Inversions of New Hope

Ian Malloy, Dennis Hollenbeck
Eigenexus, Inc.
Anchorage AK, US

Abstract

Introduced as a new protocol implemented in "Chrome Canary" for the Google Inc. Chrome browser, "New Hope" is engineered as a post-quantum key exchange for the TLS 1.2 protocol. The structure of the exchange is a combination of elliptic curve enhancements along with revised lattice-based cryptography. New Hope incorporates the key-encapsulation mechanism of Peikert which itself is a modified Ring-LWE scheme. The search space used to introduce the closest-vector problem is generated by an intersection of a tesseract and hexadecachoron, or the ℓ_∞-ball and ℓ_1-ball respectively. This intersection results in the 24-cell $\mathcal{V}$ of lattice $\mathcal{D}_4$. With respect to the density of the Voronoi cell $\mathcal{V}$, the proposed mitigation against backdoor attacks proposed by the authors of New Hope may not provide complete security against such attacks.

Keywords:

Oracle inversion; New Hope; cryptanalysis; post-quantum cryptography

1 Introduction

"New Hope" is a novel encryption scheme based on lattice cryptography and offers post-quantum security within the key exchange. New Hope uses a Montgomery form to reduce cost of implementation in terms of computational speed. As a modification to elliptic curve cryptography New Hope instead reduces cost by sending an *x*-coordinate to compute the relative *x*-coordinate of any scalar [1]. Alkim, et al. implement a rounding function $\lfloor x \rceil$ derived from the work of Peikert [2] to achieve equality with the floor function $\lfloor x + 1/2 \rfloor$. This floor function is an element of integers. New Hope employs $q = 12289$ and $n = 1024$ as constraints of lattice D_4, which results in a reduction of the modulus to $q = 12289 < 2^{14}$ [1]. Peikert defines both the rounding and floor function of New Hope, using δ sub-Gaussian and zeta functions [2]. Peikert's "canonical embedding" necessarily incorporates a homomorphic injective ring that maps (K) to $(\mathbb{C})$ which fixes pointwise$(\mathbb{Q})$ [2].

The critical nature of an unbiased modular operation presents key values which are assumed to mitigate cryptanalysis. Peikert recommends the use of small noise values to achieve this result while cautioning against cross-rounding given the determinacy that may result [2]. Any such determinacy negates an otherwise unbiased result. It is here that New Hope diverges from its basis on Peikert's work.

The creators of New Hope outline a sketch to create a backdoor in implementations of NTRU lattice-based cryptography. Concerns of a backdoor capability extended to New Hope will now be addressed in detail.

2 Parameters

The fixed parameter of (a) may potentially facilitate constructing a backdoor, using methods similar to NTRU trapdoors [1]. For mildly small values of (f, g) such that $f = g, f = 1 \bmod p$ for some prime, $(p \geq 4 * 16 + 1)$ there is a point of weakness within the set

$$a = g\frac{1}{f} \bmod q$$

With respect to $(a, b = as + e)$, it is possible to compute:

$$bf = afs + fe = gs + fe \bmod q$$

such that:

$$bf = gs + fe \bmod q$$

With small enough (g, s, f, e), computing $gs + fe \in \mathbb{Z}$ once $(s \bmod q)$ is obtained proves the scheme is then corrupted. After establishing $t = s + e \bmod p$, with the coefficient of (s) and
(e) smaller than(16), the values of (s, e) have sums within the range $(-2 * 16, 2 * 16)$. Knowing the values of (s, e) within the range of $(-2 * 16, 2 * 16)$ in terms of:

$$\bmod p \geq 4 * 16 + 1$$

is knowing them in $\mathbb{Z}$. The manipulation to create a backdoor relies on the *pseudo-inverse* of a polynomial (p) as the polynomial $(P \in \mathcal{P})$ such that $(P * p * s \equiv s \bmod q)$ for any polynomial $(s \in \mathcal{P})$ such that

$$s(1) \equiv 0 \bmod q$$

If the secret key equation can be modified to equal

$$t \equiv h * v + w \bmod q$$

it is feasible to apply a pseudo-inversion. For a detailed analysis of inversion oracles refer to the primary source of Mol and Yung [3]. Through implementing the attack developed by Mol and Yung it is possible to show that an attacker possessing both a classical and quantum computer is capable of a backdoor attack against New Hope.

3 Inversion

Given the new secret key equation derived from [3], let the following hold:

$(w = u - g), (v = F)$ for
$t \equiv u - p_q * h (\bmod q)$

$(v = u - F), (w = g)$ for

$$t \equiv p_q h + hu (\bmod q)$$

In both cases, (w, v) are binary. An oracle will output the correct key pair only when $\left(e \in E_{q,h}^{d_r}\right)$ [3]. To apply this inversion the anti-derivative of the Peikert scheme used by New Hope must be established. Per the authors of New Hope, the implementation of the key encapsulation method (KEM) relies on pseudorandom ring elements exchanged between Alice and Bob which are then used to derive the session key [1]. Alice then employs the ring element $(us = ass' + e's)$ and Bob uses $(v = bs' + e'' = ass' + es' + e'')$. The reconciliation function is $\mathrm{rec}(w, b)$ such that

$$\mathrm{rec}(w, b) = \begin{cases} 0, & \text{if } w \in I_b + E (\bmod q) \\ 1, & \text{otherwise} \end{cases}$$

The authors of New Hope set as parameters of the polynomial ring,

$$\mathcal{R}_q = \frac{\mathbb{Z}_q[X]}{X^n + 1}$$

The message sent by Alice is denoted as(b), while Bob's response is(u, r) and an element of the ring (R_q). The polynomial $(a \in \mathcal{R}_q)$ is public and constant in NTRU schemes. To generate the function which results in$(s \bmod q)$, the algebraic manipulation itself is straightforward. To begin deriving the necessary function to generate the secret key for an NTRU scheme, a pre-established value equal to $s \bmod q$ is introduced:

$$as - s * \left(\frac{1}{a} - 1\right) = s \bmod q$$

Via substitution, values of the variables (a, b) already provided are used to calculate values of t.

$$(a, b) = as + e$$
$$as - s = b - t$$

After trivial algebraic manipulations, the values of t can be equated to a set of equations, wherein the value of the constant (a) can be substituted with previously afforded values given in [1].

$$t = \begin{cases} -as + s + b \\ s + e \bmod p \end{cases}$$

Returning to the equations used to calculate t, new values of t are now substituted and the two previous equations are calculated as equal.

$$\left((as - s) * \left(\frac{1}{a} - 1\right) = (b - t) * \left(\frac{1}{a} - 1\right)\right)$$

Where $(a = fg^{-1} \bmod q)$ it is then possible to assert $(as - s + t = b)$, which in turn produces the primary equation for solving the value of $s \bmod q$.
By producing an equation that results in a required value for a backdoor attack against some NTRU lattice-based cryptography, the equation of $\left((as - s) * \left(\frac{1}{a-1}\right) = s \bmod q\right)$ generates the final steps to calculating the secret (s). Using substitution yet again, but this time of the variable a, one derives:

$$\left((fg^{-1} \bmod q)s - s\right) * \left(\frac{1}{fg^{-1} \bmod q - 1}\right) = s \bmod q$$

By simplifying the equation, we then produce:

$$\frac{(fg^{-1} \bmod q)s - s}{(fg^{-1} \bmod q) - 1} = s \bmod q$$

By stating the division in an alternate form, one then has:

$$s = s \bmod q$$

The value of the variable (q) is itself equivalent to $1 \bmod 2n$. Bearing in mind that $n = 1024$, it is known that $q \equiv 1 \bmod 2048$. An abbreviated integer table of equivalent values to $1 \bmod q$ is provided in Table 1.

2049	4097	6145
8193	10241	12289
14337	16385	18433

Table 1

The anti-derivative, or indefinite integral pertinent to this analysis is defined by the variable a which is equal to $fg^{-1} \bmod q$, which produces the equation:

$$\int \frac{\left(f\left(\frac{1}{g}\right) \bmod q\right)s - s}{\left(f\left(\frac{1}{g}\right) \bmod q\right) - 1} \mathrm{d}g = gs + \text{constant}$$

Returning to the exchange between Alice and Bob, Alice uses the equation $(us = ass' + e's)$ to send Bob a message, which Bob then uses the equation $(v = bs' + e'' = ass' + es' + e'')$ to reconcile the pair with. If the equation of

$$(s = s \bmod q)$$

can be shown to equal $\left(t \equiv h * v + w (\bmod q)\right)$, then an oracle output to break the encryption is feasible. The further constraint of $\left(e \in E_{q,h}^{d_r}\right)$ is also required. Returning to the values produced by(t), let (t) be equal to the following

$$t = \begin{cases} -as + s + b \\ s + e \bmod p \end{cases}$$

To satisfy the constraint of the variable (e) as a member of $(E_{q,h}^{d_r})$ and with the value of (q) known, one can substitute for (e) accordingly. Where (d_r) corresponds to the Hamming weights to produce an inversion oracle against NTRU [2], New Hope employs a weight value of $\left(\exp\left(\frac{-x^2}{2\sigma^2}\right)\right)$ to all integers (x) such that there is no fixed value for (a) [1], but rather each coefficient of (a) is chosen uniformly at random from $\mathbb{Z}_q$. The discrete Gaussian distribution $(D_{\mathbb{Z},\sigma})$ is parametrized by the Gaussian parameter $(\sigma \in \mathbb{R})$ defined by the previously mentioned weight of all (x). The values of $(\mathbb{Z}_q)$ for an integer $(q > 1)$ must be within the quotient ring $(\frac{\mathbb{Z}}{q\mathbb{Z}})$ such that $\mathcal{R} = \frac{\mathbb{Z}[X]}{X^n+1}$ is the ring of integer polynomials modulo $X^n + 1$ where each coefficient is reduced modulo (q).

4 Algebraic Analysis

With the intersection Voronoi $\mathcal{V}$ 24-cell treated as a convex polytope, the 16-cell ℓ_1-ball is a simplicial polytope while the ℓ_∞-ball together with the 16-cell are the only regular Euclidean 4-space tessellations. Given these parameters, the 24-cell constructed as a Voronoi tessellation having center at D_4 for any point x is expressed as:

$$x_i \in \mathbb{Z}^4 : \sum_i x_i \equiv 0 \bmod 2$$

If, for any $x_i = s$ there is some point where $s(1) \equiv 0 \bmod q$, the introduction of an inversion oracle is then verified.

Treating the lattice $\widetilde{D_2}$ as a binary field extension of the approximate *x*-coordinates, the binary field characteristic is thus two given the use of a Montgomery form for optimization of [1]. This characteristic of two implies that the binary field extension thus has order 2^n for n. Given that $q = 12289$ is equivalent to $q \equiv 1 \bmod 2n$, any treatment of the Voronoi cell in terms of the reduced lattice $\widetilde{D_2}$ must be shown to commute to the lattice in 4 dimensions.

Bearing in mind that once an attacker can compute:

$$[(b-t)*(a-1)^{-1} = (as-s)*(a-1)^{-1}]$$
$$=$$
$$s \bmod q$$

the attacker can then recover the secret key. We believe we have demonstrated such a calculation of $s \bmod q$, leaving only the treatment of *e* to be demonstrated.

We begin by treating *e* over the range of *x*-coordinates. For $b = as + e$, we easily derive $-e = \frac{as}{b}$. For the characteristic two, any element is also its additive inverse, thus $e = \frac{as}{b}$. Substituting the value of *e* for Voronoi coordinates *x*, we then find $x = \frac{as}{b}$ is equivalent to $x = \frac{(as+e)s}{as+e}$ as previously demonstrated. This trivially reduces to $x = s$, but more importantly results in $x - s = 0$. Using the property of additive inverse again, we then rephrase the equation as $-s - s = 0$. Thus, $-2s = 0$.

Returning to mod q, as derived, we may reduce the equation $-2s = 0$ with respect to modulo q. The inversion constraints of $(v = u - f)$ and $(w = g)$ with respect to:

$$t \equiv hv + w \bmod(q)$$

are adjusted via substitutions of *w* for g, and *v* with $u - f$, we return to the equivalent form of $s \bmod q$ and derive:

$$\frac{(fw^{-1} \bmod q)s - s}{(fw^{-1} \bmod q) - 1}$$

To continue we replace $u - f$ with $u - f = u - f$ and then simply subtract *u* from each side, leaving $-f = -f$. By additive inverse, we then have $f = f$ and may proceed as before. Using the *pseudo*-inverse polynomial (P, p) we proceed by using the expression $s \bmod q$ congruent to $P * p * s$. Allowing the polynomial p as an element of the ring R_q, and deriving u via substitution of $v = u - f$ as done for f we may begin constructing the expression congruent to t by adding p_q and u.

We now must demonstrate recovery (s, e) with respect to the range:

$$\bmod p \geq 4 * 16 + 1$$

Having isolated x equal to s and then showing $-2s = 0$, we apply the additive inverse to produce $-s - s = s + s$. We now have

$$s + s = 0 = s(1 + 1)$$

For a coefficient of *x* resulting in $e \bmod p$, the weight of $\exp \frac{x^2}{2\sigma^2}$ then satisfies the constraint of $e \in E_{q,h}^{d_r}$ is satisfied. Knowing $t = s + e \bmod p$, and with knowledge of public key h, we then compute $hv + w \bmod q$. Allowing $q = 2$, per the constraint of values $\mathbb{Z}_q$ for $q > 1$ with respect to $f = 1 \bmod p$ for

$$s = s \bmod q \equiv s \bmod 2$$

Using $\mathrm{rec}(w, b)$ as a function of *s*, such that: $s(w)\colon I_b + E(\bmod q)$ and assuming a zero is returned. This existence necessarily relies on $s(w)$, for any instance in which the output is not zero, then the value of one is returned for $s(w)$ during reconciliation. Having shown $x = s$, and with knowledge of *b* as values of *(a,s,e)* we may substitute values as demonstrated in this work to isolate:

$$s(1) = s = s \bmod \mathrm{q} \equiv s \bmod 2$$
$$=$$
$$0 \bmod 2$$

5 Conclusion

The anti-derivative provided opens the possibility to manipulate the secret (s) while simultaneously using the variable (g) substituted for (x) in addition to some constant. This constant added to the variables (s, g) based upon the traditionally fixed value of NTRU, though applied against New Hope facilitates an inversion of the scheme. The vectors of (x) and relative approximate coordinates are shown equivalent to e for known *s*.

References

[1] E. Alkim, L. Ducas, T. Poppelman and P. Schwabe, "Post-quantum key exchange - a new hope," *International Association for Cryptologic Research,* 2015.

[2] C. Peikert, "Lattice Cryptography for the Internet," in *Post-Quantum Cryptography*, Waterloo, Springer International Publishing, 2014, pp. 197-219.

[3] P. Mol and M. Yung, "Recovering NTRU Secret Key from Inversion Oracles," in *Public Key Cryptography - PKC 2008*, Barcelona, Springer Berlin Heidelberg, 2008, pp. 18-36.

[4] A. O. Pittenger, An Introduction to Quantum Computing Algorithms, Birkhauser, 2000.

[5] M. Boyer, G. Brassard, P. Hoeyer and A. Tapp, "Tight bounds on quantum searching," in *Proc. of the Workshop on Physics of Computation: PhysComp'96*, 2006.

[6] W. Castryck, S. Galbraith and R. R. Farashahi, "Efficient arithmetic on elliptic curves using a mixed Edwards Montgomery representation," *IACR Cryptology ePrint Archive,* p. 218, 2008.

[7] J. W. Bos, C. Costello, M. Naehrig and D. Stebila, "Post-Quantum Key Exchange for the TLS Protocol from the Ring Learning with Errors Problem," in *2015 IEEE Symposium on Security and Privacy*, San Jose, 2015.

[8] United States of America Department of Commerce, "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions," National Institute of Standards and Technology, 2015.

7 Appendix – IBMQASM 1.1 Code

```
h q[0]; h
q[1]; x q[2]; s
q[0]; cx q[1],
q[2]; t q[3];
cx q[0], q[2];
s q[3]; x q[0];
z q[1]; s q[2];
tdg q[3]; cx
q[0], q[2]; id
q[3]; cx q[1],
q[2]; h q[0];
h q[1]; h
q[2]; x q[0]; x
q[1]; x q[2];
cx q[0], q[2];
h q[0]; cx
q[1], q[2]; s
q[2]; h q[2];
tdg q[2]; h
q[2];
measure
q[0];
measure
q[1];
measure
q[2];
measure
q[3];
measure
q[4];
```