PVSS

December 1, 2023

1 Encryption scheme

Let $\mathbb{F}$ be a finite field of order q, k a parameter. Denote by $\chi_\beta^{m\times n}$ the distribution over matrices in $\mathbb{F}^{m\times n}$ where each entry of the matrix is $\leq \beta$. Let:

- n be the number of parties in the protocol.
- m the size of the secret to be shared (to each party).
- k be a LWE parameter.
- ℓ be the encoding redundancy.
- s, e be some integers.

$\mathsf{Encode}(\mathbf{x} \in \mathbb{F}^t)$:
1. Set $\Delta := \lfloor \sqrt[\ell]{q} \rfloor$.
2. For $i \in [t]$, set $\Delta(x_i) := (x_i, \Delta x_i, \ldots, \Delta^{\ell-1} x_i)$.
3. Return $\begin{bmatrix} \Delta(x_1) \\ \vdots \\ \Delta(x_t) \end{bmatrix} \in \mathbb{F}^{t\ell}$.

$\mathsf{Setup}()$:
1. Sample $\mathbf{A} \leftarrow \mathbb{F}^{k\times k}$.
2. Return $\mathbf{A}$.

$\mathsf{KeyGen}_i(\mathbf{A})$ (this is key generation for party i):
1. Sample $\mathbf{S}_i \leftarrow \chi_s^{m\ell\times k}$.
2. Sample $\mathbf{E}_i \leftarrow \chi_e^{m\ell\times k}$.
3. Set $\mathbf{B}_i := \mathbf{S}_i \mathbf{A}_i + \mathbf{E}_i \in \mathbb{F}^{m\ell\times k}$.
4. Set $\mathsf{pk}_i := \mathbf{B}_i, \mathsf{sk}_i := \mathbf{S}_i$

$\mathsf{Enc}((\mathsf{pk}_1, \ldots, \mathsf{pk}_n), \mathbf{x} \in \mathbb{F}^{mn})$:
1. Set $\mathbf{B} := \begin{bmatrix} \mathbf{B}_1 \\ \vdots \\ \mathbf{B}_n \end{bmatrix} \in \mathbb{F}^{mn\ell\times k}$.
2. Set $\mathbf{x} := \mathsf{Encode}(\mathbf{x}) \in \mathbb{F}^{nm\ell}$.
3. Sample $\mathbf{r} \leftarrow \chi_s^k$.
4. Sample $\mathbf{e}_1 \leftarrow \chi_e^k$, $\mathbf{e}_2 \leftarrow \chi_e^{mn\ell}$.
5. Set $\mathbf{c}_1 := \mathbf{A}\mathbf{r} + \mathbf{e}_1 \in \mathbb{F}^k$.

6. Set $\mathbf{c}_2 := \mathbf{B}\mathbf{r} + \mathbf{e}_2 + \mathbf{x} \in \mathbb{F}^{mn\ell}$.
7. Parse $\mathbf{c}_2$ as $(\mathbf{d}_1, \ldots, \mathbf{d}_n)$ where $\mathbf{d}_i \in \mathbb{F}^{m\ell}$.
8. Return $(\mathbf{c}_1, (\mathbf{d}_1, \ldots, \mathbf{d}_n))$.

$\mathsf{Dec}_i(\mathbf{S}_i, (\mathbf{c}_1, \mathbf{d}_i))$:
1. Set $\mathbf{x}' := \mathbf{d}_i - \mathbf{S}_i\mathbf{c}_1 \in \mathbb{F}^{m\ell}$.
2. Do an approximate decryption to recover the share from $\mathbf{x}'$.