MysteryTwister C3
THE CRYPTO CHALLENGE CONTEST

Recovering the Private Key in the Fully Homomorphic Encryption Scheme

Author: Coen Ramaekers

January 2011

Introduction

The Fully Homomorphic Encryption (FHE) scheme as described by Gentry and Halevi [GH2010] works mainly because the private key is included in the public key. This enables the scheme to “refresh” ciphertexts by decrypting and re-encrypting homomorphically. A downside on this property is obviously that the private key might be extracted from the public key.

To prevent this, the private key is added in the form of a sparse subset sum. The inability of an adversary to extract the private key from the public key is related to the Sparse Subset Sum Problem (SSSP). This problem states that it is computationally infeasible to determine whether or not a sparse subset of a large set of integers sums up to zero or another predetermined value.

Relation between FHE and SSSP

In the FHE scheme, the private key is a single integer, called w. For security reasons, w and the numbers in the given large set are very big. To reduce the size a bit, the large set is subdivided into s smaller sets, called $\mathcal{B}_k$. Each of these sets contains S integers. They are generated by geometric progressions, i.e. $\mathcal{B}_k = \{x_k \cdot R^i \mod d : i = 0, \dots, S-1\}$, for $k = 1, \dots, s$.

Now there exists a sum, consisting of s integers taken from distinct $\mathcal{B}_k$, which sums up to $w \mod d$. In other words, there exists a s-dimensional vector σ such that $\sum_{k=1}^{s} x_k \cdot R^{\sigma_k} = w \mod d$. This is in relation to SSSP, but instead of having a large set of integers and a known result, we have a large set of integers (the union of the $\mathcal{B}_k$) and an unknown result (w). As additional information one knows that the sum contains exactly one element out of each of the smaller sets $\mathcal{B}_k$.

Additional information

But there is more information included in the public key. To be able to use the private key in the scheme, it should be known "homomorphically". This means that using homomorphic operations, the private key can be reconstructed while everything remains encrypted. Therefore, c-dimensional vectors $\eta(k)$ (for $k = 1, \ldots, s$) are created. For these vectors, it holds that

$$\sum_{i=0}^{c} \sum_{j=i+1}^{c} \eta(k)_i \cdot \eta(k)_j \cdot \left((i-1) \cdot c - \binom{i}{2} + (j-i-1) \right) = \sigma_k, \quad (1)$$

$$\text{for } k = 1, \ldots, s.$$

Furthermore, exactly two of the entries for each $\eta(k)$ are non-zero and equal 1. Now every entry of these vectors are encrypted under the public key. The resulting vectors with these encrypted entries are called $\bar{\eta}(k)$.

The Challenge

The challenge is to reconstruct the private key from the public key by finding the vector σ which yields w. All the information to reconstruct the private key is given in the public key, so it is theoretically possible, but practically infeasible.

In this challenge, the following parameters are used:

S:	512
s:	15
c:	46
R:	67108864

The Challenge

In the zip archive for this challenge d (d.txt), the x_k (x(1).txt - x(15).txt), and the encrypted vectors $\bar{\eta}(k)$ (eta(1).txt - eta(15).txt) are given. One can verify the solution by decrypting the vectors $\bar{\eta}(k)$, equation 1 should hold. Decryption of a ciphertext c is given by $(c \cdot w \mod d) \mod 2$, where the modulo d operation results in the interval $[-d/2, d/2)$.

The answer to the challenge is the vector σ, with the entries seperated by commas and no spaces. For instance, if $\sigma = (1, 2, 3)$, the answer would be "1,2,3".

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