Quadratic-Homomorphic Encryption from LWE

We present the GHV encryption scheme \[\text{[GHV10]}\]. This scheme, based on the hardness of learning with errors (LWE), supports homomorphic operations that can be expressed as quadratic forms (similarly to the BGN cryptosystem \[\text{[BGN05]}\]).

1 Background

The decision-LWE problem. The D-LWE\[n, \alpha, q\] assumption asserts that it is infeasible to distinguish the distribution \(\text{LWE}_q = \{(\bar{a}, c) : \bar{a} \in R \ Z_q^n, e \leftarrow \mathcal{N}(0, \alpha q), c = \langle \bar{s}, \bar{a} \rangle + e \mod q\}\) for a random \(s \in R \ Z_q^n\) from the uniform distribution on \(\mathbb{Z}_q^n \times [0, q]\), even when the distinguisher can get any (polynomial) number of samples from these distributions that it wants. This implies that it is also infeasible to distinguish \(\text{LWE}_q = \{(\bar{a}, c) : \bar{a} \in R \ Z_q^n, e \leftarrow \mathcal{N}(0, \alpha q), c = \langle \bar{s}, \bar{a} \rangle + [e] \mod q\}\) from uniform on \(\mathbb{Z}_q^{n+1}\).

In particular, for any polynomial \(m = m(n)\), the distribution
\[
\text{LWE}[m] = \{(A, \bar{e}) : A \in R \ Z_q^{n \times m}, s \in R \ Z_q^n, \bar{e} \leftarrow \mathcal{N}(0, \alpha q)^m, \bar{e} = \bar{s}A + [\bar{e}] \mod q\}
\]
is indistinguishable from the uniform distribution on \(\mathbb{Z}_q^{(n+1) \times m}\). By an easy hybrid argument, we get that the distribution
\[
\text{LWE}[m \times m] = \{(A, C) : A \in R \ Z_q^{n \times m}, S \in R \ Z_q^{m \times n}, E \leftarrow \mathcal{N}(0, \alpha q)^{m \times m}, C = SA + [E] \mod q\}
\]
is indistinguishable from the uniform distribution on \(\mathbb{Z}_q^{(n+m) \times m}\).

Trapdoors. On the other hand, the trapdoor constructions (e.g., \[\text{[AP11]}\] or \[\text{[MP11]}\]) let us generate a nearly-uniform matrix \(A \in \mathbb{Z}_q^{n \times m}\) together with a trapdoor \(T_A\) such that given \(T_A\) we can invert the function
\[
\text{lwe}_A(\bar{s}, \bar{e}) = \bar{s}A + \bar{e} \mod q
\]
where \(\bar{s} \in \mathbb{Z}_q^n\), \(\bar{e} \in \mathbb{Z}_m\), and \(|\bar{e}|_\infty < q/8m\) (say).

In particular, the Alwen-Peikert trapdoor from \[\text{[AP11]}\] is a full-rank integer matrix \(T\) such that \(AT = 0 \mod q\) and all the entries in \(T\) are at most 3 in absolute value. Hence \(\langle \bar{s}A + \bar{e}, T \rangle = \bar{e} \times T \mod q\), but \(|\bar{e} \times T|_\infty \leq |\bar{e}|_\infty \times |T|_\infty \times m \leq \frac{q}{8m} \times 3 \times m < q/2\). This means that \((\bar{s}A + \bar{e}) \times T \mod q\) = \(\bar{e} \times T\) over the integers, so
\[
((\bar{s}A + \bar{e}) \times T \mod q) \times T^{-1} = (\bar{e} \times T) \times T^{-1} = \bar{e}.
\]

2 The Gentry-Halevi-Vaikuntanathan Cryptosystem

Key-generation. Run the Alwen-Peikert trapdoor construction to get \(A \in \mathbb{Z}_q^{n \times m}\) and the corresponding trapdoor \(T_A\). The public key is \(A\) and the secret key is \(T_A\).

Encryption\(_A(B)\). The plaintext is a binary matrix \(B \in \{0, 1\}^{m \times m}\).
1. Choose at random \(S \in R \ Z_q^{m \times n}\) and \(E \leftarrow \mathcal{N}(0, \alpha q)^{m \times m}\);
2. The ciphertext is a matrix over \(\mathbb{Z}_q^{m \times m}\), \(C = SA + 2[E] + B \mod q\).
Decryption\(_{T_A}(C)\). Note that each row of \(C\) is of the form \(\vec{c}_i = \vec{s}_i A + (2 \lceil \vec{e}_i \rceil + \vec{b}_i) \mod q\). Use the trapdoor \(T_A\) to recover the “error vector” \(\vec{x}_i = (2 \lceil \vec{e}_i \rceil + \vec{b}_i)\), then reduce modulo 2 to get \(\vec{b}_i\).

2.1 Correctness

If \(\alpha \leq 1/nm\) (say), then the probability of having any entry in \(\vec{e}\) larger than \(q/17m\) in absolute value is bounded by some \(\exp(-n)\). Therefore the “error-vectors” \(\vec{x}_i = (2 \lceil \vec{e}_i \rceil + \vec{b}_i)\) satisfy \(|\vec{x}_i|_\infty < q/8m\), and so we can recover it using the trapdoor.

Below we will need also a stronger bound: For any parameters \(k, m, q\) and \(\alpha\) and any fixed unit vector \(\vec{u} \in \mathbb{R}^m\), when we choose \(\vec{e} \leftarrow \mathcal{N}(0, \alpha q)^m\), then the probability that \(\langle \vec{u}, \vec{e}\rangle > \alpha q \cdot k\) is bounded by \(\exp(-k^2/2)\).

2.2 Security

We show that when \(q\) is odd, then a successful chosen-plaintext attacker \(A\) against the scheme implies a distinguisher \(D\) between \(\text{LWE}[m \times m]\) and uniform.

The distinguisher gets \((A, C)\) and it needs to decide if \(C = SA + E \mod q\) or \(C\) is uniform in \(\mathbb{Z}_q^{m \times m}\). It runs the attacker \(A\) with public key \(A\), and the attacker gives it two matrices \(B_0, B_1\). Then \(D\) chooses at random \(i \in R\{0,1\}\) and provides the attacker \(A\) with the “ciphertext” \(C^* = 2C + B_i\). Then \(A\) outputs a guess \(i'\), if \(i' = i\) then \(D\) outputs 1 (i.e., it guesses that the input distribution is \(\text{LWE}[m \times m]\)), and otherwise it outputs 0 (i.e., it guesses that the distribution is uniform).

If \((A, C)\) is taken from the uniform distribution then \(C^*\) is uniform (since \(q\) is odd), regardless of \(i\), hence the probability of \(i' = i\) is exactly 1/2.

If \((A, C)\) is taken from \(\text{LWE}[m \times m]\) then \(C = SA + E \mod q\) and therefore \(C^* = 2C + B_i = (2S)A + 2E + B_i \mod q\). Since \(q\) is odd and \(S\) is uniform over \(\mathbb{Z}_q\) then so is \(2S \mod q\), hence \(C^*\) is distributed exactly the same as a random encryption of \(B_i\). It follows that in this case we have \(i' = i\) with probability noticeably larger than 1/2.

2.3 Additive Homomorphism

Assume that we set \(\alpha \leq 1/mk\) for some parameter \(k\), and consider a set of \(\ell\) plaintext matrices \(B_1, \ldots, B_{\ell}\) and their encryption \(C_1, \ldots, C_{\ell}\), where \(\ell \leq o(k^2/\sqrt{\log n})\). We claim that with overwhelming probability, the matrix \(\sum_{i=1}^{\ell} C_i \mod q\) will be decrypted to the binary sum \(\sum_{i=1}^{\ell} B_i \mod 2\). This is because

\[
\sum_{i=1}^{\ell} C_i \equiv \sum_{i=1}^{\ell} \sum_{S} S_i A + 2 \sum_{i} E_i + \sum_{i} B_i \pmod{q} = SA + 2E + B \pmod{q}
\]

and since each entry in \(E\) is a sum of \(\ell\) independent Gaussians with variance \((\alpha q)^2\), then each such entry is itself a Gaussian with variance \(\ell(\alpha q)^2\). From \(\alpha \leq 1/mk\) and \(\ell \leq o(k^2/\sqrt{\log n})\) it follows that with overwhelming probability each entry in \(E\) is \(o(q/m)\) and in particular smaller than \(q/16m\), as needed for our trapdoor to work.

2.4 Multiplicative Homomorphism

Let \(C_1 = S_1 A + 2E_1 + B_1 \mod q\) and \(C_2 = S_2 A + 2E_2 + B_2 \mod q\), and let \(C = C_1 \times C_2 \mod q\). Then \(TCT^t = T(2E_1 + B_1) \times (2E_2 + B_2)T^t \pmod{q}\). If \(\alpha\) is chosen small enough so that all the entries in \(E_1, E_2\) are \(o(\sqrt{q}/m^{1.5})\), then all the entries in \(T(2E_1 + B_1)\) and \(T(2E_2 + B_2)\) are
smaller than \( o(\sqrt{q/m}) \), and so all the entries in \( T(2E_1 + B_1) \times (2E_2 + B_2^t)T^t \) are smaller than \( m \times o(\sqrt{q/m}) \times o(\sqrt{q/m}) = o(q) \). Therefore

\[
TCT^t \mod q = T(2E_1 + B_1) \times (2E_2 + B_2^t)T^t
\]

over the integers, and so we get

\[
T^{-1}(TCT^t \mod q)(T^{-1})^t = (2E_1 + B_1) \times (2E_2 + B_2^t) = B_1B_2^t \pmod{2}
\]

We can therefore multiply two ciphertext matrices, and be able to decrypt the product of the two plaintext binary matrices from the resulting product ciphertext.

References


