Implementation of BFV in Microsoft SEAL

Ryan Orendorff, Sunscreen

Microsoft SEAL implements the BFV encryption scheme in a manner slightly different than how it is defined in textbook BFV. One change not mentioned in the SEAL manual is that the encryption equation is different.

For the following:

- n is the polynomial modulus degree.
- q is the ciphertext modulus.
- p is the plaintext modulus.
- c is a ciphertext consisting of m components $c_0, c_1, \ldots, c_{m-1}$, each $\mathbb{Z}[X]_q/(x^n + 1)$.
- m is a plaintext polynomial $\mathbb{Z}[X]_p/(x^n + 1)$.
- p is a public key consisting of two components p_0 and p_1.
- u is a noise term drawn from $\mathcal{R}_3^n$ (i.e coefficients in $\{-1, 0, 1\}$)
- e is a set of noise terms drawn from the centered binomial distribution with a standard deviation of 3.2 and with degree n. In practice this polynomial has coefficients in the range of $[-32, 32]$. To match textbook BFV, this is numbered from $e_1, e_2, \ldots, e_m$.
- Δ is the floored ratio of the ciphertext to plaintext modulus, or $\text{floor}(q/t)$.

The textbook BFV equation for a fresh encryption of a message is as follows.

$$
\begin{aligned}
c_0 =& \Delta m + p_0 u + e_1 \\
c_1 =& p_1 u + e_2
\end{aligned}
$$

Instead of using Δ, SEAL performs the following operation for encrypting the first component of the ciphertext.

$$c_0 = \left\lfloor \frac{qm + \left\lfloor \frac{t+1}{2} \right\rfloor}{t} \right\rfloor + p_0 u + e_1$$

This is equivalent to the following operation (the operation actually performed by SEAL)

$$c_0 = \Delta m + \lfloor \text{frac}(q/t) m \rceil + p_0 + e_1$$

where frac is the fractional left over from q/t and can be defined as $\text{frac}(y) = y - \text{floor}(y)$ for non-negative y. For convenience we often call this remainder $r = \lfloor \text{frac}(q/t)m \rceil$. Note that $0 \leq r < t$.

This formulation allows us to write the BFV encryption method as a matrix equation, which is useful for integration with the short discrete log proof (SDLP).

$$\begin{bmatrix} \Delta & 1 & p_0 & 1 & 0 \\ 0 & 0 & p_1 & 0 & 1 \end{bmatrix} \begin{bmatrix} m \\ r \\ u \\ e_1 \\ e_2 \end{bmatrix} = \begin{bmatrix} c_0 \\ c_1 \end{bmatrix}$$

Integration with Short Discrete Log Proof

In the short discrete log proof, we prove linear relations of the following form in zero knowledge.

$$AS = T$$

where A and T are publically known matrices of polynomials, and S is the secret knowledge matrix the prover would like to demonstrate they know without revealing S. Since our BFV equation is in this form, we can map directly to A, S, and T.

$$\begin{aligned} \begin{bmatrix} \Delta & 1 & p_0 & 1 & 0 \\ 0 & 0 & p_1 & 0 & 1 \end{bmatrix} \begin{bmatrix} m \\ r \\ u \\ e_1 \\ e_2 \end{bmatrix} &= \begin{bmatrix} c_0 \\ c_1 \end{bmatrix} \\ AS &= T \end{aligned}$$

This allows us to prove that the ciphertext is well formed in zero knowledge. We can also prove that multiple ciphertexts are well formed by adding more columns to S and T.