Cryptographie
Attaques par canaux auxilliaires

December 18, 2023

1 Attaque temporelle sur RSA

Le but de cette section est de mettre en pratique l'attaque temporelle vu en cours sur l'algorithme *double-and-add*. La figure 1 présente un fragment du code des fonctions de réduction et d'exponentiation modulaire utilisées par le programme `sign_rsa`. Le code source est disponible dans le fichier `modexp.c`.

Écrire un programme permettant de retrouver la clé secrète utilisée par le programme `sign_rsa` pour signer des messages. Les paramètres publics sont donnés dans le fichier `rsa.h`

```
void montg_red(...){
  ...
  mpz_fdiv_r_2exp(temp1,T,r);
  mpz_mul(temp1,temp1,n1);
  mpz_fdiv_r_2exp(temp1,temp1,r);
  mpz_mul(temp2,temp1,n);
  mpz_add(temp1,T,temp2);
  mpz_fdiv_q_2exp(t,temp1,r);
  if (mpz_cmp(t,n) > 0){
    mpz_sub(t,t,n);
  ...
}
```

```
void modexp(...)
{
  ...
  for (int i=len-1; i>=0; i--){
    mpz_mul(Y,Y,Y);
    montg_red(Y,Y,n,r,n1);
    if (mpz_tstbit(k,i)){
      mpz_mul(Y,Y,X);
      montg_red(Y,Y,n,r,n1);
    }
  }
  ...
}
```

Figure 1: Fragment du code source du programme `sign_rsa`