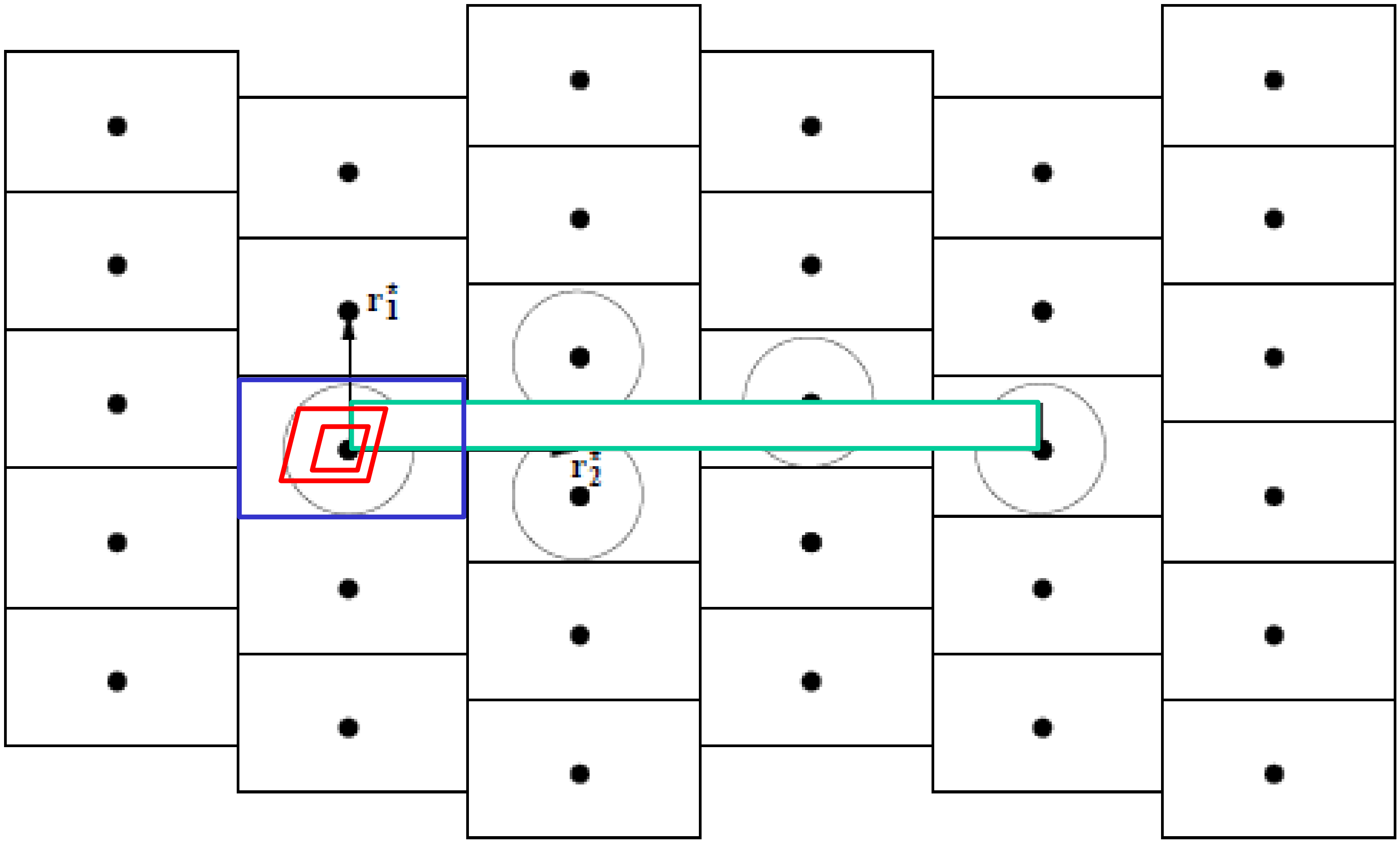
Gentry's ideal-lattice based encryption scheme

Gentry's STOC'09 paper - Part III



From Micciancio's paper

Why ideal lattices
--- as opposed to just ideals or lattices?

- We described an ideal-based encryption scheme Σ.
- Recall $X_{\text{Enc}} \triangleq \text{Samp}\left(\mathbf{B}_I, P\right)$ and $X_{\text{Dec}} \triangleq R \bmod \mathbf{B}_J^{sk}$.
- The scheme is correct for circuit C if

$$\forall\ x_1,\ \ldots,\ x_t \in X_{\text{Enc}},\ g(C)\left(x_1,\ \ldots,\ x_t\right) \in X_{\text{Dec}}.$$

- For Σ to be correct as an ordinary encryption scheme, we require: $X_{\text{Enc}} \subseteq X_{\text{Dec}}$.
- For Σ to be additively and multiplicatively homomorphic, we require: $X_{\text{Enc}} + X_{\text{Enc}} \subseteq X_{\text{Dec}}$ and $X_{\text{Enc}} \times X_{\text{Enc}} \subseteq X_{\text{Dec}}$.

- Our goal is to have $g(C)\left(X_{\text{Enc}}\right) \subseteq X_{\text{Dec}}$ for deep enough circuits C, including the decryption circuit D_Σ.
- So, we want to analyze, for example, how
$$\left(\left(X_{\text{Enc}} + X_{\text{Enc}}\right) \times \left(X_{\text{Enc}} + X_{\text{Enc}}\right)\right) \times X_{\text{Enc}} \times X_{\text{Enc}} \cdots$$
expand, and how to ensure
$$\left(\left(X_{\text{Enc}} + X_{\text{Enc}}\right) \times \left(X_{\text{Enc}} + X_{\text{Enc}}\right)\right) \times X_{\text{Enc}} \times X_{\text{Enc}} \cdots \subseteq X_{\text{Dec}}.$$
- Connecting ideals with lattices makes such analysis possible, because, with $R = \mathbb{Z}[x]/(f(x)) \cong \mathbb{Z}^n$, X_{Enc} and X_{Dec} become subsets of $\mathbb{Z}^n$ and we can analyze them geometrically.

Instantiate the ideal-based scheme

- To instantiate the (abstract) ideal-based encryption scheme using ideal lattices, we will do the following.
- Choose a polynomial $f(x)$ with integer coefficients and let ring $R = \mathbb{Z}[x]/\left(f(x)\right)$.
- Choose an element $\mathbf{s} \in R$, ideal $I = \left(\mathbf{s}\right)$, $\mathbf{B}_I$ = the rotation basis.
- Plaintext space M: a subset of $C(\mathbf{B}_I)$, centered parallelepiped.
- Samp: choose a range ℓ_{Samp} for Samp.
- Choose an ideal J and a good basis $\mathbf{B}_J^{sk}$. Let $\mathbf{B}_J^{pk} = \text{HNF}(\mathbf{B}_J^{sk})$.

Ideal Lattices

$\mathbb{Z}[x]/(f(x))$: a polynomial ring

- $\mathbb{Z}[x]$: the ring of all polynomials with integer coefficients.
- $f(x)$: a monic polynomial of degree n in $\mathbb{Z}[x]$
  - Monic means the leading coefficient is 1
  - Often choose $f(x)$ to be irreducible.
- $(f(x))$: the ideal generated by $f(x)$.
  - $(f(x)) = f(x) \cdot \mathbb{Z}[x] = \{ f(x) \cdot g(x) : g(x) \in \mathbb{Z}[x] \}$.
- $g(x) \equiv h(x) \bmod f(x)$ iff $g(x) - h(x)$ is divisible by $f(x)$.
- $\mathbb{Z}[x]$ is divided into classes (cosets) such that $g(x)$ and $h(x)$ are in the same class (coset) iff $g(x) \equiv h(x) \bmod f(x)$.

- $\mathbb{Z}[x]/(f(x))$:
  - $\mathbb{Z}[x]/(f(x))$ denotes the set of those classes (cosets).
  - Each class has exactly one polynomial of degree $\leq n-1$.
  - Thus, $\mathbb{Z}[x]/\left(f(x)\right)$ may also be defined as the set of all polynomials of degree $\leq n-1$, i.e.,

    $\mathbb{Z}[x]/\left(f(x)\right) = \left\{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 : \ a_i \in \mathbb{Z}\right\}$.
  - Addition and multiplication in $\mathbb{Z}[x]/(f(x))$ are like regular polynomial addition and multiplication except that the result is reduced modulo $f(x)$.
  - $\mathbb{Z}[x]/\left(f(x)\right)$ is a commutative ring with identity.

- If $a(x) = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ and

  $b(x) = b_{n-1}x^{n-1} + \cdots + b_1 x + b_0,$ then

  $$a(x) + b(x) = (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0).$$

- $\mathbb{Z}[\mathrm{x}]/(f(x)) \cong \mathbb{Z}^n$ as an additive group.
  - The group $\mathbb{Z}[x]/(f(x))$ is isomorphic to the lattice $\mathbb{Z}^n$.
  - $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \leftrightarrow (a_0, a_1, \ldots, a_{n-1}).$
  - Define multiplication in $\mathbb{Z}^n$ by way of multiplication in $\mathbb{Z}[x]/(f(x)),$ and then we have multiplication in $\mathbb{Z}^n$.

- Each ideal in $\mathbb{Z}[\mathrm{x}]/(f(x))$ defines a sublattice in $\mathbb{Z}^n$.

- Lattices corresponding to ideals are ideal lattices.

Rotation basis for principal ideal $(\mathbf{v})$

- Since $R = \mathbb{Z}[x]/(f(x)) \cong \mathbb{Z}^n$, we do not distinguish between ring elements in R and lattice points/vectors in $\mathbb{Z}^n$.

- Any ideal in R corresponds to a lattice in $\mathbb{Z}^n$.

- In particular, the ideal $(\mathbf{v})$ generated by $\mathbf{0} \neq \mathbf{v} \in R$ defines a lattice with basis $\mathbf{B} = [\mathbf{v}_0, \ \ldots, \ \mathbf{v}_{n-1}]$, where

$$\mathbf{v}_i = \mathbf{v} \times x^i \bmod f(x).$$

- This basis is called the rotation basis for the ideal lattice $(\mathbf{v})$.

- Not every ideal has a rotation basis.

Examples

- Ideal $(1) = R$. $1 = \mathbf{e}_1$. Rotation basis $= [\mathbf{e}_1,\ \mathbf{e}_2,\ \ldots,\ \mathbf{v}_n]$.

  Ideal lattice $= \mathbb{Z}^n$.

- Ideal $(2) = 2 \times R = \{$all polynomials in R with even coefficients$\}$.

  Rotation basis: $[2\mathbf{e}_1,\ 2\mathbf{e}_2,\ \ldots,\ 2\mathbf{v}_n]$.

  Corresponding lattice, $2\mathbb{Z}^n = \left\{\begin{array}{l}\text{all lattice points in } \mathbb{Z}^n \\ \text{with even coordinates}\end{array}\right\}$.

- Q: Find the rotation basis of $(2 + x)$ or $(2\mathbf{e}_1 + \mathbf{e}_2)$.

$\mathbb{Q}[x]/(f(x))$ and fractional ideals

- $\mathbb{Q}[x]$: the ring of polynomials with rational coefficients.
- $\mathbb{Q}[x]/(f(x)) = \left\{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 : a_i \in \mathbb{Q}\right\}$.
- If I is an ideal in $R = \mathbb{Z}[x]/(f(x))$, define I^{-1} as

$$I^{-1} \triangleq \left\{\mathbf{v} \in \mathbb{Q}[x]/(f(x)) : \mathbf{v} \times I \subseteq R\right\} \supseteq R.$$

  - I^{-1} is a fractional ideal. It behaves like an ideal of R except that it is not necessarily contained in R.
  - $I\,I^{-1} \subseteq R$. I is said to be invertible if $I\,I^{-1} = R$.
- All invertible (fractional) ideals form a group with R as the identity.

$\mathbb{Q}[\mathrm{x}]/(f(x))$ and fractional ideals

- If $I=(\mathbf{v})$, then $I^{-1}=\left(\mathbf{v}^{-1}\right)$ is generated by $\mathbf{v}^{-1}\in\mathbb{Q}[x]/(f(x))$.
  - $\mathbf{v}^{-1}$ exists if $f(x)$ is irreducible.
- I^{-1} defines a lattice in $\mathbb{R}^n$, not necessarily in $\mathbb{Z}^n$.
- We have $(\det I)\cdot\left(\det I^{-1}\right)=1.$
- Recall: $\det I=\left|\det \mathbf{B}_I\right|=\det\left(L(\mathbf{B}_I)\right)=\mathrm{vol}\left(P(\mathbf{B}_I)\right),$ the volumn of the fundamental parallelepiped of the lattice defined by I.
- $\det I=$ the index $[R:I]\triangleq$ the number of elements in R/I.

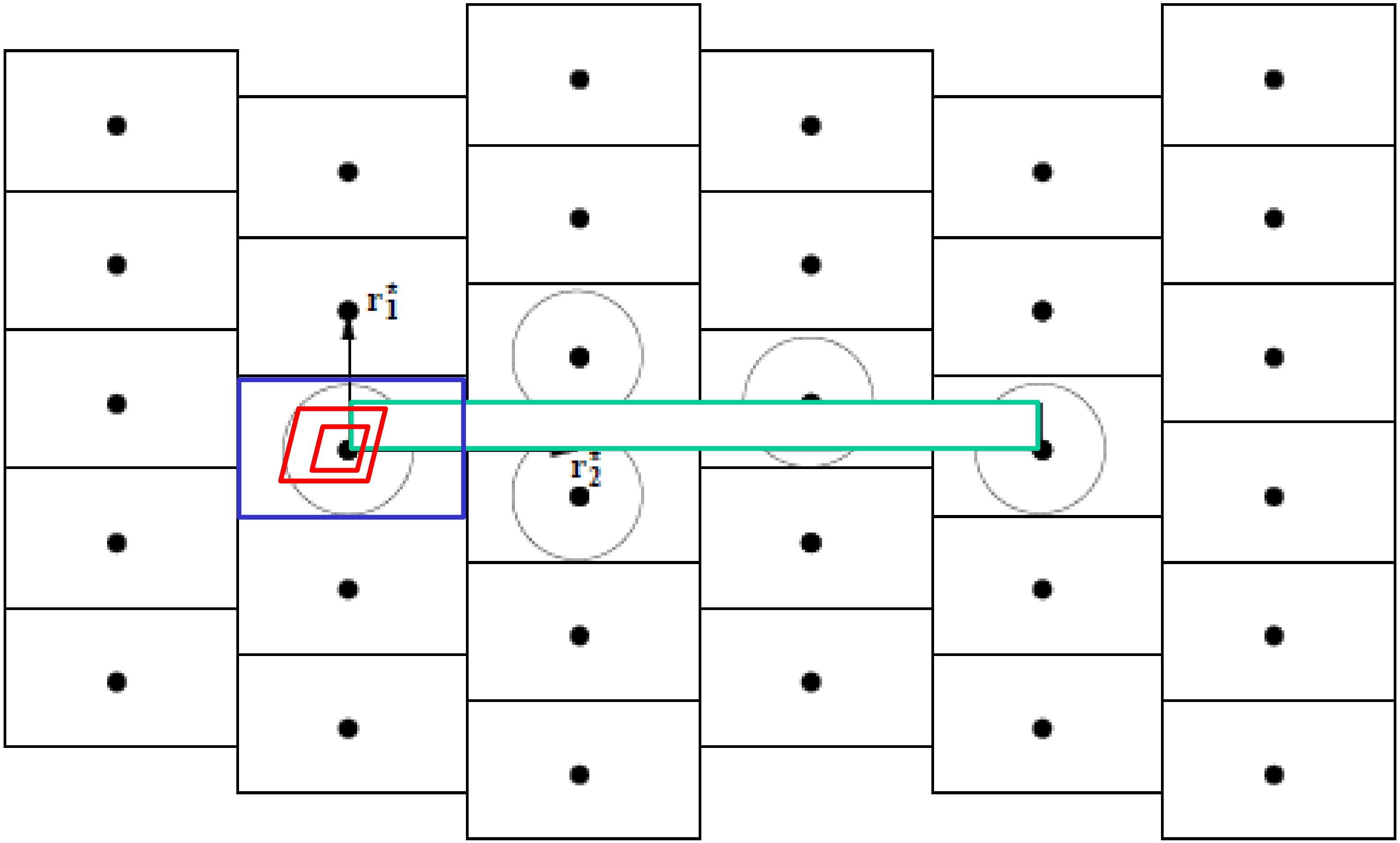
Review

- Hermite nornal form (HNF):
  - a basis which is skiny, skew, and will be used as a *pk*.
- Centered fundamental parallelepiped: $//\mathbf{B} = [\mathbf{b}_1, \ \ldots, \ \mathbf{b}_n]//$

$$P(\mathbf{B}) \triangleq \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i : x_i \in [-1/2, \ 1/2) \right\}.$$

- $\mathbf{t} \bmod \mathbf{B} \triangleq$ the unique $\mathbf{t}' \in P(\mathbf{B})$ with $\mathbf{t} - \mathbf{t}' \in L(\mathbf{B})$.
- $\mathbf{t} \bmod \mathbf{B}$ can be efficiently computed as $\mathbf{t} - \mathbf{B} \cdot \lfloor \mathbf{B}^{-1} \cdot \mathbf{t} \rceil$.
- $\lfloor x \rceil \triangleq x$ rounded to the nearest integer.
- $\|\mathbf{B}\| \triangleq \max \{ \|\mathbf{b}_i\| : \mathbf{b}_i \in \mathbf{B} \}$.

Instantiating the ideal-based scheme using ideal lattices



From Micciancio's paper

Recall:

- To instantiate the (abstract) ideal-based encryption scheme using (ideal) lattices, we will do the following.
- Choose a polynomial $f(x)$ and let ring $R = \mathbb{Z}[x] \big/ \big(f(x) \big)$.
- Choose a vector $\mathbf{s}$, let ideal $I = \big(\mathbf{s} \big)$, let $\mathbf{B}_I$ = the rotation basis.
- Plaintext space M: a subset of $P(\mathbf{B}_I)$.
- Samp: choose a range ℓ_{Samp} for Samp.
- Choose an ideal J and a good basis $\mathbf{B}_J^{sk}$.

  Let $\mathbf{B}_J^{pk} = \text{HNF}(\mathbf{B}_J^{sk})$.
- Our goal is to have $g(C)\big(X_{\text{Enc}} \big) \subseteq X_{\text{Dec}}$ for deep enough circuits C, including the decryption circuit D_Σ.

Balls: $\mathcal{B}(r_{\text{Enc}})$ and $\mathcal{B}(r_{\text{Dec}})$

- $X_{\text{Enc}} \triangleq \text{Samp}\left(\mathbf{B}_I, M\right).$

  $X_{\text{Dec}} \triangleq R \bmod \mathbf{B}_J^{sk} = P(\mathbf{B}_J^{sk}).$

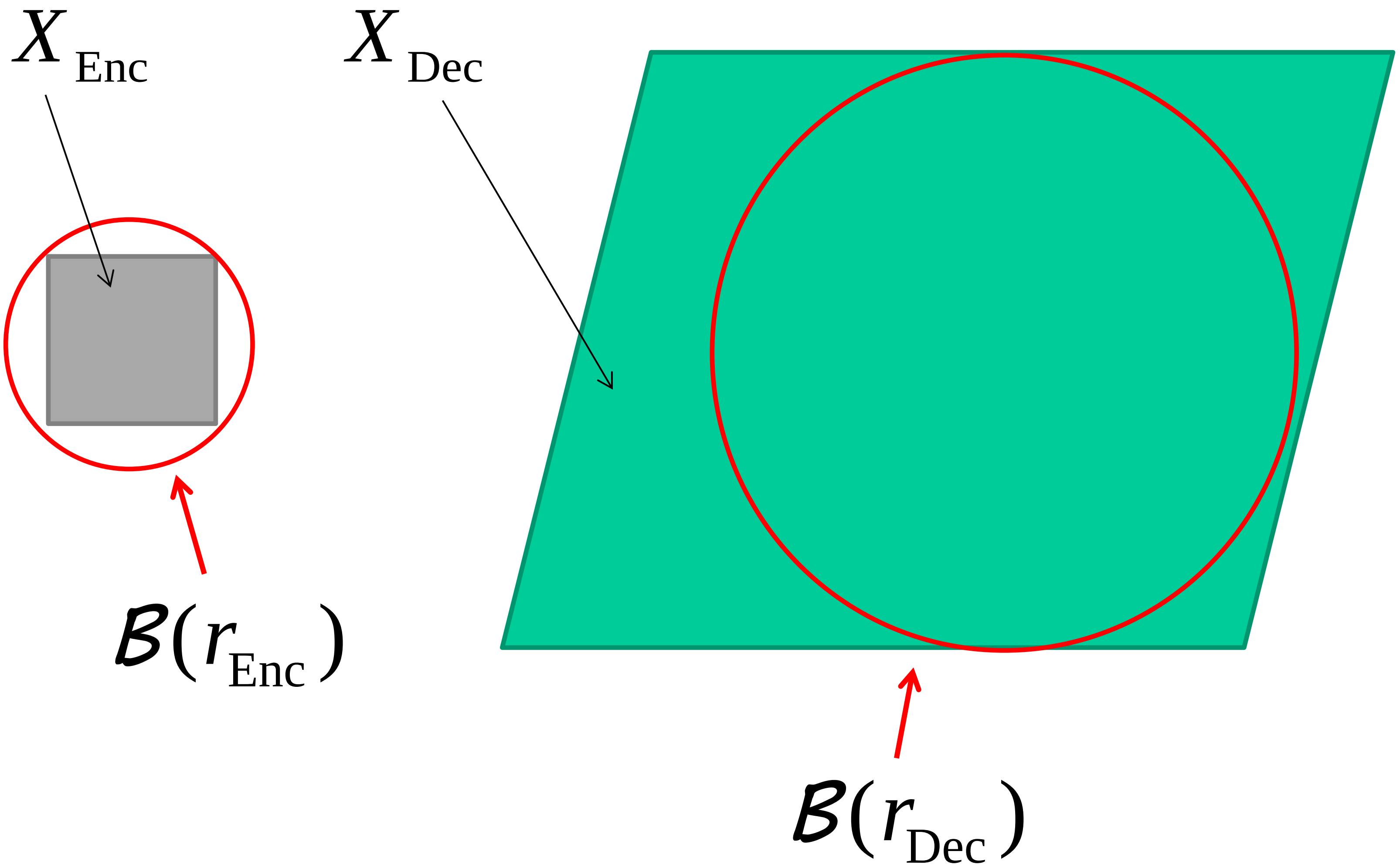
- Define: $r_{\text{Enc}} \triangleq$ the smallest radius s.t. $X_{\text{Enc}} \subseteq \mathcal{B}(r_{\text{Enc}}),$

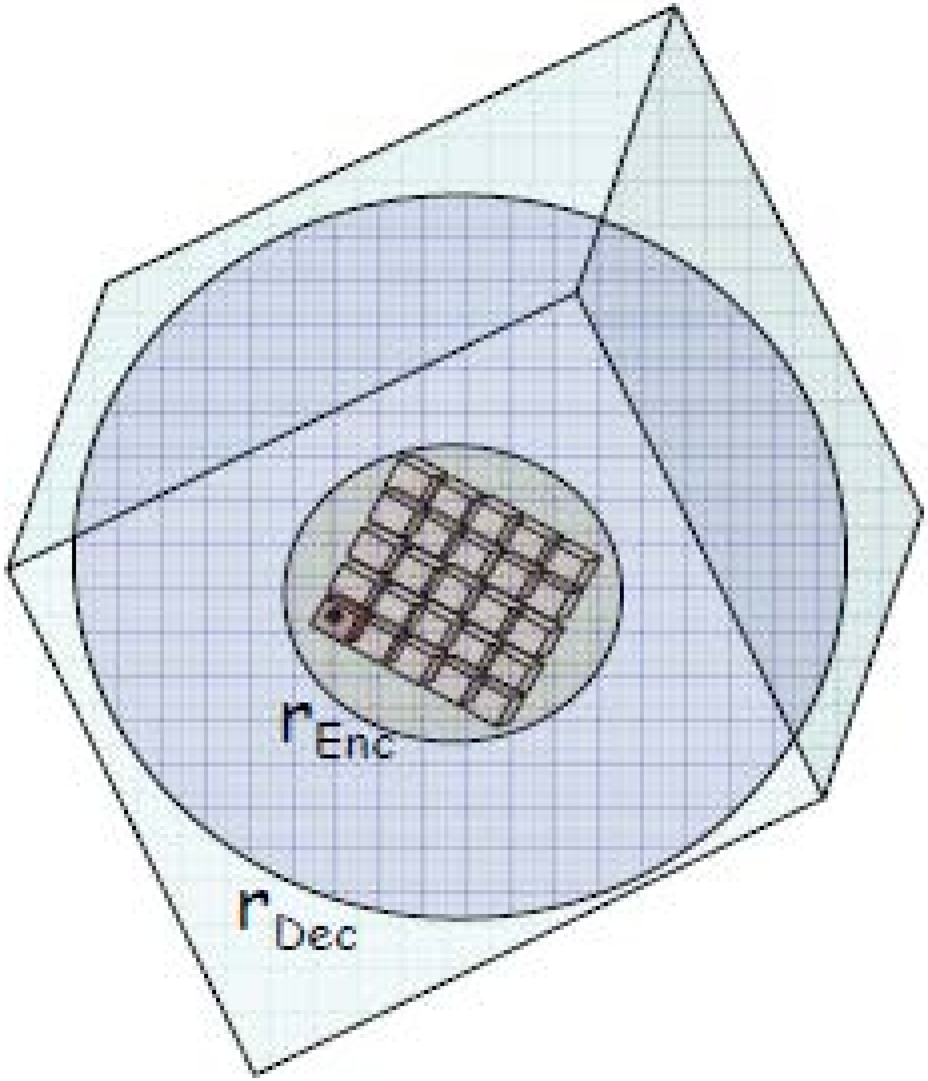
  $r_{\text{Dec}} \triangleq$ the largest radius s.t. $\mathcal{B}(r_{\text{Dec}}) \subseteq X_{\text{Dec}}.$

- Theorem (a sufficient condition for permitted circuits):

  A $\bmod \mathbf{B}_I$-circuit C (including the identity circuit) with $t \geq 1$ inputs is a permitted circuit for the schecme if:

$$\forall\, x_1, \ldots, x_t \in \mathcal{B}(r_{\text{Enc}}),\ g(C)\left(x_1, \ldots, x_t\right) \in \mathcal{B}(r_{\text{Dec}}).$$


X_{Enc}
X_{Dec}
$\mathcal{B}(r_{\text{Enc}})$
$\mathcal{B}(r_{\text{Dec}})$


r Enc
r Dec

Expansion of vectors with operations

- Starting from $\mathcal{B} := \mathcal{B}(r_{\mathrm{Enc}})$, how does $\mathcal{B}$ expand with addition and multiplication?
- $\|\mathbf{u}+\mathbf{v}\| \leq \|\mathbf{u}\| + \|\mathbf{v}\|$ for all $\mathbf{u},\mathbf{v} \in R$ (triangle inequality).
- $\|\mathbf{u}\times\mathbf{v}\| \leq \gamma_{\mathrm{Mult}} \|\mathbf{u}\| \cdot \|\mathbf{v}\|$ for all $\mathbf{u},\mathbf{v} \in R$, where γ_{Mult} is a factor dependent on *R*. Let $m = \gamma_{\mathrm{Mult}}$.
- If input vectors are in $\mathcal{B}(r)$, then after a *m*-fan-in addition or a 2-fan-in multiplication, the output vector is in $\mathcal{B}(mr^2)$.

- By induction, if input vectors are in $\mathcal{B}(r_{\text{Enc}})$, then after k levels of m-fan-in addition and/or 2-fan-in multiplication, the result is in $\mathcal{B}(m^{2^k-1} r_{\text{Enc}}^{2^k}) \subseteq \mathcal{B}\left((m r_{\text{Enc}})^{2^k}\right)$.
- We will have $(m r_{\text{Enc}})^{2^k} \le r_{\text{Dec}}$ if $k \le \log\log r_{\text{Dec}} - \log\log m r_{\text{Enc}}$.
- Theorem: The proposed scheme Σ correctly evaluates circuits of depth up to $\log\log r_{\text{Dec}} - \log\log\left(\gamma_{\text{Mult}} \cdot r_{\text{Enc}}\right)$.
- To maximize the depth of permitted circuits, we will attempt to minimize r_{Enc} and γ_{Mult} and maximize r_{Dec} subject to security constraints.

Security constraints

- Roughly: the ratio $r_{\text{Dec}}/r_{\text{Enc}}$ must be $\leq$ subexponential.
- Recall: the security of the abstract scheme relies on the hardness of ICP.
- In the setting of ideal lattices (where $\boldsymbol{\pi}'$ is chosen to be shorter than r_{Enc} and $\mathbf{t} := \bmod \mathbf{B}_J^{pk}$), ICP becomes: Decide whether $\mathbf{t}$ is within a small distance (r_{Enc}) of lattice J, or is uniformly random modulo J.
- This is a decision version of BDDP, which is not surprising since the abstract scheme is a variant of GGH and the security of GGH relies on the hardness of BDDP.

- Roughly: the ratio $r_{\text{Dec}}/r_{\text{Enc}}$ must be $\leq$ sub-exponential.
- If r_{Enc} is too small, say $r_{\text{Enc}} \leq \lambda_1(J)/2^n$, BDDP can be solved using, for example, the LLL algorithm.
- No algorithm is known to solve BDDP if $r_{\text{Enc}} \geq \lambda_1(J)/2^{n^c}$, $c < 1$.
- On the other hand, by definition, we have $r_{\text{Dec}} \leq \lambda_1(J)$.
- Thus, for BDDP to be hard, we require

$$r_{\text{Dec}}/r_{\text{Enc}} \leq 2^{n^c}, \quad c < 1 \quad \text{//sub-exponential//}$$

- If we choose $r_{\text{Dec}} = 2^{n^{c_1}}$, $\gamma_{\text{Mult}} \cdot r_{\text{Enc}} = 2^{n^{c_2}}$, then the scheme can handle circuits of depth up to $(c_1 - c_2)\log n$.

Minimizing $\gamma_{\mathrm{Mult}}(R)$

- Goal: Set $f(x)$ so that $R = \mathbb{Z}[x]/(f(x))$ has a small $\gamma_{\mathrm{Mult}}(R)$.
- To this end, we only have to choose $f(x)$ such that $f(x)$ and $g(x)$ have small norms, due to the following theorem.
- Theorem: If $f(x)$ is a monic polynomial of degree n then

$$\gamma_{\mathrm{Mult}}(R) \le \sqrt{2n} \cdot \left(1 + 2n \cdot \|f\| \cdot \|g\|\right),$$

where $g(x) = F(x)^{-1} \bmod x^{n-1}$ //inverse in $\mathbb{Q}[x]/(x^{n-1})$//

$F(x) = x^n f(1/x)$ //reversing the coefficients of $f(x)$//

$\|p\| = \sqrt{\sum a_i^2}$ for $p(x) = a_n x^n + \cdots + a_0$ //polynomial norm//

- Theorem: If $f(x) = x^n - h(x)$ where $h(x)$ has degree at most $n-(n-1)/k,\ k \geq 2,$ then, for $R = \mathbb{Z}[x]/(f(x)),$

$$\gamma_{\text{Mult}}(R) \leq \sqrt{2n} \cdot \left(1 + 2n\left(\sqrt{(k-1)n}\,\|f\|\right)^k\right).$$

- Theorem: Let $f(x) = x^n \pm 1$ and $R = \mathbb{Z}[x]/(f(x))$. Then,

$$\gamma_{\text{Mult}}(R) \leq \sqrt{n}.$$

- There are non-fatal attacks on hard problems over this ring.

Minimizing r_{Enc}

- Let $R = \mathbb{Z}[x]/\left(f(x)\right)$ with $f(x) = x^n - 1$ and so $\gamma_{\text{Mult}}(R) \le \sqrt{n}$.
- Let $\mathbf{s} \in R$, and $I = (\mathbf{s})$ the ideal generated by $\mathbf{s}$,

  $\mathbf{B}_I = \left(\mathbf{s}_0, \ \ldots, \ \mathbf{s}_{n-1}\right)$ the rotation basis of $\mathbf{s}$, $\left\|\mathbf{B}_I\right\| = \max\left\{\left\|\mathbf{s}_i\right\|\right\}$,

  $L(\mathbf{B}_I)$ the lattice generated by $\mathbf{B}_I$,

  $P(\mathbf{B}_I)$ the centered fundamental parallelepiped,

  $M \subseteq P(\mathbf{B}_I)$ the message space, $\mathbf{x} \in M$ a message,

  $\text{Samp}\left(\mathbf{B}_I, \mathbf{x}\right) := \mathbf{x} + \text{Samp}_1\left(R\right) \times \mathbf{s}.$
- We want $\text{Samp}\left(\mathbf{B}_I, M\right) \triangleq X_{\text{Enc}} \subseteq \mathcal{B}(r_{\text{Enc}})$.
- Let ℓ_{Samp_1} be an upper bound on $\left\|\mathbf{r}\right\|$, $\mathbf{r} \leftarrow \text{Samp}_1\left(R\right)$.

- Theorem: $r_{\text{Enc}} \le n \cdot \|\mathbf{B}_I\| + \sqrt{n} \cdot \ell_{\text{Samp}_1} \cdot \|\mathbf{B}_I\|.$

  Proof : $r_{\text{Enc}} = \max\left\{\|\mathbf{x} + \mathbf{r} \times \mathbf{s}\| : \mathbf{x} \in M,\ \mathbf{r} \leftarrow \text{Samp}_1(R)\right\}.$

  Since $\mathbf{x} \in M \subseteq P(\mathbf{B}_I) \Rightarrow \|\mathbf{x}\| \le \left\|\sum_{i=0}^{n-1} \mathbf{s}_i / 2\right\| \le n \cdot \|\mathbf{B}_I\|$

  $\Rightarrow \|\mathbf{x} + \mathbf{r} \times \mathbf{s}\| \le \|\mathbf{x}\| + \|\mathbf{r} \times \mathbf{s}\| \le n \cdot \|\mathbf{B}_I\| + \sqrt{n} \cdot \ell_{\text{Samp}_1} \cdot \|\mathbf{B}_I\|.$

- May choose $\mathbf{s} = 2\mathbf{e}_1$ to make $\|\mathbf{B}_I\|$ small. Q: why not $\mathbf{s} = \mathbf{e}_1$?

- The size of ℓ_{Samp_1} is a security. It needs to be large enough to make $\mathbf{t} \leftarrow \text{Samp}_1(R) \bmod \mathbf{B}_J^{pk}$ in ICP sufficiently random.

- May set $\ell_{\text{Samp}_1} = n$ and let Samp_1 sample uniformly in $\mathbb{Z}^n \cap \mathcal{B}(n)$.

- With this setting, $r_{\text{Enc}} \le 2n + 2n^{1.5}$.

Maximizing r_{Dec}

- Recall: the decryption equation: $\pi \leftarrow \left(\psi \bmod \mathbf{B}_J^{\text{sk}}\right) \bmod \mathbf{B}_I$.
- We want $\mathcal{B}(r_{\text{Dec}}) \subseteq X_{\text{Dec}} \triangleq P(\mathbf{B}_J^{sk})$.
- To have a large r_{Dec}, the shape of $P(\mathbf{B}_J^{sk})$ is important.

  $\mathbf{B}_J^{sk}$

  We want it to be "fat" (i.e. containing a large ball).
- The "fattest" parallelepiped is that associated with basis

  $t \cdot \mathbf{E} = \left(t \cdot \mathbf{e}_1,\ \ldots,\ t \cdot \mathbf{e}_n\right)$, containing a ball of radius t.
- So, we will choose our $\mathbf{B}_J^{sk}$ to be "close" to $t \cdot \mathbf{E}$.

  Q: why not simply letting $\mathbf{B}_J^{sk} = \left(t \cdot \mathbf{e}_1,\ \ldots,\ t \cdot \mathbf{e}_n\right)$?

- Theorem: Let $t \geq 4n \cdot s \cdot \gamma_{\text{Mult}}(R)$. Suppose $\mathbf{v}_1 \in t \cdot \mathbf{e}_1 + \mathcal{B}(s)$, i.e., within distance s of $t \cdot \mathbf{e}_1$. Let $\mathbf{B}_J^{sk}$ be the rotation basis of $\mathbf{v}_1$. Then, $P(\mathbf{B}_J^{sk})$ circumscribes a ball of radius at least $t/4$.

Proof: We have $\mathbf{B}_J^{sk} = \left(\mathbf{v}_1, \ \ldots, \ \mathbf{v}_n\right)$, with $\mathbf{v}_i = \mathbf{v}_1 \times x^{i-1}$.

The difference $\mathbf{z}_j = \mathbf{v}_j - t \cdot \mathbf{e}_j$ has length

$$\left\|\mathbf{z}_j\right\| = \left\|\mathbf{v}_j - t \cdot \mathbf{e}_j\right\| = \left\|\left(\mathbf{v}_1 - t \cdot \mathbf{e}_1\right) \times x^{j-1}\right\| \leq s \cdot \gamma_{\text{Mult}}(R).$$

For every point $\mathbf{a}$ on the surface of $P(\mathbf{B}_J^{sk})$, we have

$$\mathbf{a} = \pm\frac{1}{2} \cdot \mathbf{v}_i + \sum_{j \neq i} a_j \mathbf{v}_j \text{ for some } i \text{ and } \left|a_j\right| \leq 1/2.$$

We will show $\left\|\mathbf{a}\right\| \geq t/4$, from which the theorem will follow.

$$\mathbf{a} = \pm\frac{1}{2}\cdot\mathbf{v}_i + \sum_{j\neq i} a_j \mathbf{v}_j, \quad |a_j| \leq 1/2.$$

$$\|\mathbf{a}\| \;\geq\; |\langle \mathbf{a}, \mathbf{e}_i \rangle| \;\geq\; \left| \frac{1}{2}\cdot\langle \mathbf{v}_i, \mathbf{e}_i \rangle + \sum_{j\neq i} a_j \langle \mathbf{v}_j, \mathbf{e}_i \rangle \right|$$

$$= \;\left| \frac{1}{2}\cdot t + \frac{1}{2}\cdot\langle \mathbf{z}_i,\ \mathbf{e}_i \rangle + \sum_{j\neq i} a_j \langle \mathbf{z}_j,\ \mathbf{e}_i \rangle \right|$$

$$\geq\; t/2 - \left| n\langle \mathbf{z}_j,\ \mathbf{e}_i \rangle \right| \;\geq\; t/2 - n\|\mathbf{z}_j\| \;\geq\; t/2 - n\cdot s\cdot\gamma_{\mathrm{Mult}}(R)$$

$\geq\; t/2 - t/4 \;\geq\; t/4,$ where we have used

$$\langle \mathbf{v}_i, \mathbf{e}_i \rangle = \langle \mathbf{z}_i + t\cdot\mathbf{e}_i,\ \mathbf{e}_i \rangle = t + \langle \mathbf{z}_i,\ \mathbf{e}_i \rangle$$

$$\langle \mathbf{v}_j, \mathbf{e}_i \rangle = \langle \mathbf{z}_j + t\cdot\mathbf{e}_j,\ \mathbf{e}_i \rangle = \langle \mathbf{z}_j,\ \mathbf{e}_i \rangle$$

Generating $\mathbf{B}_J^{\mathrm{sk}}$ and $\mathbf{B}_J^{\mathrm{pk}}$

- By the theorem, we may generate $\mathbf{B}_J^{sk}$ and $\mathbf{B}_J^{pk}$ as follows:
  - Randomly generate a vector $\mathbf{v}$ within distance s of $t \cdot \mathbf{e}_1$.
  - Let $\mathbf{B}_J^{sk}$ be the rotation basis of $\mathbf{v}$.
  - Let $\mathbf{B}_J^{pk}$ be the HNF of $\mathbf{B}_J^{sk}$.
- We have to choose s, t, ℓ_{Samp} to ensure that $r_{\mathrm{Dec}}/r_{\mathrm{Enc}}$ is sub-exponential.

An example instantiation of the abstract scheme

- Ring: $R = \mathbb{Z}[x]/(f(x))$, $f(x) = x^n - 1$, $\gamma_{\text{Mult}} \le \sqrt{n}$.
- Ideal: $I = (2) = 2\mathbb{Z}^n$. $\mathbf{B}_I = (2\mathbf{e}_1, \ \ldots, \ 2\mathbf{e}_n)$. $r_{\text{Enc}} \le 2n + 2n^{3/2}$.
- Plaintext space: (a subset of) $\{(x_1, \ \ldots, \ x_n) : x_i \in \{0, -1\}\}$.
- Samp_1: samples uniformly in $\mathbb{Z}^n \cap \mathcal{B}(n)$.
- $\text{Samp}(\mathbf{B}_I, \boldsymbol{\pi})$: $\boldsymbol{\pi} + 2\mathbf{r}$ with $\mathbf{r} \leftarrow \text{Samp}_1$.
- Ideal: J

How good is it?

- An improvement over previous work.
- Boneh-Goh-Nissim (2005):
  - quadratic formulas with any number of monomials.
  - plaintext space: $\log \lambda$ bits for security prameter λ.
- Gentry (2009):
  - polynomials of degree $\log n$.
  - plaintext space: larger.
- Not bootstrappable yet!

Why not bootstrappable?

- Decryption $\left(\psi - \mathbf{B}_J^{\mathrm{sk}} \cdot \lfloor (\mathbf{B}_J^{\mathrm{sk}})^{-1} \cdot \psi \rceil\right) \bmod \mathbf{B}_I$ involves adding n vectors.
- Adding n k-bit numbers in $[0,1)$ requires a constant fan-in boolean circuit of depth $\Omega(\log n + \log k)$:
  - 3-for-2: convert 3 numbers to 2 numbers with the same sum; this can be done with a circuit of constant depth, say depth c.
  - It takes a circuit of depth $\approx c \log_{3/2} n$ to convert n numbers to 2 numbers with the same sum.
  - It needs depth $\Omega(\log k)$ to add the final two numbers.
- The proposed scheme permits circuits of depth $O(\log n)$.

Tweak 1 to simplify the decryption circuit

- Tweak: Narrow the permitted circuits from $\mathcal{B}(r_{\text{Dec}})$ ot $\mathcal{B}(r_{\text{Dec}}/2)$.
- Purpose: To ensure that the ciphertexts vectors are closer to the lattice J than they strictly need to be, so that less precision is needed to ensure the correctness of decryption.
- Allowing the coefficients of $(\mathbf{B}_J^{\text{sk}})^{-1} \cdot \psi$ to be very close to half-integrgs (i.e., ψ very close to the sphere of $\mathcal{B}(r_{\text{Dec}})$) would require high precision (large k) to ensure correct rounding.

- Lemma: If ψ is a valid ciphertext after tweak 1, i.e., $\|\psi\| < r_{\text{Dec}}/2$, then each coefficient of $(\mathbf{B}_J^{\text{sk}})^{-1} \cdot \psi$ is within $1/4$ of an integer.
- With Tweak 1, we can reduce the precision to $O(\log n)$ bits, and cut the the circuit depth of adding n numbers to $\Omega(\log n + \log\log n) = \Omega(\log n)$.
- The new maximum depth of permitted circuits is $\log\log\left(r_{\text{Dec}}/2\right) - \log\log\left(\gamma_{\text{Mult}} \cdot r_{\text{Enc}}\right)$, almost the same as the original depth, which can be as large as $O(\log n)$.
- Unfortunately, the constant hidden in $\Omega(\log n)$ is >1, while that in $O(\log n)$ <1. So, still not bootstrappable.

Tweak 2, optional, more technical, less essential

- Tweak: Modify $\text{Decrypt}(sk, \psi)$ from

  $$\left(\psi - \mathbf{B}_J^{\text{sk}} \cdot \lfloor (\mathbf{B}_J^{\text{sk}})^{-1} \cdot \psi \rceil\right) \bmod \mathbf{B}_I \;\Rightarrow\; \left(\psi - \lfloor \mathbf{v}_J^{\text{sk}} \times \psi \rceil\right) \bmod \mathbf{B}_I$$

  for some vector $\mathbf{v}_J^{\text{sk}} \in J^{-1}$.

- Purpose: To reduce the secret key size (as well as public key size in bootstrapping) and per-gate computation in decryption (from matrix-vector mult to ring mult).

- To use this tweak, we will need to replace

$$\mathcal{B}(r_{\text{Dec}}) \;\Rightarrow\; \mathcal{B}\left(2 \cdot r_{\text{Dec}} / (n^{1.5} \gamma_{\text{Mult}}{}^{2} \|\mathbf{B}_I\|)\right)$$

Decryption complexity of the tweaked scheme

- Decrypt(sk, ψ): $\pi \leftarrow \left(\psi - \lfloor \mathbf{v}_J^{\text{sk}} \times \psi \rceil\right) \bmod \mathbf{B}_I$
  - If Tweak 2 is used, $\mathbf{B}_J^{\text{sk1}} = \mathbf{I}$ and $\mathbf{B}_J^{\text{sk2}}$ is some rotation matrix, otherwise, $\mathbf{B}_J^{\text{sk1}} = \mathbf{B}_J^{\text{sk}}$ and $\mathbf{B}_J^{\text{sk2}} = \left(\mathbf{B}_J^{\text{sk}}\right)^{-1}$.
- Split the computation of decryption into three steps:
  - Step 1: Generate n vectors $\mathbf{x}_i$ with sum $\mathbf{B}_J^{\text{sk2}} \cdot \psi$.
  - Step 2: From the n vectors $\mathbf{x}_i$, generate integer vectors $\mathbf{y}_1, \ldots, \mathbf{y}_n, \mathbf{y}_{n+1}$ with sum $\lfloor \sum \mathbf{x}_i \rceil$.
  - Step 3: Compute $\pi \leftarrow \left(\psi - \mathbf{B}_J^{\text{sk1}} \cdot \sum \mathbf{y}_i\right) \bmod \mathbf{B}_I$.

Plaintext space

- As a somewhat homomorphic scheme, Gentry's scheme provides a large plaintext space, $R \bmod \mathbf{B}_I = P(\mathbf{B}_I)$.
- However, in order to make the scheme bootstrappable, Gentry has to limit the plaintext space to $\{0,1\} \bmod \mathbf{B}_I$.
- Evaluate evaluates $\bmod \mathbf{B}_I$-circuits. For bootstrapping, the decryption circuit must be composed of $\bmod \mathbf{B}_I$-gates.
- Ordinary boolean operations can be esaily emulated with $\bmod \mathbf{B}_I$ operations.

Decryption complexity of the tweaked scheme

- Decrypt(sk, ψ): $\pi \leftarrow \left(\psi - \mathbf{B}_J^{\text{sk1}} \cdot \lfloor \mathbf{B}_J^{\text{sk2}} \cdot \psi \rceil\right) \bmod \mathbf{B}_I$
  - If Tweak 2 is used, $\mathbf{B}_J^{\text{sk1}} = \mathbf{I}$ and $\mathbf{B}_J^{\text{sk2}}$ is some rotation matrix, otherwise, $\mathbf{B}_J^{\text{sk1}} = \mathbf{B}_J^{\text{sk}}$ and $\mathbf{B}_J^{\text{sk2}} = \left(\mathbf{B}_J^{\text{sk}}\right)^{-1}$.
- Split the computation of decryption into three steps:
  - Step 1: Generate n vectors $\mathbf{x}_i$ with $\sum \mathbf{x}_i = \mathbf{B}_J^{\text{sk2}} \cdot \psi$.
  - Step 2: From the n vectors $\mathbf{x}_i$, generate integer vectors $\mathbf{y}_1, \ldots, \mathbf{y}_n, \mathbf{y}_{n+1}$ with $\sum \mathbf{y}_i = \lfloor \sum \mathbf{x}_i \rceil$.
  - Step 3: Compute $\pi \leftarrow \left(\psi - \mathbf{B}_J^{\text{sk1}} \cdot \sum \mathbf{y}_i\right) \bmod \mathbf{B}_I$.

Squashing the Decryption Circuit

Squashing

- A technique to lower the complexity of the decryption circuit, so as to make the encryption scheme bootstrapable.
- Basic idea is to split the decryption algorithm into two phases:
  - computationally intensive, secret-key independent, by the encrypter.
  - computationally lightweight, secret-key dependent, by the decrypter :
- Properties: Does not reduce the evaluation capacity (i.e., the set of permitted circuits remains the same), but may potentially weakens security.

Squashing: generic version

- $\mathcal{E}^*$: the original encryption scheme.
- $\mathcal{E}$: to be constructed from $\mathcal{E}^*$ using two algorithms,

  SplitKey and ExpandCT.

- KeyGen(λ): $(pk^*, sk^*) \leftarrow \text{KeyGen}^*(\lambda)$

  $$(pk, sk) \leftarrow \text{SplitKey}(pk^*, sk^*)$$

  where sk is the (new) secret key and $pk := (pk^*,\ \tau)$.

- $\text{Encrypt}(pk, \pi)$: $\psi^* \leftarrow \text{Encrypt}^*(pk^*, \pi)$

  $$x \leftarrow \text{ExpandCT}(pk, \psi^*)$$ //heavy use of τ//

  $$\psi \leftarrow (\psi^*, x)$$

- Decrypt(sk, ψ): decrypts ψ^* making use of sk^* and x.

  It is desired that Decrypt(sk, ψ) works whenever Decrypt*(sk^*, ψ^*) does.

- Add(pk, ψ_1, ψ_2): $(\psi_1^*, \psi_2^*) \leftarrow$ extracted from (ψ_1, ψ_2)

$$\psi^* \leftarrow \text{Add}^*(pk^*, \psi_1^*, \psi_2^*)$$

$$x \leftarrow \text{ExpandCT}(pk, \psi^*)$$

$$\psi \leftarrow (\psi^*, x)$$

- Mult(pk, ψ_1, ψ_2): similar.

Squash: concrete scheme

- Let $\mathcal{E}^*$ be the encryption scheme with Tweak 2. Let $\mathbf{v}_J^{sk^*}$ be the secret key, which is an element of the fractional ideal J^{-1}. Recall the decryption equation:

$$\pi := \left(\psi^* - \left\lfloor \mathbf{v}_J^{sk^*} \times \psi^* \right\rceil\right) \bmod \mathbf{B}_I$$

- Let $\mathbf{t}_i \in_u J^{-1} \bmod \mathbf{B}_I$, $i \in U$. //uniformly generate a set of $\mathbf{t}_i$ //

- Let $S \subset U$ be a sparse subset s.t. $\sum_{i \in S} \mathbf{t}_i = \mathbf{v}_J^{sk^*} \bmod \mathbf{B}_I$

- SplitKey(pk^*, sk^*):

$$\tau := \{\mathbf{t}_i\}_{i \in U}. \quad pk := (pk^*, \ \tau). \quad sk := S \ \text{(encoding of } S\text{)}.$$

- ExpandCT(pk, ψ^*): //recall $pk = (pk^*, \tau)$//
  - Compute $\mathbf{c}_i := \mathbf{t}_i \times \psi^* \mod \mathbf{B}_I$ for $i \in U$.
  - The expanded ciphertext is $\psi := \left(\psi^*, \{\mathbf{c}_i\}_{i \in U}\right)$.

- Decrypt(pk, ψ):
  - Recall $\pi := \left(\psi^* - \left\lfloor \mathbf{v}_J^{sk^*} \times \psi^* \right\rceil\right) \mod \mathbf{B}_I$
  - Recall $\mathbf{v}_J^{sk^*} \equiv \sum_{i \in S} \mathbf{t}_i \mod \mathbf{B}_I$.
  - Thus, $\mathbf{v}_J^{sk^*} \times \psi^* \equiv \sum_{i \in S} \mathbf{t}_i \times \psi^* \equiv \sum_{i \in S} \mathbf{c}_i \mod \mathbf{B}_I$.
  - Thus, $\pi := \left(\psi - \left\lfloor \sum_{i \in S} \mathbf{c}_i \right\rceil\right) \mod \mathbf{B}_I$.