An extension of the NTRU Cryptosystem

Shutaro Inoue & Yosuke Sato

We propose an extension of the public-key Cryptosystem NTRU reported in [2].

NTRU is constructed with unary polynomial rings as follows.
Let n be a natural number and p, q be prime numbers such that p is relatively-small and q is much bigger than p(denoted $q \gg p$). Z_p and Z_q denote finite Galois fields with characteristic p and q. We abuse the notation $\langle x^n - 1 \rangle$ to denote both the ideals generated by $x^n - 1$ in unary polynomial rings $Z_p[x]$ and $Z_q[x]$. A plain text space is a residue class ring $Z_p[x]/\langle x^n - 1 \rangle$. A cipher text space is a residue class ring $Z_q[x]/\langle x^n - 1 \rangle$. A public key H is an element of $Z_q[x]/\langle x^n - 1 \rangle$. Using a random element R of $Z_q[x]/\langle x^n - 1 \rangle$. An encryption function f of NTRU is constructed as follows.

$$\begin{array}{rccc} f: & Z_p[x]/\langle x^n-1\rangle & \to & Z_q[x]/\langle x^n-1\rangle \\ & \cup & & \cup \\ & M & \mapsto & pHR+M \end{array}$$

An extension of NTRU is studied in [4]. They extend NTRU using multivariate polynomial rings as follows.
Let $\bar{x}$ denote variables $x_1, \cdots, x_m$. Let p and q be prime numbers such that $q \gg p$. Let $f_1, \cdots, f_l$ be polynomials in $Z[\bar{x}]$. Considering $f_1, \cdots, f_l$ both as elements of $Z_p[\bar{x}]$ and as elements of $Z_q[\bar{x}]$, we abuse the notation I to denote both the ideals in $Z_p[\bar{x}]$ and $Z_q[\bar{x}]$ generated by $f_1, \cdots, f_l$. A plain text space is a residue class ring $Z_p[\bar{x}]/I$. A cipher text space is a residue class ring $Z_q[\bar{x}]/I$. A public key H is an element of $Z_q[\bar{x}]/I$. Using a random element R of $Z_q[x]/P$. An encryption function f is constructed as follows.

$$\begin{array}{rccc} f: & Z_p[\bar{x}]/I & \to & Z_q[\bar{x}]/I \\ & \cup & & \cup \\ & M & \mapsto & pHR+M \end{array}$$

In both NTRU and the above extension, they use the same generating polynomials. In our extension, we use different sets of generating polynomials for the ideals of two residue class rings. Our Cryptosystem is constructed as follows.
Let p, q and $\bar{x}$ be the same as above. Let $f_1, \cdots, f_l$ be polynomials in $Z[\bar{x}]$. Considering $f_1, \cdots, f_l$ as elements of $Z_p[\bar{x}]$, let P denote the ideal generated by them in $Z_p[\bar{x}]$. Let Q be an ideal in $Z_q[\bar{x}]$ which satisfies certain properties. A plain text space is a residue

class ring $Z_p[\bar{x}]/P$. A cipher text space is a residue class ring $Z_q[\bar{x}]/Q$. A public key H is an element of $Z_q[\bar{x}]/Q$. Using a random element $r_1, \cdots, r_l$ of $Z_q[\bar{x}]/Q$.

$$\begin{array}{rccc} f: & \underset{\cup}{Z_p[\bar{x}]/P} & \rightarrow & \underset{\cup}{Z_q[\bar{x}]/Q} \\ & M & \mapsto & H\sum_{i=1}^{l} f_i r_i + M \end{array}$$

We give a sufficient condition for the above "certain properties" which is feasible for a public-key Cryptosystem. One of the most important benefit for using two generating sets of polynomials is that we can increase the number of random polynomials for encryption and improve the security from a brute-force attack. We also show that our extension obtains a better security from Lattice attacks.

References

[1] D. Coppersmith and A. Shamir, "Lattice attacks on NTRU", EUROCRYPT 1997, Lecture Notes in Computer Science, Vol. 1233, 1997, pp. 52–61.

[2] J. Hoffstein, J. Pipcher and J. Silverman, "NTRU: A Ring-Based Public Key Cryptosystem", CRYPTO 1996, Lecture Notes in Computer Science, Vol. 1423, 1998, pp. 267–288.

[3] J. Hoffstein, J. Pipher, and J. Silverman, "NTRUSIGN:Digital signatures using the NTRU lattice", CT-RSA 2003, Lecture Notes in Computer Science, Vol. 2612, 2003, pp. 122–140.

[4] M. Caboara, F. Caruso and C. Traverso, "Groebner bases for public key cryptography", Proceedings of the twenty-first international symposium on Symbolic and algebraic computation(ISSAC '08), pp 315-323, ACM Press, 2008.