MysteryTwister C3
THE CRYPTO CHALLENGE CONTEST

Lunchtime Attack on the Fully Homomorphic Encryption Scheme

Author: Coen Ramaekers

January 2011

Introduction

The Fully Homomorphic Encryption Scheme as presented by Gentry and Halevi [GH2010] turns out to be vulnerable to so called lunchtime attacks [LMSV2010]. This means that an adversary which has access to an oracle which can decrypt ciphertexts can recover the private key by decrypting carefully chosen ciphertexts.

Because one can use such an oracle, this type of attack is often referred to as a lunchtime attack, since in practise one might be able to abuse the secretholder's computer while he is out for lunch.

The Scheme (Very Short)

To thoroughly explain the scheme is out of scope for this challenge. In addition, full knowledge of the scheme has no advantage in solving the challenge. The attack to be used will be fully explained. The plaintext space of this scheme is only a single bit, and a ciphertext as produced by the scheme will be an integer $c \in [0, d)$, for some d which is publically known.

So any integer chosen in this interval will be decrypted by the oracle to either 0 or 1. The decryption is computed by $(c * w \mod d) \mod 2$, where the modulo d operation maps to the interval $[-d/2, d/2)$. So the only knowledge required for decryption is the integer w.

The Attack

It can be shown that w lies in the interval $[0, d)$. So at first, we select a lower- and upperbound $L = 0$ and $U = d - 1$. Next we will narrow this interval until $L = U = w$.

This can be done by the algorithm given on the right side.

```
$L \leftarrow 0$, $U \leftarrow d - 1$
while $U - L > 1$ do
    $c \leftarrow \lfloor d/(U - L) \rfloor$
    $b \leftarrow \mathcal{O}_D(c)$
    $q \leftarrow (c + b) \mod 2$
    $k \leftarrow \lfloor Lc/d + 1/2 \rfloor$
    $B \leftarrow (k + 1/2) * d/c$
    if $(k \mod 2 = q)$ then
        $U \leftarrow \lfloor B \rfloor$
    else
        $L \leftarrow \lceil B \rceil$
    end if
end while
return $L$
```

The Challenge

Attached in the zip archive to this challenge, one will find the value for d (public.txt), this is the only further information required to find the secret key. The oracle is available as cgi script via `http://www.mysterytwisterc3.org/cgi-bin/mtc3-ramae-11-homomorphic.cgi`. If one for instance wants to decrypt the ciphertext "1234", one queries the oracle by appending "?c=1234" to the url.

It is advisable to automate the oracle requests, since one might require numerous. Also within the zip archive, one will find a series of encrypted bits (cipher.txt). These bits form a message in ASCII, which is the answer to this challenge.

References

- Craig Gentry and Shai Halevi. Implementing Gentry's Fully-Homomorphic Encryption Scheme. Manuscript, 2010. https://researcher.ibm.com/researcher/view_project.php?id=1579

- J. Loftus and A. May and N.P. Smart and F. Vercauteren. On CCA-Secure Fully Homomorphic Encryption. Cryptology ePrint Archive, Report 2010/560, 2010. http://eprint.iacr.org/2010/560