Cryptology ePrint Archive: Report 2013/057

CRT-based Fully Homomorphic Encryption over the Integers

Jinsu Kim and Moon Sung Lee and Aaram Yun and Jung Hee Cheon

Abstract: In 1978, Rivest, Adleman and Dertouzos introduced the basic concept of privacy homomorphism that allows computation on encrypted data without decryption. It was elegant work that precedes the recent development of fully homomorphic encryption schemes although there were found some security flaws, e.g., ring homomorphic schemes are broken by the known-plaintext attacks. In this paper, we revisit one of their proposals, in particular the third scheme which is based on the Chinese Remainder Theorem and is ring homomorphic. The previous result is that only a single pair of known plaintext/ciphertext can break this scheme. However, by exploiting the standard technique to insert an error to a message before encryption, we can cope with this problem. We present a secure modification of their proposal by showing that the proposed scheme is fully homomorphic and secure against the chosen plaintext attacks under the decisional approximate GCD assumption {{and the sparse subset sum assumption}} when the message space is restricted to $\Z_2^k$.

Interestingly, the proposed scheme can be regarded as a generalization of the DGHV scheme with larger plaintext. Our scheme has $\tilde{O}(\lambda^5)$ overhead while the DGHV has ${\tilde{O}}(\lambda^8)$ for the security parameter λ. When restricted to the homomorphic encryption scheme with depth-$O(\log \lambda)$, the overhead is reduced to $\tilde{O}(\lambda)$. Our scheme can be used in applications requiring a large message space $\Z_Q$ for $\log Q=O(\lambda^4)$ or SIMD style operations on $\Z_Q^k$ for $\log Q=O(\lambda), k=O(\lambda^3)$, with $\tilde{O}(\lambda^5)$ ciphertext size as in the DGHV.

Category / Keywords: public-key cryptography / privacy homomorphism, Chinese remainder theorem, homomorphic encryption, approximate gcd, DGHV

Date: received 5 Feb 2013

Contact author: kjs2002 at snu ac kr