mathcal{P} .

Construction I. A file encryption key of HE-BKEM is a random element located in a subspace of the underlying HE scheme's message space \mathcal{M} . We want to take a small file encryption key k and add a large blinding value k' to produce a slightly larger blinded key \tilde{k} , hence, the corresponding key sets should satisfy $\mathcal{K}_F \subseteq \mathcal{K}_R \subseteq \mathcal{K}_B \subseteq \mathcal{M}$. Suppose \mathcal{M} is HE scheme's message space with generators $1, x, \dots, x^{n-1}$ and order q , i.e. $\mathcal{M} = \{d_0 + d_1x + \dots + d_{n-1}x^{n-1} \mid d_i \in \mathbb{F}_q\}$. The addition of two elements in \mathcal{M} is defined as follows

$$\begin{aligned} & (a_0 + a_1x + \dots + a_{n-1}x^{n-1}) + (b_0 + b_1x + \dots + b_{n-1}x^{n-1}) \\ &= (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_{n-1} + b_{n-1})x^{n-1} \end{aligned}$$

Suppose $\mathcal{K}_F = \{d_0 + d_1x + \dots + d_{n-1}x^{n-1} \mid d_i \in \mathbb{Z}_{\lfloor \sqrt{q/2} \rfloor}\}$ and $\mathcal{K}_R = \{d_0 + d_1x + \dots + d_{n-1}x^{n-1} \mid d_i \in \mathbb{Z}_{\lfloor q/2 \rfloor}\}$. For any $c_i \in \{\lfloor \sqrt{q/2} \rfloor, \dots, \lfloor q/2 \rfloor\}$ and any $a_i \in \mathbb{Z}_{\lfloor \sqrt{q/2} \rfloor}$ there exists a unique $b_i = c_i - a_i \in \mathbb{Z}_{\lfloor q/2 \rfloor}$. As such, for these restricted $c_0 + c_1x + \dots + c_{n-1}x^{n-1}$ and for any $a_0 + a_1x + \dots + a_{n-1}x^{n-1} \in \mathcal{K}_F$ there exists a unique $b_0 + b_1x + \dots + b_{n-1}x^{n-1} \in \mathcal{K}_R$ such that $(a_0 + a_1x + \dots + a_{n-1}x^{n-1}) + (b_0 + b_1x + \dots + b_{n-1}x^{n-1}) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$. Then

$$\mathbf{S} = \{d_0 + d_1x + \dots + d_{n-1}x^{n-1} \mid d_i \in \{\lfloor \sqrt{q/2} \rfloor, \dots, \lfloor q/2 \rfloor\}\}$$

Note that for any $i \in \{0, \dots, n-1\}$,

$$\Pr[a_i + b_i \in \{\lfloor \sqrt{q/2} \rfloor, \dots, \lfloor q/2 \rfloor\} \mid a_i \xleftarrow{\$} \mathbb{Z}_{\lfloor \sqrt{q/2} \rfloor}, b_i \xleftarrow{\$} \mathbb{Z}_{\lfloor q/2 \rfloor}] = 1 - \frac{\lfloor \sqrt{q/2} \rfloor - 1}{\lfloor q/2 \rfloor},$$

so the probability that a blinded key is located in the ϵ -blinded blinded set is

$$\Pr[\tilde{k} = k + k' \in \mathbf{S} \mid k \xleftarrow{\$} \mathcal{K}_F, k' \xleftarrow{\$} \mathcal{K}_R] = \left(1 - \frac{\lfloor \sqrt{q/2} \rfloor - 1}{\lfloor q/2 \rfloor}\right)^n \approx 1 - \frac{n}{\lfloor \sqrt{q/2} \rfloor}.$$

In this construction, HE-BKEM has ϵ -blinded blinded keys with $\epsilon = n/\lfloor \sqrt{q/2} \rfloor$. For suitably large q , the above ϵ can be made negligible.

Construction II. Let the file encryption key k be an element in a subset of \mathcal{M} : we want to add a random blinding value k' from the whole message space \mathcal{M} to produce a random-looking blinded key \tilde{k} , hence, the corresponding key sets should satisfy $\mathcal{K}_F \subseteq \mathcal{K}_R = \mathcal{K}_B = \mathcal{M}$. For any blinded key $\tilde{k} \in \mathcal{M}$ and any file encryption key $k \in \mathcal{K}_F$ there exists a unique random value $k' = \tilde{k} - k \pmod{\mathbf{B}} \in \mathcal{M}$ such that $\tilde{k} = k + k' \pmod{\mathbf{B}}$, thus the ϵ -blinded blinded set \mathbf{S} is \mathcal{M} and thus

$$\Pr[\tilde{k} = k + k' \pmod{\mathbf{B}} \in \mathbf{S} \mid k \xleftarrow{\$} \mathcal{K}_F, k' \xleftarrow{\$} \mathcal{M}] = 1.$$

In this construction, HE-BKEM has ϵ -blinded blinded keys with $\epsilon = 0$.

Remark 2. Both of these constructions can be applied to our HE-BKEM schemes.

5.3 Construction of fresh-looking blinded encapsulations

We claim that HE-BKEM in Figure 8 has ϵ -blinded blinded encapsulations with negligible ϵ . The idea is to take the small constant ciphertext and add a ciphertext with large error(s) and the resulting ciphertext should look like a fresh ciphertext with large error(s). The details are given in the following lemma.

Lemma 4. Let HE-BKEM be a homomorphic based BKEM with the underlying homomorphic encryption scheme described in Section 2.3 or 2.4. Let ek be any encapsulation key, and recall that the encryption algorithm $\text{Enc}_{\text{HE}}(ek, s, \cdot)$ uses the discrete Gaussian distribution $D_{L,s,\mathbf{0}}$ as the error distribution. Suppose $C_0 = \text{Enc}_{\text{HE}}(ek, s, k_0)$ is an encapsulation of the underlying file encryption key k_0 . For any $\epsilon \in (0, 1)$, let $s \geq \eta_\epsilon(L)$ and $r \geq 2^{\omega(\log(n))} \cdot s$, then the statistical distance between the following distributions is negligible

$$\begin{aligned} X &= \{C_0 \oplus_1 C' \mid k' \xleftarrow{\$} \mathcal{K}_R, C' \leftarrow \text{Enc}_{\text{HE}}(ek, r, k')\} \\ Y &= \{C \mid k' \xleftarrow{\$} \mathcal{K}_R, C \leftarrow \text{Enc}_{\text{HE}}(ek, r, k_0 \oplus_2 k')\}. \end{aligned}$$

Proof. We prove the result for Gentry's scheme; similar analysis for NTRU follows the same approach. Suppose $C_0 = k_0 + e_0$, where $e_0 \leftarrow D_{L,s,\mathbf{0}}$. Then

$$C_0 \oplus_1 \text{Enc}_{\text{HE}}(ek, r, k') = k_0 + e_0 + k' + D_{L,r,\mathbf{0}} = k_0 + k' + e_0 + D_{L,r,\mathbf{0}}.$$

By Lemma 1, we have $\|e_0\| > s\sqrt{n}$ with negligible probability. For $\|e_0\| \leq s\sqrt{n}$, we have $\frac{\|e_0\|}{r} \leq \frac{\sqrt{n}}{2^{\omega(\log(n))}}$, which is negligible for sufficient large n . By Lemma 2, we have $e_0 + D_{L,r,\mathbf{0}} \stackrel{s}{\approx} D_{L,r,\mathbf{0}}$. Therefore,

$$C_0 \oplus_1 \text{Enc}_{\text{HE}}(ek, r, k') \stackrel{s}{\approx} k_0 + k' + D_{L,r,\mathbf{0}} = \text{Enc}_{\text{HE}}(ek, r, k_0 \oplus_2 k').$$

□

5.4 Indistinguishability of our HE-BKEM

The HE-BKEM schemes, defined in Section 5.1, have random-looking blinded keys, which follows from the designs discussed in Section 5.2. Furthermore, these schemes have fresh-looking blinded encapsulations, which follows from Lemma 4 discussed in Section 5.3. The following corollaries show GHE-BKEM and NTRU-BKEM are IND-secure BKEMs with post-quantum security.

Corollary 1. Let GHE-BKEM be a homomorphic-based BKEM described in Section 5.1. For negligible ϵ, ϵ_2 , choose parameters as in Lemma 4, Theorem 1 and Thm. 2. Suppose GHE-BKEM has ϵ_2 -blinded blinded keys. If there is an algorithm that breaks the indistinguishability of GHE-BKEM, i.e. the distinguishing advantage of this algorithm against GHE-BKEM getting r blinded encapsulation and their blinded decapsulation tuples is non-negligible, then there exists a quantum algorithm that solves worst-case SIVP.

Proof. By Lemma 4 there exists a negligible ϵ_1 such that GHE-BKEM has ϵ_1 -blinded blinded encapsulations. Then we can apply Theorem 5, which states that if there is an algorithm that breaks the indistinguishability of GHE-BKEM then there exists an algorithm breaks IND-CPA security of GHE, and by Theorem 3 we have a quantum algorithm that solves worst-case SIVP. □

Corollary 2. Let NTRU-BKEM be a homomorphic-based BKEM described in Section 5.1. For negligible ϵ, ϵ_2 , choose parameters as in Lemma 4, Lemma 3, and Thm. 4. Suppose NTRU-BKEM has ϵ_2 -blinded blinded keys. If there is an algorithm that breaks indistinguishability of NTRU-BKEM then there exists a quantum algorithm that solves $O(\sqrt{n}/\alpha)$ -approximate SIVP (or SVP) on ideal lattices.

Proof. Similar to the proof of Corollary 1, from Lemma 4 and Theorem 5 we know that if there is an algorithm that breaks the indistinguishability of NTRU-BKEM then there exists an algorithm that breaks IND-CPA security of NTRU. By Lemma 3 there exists an adversary solving $\text{R-LWE}_{\text{HNF}}^{\times}$ and by Theorem 4 there exists a quantum algorithm that solves SIVP. \square

Parameter settings. For our HE-BKEM schemes, the parameters of the underlying homomorphic encryption schemes are chosen from Gentry [Gen09] or Stehlé and Steinfeld [SS11], which is required to achieve IND-CPA security. Furthermore, our BKEM schemes require that $r = 2^{\omega(\log(n))} \cdot s$, where s is the standard deviations of a “narrow” Gaussian distributions $D_{L,s,0}$ and r is the standard deviations of a “wider” Gaussian distributions $D_{L,r,0}$. We also follows the designs discussed in Section 5.2 to construct random-looking blinded keys. We conclude that for these parameter settings our proposed BKEM schemes are post-quantum secure.

6 Conclusions and Future Work

In this work, we furthered the understanding of cloud-assisted key transport and provided instantiations that are secure even in the presence of quantum computers. In the process, we demonstrated the necessary properties of an underlying key encapsulation mechanism, to meet the desirable security properties for this environment.

The main avenue for future work is for truly efficient schemes, that are comparable at the scale of a cloud storage provider with the DDH- and RSA-based protocols given by Boyd et al. in prior work. This task is not straightforward: blinding in the schemes we consider invokes the need for large parameters to hide the secret values – this alone makes these lattice-based schemes less efficient.

Acknowledgements. We would like to thank Liqun Chen and Martijn Stam for a number of useful suggestions for improvement, and anonymous reviewers for valuable comments in improving earlier versions of this work. Gareth T. Davies has been supported by the European Research Council (ERC) under the European Union’s Horizon 2020 research and innovation programme, grant agreement 802823.

References

- [ABD⁺a] Erdem Alkim, Joppe W. Bos, Léo Ducas, Karen Easterbrook, Brian LaMacchia, Patrick Longa, Ilya Mironov, Valeria Nikolaenko, Chris Peikert, Ananth Raghunathan, and Douglas Stebila. FrodoKEM: Learning With Errors Key Encapsulation. <https://frodokem.org/files/FrodoKEM-specification-20190330.pdf>. Submission to the NIST Post-Quantum Standardization project, round 2.
- [ABD⁺b] Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS-Kyber (version 2.0). <https://pq-crystals.org/kyber/data/kyber-specification-round2.pdf>. Submission to the NIST Post-Quantum Standardization project, round 2.
- [ABD16] Martin Albrecht, Shi Bai, and Léo Ducas. A subfield lattice attack on overstretched NTRU assumptions - cryptanalysis of some FHE and graded encoding schemes. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO (1)*, pages 153–178. Springer-Verlag, 2016.

- [ADPS16] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum key exchange - A new hope. In Thorsten Holz and Stefan Savage, editors, *USENIX Security Symposium*, pages 327–343. USENIX Association, 2016.
- [AGJ19] Nimrod Aviram, Kai Gellert, and Tibor Jager. Session resumption protocols and efficient forward security for TLS 1.3 0-RTT. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT (2)*, volume 11477 of *Lecture Notes in Computer Science*, pages 117–150. Springer, 2019.
- [AGKS05] Masayuki Abe, Rosario Gennaro, Kaoru Kurosawa, and Victor Shoup. Tagkem/dem: A new framework for hybrid encryption and A new analysis of kurosawadesmedt KEM. In Ronald Cramer, editor, *EUROCRYPT*, volume 3494 of *Lecture Notes in Computer Science*, pages 128–146. Springer, 2005.
- [BCD⁺16] Joppe W. Bos, Craig Costello, Léo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan, and Douglas Stebila. Frodo: Take off the ring! practical, quantum-secure key exchange from LWE. In Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi, editors, *ACM Conference on Computer and Communications Security*, pages 1006–1018. ACM, 2016.
- [BCLvV17] Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal. NTRU prime: Reducing attack surface at low cost. In Carlisle Adams and Jan Camenisch, editors, *SAC*, volume 10719 of *Lecture Notes in Computer Science*, pages 235–260. Springer, 2017.
- [BDGJ18] Colin Boyd, Gareth T. Davies, Kristian Gjøsteen, and Yao Jiang. Offline assisted group key exchange. In Liqun Chen, Mark Manulis, and Steve Schneider, editors, *ISC*, volume 11060 of *Lecture Notes in Computer Science*, pages 268–285. Springer, 2018.
- [BGV12] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. In Shafi Goldwasser, editor, *ITCS*, pages 309–325. ACM, 2012.
- [BLLN13] Joppe W. Bos, Kristin E. Lauter, Jake Loftus, and Michael Naehrig. Improved security for a ring-based fully homomorphic encryption scheme. In Martijn Stam, editor, *IMACC*, volume 8308 of *Lecture Notes in Computer Science*, pages 45–64. Springer, 2013.
- [BV11] Zvika Brakerski and Vinod Vaikuntanathan. Fully homomorphic encryption from ring-lwe and security for key dependent messages. In Phillip Rogaway, editor, *CRYPTO*, volume 6841 of *Lecture Notes in Computer Science*, pages 505–524. Springer, 2011.
- [CCG⁺18] Katriel Cohn-Gordon, Cas Cremers, Luke Garratt, Jon Millican, and Kevin Milner. On ends-to-ends encryption: Asynchronous group messaging with strong security guarantees. In David Lie, Mohammad Mannan, Michael Backes, and XiaoFeng Wang, editors, *CCS*, pages 1802–1819. ACM, 2018.
- [CDH⁺] Cong Chen, Oussama Danba, Jeffrey Hoffstein, Andreas Hülsing, Joost Rijneveld, John M. Schanck, Peter Schwabe, William Whyte, and Zhenfei Zhang. NTRU). <https://ntru.org/f/ntru-20190330.pdf>. Submission to the NIST Post-Quantum Standardization project, round 2.

- [CHK⁺16] Jung Hee Cheon, Kyoohyung Han, Jinsu Kim, Changmin Lee, and Yongha Son. A practical post-quantum public-key cryptosystem based on spLWE. In Seokhie Hong and Jong Hwan Park, editors, *ICISC*, volume 10157 of *Lecture Notes in Computer Science*, pages 51–74, 2016.
- [CJL16] Jung Hee Cheon, Jinhyuck Jeong, and Changmin Lee. An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without a low-level encoding of zero. *LMS Journal of Computation and Mathematics*, 19(A):255–266, 2016.
- [CKKS17] Jung Hee Cheon, Andrey Kim, Miran Kim, and Yong Soo Song. Homomorphic encryption for arithmetic of approximate numbers. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT (1)*, volume 10624 of *Lecture Notes in Computer Science*, pages 409–437. Springer, 2017.
- [CS01] Ronald Cramer and Victor Shoup. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. Cryptology ePrint Archive, Report 2001/108, 2001. <https://eprint.iacr.org/2001/108>.
- [CS03] Ronald Cramer and Victor Shoup. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. *SIAM J. Comput.*, 33(1):167–226, 2003.
- [Den03] Alexander W. Dent. A designer’s guide to KEMs. In Kenneth G. Paterson, editor, *IMACC*, volume 2898 of *Lecture Notes in Computer Science*, pages 133–151. Springer, 2003.
- [DJSS18] David Derler, Tibor Jager, Daniel Slamanig, and Christoph Striecks. Bloom filter encryption and applications to efficient forward-secret 0-rtt key exchange. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT (3)*, volume 10822 of *Lecture Notes in Computer Science*, pages 425–455. Springer, 2018.
- [DKRV18] Jan-Pieter D’Anvers, Angshuman Karmakar, Sujoy Sinha Roy, and Frederik Vercauteren. Saber: Module-LWR based key exchange, cpa-secure encryption and cca-secure KEM. In Antoine Joux, Abderrahmane Nitaj, and Tajjeeddine Rachidi, editors, *AFRICACRYPT*, volume 10831 of *Lecture Notes in Computer Science*, pages 282–305. Springer, 2018.
- [FV12] Junfeng Fan and Frederik Vercauteren. Somewhat practical fully homomorphic encryption. Cryptology ePrint Archive, Report 2012/144, 2012. <https://eprint.iacr.org/2012/144>.
- [Gen09] Craig Gentry. *A Fully Homomorphic Encryption Scheme*. PhD thesis, Stanford University, Stanford, CA, USA, 2009. AAI3382729.
- [GHJL17] Felix Günther, Britta Hale, Tibor Jager, and Sebastian Lauer. 0-RTT key exchange with full forward secrecy. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT (3)*, volume 10212 of *Lecture Notes in Computer Science*, pages 519–548, 2017.
- [GM15] Matthew D. Green and Ian Miers. Forward secure asynchronous messaging from puncturable encryption. In *IEEE Symposium on Security and Privacy*, pages 305–320. IEEE Computer Society, 2015.
- [GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In Cynthia Dwork, editor, *STOC*, pages 197–206. ACM, 2008.

- [GSW13] Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In Ran Canetti and Juan A. Garay, editors, *CRYPTO (1)*, volume 8042 of *Lecture Notes in Computer Science*, pages 75–92. Springer, 2013.
- [HK07] Dennis Hofheinz and Eike Kiltz. Secure hybrid encryption from weakened key encapsulation. In Alfred Menezes, editor, *CRYPTO*, volume 4622 of *Lecture Notes in Computer Science*, pages 553–571. Springer, 2007.
- [HPS98] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In Joe Buhler, editor, *ANTS*, volume 1423 of *Lecture Notes in Computer Science*, pages 267–288. Springer, 1998.
- [HRSS17] Andreas Hülsing, Joost Rijneveld, John M. Schanck, and Peter Schwabe. High-speed key encapsulation from NTRU. In Wieland Fischer and Naofumi Homma, editors, *CHES*, volume 10529 of *Lecture Notes in Computer Science*, pages 232–252. Springer, 2017.
- [KD04] Kaoru Kurosawa and Yvo Desmedt. A new paradigm of hybrid encryption scheme. In Matthew K. Franklin, editor, *CRYPTO*, volume 3152 of *Lecture Notes in Computer Science*, pages 426–442. Springer, 2004.
- [LATV12] Adriana López-Alt, Eran Tromer, and Vinod Vaikuntanathan. On-the-fly multi-party computation on the cloud via multikey fully homomorphic encryption. In Howard J. Karloff and Toniann Pitassi, editors, *STOC*, pages 1219–1234. ACM, 2012.
- [LLJ⁺] Xianhui Lu, Yamin Liu, Dingding Jia, Haiyang Xue, Jingnan He, Zhenfei Zhang, Zhe Liu, Hao Yang, Bao Li, and Kunpeng Wang. LAC Lattice-based Cryptosystems. Submission to the NIST Post-Quantum Standardization project, round 2.
- [LPR10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In Henri Gilbert, editor, *EUROCRYPT*, volume 6110 of *Lecture Notes in Computer Science*, pages 1–23. Springer, 2010.
- [LPR13a] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. *J. ACM*, 60(6):43:1–43:35, November 2013.
- [LPR13b] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. A toolkit for Ring-LWE cryptography. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT*, volume 7881 of *Lecture Notes in Computer Science*, pages 35–54. Springer, 2013.
- [MP16] Moxie Marlinspike and Trevor Perrin. The X3DH key agreement protocol. <https://signal.org/docs/specifications/x3dh/>, November 2016.
- [MR07] Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on gaussian measures. *SIAM J. Comput.*, 37(1):267–302, April 2007.
- [NIS] NIST Post-Quantum Cryptography Standardization. <https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization>. Accessed: 2019-11-15.
- [SS11] Damien Stehlé and Ron Steinfeld. Making NTRU as secure as worst-case problems over ideal lattices. In Kenneth G. Paterson, editor, *EUROCRYPT*, Lecture Notes in Computer Science, pages 27–47. Springer-Verlag, 2011.

[The] The messaging layer security (MLS) protocol. Internet draft, in progress. <https://datatracker.ietf.org/wg/mls/about>. Accessed: 2019-11-25.