SECURITY OF HOMOMORPHIC ENCRYPTION

Melissa Chase, Hao Chen, Jintai Ding, Shafi Goldwasser, Sergey Gorbunov, Jeffrey Hoffstein, Kristin Lauter, Satya Lokam, Dustin Moody, Travis Morrison, Amit Sahai, Vinod Vaikuntanathan

We met as a group during the Homomorphic Encryption Standardization Workshop on July 13-14, 2017, hosted at Microsoft Research in Redmond. Researchers from around the world represented a number of different communities: government, industry, and academia. There are at least 6 research groups around the world who have made libraries for general-purpose homomorphic encryption available ([SEAL], [HElib], [Palisade], [cuHE], [NFLLib], [HEAAN]) for applications and general-purpose use, and demos were shown of all 6 libraries. All 6 of these general-purpose libraries for homomorphic encryption were based on RLWE-based systems (Ring Learning With Errors), and all libraries implemented one of two encryption schemes (BGV or B/FV) and also displayed common choices for the underlying ring, error distribution, and parameter selection.

Homomorphic Encryption is a breakthrough new technology which can enable private cloud storage and computation solutions. Demos shown at the workshop included a SEAL demo of CryptoNets, which performs efficient computation of image processing tasks such as hand-writing recognition on encrypted data using neural nets. Many other applications are described in detail in the white paper by the Applications group. In order for Homomorphic Encryption to be adopted in medical, health, and financial sectors to protect data and patient and consumer privacy, it will have to be standardized, most likely by multiple standardization bodies and government agencies. An important part of standardization is broad agreement on security levels for varying parameter sets. Although extensive research and benchmarking has been done in the research community to establish the foundations for this effort, it is hard to find all the information in one place, along with concrete parameter recommendations for applications and deployment.

This document is an attempt to capture the collective knowledge at the workshop regarding the currently known state of security of these schemes, to specify the schemes, and to recommend a wide selection of parameters to be used for homomorphic encryption at various security levels. We describe known attacks and their estimated running times in order to make these parameter recommendations. We also describe additional features of these encryption schemes which make them useful in different applications and scenarios. Many sections of this document are intended for direct use as a first draft of parts of the standard to be prepared by the Working Group formed at this workshop.

Outline of the document:

Section 1: introduces notation and definitions.
Section 2: defines the security properties for homomorphic encryption.
Section 3: describes the BGV and B/FV schemes, plus refers to three alternative schemes: YASHE, NTRU/LTV, and GSW.
Section 4: describes the security assumptions, such as the RLWE assumption.
Section 5: describes known attacks and recommends concrete parameters.
Section 6: describes additional features of the schemes.

Section 1. INTERFACES AND DEFINITIONS

- ParamGen(λ, P, K, B) → Params

The parameter generation algorithm is used to instantiate various parameters used in the HE algorithms outlined below. As input, it takes:

- λ denotes the desired security level of the scheme. For instance, 128-bit security ($\lambda = 128$) or 256-bit security.
- P denotes the modulus of the plaintext numbers one wants to encrypt. For instance, $P = 1024$ implies that each individual element of the message space is chosen from range (0, 1023) and all operations over individual elements are performed modulo P.
- K denotes the dimension of the vectors to be encrypted. For instance, $K = 100, P = 1024$ means the messages to be encrypted are vectors $(V_1, \dots, V_K)$ where each V_i is chosen from the range (0, 1023) and operations are performed component-wise. That is, by defintion, $(V_1, \dots, V_K) + (V_1', \dots, V_K') = (V_1 + V_1', \dots, V_K + V_K')$. The multiplication operation over two vectors is defined similarly. The space of all possible vectors $(V_1, \dots, V_K)$ is referred to as the message space (MS).
- B: denotes an auxiliary parameter that is used to control the complexity of the programs/circuits that one can expect to run over the encrypted messages. Lower parameters denotes “smaller”, or less expressive, or less complex programs/circuits. Lower parameters, generally means smaller parameters of the entire scheme. This, as a result, translates into smaller ciphertexts and more efficient evaluation procedures. Higher parameters, generally increases key sizes, ciphertext sizes, and complexity of the evaluation procedures. Higher parameters are, of course, necessary to evaluate more complex programs.

- PubKeygen(Params) → SK, PK, EK

The public key-generation algorithm is used to generate a pair of secret and public keys. The public key can be shared and used by anyone to encrypt messages. The secret key should be kept private by a user and can be used to decrypt messages. The algorithm also generates an evaluation key that is needed to perform homomorphic operations over the ciphertexts. It should

be given to any entity that will perform homomorphic operations over the ciphertexts. Any entity that has only the public and the evaluation keys cannot learn anything about the messages from the ciphertexts only.

- SecKeygen(Params) → SK, EK

The secret key-generation algorithm is used to generate a secret key. This secret key is needed to both encrypt and decrypt messages by the scheme. It should be kept private by the user. The algorithm also generates an evaluation key that is needed to perform homomorphic operations over the ciphertexts. The evaluation key should be given to any entity that will perform homomorphic operations over the ciphertexts. Any entity that has only the evaluation key cannot learn anything about the messages from the ciphertexts only.

- PubEncrypt(PK, M) → C

The public encryption algorithm takes as input the public key of the scheme and any message M from the message space. The algorithm outputs a ciphertext C. This algorithm generally needs to be randomized (that is, use random or pseudo-random coins) to satisfy the security properties.

- SecEncrypt(SK, M) → C

The secret encryption algorithm takes as input the secret key of the scheme and any message M from the message space. The algorithm outputs a ciphertext C. This algorithm generally needs to be randomized (that is, use random or pseudo-random coins) to satisfy the security properties.

- Decrypt(SK, C) → M

The decryption algorithm takes as input the secret key of the scheme, SK, and a ciphertext C. It outputs a message M from the message space. The algorithm may also output special symbol FAIL, if the decryption cannot successfully recover the encrypted message M.

- EvalAdd(Params, EK, C1, C2) → C3.

EvalAdd is a randomized algorithm that takes as input the system parameters Params, the evaluation key EK, two ciphertexts C1 and C2, and outputs a ciphertext C3.

The correctness property of EvalAdd is that if C1 is an encryption of plaintext element M1 and C2 is an encryption of plaintext element M2, then C3 should be an encryption of M1+M2.

- EvalAddConst(Params, EK, C1, M2) → C3.

EvalAddConst is a randomized algorithm that takes as input the system parameters Params, the evaluation key EK, a ciphertext C1, and a plaintext M2, and outputs a ciphertext C3.

The correctness property of EvalAddConst is that if C1 is an encryption of plaintext element M1, then C3 should be an encryption of M1+M2.

- EvalMult(Params, EK, C1, C2) → C3.

EvalMult is a randomized algorithm that takes as input the system parameters Params, the evaluation key EK, two ciphertexts C1 and C2, and outputs a ciphertext C3.

The correctness property of EvalMult is that if C1 is an encryption of plaintext element M1 and C2 is an encryption of plaintext element M2, then C3 should be an encryption of M1*M2.

- EvalMultConst(Params, EK, C1, M2) → C3.

EvalMultConst is a randomized algorithm that takes as input the system parameters Params, the evaluation key EK, a ciphertexts C1, and a plaintext M2, and outputs a ciphertext C3.

The correctness property of EvalMultConst is that if C1 is an encryption of plaintext element M1, then C3 should be an encryption of M1*M2.

- Refresh(Params, flag, EK, C1) → C2.

Refresh is a randomized algorithm that takes as input the system parameters Params, a multi-valued flag (which can be either one of “Relinearize”, “ModSwitch” or “Bootstrap”), the evaluation key EK, and a ciphertext C1, and outputs a ciphertext C2.

The correctness property of Refresh is that if C1 is an encryption of plaintext element M1, then C2 should be an encryption of M1 as well.

The desired property of the Refresh algorithm is that it turns a “complex” ciphertext of a message into a “simple” one of the same message. Two embodiments of the Refresh algorithm are (a) the bootstrapping procedure, which takes a ciphertext with large noise and outputs a ciphertext of the same message with a fixed amount of noise; and (b) the key-switching procedure, which takes a ciphertext under one key and outputs a ciphertext of the same message under a different key.

- ValidityCheck(Params, EK, [C], COMP) → flag.

ValidityCheck is a deterministic algorithm that takes as input the system parameters Params, the evaluation key EK, an array of ciphertexts [C], and a specification of the homomorphic computation encoded as a straight-line program COMP, and outputs a Boolean flag.

The correctness property of ValidityCheck is that if ValidityCheck outputs flag = 1, then doing the homomorphic computation COMP on the vector of ciphertexts [C] produces a ciphertext that decrypts to the correct answer.

Section 2. PROPERTIES

1. Semantic Security or IND-CPA Security:

At a high level, a homomorphic encryption scheme is said to be secure if no adversary has an advantage in guessing (better than ½ chance) whether a given ciphertext is an encryption of two different messages. This requires encryption to be randomized so that two different encryptions of the same message do not look the same.

Suppose a user runs the parameter and the key-generation algorithms to provide the key tuple. An adversary is assumed to have the parameters, the evaluation key EK, a public key PK (only in the public-key scheme), and can obtain encryptions of messages of its choice. The adversary is then given an encryption of one of two messages (computed by the above encryption algorithm) of its choice without knowing which message the encryption corresponds to. The security of HE then guarantees that the adversary cannot guess which message the encryption corresponds to with significant advantage better than a ½ chance. This captures the fact that no information about the messages is revealed in the ciphertext.

2. Compactness

The compactness property of a homomorphic encryption scheme guarantees that homomorphic operations on the ciphertexts do not expand the length of the ciphertexts. That is, any evaluator can perform an arbitrary supported list of evaluation function calls and obtain a ciphertext in the ciphertext space (that does not depend on the complexity of the evaluated functions).

3. Efficient decryption

Efficient decryption property says that the homomorphic encryption scheme always guarantees that the decryption runtime does not depend on the functions which was evaluated on the ciphertexts.

Section 3. HOMOMORPHIC ENCRYPTION SCHEMES

In this section, we describe the two primary schemes that we recommend for implementation of homomorphic encryption, [BGV12] and [B12]/[FV12]. In addition, we refer to 3 alternative schemes [YASHE], [NTRU]/[LTV], [GSW]. These alternative schemes have features which BGV and B/FV do not have, however they also have disadvantages with respect to performance and security.

a. Brakerski-Gentry-Vaikuntanathan (BGV)

We focus here on describing the basic version of the BGV encryption scheme. Optimizations to the basic scheme will be discussed at the end of this section.

- BGV.ParamGen(λ, P, K, B) → Params.

Recall that λ is the security level parameter, $P > 1$ is an integer plaintext modulus and $K \geq 1$ is an integer vector length.

In the basic BGV scheme, the auxiliary input B is simply an integer that determines the maximum multiplicative depth of the homomorphic computation which is simply the maximum number of sequential multiplications required to perform the computation. For example, the function $f(x_1, x_2, x_3, x_4) = x_1x_2 + x_3x_4$ has multiplicative depth 1.

In the basic BGV scheme, the parameters *param* consists of the degree parameter n, the ciphertext modulus parameter q, and the error distribution χ which is a discrete Gaussian distribution with standard deviation parameter α set according to the security guidelines specified in Section 5.

- BGV.SecKeygen(params) → SK, EK

In the basic BGV scheme, the secret key SK is an element s chosen from the error distribution χ.

In the basic BGV scheme, there is no evaluation key EK.

- BGV.PubKeygen(params) → SK, PK, EK.

In the basic BGV scheme, PubKeygen first runs SecKeygen and obtains (SK, EK) where SK is an element s that belongs to the ring R.

PubKeygen chooses a uniformly random element a from the ring R/qR and outputs the public key PK which is a pair of ring elements $(a, b) = (a, a * s + p * e)$ where e is chosen from the error distribution χ.

- BGV.SecEncrypt(SK, M) → C

In the basic BGV scheme, SecEncrypt first maps the message M which comes from the plaintext space Z_p^k into an element of the ring R/pR.

SecEncrypt then samples a uniformly random element *a* from the ring R/qR and outputs the pair of ring elements $(c_0, c_1) = (a, a * s + p * e + M)$ where e is chosen from the error distribution χ.

- BGV.PubEncrypt(PK, M) → C

In the basic BGV scheme, Pub.Encrypt first maps the message M which comes from the plaintext space Z_p^k into an element of the ring R/pR. Recall that the public key PK is a pair of elements (a, b).

PubEncrypt then samples three uniformly random elements r, f and f' from the error distribution χ and outputs the pair of ring elements $(c_0, c_1) = (a * r + f, b * r + p * f' + M)$.

- BGV.Decrypt(SK, C) → M

In the basic BGV scheme, Decrypt takes as input the secret key which is an element s of the ring R, and a ciphertext C $= (c_0, c_1)$ which is a pair of elements from the ring R/qR.

We remark that a ciphertext C produced as the output of the encryption algorithm has two elements in R/qR, but upon homomorphic evaluation, ciphertexts can grow to have more ring elements. The decryption algorithm has to be modified appropriately to handle such ciphertexts.

Decrypt first computes the ring element $c_0 * s + c_1$ over R/qR and interprets it as an element c' in the ring R. It then computes c' (mod p), an element of R/pR, which it outputs.

- BGV.EvalAdd(Params, EK, C1, C2) → C3.

In the basic BGV scheme, EvalAdd takes as input ciphertexts C1 = $(c_{1,0}, c_{1,1})$ and C2 = $(c_{2,0}, c_{2,1})$ and outputs C3 = $(c_{1,0} + c_{2,0}, c_{1,1} + c_{2,1})$.

- BGV.EvalMult(Params, EK, C1, C2) → C3.

In the basic BGV scheme, EvalMult takes as input ciphertexts C1 = $(c_{1,0}, c_{1,1})$ and C2 = $(c_{2,0}, c_{2,1})$ and outputs C3 = $(c_{1,0} * c_{2,0}, c_{1,0} * c_{2,1} + c_{1,1} * c_{2,0}, c_{1,1} * c_{2,1})$.

The Full BGV Scheme

In the basic BGV scheme, ciphertexts grow as a result of EvalMult. For example, given two ciphertexts each composed of two ring elements, EvalMult as described above results in three ring elements. This can be further repeated, but has the disadvantage that upon evaluating a degree-d polynomial on the plaintexts, the resulting ciphertext has $d + 1$ ring elements.

This deficiency is mitigated in the full BGV scheme, with two additional procedures. The first is called “Key Switching” or “Relinearization” which is implemented by calling the Refresh subroutine with flag = “KeySwitch”, and the second is “Modulus Switching” or “Modulus

Reduction" which is implemented by calling the Refresh subroutine with flag = "ModSwitch". Support for key switching and modulus switching also necessitates augmenting the key generation algorithm.

For details on the implementation of the full BGV scheme, we refer the reader to [BGV12].

Properties Supported. The BGV scheme supports many features described in Section 6, including packed evaluations of circuits and can be extended into a threshold homomorphic encryption scheme. In terms of security, the BGV homomorphic evaluation algorithms can be augmented to provide evaluation privacy. Note that evaluation privacy is defined below with respect to semi-honest adversaries.

b. Brakerski/Fan-Vercauteren (BFV)

We assume the parameters are instantiated following the recommendations outlined in Section 5. The parameters include:

- Two distributions D_1, D_2
- a ring R and its corresponding integer modulo q
- Integer T, and $L = \log_T q$. T is the bit-decomposition modulus.
- Plaintext modulus P, and plaintext ring R/PR
- Integer $W = \lfloor q/P \rfloor$

- BFV.SecKeygen(Params)

The secret key SK of the encryption scheme is a random element S from the distribution D_2 defined as per Section 5. The evaluation key consists of L LWE samples encoding the secret S in a specific fashion.
In particular, for $i = 0, \dots, L$, sample a random A_i from R and error E_i from D_1, compute

$$EK_i = \left(-(A_i S + E_i) + T^i S^2, A_i\right),$$

and set $EK = (EK_0, \dots, EK_L)$.

- BFV.PubKeygen(params):

The secret key SK of the encryption scheme is a random element S from the distribution D2 defined as per Section XYZ. The public key is a random LWE sample with the secret S. In particular, it is computed by sampling a random element A from R and an error E from the distribution D_1 and setting:
$PK = (-(AS + E), A)$, where all operations are performed over the ring R.

The evaluation key is computed as in BFV.SecKeygen.

- BFV.PubEncrypt(PK, M):

BFV.Pub.Encrypt first maps the message M which comes from the message space into an element in the ring R/PR .

To encrypt a message M from R/PR, parse the public key as a pair PK_0, PK_1. Encryption consists of two LWE samples using a secret U where PK_0, PK_1 is treated as public randomness. The first LWE sample encodes the message M, whereas the second sample is auxiliary.

In particular, C = $(PK_0 * U + E_1 + W * M, PK_1 * U + E_2)$ where U is a sampled from D_2, and E_1, E_2 are sampled from D_1.

- BFV.SecEncrypt(PK, M):

- BFV.Decrypt(SK, C):

The main invariant of the BFV scheme is that when we interpret the elements of a ciphertext C as the coefficients of a polynomial then, C(S) = $W * M + E$ for some "small" error E. From it, M can be recovered easily by dividing by W and rounding the result.

- BFV.EvalAdd(EK, C1, C2):

Parse the ciphertexts as $C_i = (C_{i,0}, C_{i,1})$. Then, addition simply corresponds to component-wise addition of two ciphertext components.
That is, $C^+ = (C_{1,0} + C_{2,0}, C_{1,1} + C_{2,1})$.
It is easy to verify that $C^+(S) = W * (M_1 + M_2) + E$, where M1, M2 are messages encrypted in C1, C2 and E is the new error component.

- BFV.EvalMult(EK, C1, C2):

To multiple two ciphertexts, we interpret each ciphertext as a list of polynomial coefficients over a variable. EvalMult is just a polynomial multiplication (followed by a rounding step to the nearest integer).
Concretely, $C^* = round((P/q)C_1 * C_2) \ mod \ q$. Recalls that $W = \lfloor q/P \rfloor$).
It is somewhat easy to verify that $C^*(S) = W * (M_1 * M_2) + E$, for some new error E.

One may note that the ciphertext size increases in this operation. One may apply a Refresh algorithm to obtain a new compact ciphertext of the original size encoding the same message $M_1 * M_2$.

Properties Supported. The complete BFV scheme supports many features described in Section 6, including packed evaluations of circuits and can be extended into a threshold homomorphic encryption scheme. In terms of security, the BFV homomorphic evaluation algorithms can be augmented to provide evaluation privacy.

For details on the implementation of the full BFV scheme, we refer the reader to [B12], [FV12].

c. Comparison between BGV and BFV

When implementing HE schemes, there are many choices which can be made to optimize performance for different architectures and different application scenarios. This makes a direct comparison of these schemes quite challenging. A paper by Costache and Smart [CS16] gives some initial comparisons between BGV, B/FV and two of the schemes described below: YASHE and LTV/NTRU. A paper by Kim and Lauter [KL15] compares the performance of the BGV and YASHE schemes in the context of applications. Since there is further ongoing work in this area, we leave this comparison as an open research question.

d. Other Schemes

Yet Another Somewhat Homomorphic Encryption ([YASHE]) is similar to the BGV and BFV schemes and offers the same set of features.

The scheme NTRU/Lopez-Alt-Tromer-Vaikuntanathan ([NTRU]/[LTV]) relies on the NTRU assumption (also called the “small polynomial ratios assumption”). It offers all the features of BGV and BFV, and in addition, also offers an extension that supports multi-key homomorphism.

The scheme proposed by Gentry-Sahai-Waters [GSW13] offers a different set of trade-offs between advantages and disadvantages.

Section 4. SECURITY ASSUMPTIONS

This section describes the problems which are assumed to be hard as the basis for the security of the homomorphic encryption schemes. Known security reductions to other problems are not included here. Section 5 describes the best currently known attacks on these problems and their concrete running times.

a. The Learning with Errors (LWE) Assumption

The LWE assumption is defined by a triple of parameters (n, m, q, χ) where n is a positive integer referred to as the “dimension parameter”, q is a positive integer referred to as the “modulus parameter” and χ is a probability distribution over rational integers referred to as the “error distribution”.

The LWE assumption requires that the following two probability distributions are computationally indistinguishable:

Distribution 1. Choose a uniformly random matrix $n \times m$ matrix A, a uniformly random (row) vector s from the vector space Z_q^n, and a (row) vector e from Z^m where each coordinate is chosen from the error distribution χ. Compute $b := sA + e$. By definition, all computations here are carried out modulo q. Output (A, b).

Distribution 2. Choose a uniformly random $n \times m$ matrix A, and a uniformly random (row) vector b from Z_q^m. Output (A, b).

The error distribution χ can be either a discrete Gaussian distribution over the integers, or another distribution supported on small integers. We refer the reader to Section 5.3 for more details on particular error distributions, algorithms for sampling from these distributions, and the associated security implications.

b. The Ring Learning with Errors (RLWE) Assumption

The RLWE assumption is a specific case of LWE where the matrix A is chosen to have special algebraic structure.

The RLWE assumption is defined by a triple of parameters (n, m, q, χ) where n is a positive integer which is a power of two, referred to as the "degree parameter", q is a positive integer referred to as the "modulus parameter" and χ is a probability distribution over the ring $R := Z[X]/(X^n + 1)$, referred to as the "error distribution".

The RLWE assumption requires that the following two probability distributions are computationally indistinguishable:

Distribution 1. Choose a uniformly random element a from the ring R/qR, a uniformly random element s from the ring R/qR, and an element e from the ring R chosen from the error distribution χ. Compute $b := sa + e$. By definition, all computations here are carried out over the ring R/qR. Output (a, b).

Distribution 2. Choose a uniformly random element a from the ring R/qR, and a uniformly random element b from the ring R/qR. Output (a, b).

The error distribution χ can be either a discrete Gaussian distribution over the ring R, or another distribution supported on "small" ring elements. We refer the reader to Section 5.3 for more details on particular error distributions, algorithms for sampling from these distributions, and the associated security implications.

Section 5. Attacks and Secure Parameter Selection

Assessing the best attacks and explaining the running times of the attacks

We review attacks on the LWE problem and use them to suggest concrete parameter choices. The schemes described above all have versions based on the LWE and the RLWE assumptions. When the schemes based on RLWE are instantiated with rings which are 2-power cyclotomic rings, we do not currently know better attacks on RLWE than on LWE. The following estimates and attacks refer to attacks on the LWE problem with the specified parameters. In a later section, we will discuss security issues related to varying the choice of ring to non-2-power cyclotomic fields.

Much of this section is based on the paper by Albrecht, Player, and Scott [APS15] and the online *Estimator* tool which accompanies that paper. Estimated security levels in all the tables in this section were obtained by running the *Estimator* based on its state in July 2017. The tables in this section give the best attacks (in terms of running time in bits) among all known attacks as implemented by the *Estimator* tool. As attacks or implementations of attacks change, or as new attacks are found, these tables will need to be updated. A sound strategy for standardization might be be to take currently predicted security levels and augment the requirements to allow for future improvements to attacks based on a historical analysis of how fast attacks have improved over time. First, we describe all the attacks which give the best running times when working on parameter sizes in the range which are interesting for Homomorphic Encryption.

5.1 Descriptions of attack algorithms

a. The uSVP attack

The unique shortest vector attack takes as input a sequence of m LWE samples of the form $(a_i, \langle a_i, s\rangle + e_i)$. Here, a_i are n-dimensional vectors chosen randomly and uniformly from Z_q^n, s is a fixed secret n-dimensional vector, the e_i are chosen from a discrete Gaussian distribution with mean 0, and standard deviation $\sigma = \alpha q / \sqrt{2\pi}$, and $\langle a, s\rangle$ represents the inner product of a and s. Note that α is a public parameter. The coefficients of the secret s are often drawn from a uniform distribution, or from the same discrete Gaussian distribution as the errors e_i. The lattice reduction attack sketched here applies to all of these instances, but the corresponding lattice is altered accordingly. The unique shortest vector attack translates the sequence of m samples into an appropriate $m + n + 1$ by $m + n + 1$ matrix. The rows of this matrix generate a lattice, and will contain information revealing the m secret errors $e_1, e_2, \ldots, e_m$. Thus if the shortest vector can be recovered, the secret s can usually be recovered as long as m is sufficiently larger than n.

Given enough time, BKZ 2.0 lattice reduction will solve the problem of locating this shortest vector, and hence solve the LWE problem, if the ratio of the length of the expected shortest vector of the lattice by the length of the actual shortest vector (the target) is greater than a

certain quantity. Let $e = 2.7108\ldots$; in [AFG14, APS15] it is shown that for practical choices of parameters given in this document, for any $\epsilon' > 1$, this quantity is greater than $q^{-\frac{n}{m}}/(\epsilon'\alpha\sqrt{2e})$ with probability greater than

$$\rho(m, \epsilon') = 1 - \left(\epsilon' e^{\frac{1-\epsilon'^2}{2}}\right)^m.$$

They also show that if the root-Hermite factor δ_0 satisfies

$$\log(\delta_0) = \log^2 \frac{\epsilon'\tau\alpha\sqrt{2e}}{4n \log q},$$

then the optimal choice of m is $m = \sqrt{n \log(q)/\log(\delta_0)}$. They also remark that τ can be taken to equal 0.4. Assuming the Gaussian heuristic for their lattice, they ultimately establish that for an LWE problem with parameters n, q, α, the problem has a probability of at least $\frac{\rho(m,\epsilon')}{10}$ of being ultimately solvable by BKZ 2.0, with the optimal choice of m given above. The length of time required to solve the problem is determined by n and δ_0. It is an open research problem to more precisely predict the exact relationship between time required to solve the problem and n, δ_0 as n increases (see Section 5.2 below for further discussion).

b. The Decoding attack on LWE

This attack solves the search-LWE problem by viewing it as the equivalent *Bounded Distance Decoding* (BDD) problem on q-ary lattices. The attack is due to Lindner and Peikert [LP11] with improvements and variations suggested by Albrecht et al. [APS15].

The algorithm works on the lattice given by integer vectors z such that $z = A^T s \bmod q$, where $s \in Z_q^n$ is the secret vector, A is an $m \times n$ matrix, and m denotes the number of samples used in the attack. It starts with a sufficiently reduced basis, e.g., using BKZ 2.0, and then applies a modified version of the recursive *Nearest Plane* algorithm due to Babai [Bab86]. Given a basis **B** and a target vector t, the Nearest Plane algorithm finds a vector v such that the error vector $e = t - v$ falls in the fundamental parallelepiped of the Gram-Schmidt orthogonalization (GSO) of **B**.

Lindner and Peikert note that for a BKZ-reduced basis **B**, the fundamental parallelepiped is long and thin, by the Geometric Series Assumption (GSA) due to Schnorr that the GSO of a BKZ-reduced basis decay geometrically and this makes the probability that the Gaussian error vector e falls in the corresponding fundamental parallelepiped very low. To improve this success probability, they "fatten" the parallelepiped by essentially scaling its principal axes. They do this by running the Nearest Plane algorithm on several distinct planes at each level of recursion. For a Gaussian error vector e, the probability that it falls in this fattened parallelepiped is expressed in terms of the scaling factors and the lengths of the GSO of **B**.

The run time of the Nearest Planes algorithm mainly depends on the number of points enumerated, which is the product of the scaling factors. The run time of the basis reduction step depends on the quality of the reduced basis, expressed, for instance, by the root Hermite factor δ_0. The scaling factors and the quality of the basis together determine the success probability of the attack. Hence to maximize the success probability, the scaling factors are determined based on the (predicted) quality of the BKZ-reduced basis. There is no closed formula for the scaling factors and there seems to be no algorithmic approach to determine them. In practice, these are determined by experimentation and can be chosen to be powers of two. The scaling factors and the quality of the basis are chosen to achieve a target success probability and to minimize the running time (by balancing its first and second components mentioned above)

c. The dual attack

The dual attack solves the decisional problem, so it does not recover the secret. This works well for "small" or "short" secrets.

This attack is to distinguish the case of m LWE samples (A, c) from m uniformly random samples. In an LWE sample, we have $c = As + e$, where e is the error vector.

The attack will first find a short row vector v such that $vA = 0$. We present it as a lattice problem: find a vector v in the scaled (by q) dual lattice of the lattice generated by A,

$$L = \{w \in Z_q^m \mid wA \equiv 0 \, mod \, q\}.$$

This is known as solving the Short Integer Solutions problem (SIS).

Now consider $\langle v, c\rangle$; if $c = As + e$, then we have that $\langle v, c\rangle = \langle v, Ac + e\rangle = \langle v, e\rangle$, where e follows a Gaussian distribution over Z/qZ. This means the result should give small samples, as both v and e are small. On the other hand, if c is uniformly random then $\langle v, c\rangle$ is uniformly random on Z/qZ. By looking at $\langle v, c\rangle$, we may distinguish these two cases, thus solving the Decision-LWE problem.

We must however ensure that indeed v is short enough, since if v is too large, the (Gaussian) distribution of $\langle v, e\rangle$ will be too flat to distinguish from random. There is a claim in [LP11] that for an LWE instance with parameters n, α, q and a vector v of length $|v|$ in the scaled dual lattice $L = \{w \in Z_q^m \mid wA \equiv 0 \, mod \, q\}$, the advantage of distinguishing $\langle v, e\rangle$ from random is close to $exp\,(-\pi(|v| \cdot \alpha)^2)$. To obtain a probability ϵ of success in solving an LWE instance parametrized by n, q and α via the SIS strategy, we require a vector v of norm

$$|v| = \sqrt{\frac{ln\left(\frac{1}{\epsilon}\right)}{\pi}} \,/\, \alpha.$$

Concretely, the attack applies a conventional lattice reduction algorithm, in particular, BKZ 2.0, to return the shortest non-zero vector it can find, which is then used to distinguish the samples. There are heuristic estimates to obtain the computational complexity to find the desired vector

for the distinguishing attack.

5.2 Lattice Reduction algorithm: BKZ

BKZ is an iterative, block-wise algorithm for basis reduction. It requires solving the SVP problem (using sieving or enumeration, say) in a smaller dimension β, the block size. First, the input lattice L is LLL reduced, giving a basis $\{b_0, \dots, b_{n-1}\}$. For $0 \leq i \leq n-1$, the vectors $b_i, \dots, b_{\min(i+\beta-1,n)}$ are projected onto the orthogonal complement of the span of $b_0, \dots, b_{\{i-1\}}$; this projection is called a local block. In the local block, we find a shortest vector, view it as a vector b of L, and perform LLL on the list of (now linearly dependent) vectors $\{b_i, \dots, b_{\min(i+\beta-1,n)}, b\}$. We use the resulting vectors to update $\{b_i, \dots, b_{\min(i+\beta-1,n)}\}$. This process is repeated until a basis is not updated after a full pass.

There have been improvements to BKZ, which are collectively referred to BKZ 2.0 (see [CN11] for example). The authors of [AFG14, APS15] take these improvements into account in their analysis of the quality and runtime of BKZ and in their estimator.

Given a lattice basis $\{b_0, \dots, b_{n-1}\}$ of a lattice L, we can measure how reduced the basis is with the root-Hermite factor δ_0, defined as follows: assume that b_0 is the shortest vector of the basis and define the volume of L, $vol(L)$, to be $\sqrt{\det(B^T B)}$ where B is a matrix consisting of the vectors of any basis of L. Then define δ_0 so that $\delta_0^n = |b_0|/vol(L)^{1/n}$. While many attacks on LWE base their runtime and advantage on achieving a certain δ_0, it is difficult to capture the runtime required to achieve such a δ_0 in terms of the blocksize β, or the number of rounds of BKZ. The runtime largely depends also on what method is used to solve the SVP in the local blocks. For a detailed discussion of the state of the art, see [APS15], where estimates for the number of clock cycles t_β required to solve SVP in dimension β using the various methods can be found. In our tables, we always chose the sieving method, which is faster but requires exponential memory. In particular, from [APS15] we have $\log(t_\beta) = .3366\beta + 12.31$, and if we take the estimate in [APS15] for the number of rounds of BKZ required to be $\frac{n^2 \log(n)}{\beta^2}$, this results in a total runtime for BKZ in dimension n with blocksize β to be $\frac{n^3 \log(n)}{\beta^2} t_\beta$ clock cycles; for a detailed explanation of these estimates, see [APS15], Section 3.2.

We note that the estimator allows specification of multiple cost models for solving SVP:

- “lp” The Lindner-Peikert model, taken from [LP11], which does not take into account the improvements in BKZ 2.0.
- “sieve” Assumes sieving is used as the SVP oracle. We chose this for our tables as it provides the lowest security estimates for given n, α, q. It may be impractical due to the memory requirements, however, for sieving.
- “enum” Based on the model in [CN11] which takes into account improvements in solving the SVP with enumeration.
- “qsieve” Model based on estimates for a quantum algorithm for sieving from [LMvP13]. Our tables for quantum security estimates use this model.

5.3. Parameter recommendations

Specifying an LWE or a Ring-LWE scheme for encryption requires specifying a ring, R, of a given dimension, n, along with a ciphertext modulus q, and a choice for the error distribution and a choice for a secret distribution.

Ring. In practice, we take the ring R to be a 2-power cyclotomic ring $R = Z[x]/(x^n + 1)$, where n is a power of 2.

Error distribution. The error is usually chosen from a Discrete Gaussian distribution with width $\sigma = 8/\sqrt{2\pi}$. Selecting the error according to a Discrete Gaussian distribution is motivated by theoretical security reductions proved in [LPR13]. However, those theoretical guarantees do not apply to fixed small error widths such as $\sigma = 8/\sqrt{2\pi}$, and would instead require that the error width grow with the square root of the dimension of the lattice, $\sqrt{n}$. None of the known attacks appear to take advantage of the shape of the error distribution, only the width; however, the analysis of the security levels given below relies on running time estimates which assume that the shape of the error distribution is Discrete Gaussian. For that reason we continue to assume that the error is chosen from a Discrete Gaussian distribution of fixed small width. The width is chosen to be small for practical performance reasons, and is justified by the concrete running times of known attacks with those error widths. However, over time if attacks improve or new attacks are found, the width of the error may need to be increased in practice.

Secret key. For efficiency reasons, in practice we often choose the secret from a non-uniform distribution, such as the *ternary distribution,* which means to select uniformly from $\{-1,0,1\}$. In the recommended parameters given below, we will present tables for three choices of secret-distribution: {uniform, error, and ternary}. We will not present tables for sparse secrets because we do not suggest standardizing the case of sparse secret due to significantly better known attacks which are not stable enough to assess since they continue to be improved.

Number of samples. For most of the attacks listed in the tables below, it is assumed that a certain number of samples are used in the attack. From an RLWE ciphertext, we can obtain $n \log_T q$ LWE samples, where T is the bit-decomposition modulus.

Sampling Methods. We restrict to the case where $R = Z[x]/(x^n + 1)$, where n is a power of 2. In this case, the Discrete Gaussian distribution on R can be generated as

$$e = \sum_{i=0}^{n-1} e_i x^i \ ,$$

where each e_i follows a discrete Gaussian distribution over the integers. Therefore, it suffices to sample from a discrete Gaussian distribution over the integers of width $s > 0$, which we denote by $D_{Z,s}$.

There are several known methods to sample from $D_{Z,s}$, including rejection sampling, inversion sampling, Discrete Zuggurat, Bernoulli-type, Knuth-Yao and Von Neumann-type. For efficiency, we recommend the Von Neumann-type sampling method introduced by Karney in [Kar16].

Constant-time sampling. In the aforementioned sampling methods, the time it takes to generate one sample could leak information about the actual sample. Therefore, it is important that the entire error-sampling process is constant-time. To achieve this, one possible method is to fix some upper bound $T > 0$ such that sampling all the n coordinates e_i sequentially without interruption takes time less than T time with overwhelming probability. Then after these samples are generated, using time t, we wait for $(T - t)$ time units, so that the entire error-generating time always takes time T. In this way, the total time does not reveal information about the generated error polynomial.

Ring-LWE security for other rings. As noted above, in practice in the application of homomorphic encryption we use error distributions of small width. When using error distributions with small width and considering other rings besides the *2*-power cyclotomic rings, there are better known attacks on the RLWE problem. These attacks and examples of weak rings were first given in [ELOS15] and [CLS15], and were subsequently improved in [CLV16a], [CLV16b], and [CLS16]. Because rings can be weak with respect to these attacks in many different ways depending on their geometry, and we don't have uniform ways to check for such weakness yet, we do not recommend using non-cyclotomic rings for cryptography. For general cyclotomic rings (which are not 2-power cyclotomics), there is more research to be done: for prime cyclotomics an efficient concrete attack on search RLWE was given in [CLS15] when *q* is the ramified prime, and an efficient attack on the decision RLWE problem was given for other choices of *q*. There are also strong incentives to use *2*-power cyclotomic rings for performance reasons, so unless there are better attacks it makes sense to standardize those anyway.

5.4 TABLES of RECOMMENDED PARAMETERS

In practice, in order to implement homomorphic encryption for a particular application or task, the application will have to select a dimension n, and a ciphertext modulus q, (along with a plaintext modulus and a choice of encoding which are not discussed here). For that reason, we give pairs of (n, q) which achieve different security levels for each n. In other words, given n, the table below recommends a value of q which will achieve a given level of security (e.g. 128 bits) for the given error width $\sigma \approx 3.2$.

We have the following tables for 3 different security levels, 128-bit, 192-bit, and 256-bit security, where the secret follows the uniform, error, and ternary distributions. For applications, we give values of n from $n = 2^k$ where $k = 11, \ldots, 15$. We note that we used commit f59326c of the lwe-estimator of [APS15], which the authors continue to develop and improve. The tables give estimated running times (in bits) for the three attacks described in Section 5.1: uSVP, dec (decoding attack), and dual.

distribution	n	security level	log(q)	uSVP	dec	dual
uniform	1024	128	31	130.6	133.8	147.5
		192	22	203.6	211.2	231.8
		256	18	269.9	280.5	303.6
	2048	128	59	129.5	129.7	139.2
		192	42	194.0	197.6	212.4
		256	33	263.8	270.7	289.9
	4096	128	113	131.9	129.4	136.8
		192	80	192.7	193.2	203.2
		256	63	260.7	263.6	277.6
	8192	128	222	132.9	128.9	134.9
		192	157	195.4	192.8	200.6
		256	124	257.0	256.8	266.7
	16384	128	440	133.9	129.0	133.0
		192	310	196.4	192.4	198.7
		256	243	259.5	256.6	264.1
	32768	128	880	134.3	129.1	131.6
		192	612	198.8	193.9	198.2
		256	480	261.6	257.6	263.6

distribution	n	security level	log(q)	uSVP	dec	dual
(-1,1)	1024	128	29	139.6	145.9	128.9
		192	20	226.9	241.2	196.8
		256	15	344.3	366.1	273.9
	2048	128	56	136.2	137.9	128.3
		192	39	210.3	217.5	194.6
		256	30	294.5	307.5	268.8
	4096	128	110	135.1	133.5	128.5
		192	77	203.1	205.5	192.4
		256	60	274.7	280.4	259.0
	8192	128	219	134.6	130.9	128.6
		192	153	200.3	199.0	193.1
		256	119	268.7	270.0	257.9
	16384	128	441	133.3	128.7	128.1
		192	306	199.0	195.3	192.4

		256	239	263.8	261.6	257.2
	32768	128	885	133.4	128.2	128.0
		192	615	197.4	192.8	192.2
		256	479	261.9	258.2	257.0

distribution	n	security level	log(q)	uSVP	dec	dual
error	1024	128	31	130.6	133.8	129.6
		192	22	203.6	211.2	200.8
		256	19	269.9	280.5	259.5
	2048	128	58	132.1	132.4	130.2
		192	42	194.0	197.6	190.6
		256	33	263.8	270.7	258.1
	4096	128	113	131.9	129.4	128.8
		192	80	195.6	196.1	192.2
		256	62	266.0	268.9	259.3
	8192	128	223	132.3	128.3	128.0
		192	157	195.4	192.8	192.3
		256	123	259.6	259.4	256.2
	16384	128	443	133.0	128.1	129.3
		192	310	196.4	192.4	193.9
		256	243	259.5	256.6	259.3
	32768	128	886	133.4	128.2	129.4
		192	616	197.4	192.5	192.2
		256	481	261.0	257.0	256.2

Post-quantum security. The BKZ.qsieve model assumes access to a quantum computer and gives lower estimates than BKZ.sieve. In what follows, we give tables of recommended ("Post-quantum") parameters which achieve the desired levels of security against a quantum computer.

distribution	n	security level	log(q)	uSVP	dec	dual
uniform	1024	128	29	131.9	136.4	149.9
		192	21	200.3	209.9	200.3
		256	17	269.8	284.1	303.8
	2048	128	56	128.1	128.9	138.1
		192	39	196.7	201.7	216.1
		256	31	263.5	272.2	290.1

4096	128	107	130.6	128.4	135.6
	192	76	192.1	192.2	203.2
	256	59	260.2	264.17	277.7
8192	128	209	132.4	128.3	134.4
	192	147	194.7	192.9	200.4
	256	116	256.2	256.6	266.2
16384	128	415	132.9	128.5	132.2
	192	290	195.7	192.1	198.5
	256	226	259.8	257.3	265.0
32768	128	831	133.1	128.1	130.5
	192	575	196.9	192.3	196.2
	256	449	260.3	261.1	262.3

distribution	n	security level	log(q)	uSVP	dec	dual
(-1,1)	1024	128	27	141.6	149.3	130.6
		192	19	224.6	241.6	193.9
		256	14	350.8	378.7	274.4
	2048	128	52	138.1	140.8	130.2
		192	36	214.4	223.4	197.8
		256	28	296.1	312.1	267.0
	4096	128	103	135.4	134.2	128.6
		192	72	203.2	206.2	192.2
		256	56	274.8	281.9	259.0
	8192	128	202	134.0	130.7	128.0
		192	143	200.3	199.3	192.9
		256	111	268.6	270.8	257.6
	16384	128	413	133.4	129.0	128.2
		192	286	198.6	195.3	192.1
		256	223	263.8	261.5	256.5
	32768	128	829	133.3	128.4	128.2
		192	574	197.5	193.1	192.0
		256	449	260.0	256.1	256.4

distribution	n	security level	log(q)	uSVP	dec	Dual
error	1024	128	29	131.9	136.4	131.5
		192	21	200.3	209.9	197.5
		256	17	269.8	284.1	259.0
	2048	128	55	130.7	131.5	129.0
		192	39	196.7	201.7	193.1
		256	31	263.5	272.2	257.3
	4096	128	106	132.0	129.7	128.9
		192	74	198.2	199.6	195.2
		256	58	266.6	269.7	258.8
	8192	128	208	132.4	128.3	128.0
		192	146	196.3	194.3	193.5
		256	114	261.5	262.0	258.2
	16384	128	415	132.9	128.5	129.3
		192	289	195.7	192.1	193.7
		256	226	259.8	257.3	260.2
	32768	128	831	133.1	128.1	129.5
		192	575	197.2	192.8	192.0
		256	449	260.3	256.1	257.5

Section 6. Additional Features & Discussion

Distributed HE

Homomorphic Encryption is especially suitable to use for multiple users who may want to run computations on an aggregate of their sensitive data. For the setting of multiple users, an additional property which we call threshold-HE is desirable. In threshold-HE the key-generation algorithms, encryption and decryption algorithms are replaced by a distributed-key-generation (DKG) algorithm, distributed-encryption (DE) and distributed-decryption (DD) algorithms. Both the distributed-key-generation algorithm and the distributed-decryption algorithm are executed via an interactive process among the participating users. The evaluation algorithms EvalAdd, EvalMult, EvalMultConst, EvalAddConst and Refresh remain unchanged.

We will now describe the functionality of the new algorithms.

We begin with the distributed-key-generation (DKG) algorithm to be implemented by an interactive protocol among t parties $p_1, \ldots, p_t$. The DKG algorithm is a randomized algorithm.
The inputs to DKG are: security parameter, number of parties t, and threshold parameter d.
The output of DKG is a vector of secret keys $s = (s_1, \ldots, s_t)$ of dimension t and a public evaluation key Ek where party p_i receives (Ek,s_i).
We remark that party p_i doesn't receive s_j for $i \neq j$ and party i should maintain the secrecy of its secret key s_i.

Next, the distributed-encryption (DE) algorithm is described.
The DE algorithm is a randomized algorithm which can be run by any party p_i
The inputs to DE run by party p_i are: the secret key s_i and the plaintext M
The output of DE is a ciphertext C.

Finally, we describe the distributed-decryption (DD) algorithm to be implemented by an interactive protocol among a subset of the t parties $p_1, \ldots, p_t$.
The DD algorithm is a randomized algorithm.
The inputs to DD are: a subset of secret keys $s = (s_1, \ldots, s_t)$, the threshold parameter d, and a ciphertext C. In particular, every participating party p_i provides the inputs_i. The ciphertext C can be provided by any party.
The output of DD is: plaintext M.

The correctness requirement that the above algorithms should satisfy is as follows.
If at least d of the parties correctly follow the prescribed interactive protocol that implements the DD decryption algorithm, then the output of the decryption algorithm will be correct.
The security requirement is for semantic security to hold as long as fewer than d parties collude adversarially.

An example usage application for (DKG,DE,DD) is for two hospitals, $t = 2$ and $d = 2$ with sensitive data sets M_1 and M_2(respectively) who want to compute some analytics F on the joint data set without revealing anything about M_1 and M_2 except for what is revealed by $F(M_1, M_2)$.

In such a case the two hospitals execute the interactive protocol for DKG and obtain their respective secret keys s_1 and s_2 and the evaluation key EK. They each use DE on secret key s_i and data M_i to produce ciphertext Ci. The evaluation algorithms on C1, C2 and the evaluation key EK allow the computation of a ciphertext C which is an encryption of $F(M_1, M_2)$. Now, the hospitals execute the interactive protocol DD using their secret keys and ciphertext C to obtain $F(M_1, M_2)$.

Active Attacks

One can consider stricter security requirements beyond semantic security. For example, Suppose a client holds data M and wishes to compute $F(M)$ for a specified algorithm F.

The client outsources the computation of $F(M)$ to a cloud maintaining the privacy of M as follows. The client encrypts M into ciphertext C and hands C to the cloud server. The server is supposed to use the evaluation algorithms to compute a ciphertext C' which is an encryption of $F(M)$ and return this to the client for decryption.
Suppose that instead the cloud computes some other C'' which is the encryption of $G(M)$ for some other function G. This may be problematic to the client as it would introduce errors of potentially significant consequences. This is an example of an active attack which is not ruled out by semantic security.

We remark that to such attacks against homomorphic encryption schemes cannot be prevented without additional measures.

Another, possibly even more severe attack, is the situation where the adversary somehow gains temporary ability to decrypt certain C's of its choice with the goal of learning sensitive data of the client. Again, this attack is not addressed by the semantic security guarantee.

Evaluation Privacy

A desirable additional security property beyond semantic security would be that the ciphertext C hides which computations were performed homomorphically to obtain C. We call this security requirement *Evaluation Privacy.*
For example, suppose a cloud service offers a service in the form of computing a proprietary machine learning algorithm F on the client's sensitive data. As before, the client encrypts its data M to obtain C and sends the cloud C and the evaluation key EK. The cloud now computes C' which is an encryption of $F(M)$ to hand back to the client. Evaluation privacy will guarantee that C' does not reveal anything about the algorithm F which is not derivable from the pair $(M, F(M))$. Here we can also distinguish between semi-honest and malicious evaluation privacy depending on whether the ciphertext C is generated correctly according to the Encrypt algorithm.

A weaker requirement would be to require evaluation privacy only with respect to an adversary who does not know the secret decryption key. This may be relevant for an adversary who intercepts encrypted network traffic.

Key Evolution

Say that a corpus of ciphertexts encrypted under a secret key SK is held by a server, and the client who owns SK realizes that SK may have been compromised.
It is desirable for an encryption scheme to have the following *key evolution* property. Allow the client to generate a new secret key SK' which replaces SK, a new evaluation key EK', and a transformation key TK such that: the server, given only TK and EK', may convert all ciphertexts

in the corpus to new ciphertexts which (1) can be decrypted using SK' and (2) satisfy semantic security even for an adversary who holds SK.

Any sufficiently homomorphic encryption scheme satisfies the key evolution property as follows. Let TK be the encryption of SK under SK'. Namely, TK is a ciphertext which when decrypted using secret key SK' yields SK. A server given TK and EK', can convert a ciphertext C in the corpus into C' by homomorphically evaluating the decryption process. Security follows from semantic security of the original homomorphic encryption scheme.

Proxy Re-encryption

Imagine two parties each with a different secret key SK1 and Sk2 respectively.
They wish to enable a third party to convert ciphertext decryptable with SK1 to ciphertext (with the same underlying plaintext) decryptable with SK2.
The idea is to generate a so called re-encryption key TK, the knowledge of which allows this conversion to occur and to hand TK to the third party. We they say that the third party is a *proxy* which performs *proxy re-encryption*.
Note that the key evolution procedure described above can also be utilized to achieve Proxy re-encryption. In this case SK1=SK and SK2=Sk'.

The security property required is that the third party holding TK cannot decrypt ciphertexts which can be decrypted with SK1 or SK2 alone.
This security property follows from semantic security of the original homomorphic encryption scheme.

Side Channel Attacks

Side channel attacks consider adversaries who can obtain partial information about the secret key of an encryption scheme, for example by running timing attacks during the execution of the decryption algorithm. A desirable security requirement from an encryption scheme is resiliency against such attacks, often referred to as *leakage resiliency*. That is, it should be impossible to violate semantic security even in presence of side channel attacks. Naturally, leakage resilience can hold only against limited information leakage about the secret key.

An attractive feature of encryption schemes based on intractability of integer lattice problems, and in particular known HE schemes based on intractability of integer lattice problems, is that they satisfy leakage resilience to a great extent. This is in contrast to public-key cryptosystems such as RSA.

Identity Based Encryption

In an identity based encryption scheme it is possible to send encrypted messages to users without knowing either a public key or a secret key, but only the identity of the recipient where the identity can be a legal name or an email address.

This is possible as long as there exists a trusted party (TP) that publishes some public parameters PP and holds a master secret key MSK. A user with identity X upon authenticating herself to the TP (e.g. by showing a government issued ID), will receive a secret key SK_x that the user can use to decrypt any ciphertext that was sent to the identity X. To encrypt message M to identity X, one needs only to know the public parameters PP and X.

Identity based homomorphic encryption is a variant of public key homomorphic encryption which may be desirable.
Remark: A modification of GSW supports identity based homomorphic encryption.

Appendix A

Organizers

Kristin Lauter	klauter@microsoft.com
Vinod Vaikuntanathan	vinod.nathan@gmail.com

Contributors

Melissa Chase	melissac@microsoft.com
Hao Chen	haoche@microsoft.com
Jintai Ding	jintai.ding@gmail.com
Shafi Goldwasser	shafi@theory.csail.mit.edu
Sergey Gorbunov	sgorbunov100@gmail.com
Jeffrey Hoffstein	hoffsteinjeffrey@gmail.com
Satya Lokam	Satya.Lokam@microsoft.com
Dustin Moody	dustin.moody@nist.gov
Travis Morrison	txm950@psu.edu
Amit Sahai	amitsahai@gmail.com

References

[AFG14] Martin R. Albrecht, Robert Fitzpatrick, and Florian Gopfert: *On the Efficacy of Solving LWE by Reduction to Unique-SVP*. In Hyang-Sook Lee and Dong-Guk Han, editors, ICISC 13,

volume 8565 of LNCS, pages 293-310. Springer, November 2014.

[APS15] Martin R. Albrecht, Rachel Player and Sam Scott. *On the concrete hardness of Learning with Errors*. Journal of Mathematical Cryptology. Volume 9, Issue 3, Pages 169–203, ISSN (Online) 1862-2984, October 2015.

[Bab86] László Babai: *On Lovász' lattice reduction and the nearest lattice point problem,* Combinatorica, 6(1):1-3, 1986.

[BGV12]: Zvika Brakerski, Craig Gentry, Vinod Vaikuntanathan. *(Leveled) fully homomorphic encryption without bootstrapping.* In ITCS '12 Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. Pages 309-325.

[B12] Zvika Brakerski. *Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP,* In CRYPTO 2012. Pages 868 – 886.

[CIV16a] W. Castryck, I. Iliashenko, F. Vercauteren, *Provably weak instances of ring-lwe revisited.* In: Eurocrypt 2016. vol. 9665, pp. 147–167. Springer (2016)

[CIV16b] W. Castryck, I. Iliashenko, F. Vercauteren, *On error distributions in ring-based LWE.* LMS Journal of Computation and Mathematics 19(A), 130–145 (2016) 7.

[CLS15] Hao Chen, Kristin Lauter, Katherine E. Stange, *Attacks on Search RLWE***,** Cryptology ePrint Archive, Report 2015/971, 2015. https://eprint.iacr.org/2015/971

[CLS16] Hao Chen, Kristin Lauter, Katherine E. Stange. *Vulnerable Galois RLWE families and improved attacks.* In SAC 2016. Cryptology ePrint Archive, Report 2016/193, 2016.

[CN11] Y. Chen, P.Q. Nguyen. *BKZ 2.0: Better Lattice Security Estimates*. In: Lee D.H., Wang X. (eds) Advances in Cryptology – ASIACRYPT 2011. ASIACRYPT 2011. Lecture Notes in Computer Science, vol. 7073. Springer, Berlin, Heidelberg.

[CS16] Ana Costache, Nigel P. Smart, *Which Ring Based Somewhat Homomorphic Encryption Scheme is Best?* Topics in Cryptology - CT-RSA 2016, LNCS, volume 9610, Pages 325-340.

[GSW] C. Gentry, A. Sahai, and B. Waters. *Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based*. In *CRYPTO 2013* (Springer).

[ELOS15] Yara Elias, Kristin Lauter, Ekin Ozman, Katherine E. Stange*, Provably weak instances of Ring-LWE,* CRYPTO 2015

[FV12] J. Fan and F. Vercauteren. *Somewhat practical fully homomorphic encryption*. Cryptology ePrint Archive, Report 2012/144, 2012. http://eprint.iacr.org/2012/144.pdf

[Kar16] C.F.F. Karney, *Sampling Exactly from the Normal Distribution*. ACM Transactions on Mathematical Software, 42, Article No. 3.

[KL15] Miran Kim and Kristin Lauter, *Private Genome Analysis through Homomorphic Encryption,* BioMedCentral Journal of Medical Informatics and Decision Making 2015 15 (Suppl 5)**:**S3.

[LMvP13] Laarhoven T., Mosca M., van de Pol J. (2013) *Solving the Shortest Vector Problem in Lattices Faster Using Quantum Search.* In: Gaborit P. (eds) Post-Quantum Cryptography. PQCrypto 2013. Lecture Notes in Computer Science, vol 7932. Springer, Berlin, Heidelberg.

[LP11] Richard Lindner and Chris Peikert: *Better key sizes (and attacks) for LWE-based encryption.* In Topics in Cryptology - CT-RSA 2011 - The Cryptographers' Track at the RSA Conference 2011, Aggelos Kiayias, Editor, volume 6558 of LNCS, pages 319—339.

[LTV] A. Lopez-Alt, E. Tromer, and V. Vaikuntanathan. *On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption.* In STOC, pages 1219–1234, 2012.

[LPR13] Vadim Lyubashevsky, Chris Peikert, and Oded Regev : *On Ideal Lattices and Learning with Errors over Rings.* Journal of the ACM (JACM), Volume 60, Issue 6, November 2013, Article No. 43.

[NTRU] J. Hoffstein, J. Pipher, and J. H. Silverman. *NTRU: A ring-based public key cryptosystem.* In J. Buhler, editor, ANTS, volume 1423 of Lecture Notes in Computer Science, pages 267–288. Springer, 1998.

[YASHE] Joppe W. Bos, Kristin Lauter, Jake Loftus, and Michael Naehrig. *Improved Security for a Ring-Based Fully Homomorphic Encryption Scheme*, in IMA CC 2013. **http://eprint.iacr.org/2013/075.pdf**

Software references for 6 Homomorphic Encryption libraries:

[SEAL] **http://sealcrypto.org**

[HElib] **https://github.com/shaih/HElib**

[NFLlib] **https://github.com/CryptoExperts/FV-NFLlib**

[Palisade] **https://git.njit.edu/groups/palisade**

[cuHE] **https://github.com/vernamlab/cuHE**

[HEAAN] **https://github.com/kimandrik/HEAAN**