HOMOMORPHIC ENCRYPTION

JUSTIN SAHS

1. Correctness of the Somewhat Homomorphic Scheme

Definition. A somewhat homomorphic scheme is said to be *correct* if $D_{\mathcal{E}}(E_{\mathcal{E}}(m)) = m$, and for $c_i = E_{\mathcal{E}}(m_i)$, $D_{\mathcal{E}}(V_{\mathcal{E}}(C, \langle c_0, \ldots, c_n \rangle)) = C(\langle m_0, \ldots, m_n \rangle)$.

Lemma 1.1. *If c is output from $E_{\mathcal{E}}(m)$, then $c = a \cdot p + (2b+m)$ where $|2b+m| < p$.*

Proof. From Lemma A.1, $c = a \cdot p + (2b + m)$ for some a and b such that $|2b + m| \leq \tau 2^{\rho+3}$. Then,

$$\begin{aligned}
|2b + m| &\leq \tau 2^{\rho+3} \\
&= \gamma\omega(\log \lambda)2^{\rho+3} \\
&= \gamma\omega(\log \lambda)2^{\omega(\log \lambda)} \\
&= \omega(\eta^2 \log \lambda)\omega(\log \lambda)2^{\omega(\log \lambda)} \\
&= \omega(\rho\Theta(\lambda \log^2 \lambda) \log \lambda)\omega(\log \lambda)2^{\omega(\log \lambda)} \\
&= \omega(\omega(\log \lambda)\Theta(\lambda \log^2 \lambda) \log \lambda)\omega(\log \lambda)2^{\omega(\log \lambda)} \\
&= \omega(\lambda \log^5 \lambda 2^{\log \lambda})
\end{aligned}$$

Additionally,

$$\begin{aligned}
p &= \omega(2^{\eta}) \\
&= \omega(2^{\rho\Theta(\lambda \log^2 \lambda)}) \\
&= \omega(2^{\omega(\log \lambda)\Theta(\lambda \log^2 \lambda)}) \\
&= \omega(2^{\lambda \log^3 \lambda})
\end{aligned}$$

so we have

$$2^{\log \lambda} \leq |2b + m| \leq 2^{\log^2 \lambda}$$

so $|2b + m| < 2^{\lambda \log^3 \lambda} \leq p$. $\square$

Theorem 1.2. $\mathcal{E}$ *is correct.*

Proof. From Lemma 1.1 and Lemma A.2, we have that

$$\begin{aligned} m' &\leftarrow (c \bmod p) \bmod 2 \\ &= 2b + m \bmod 2 \\ &= m \bmod 2 \\ &= m \end{aligned}$$

for any $c = E_{\mathcal{E}}(m)$ or $c = V_{\mathcal{E}}(C, \langle c_0, \ldots, c_n \rangle)$, so the scheme is correct. $\square$

2. Correctness of the Fully Homomorphic Scheme