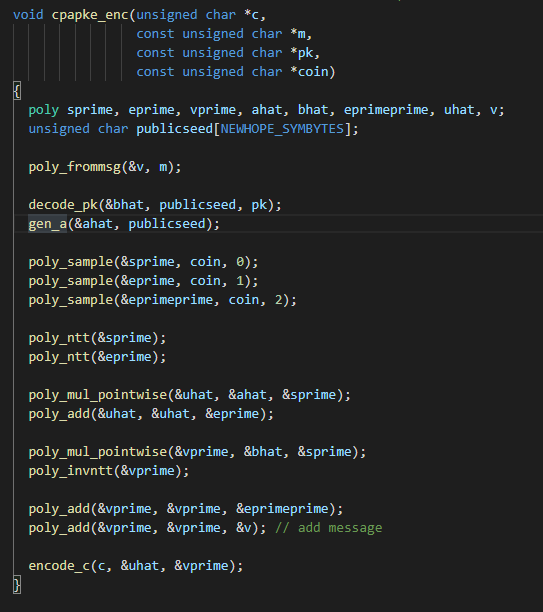
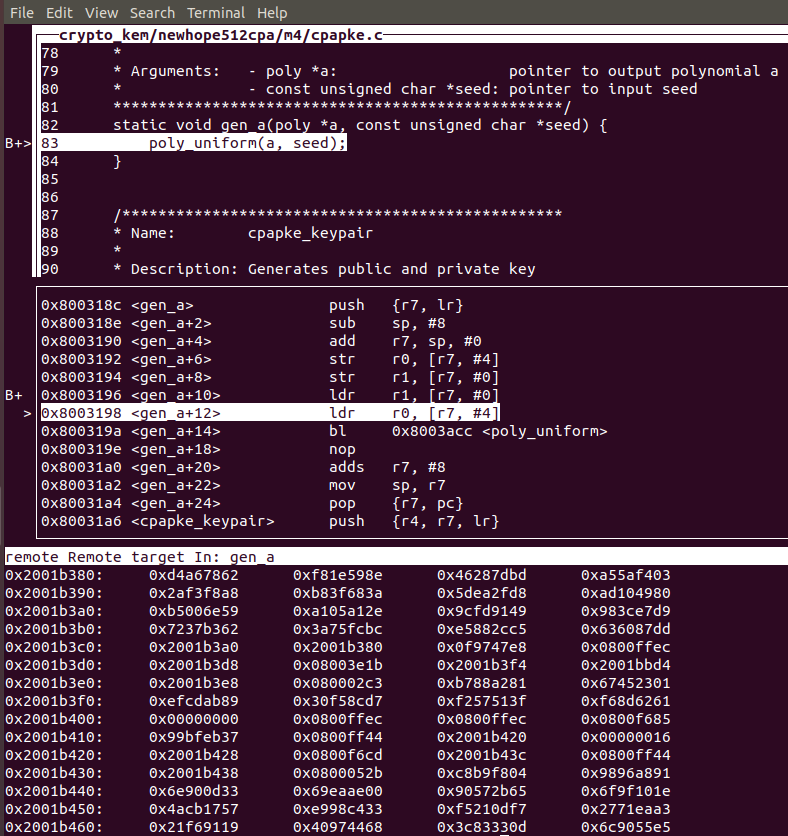
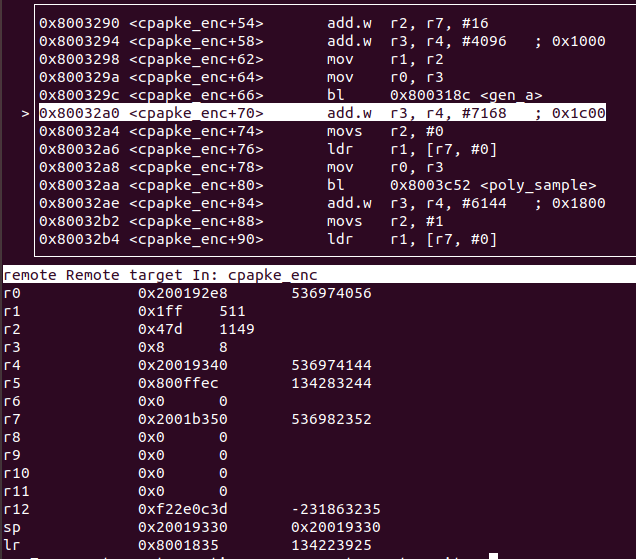
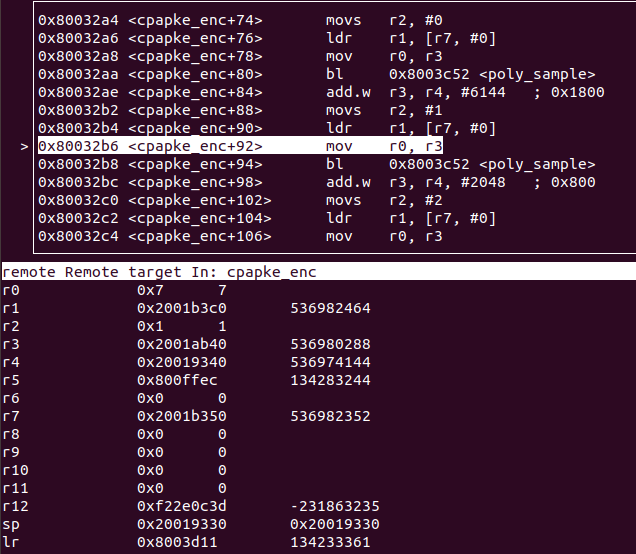
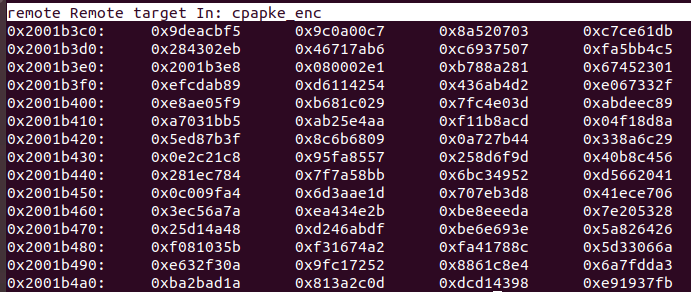
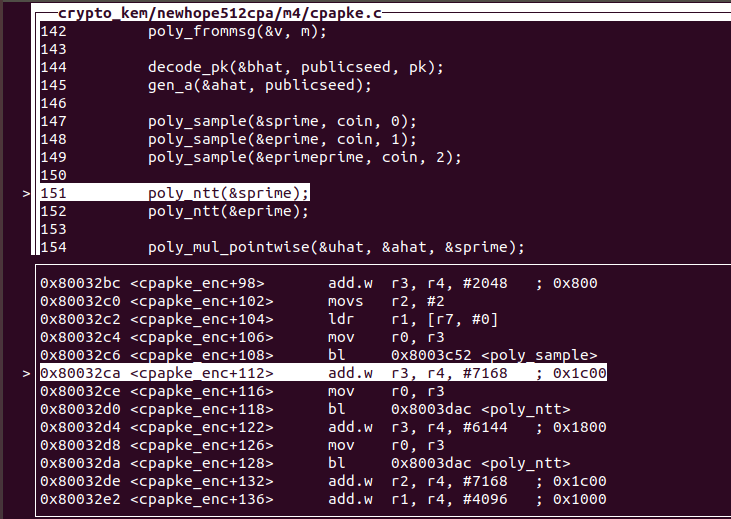
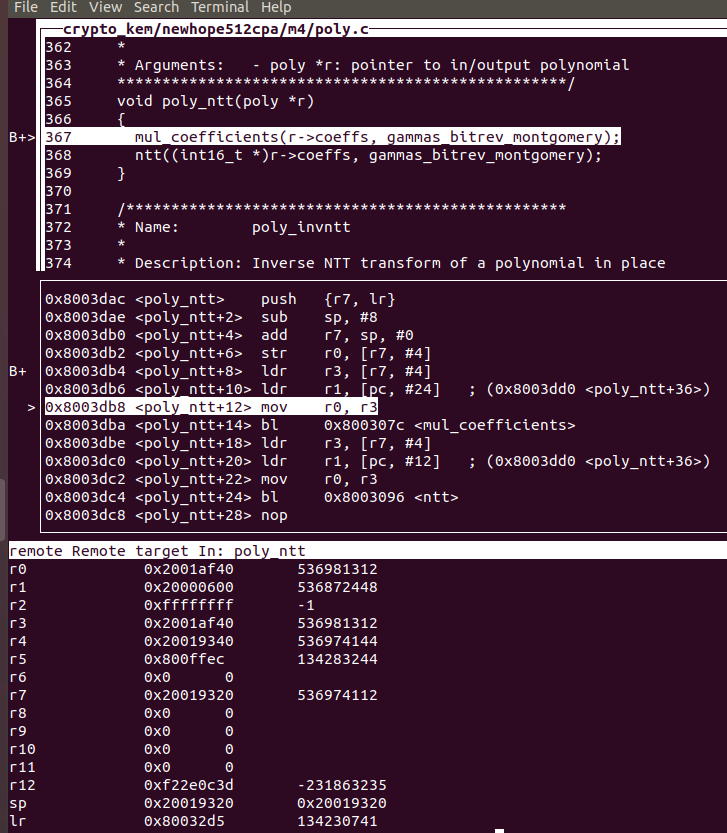
1. To see the ldr instructions before NTT
2. In cpapke\_enc function, I set the breakpoint at gen\_a  
     
   

So in the function to generate a, there is a load instruction about r1, which load r1 with   
0x2001b380. While in 0x2001b400 there is an all zero data.  
I also check the value r7, which value is 0x20019320, and in 20019330 there has an all zero data.

1. Then after gen\_a, the value in r1 changed too  
     
   It seems that in gen\_a there are other instructions use r1 to store some data?
2.   
   After gen\_a is poly\_sample. Every time after poly\_sample there is a ldr of r1. While this time the r1 changed to 0x2001b3c0 not 0x2001b380  
   
3. After poly\_sample, r1 changed to 0x200190f8  
   again there is no zero data  
   
4. And then again go into the poly\_ntt function and we have already checked.  
     
   And at this point we may need to check practically if we can load the wrong data in r1 before and after the mul\_coefficients and ntt.  
   The main idea is that we need to find some ldr instructions that could load wrong address to r1 so that the twiddle in the ntt function might load wrong values like all zero. And we can go on the analysis.