Remarks on Quaternions/Octonion Based Diffie-Hellman Key Exchange Protocol Submitted to NIST PQC Project[*]

Yongge Wang
Department of SIS, UNC Charlotte, USA
and
Qutaibah m. Malluhi
Department of Computer Science, Qatar University, Qatar.

December 26, 2017

Abstract

In November 2017, Juan edro Hecht and Jorge Alejandro Kamlofsky submitted a quaternions/octonions based Diffie-Hellman key agreement protocol HK17 to NIST post quantum cryptography project. Daniel J. Bernstein and Tanja Lange showed how to break the scheme in $O(p)$ steps where p is the modulo used in the scheme. One may wonder whether the scheme could be secure if p is sufficiently large (e.g., p is 1000 bits long)? In this note, we show that the scheme could be broken by solving a homogeneous quadratic equation system of eight equations in four unknowns. Thus no matter how big the p it is, it could be trivailly broken using Kipnis and Shamir's relinearization techniques.

1 Octonions

The HK17 protocol [3] submitted to NIST is based on quaternions and octonions. To simplify our discussion, we only discuss the octonions based HK17 in this note. Octonion (see, e.g., Baez [1]) is the largest among the four normed division algebras: real numbers $\mathbb{R}$, complex numbers $\mathbb{C}$, quaternions $\mathbb{H}$, and octonions $\mathbb{O}$. The real numbers have a complete order while the complex numbers are not ordered. The quaternions are not commutative and the octonions are neither commutative nor associative. Quaternions were invented by Hamilton in 1843. Octonions were invented by Graves (1844) and Cayley (1845) independently.

In mathematics, a vector space commonly refers to a finite-dimensional module over the real number field $\mathbb{R}$. An algebra A refers to a vector space that is equipped with a multiplication map $\times : A^2 \to A$ and a nonzero unit $1 \in A$ such that $1 \times a = a \times 1 = a$. The multiplication $a \times b$ is usually abbreviated as $a \cdot b$ or ab. An algebra A is a division algebra if, for any $a, b \in A$, $ab = 0$ implies either $a = 0$ or $b = 0$. Equivalently, A is a division algebra if and only if the operations of left and right multiplication by any nonzero element are invertible. A normed division algebra is an algebra that is also a normed vector space with $\|ab\| = \|a\|\|b\|$.

An algebra is power-associative if the sub-algebra generated by any single element is associative and an algebra is alternative if the sub-algebra generated by any two elements is associative. It is straightforward to show that if the sub-algebra generated by any three elements is associative, then the algebra itself is associative. Artin's theorem states that an algebra is alternative if and only if for all $a, b \in A$, we have

$$(aa)b = a(ab), \qquad (ab)a = a(ba), \qquad (ba)a = b(aa).$$

[*] The work reported in this note was done when the first author is visiting Qatar University. The work is supported by Qatar Foundation Grants NPRP8-2158-1-423 and NPRP X-063-1-014.

It is well known that $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$ are the only normed division algebras and $\mathbb{O}$ is an alternative division algebra. It is also known that division algebras can only have dimension 1, 2, 4, or 8.

Using the same approach of interpreting a complex number $a + bi$ as a pair $[a, b]$ of real numbers, quaternions $\mathbb{H}$ (respectively, octonions $\mathbb{O}$) can be constructed from $\mathbb{C}$ (respectively, from $\mathbb{H}$) using the Cayley-Dickson construction formula $[a, b]$ where $a, b \in \mathbb{C}$ (respectively, $a, b \in \mathbb{H}$). The addition and multiplication are defined as follows.

$$[a, b] + [c, d] = [a + c, b + d], \quad [a, b][c, d] = [ac - db^*, a^*d + cb] \tag{1}$$

where $a, b, c, d \in \mathbb{C}$ (respectively, $a, b, c, d \in \mathbb{H}$) and a^* is the conjugate of a. Specifically, the conjugate of a real number a is defined as $a^* = a$ and the conjugate of a complex number or a quaternion number $[a, b]$ is defined by $[a, b]^* = [a^*, -b]$. Throughout the paper, we will use the following notations for real and imaginary part of an octonion $\mathbf{a} \in \mathbb{O}$,

$$\text{Re}(\mathbf{a}) = (\mathbf{a} + \mathbf{a}^*)/2 \in \mathbb{R}, \qquad \text{Im}(\mathbf{a}) = (\mathbf{a} - \mathbf{a}^*)/2.$$

It is straightforward to check that for a complex number (or a quaternion or an octonion), we have

$$[a, b][a, b]^* = [a, b]^*[a, b] = \|[a, b]\|^2[1, 0].$$

Thus all of $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$ are division algebras (that is, each non-zero element has a multiplicative inverse). Though Cayley-Dickson construction provides a nice approach to study normed division algebras systematically, it is more intuitive to use vectors in $\mathbb{R}^4$ to denote quaternion numbers and vectors in $\mathbb{R}^8$ to denote octonion numbers.

Each octonion number is a vector $\mathbf{a} = [a_0, \cdots, a_7] \in \mathbb{R}^8$. The norm of an octonion $\mathbf{a} = [a_0, \cdots, a_7]$ is defined as $\|\mathbf{a}\| = \sqrt{a_0^2 + \cdots + a_7^2}$. By the inductive Cayley-Dickson construction, the conjugate of an octonion $\mathbf{a}$ is $\mathbf{a}^* = [a_0, -a_1, \cdots, -a_7]$ and the inverse is $\mathbf{a}^{-1} = \mathbf{a}^*/\|\mathbf{a}\|^2$.

For each octonion number $\mathbf{a} = [a_0, \cdots, a_7]$, let $\alpha = [a_1, \cdots, a_7]$ and

$$B_{\mathbf{a}} = \begin{pmatrix} a_0 & a_4 & a_7 & -a_2 & a_6 & -a_5 & -a_3 \\ -a_4 & a_0 & a_5 & a_1 & -a_3 & a_7 & -a_6 \\ -a_7 & -a_5 & a_0 & a_6 & a_2 & -a_4 & a_1 \\ a_2 & -a_1 & -a_6 & a_0 & a_7 & a_3 & -a_5 \\ -a_6 & a_3 & -a_2 & -a_7 & a_0 & a_1 & a_4 \\ a_5 & -a_7 & a_4 & -a_3 & -a_1 & a_0 & a_2 \\ a_3 & a_6 & -a_1 & a_5 & -a_4 & -a_2 & a_0 \end{pmatrix}$$

Using the matrix $B_{\mathbf{a}}$, we can define two associated 8×8 matrices

$$A^l_{\mathbf{a}} = \begin{pmatrix} a_0 & \alpha \\ -\alpha^T & B_{\mathbf{a}} \end{pmatrix} \quad \text{and} \quad A^r_{\mathbf{a}} = \begin{pmatrix} a_0 & \alpha \\ -\alpha^T & B^T_{\mathbf{a}} \end{pmatrix} \tag{2}$$

Then for two octonions $\mathbf{a} = [a_0, \cdots, a_7]$ and $\mathbf{b} = [b_0, \cdots, b_7]$, we can add them as $\mathbf{a}+\mathbf{b} = [a_0+b_0, \cdots, a_7+b_7]$ and multiply them as $\mathbf{ab} = \mathbf{b}A^l_{\mathbf{a}} = \mathbf{a}A^r_{\mathbf{b}}$. We also note that

$$A^l_{\mathbf{a}^{-1}} = \frac{1}{\|\mathbf{a}\|^2} \begin{pmatrix} a_0 & -\alpha \\ \alpha^T & B^T_{\mathbf{a}} \end{pmatrix} \quad \text{and} \quad A^r_{\mathbf{a}^{-1}} = \frac{1}{\|\mathbf{a}\|^2} \begin{pmatrix} a_0 & -\alpha \\ \alpha^T & B_{\mathbf{a}} \end{pmatrix} \tag{3}$$

In the following, we first present some properties of the two associate matrices. For any octonion $\mathbf{a} = [a_0, \cdots, a_7]$, it is straightforward to show that

$$B_{\mathbf{a}}\alpha^T = B^T_{\mathbf{a}}\alpha^T = a_0\alpha^T \tag{4}$$

and

$$\begin{array}{rcl} B_{\mathbf{a}}B_{\mathbf{a}} &=& \alpha^T\alpha - \|\mathbf{a}\|^2\mathbf{I}_{7\times 7} + 2a_0B_{\mathbf{a}} \\ B_{\mathbf{a}}^TB_{\mathbf{a}}^T &=& \alpha^T\alpha - \|\mathbf{a}\|^2\mathbf{I}_{7\times 7} + 2a_0B_{\mathbf{a}}^T \\ B_{\mathbf{a}}B_{\mathbf{a}}^T &=& -\alpha^T\alpha + \|\mathbf{a}\|^2\mathbf{I}_{7\times 7} \\ B_{\mathbf{a}}^TB_{\mathbf{a}} &=& -\alpha^T\alpha + \|\mathbf{a}\|^2\mathbf{I}_{7\times 7} \end{array} \tag{5}$$

Thus we have

$$\begin{array}{rcl} A_{\mathbf{a}}^lA_{\mathbf{a}}^r &=& \begin{pmatrix} a_0^2 - \alpha\alpha^T & a_0\alpha + \alpha B_{\mathbf{a}}^T \\ -a_0\alpha^T - B_{\mathbf{a}}\alpha^T & -\alpha^T\alpha + B_{\mathbf{a}}B_{\mathbf{a}}^T \end{pmatrix} \\ &=& \begin{pmatrix} a_0^2 - \alpha\alpha^T & a_0\alpha + \alpha B_{\mathbf{a}}^T \\ -a_0\alpha^T - B_{\mathbf{a}}^T\alpha^T & -\alpha^T\alpha + B_{\mathbf{a}}^TB_{\mathbf{a}} \end{pmatrix} \\ &=& A_{\mathbf{a}}^rA_{\mathbf{a}}^l \\ &=& \begin{pmatrix} a_0^2 - \alpha\alpha^T & 2a_0\alpha \\ -2a_0\alpha^T & -\alpha^T\alpha + B_{\mathbf{a}}B_{\mathbf{a}}^T \end{pmatrix} \end{array} \tag{6}$$

By substituting (5) into (6), we get

$$\begin{array}{rcl} A_{\mathbf{a}}^lA_{\mathbf{a}}^r &=& A_{\mathbf{a}}^rA_{\mathbf{a}}^l \\ &=& \begin{pmatrix} 2a_0^2 - \|\mathbf{a}\|^2 & 2a_0\alpha \\ -2a_0\alpha^T & -2\alpha^T\alpha + \|\mathbf{a}\|^2\mathbf{I}_{7\times 7} \end{pmatrix} \end{array} \tag{7}$$

Similarly, we can get

$$\begin{array}{rcl} A_{\mathbf{a}}^lA_{\mathbf{a}}^l &=& \begin{pmatrix} a_0^2 - \alpha\alpha^T & a_0\alpha + \alpha B_{\mathbf{a}} \\ -a_0\alpha^T - B_{\mathbf{a}}\alpha^T & -\alpha^T\alpha + B_{\mathbf{a}}B_{\mathbf{a}} \end{pmatrix} \\ &=& \begin{pmatrix} 2a_0^2 - \|\mathbf{a}\|^2 & 2a_0\alpha \\ -2a_0\alpha^T & 2a_0B_{\mathbf{a}} - \|\mathbf{a}\|^2\mathbf{I}_{7\times 7} \end{pmatrix} \\ &=& 2a_0A_{\mathbf{a}}^l - \|\mathbf{a}\|^2\mathbf{I}_{8\times 8} \end{array} \tag{8}$$

and

$$\begin{array}{rcl} A_{\mathbf{a}}^rA_{\mathbf{a}}^r &=& \begin{pmatrix} a_0^2 - \alpha\alpha^T & a_0\alpha + \alpha B_{\mathbf{a}} \\ -a_0\alpha^T - B_{\mathbf{a}}\alpha^T & -\alpha^T\alpha + B_{\mathbf{a}}^TB_{\mathbf{a}}^T \end{pmatrix} \\ &=& \begin{pmatrix} 2a_0^2 - \|\mathbf{a}\|^2 & 2a_0\alpha \\ -2a_0\alpha^T & 2a_0B_{\mathbf{a}}^T - \|\mathbf{a}\|^2\mathbf{I}_{7\times 7} \end{pmatrix} \\ &=& 2a_0A_{\mathbf{a}}^r - \|\mathbf{a}\|^2\mathbf{I}_{8\times 8} \end{array} \tag{9}$$

Finally, it is easy to check that

$$A_{\mathbf{a}}^lA_{\mathbf{a}^{-1}}^l = A_{\mathbf{a}^{-1}}^lA_{\mathbf{a}}^l = A_{\mathbf{a}}^rA_{\mathbf{a}^{-1}}^r = A_{\mathbf{a}^{-1}}^rA_{\mathbf{a}}^r = \mathbf{I}_{8\times 8}.$$

But generally, we have $A_{\mathbf{a}}^lA_{\mathbf{a}^{-1}}^r \neq \mathbf{I}_{8\times 8}$. We conclude this section with the following theorem that will be used frequently throughout this paper.

Theorem 1.1 *For* $\mathbf{a} \in \mathbb{O}$*, we have* $\mathbf{a}^2 = 2\mathrm{Re}(\mathbf{a})\mathbf{a} - \|\mathbf{a}\|^2\mathbf{1}$ *where* $\mathbf{1} = [1, 0, 0, 0, 0, 0, 0, 0]$.

Proof. The identity $\mathbf{a}^* = 2\mathrm{Re}(\mathbf{a})\mathbf{1} - \mathbf{a}$ implies $\|\mathbf{a}\|^2 = \mathbf{a}\mathbf{a}^* = 2\mathrm{Re}(\mathbf{a})\mathbf{a} - \mathbf{a}^2$. □

Theorem 1.2 *For all* $\mathbf{a}, \mathbf{b} \in \mathbb{O}$*, we have* $(\mathbf{ab})^* = \mathbf{b}^*\mathbf{a}^*$.

Proof. By the fact that the octonion algebra is alternative, we have

$$(\mathbf{ab})(\mathbf{b}^*\mathbf{a}^*) = \mathbf{a}(\mathbf{bb}^*)\mathbf{a}^* = \|\mathbf{a}\|^2\|\mathbf{b}\|^2.$$

Thus $(\mathbf{ab})^{-1} = (\mathbf{b}^*\mathbf{a}^*)/(\|\mathbf{a}\|^2\|\mathbf{b}\|^2)$. Since $(\mathbf{ab})^{-1} = (\mathbf{ab})^*/(\|\mathbf{ab}\|^2)$, the theorem is proved. □

Theorem 1.3 *(Moufang identities [2]) Let* $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{O}$*. Then we have*

$$\begin{aligned}
\mathbf{c}(\mathbf{a}(\mathbf{cb})) &= ((\mathbf{ca})\mathbf{c})\mathbf{b} \\
\mathbf{a}(\mathbf{c}(\mathbf{bc})) &= ((\mathbf{ac})\mathbf{b})\mathbf{c} \\
(\mathbf{ca})(\mathbf{bc}) &= (\mathbf{c}(\mathbf{ab}))\mathbf{c} \\
(\mathbf{ca})(\mathbf{bc}) &= \mathbf{c}((\mathbf{ab})\mathbf{c})
\end{aligned}$$

2 Octonions $\mathbb{O}(\mathbb{Z}_q)$ over $\mathbb{Z}_q$ and Octonions $\mathbb{O}(\mathbb{F}_q)$ over $\mathbb{F}_q$

In the preceding section, we briefly discussed the properties of octonions. Instead of using real numbers, one may also construct "octonions" over any field $\mathbb{F}_q$ with $q = p^m$ or over any ring $\mathbb{Z}_q$ with $q = p_1^{r_1} \cdots p_m^{r_m}$. In this section, we discuss octonions $\mathbb{O}(\mathbb{Z}_q)$ over $\mathbb{Z}_q$. Generally, all theorems except division-related results for octonions hold in $\mathbb{O}(\mathbb{Z}_q)$. It is straightforward to show that $\mathbb{O}(\mathbb{Z}_q)$ is a normed algebra. However, it is not a division algebra.

An octonion $\mathbf{z} \in \mathbb{O}(\mathbb{Z}_q)$ is isotropic if $\|\mathbf{z}\|= 0$. By Theorem 6.26 in Lidl and Niederreiter [5, page 282], there are $q^7 + q^4 - q^3 = (q^4 - 1)(q^3 + 1) + 1$ isotropic vectors in $\mathbb{F}_q^8$. Let $\mathbf{a} \in \mathbb{O}(\mathbb{Z}_q)$ be a non-zero isotropic octonion. Then $\mathbf{aa}^* = \|\mathbf{a}\|^2= 0$. That is, $\mathbf{a}$ has no multiplicative inverse. It follows that $\mathbb{O}(\mathbb{Z}_q)$ is not a division algebra. This also shows that $\mathbb{O}(\mathbb{Z}_q)$ is not nicely normed. Note that an algebra over $\mathbb{Z}_q$ is nicely normed if $\mathbf{a} + \mathbf{a}^* \in \mathbb{Z}_q$ and $\mathbf{aa}^* = \mathbf{a}^*\mathbf{a} > 0$ for all non zero $\mathbf{a} \in \mathbb{O}(\mathbb{Z}_q)$.

It is straightforward that Theorem 1.1 holds for $\mathbb{O}(\mathbb{Z}_q)$. We use an alternative proof to show that Theorem 1.2 holds for $\mathbb{O}(\mathbb{Z}_q)$ also. Note that the proof of Theorem 1.2 is not valid for $\mathbb{O}(\mathbb{Z}_q)$ since it uses octonion inverse properties.

Theorem 2.1 *For all* $\mathbf{a}, \mathbf{b} \in \mathbb{O}(\mathbb{Z}_q)$*, we have* $(\mathbf{ab})^* = \mathbf{b}^*\mathbf{a}^*$.

Proof. By the definition in (2), we have $A^r_{\mathbf{a}^*} = (A^r_{\mathbf{a}})^T$. First, the identity $\mathbf{1b}^*\mathbf{a}^* = \mathbf{1}(A^r_{\mathbf{b}})^T(A^r_{\mathbf{a}})^T = \mathbf{1}(A^r_{\mathbf{a}}A^r_{\mathbf{b}})^T$ implies that $\mathbf{b}^*\mathbf{a}^*$ is the first column of $A^r_{\mathbf{a}}A^r_{\mathbf{b}}$. Secondly, the identity $\mathbf{1ab} = \mathbf{1}(A^r_{\mathbf{a}}A^r_{\mathbf{b}})$ implies that $(\mathbf{ab})^*$ is also the first column of $A^r_{\mathbf{a}}A^r_{\mathbf{b}}$. It follows that $(\mathbf{ab})^* = \mathbf{b}^*\mathbf{a}^*$. □

Finally, Theorem 1.1 implies the following result.

Theorem 2.2 *For an isotropic octonion* $\mathbf{a} \in \mathbb{O}(\mathbb{Z}_q)$*, we have* $\mathbf{a}^2 = 2\mathrm{Re}(\mathbf{a})\mathbf{a}$.

For more related discussion, the reader is referred to Wang and Malluhi [7].

3 HK17

In this section, we describe the HK17 protocol. In the HK17 proposal [3], the authors used a normalization process for octonions, it is not clear from the proposal description whether the computation will work correctly if the normalization is used. Instead, we believe the protocol is essentially based on $\mathbb{O}(\mathbb{F}_p)$ for a prime p. In the following, we first give a slightly different description of the HK17 protocol than the one in [3]. It is straightforward to show that our description is more general and the HK17 in [3] is a special case. The HK17 protocol proceeds as follows:

1. Alice chooses two octonions $\mathbf{o}_A, \mathbf{o}_B \in \mathbb{O}(\mathbb{F}_p)$ where $p = 13$ or 251 or 65521 or 4294967279.
2. Alice sends both $\mathbf{o}_A$ and $\mathbf{o}_B$ to Bob (in the public channel).
3. Alice chooses two private polynomials $f_1(x), f_2(x) \in \mathbb{F}_p[x]$ as her private key.
4. Bob chooses two private polynomials $g_1(x), g_2(x) \in \mathbb{F}_p[x]$ as his private key.
5. Alice sends $\mathbf{r}_A = f_1(\mathbf{o}_A)\mathbf{o}_B f_2(\mathbf{o}_A)$ to Bob over the public channel.
6. Bob sends $\mathbf{r}_B = g_1(\mathbf{o}_A)\mathbf{o}_B g_2(\mathbf{o}_A)$ to Alice over the public channel.
7. The shared secret is $\mathbf{k}_A = f_1(\mathbf{o}_A)\mathbf{r}_B f_2(\mathbf{o}_A)$ and $\mathbf{k}_B = g_1(\mathbf{o}_A)\mathbf{r}_A g_2(\mathbf{o}_A)$.

4 Break HK17 in $O(1)$ steps

For any given octonion $\mathbf{a} \in \mathbb{O}(\mathbb{F}_p)$, Theorem 1.1 shows that $\mathbf{a}^2 = 2\text{Re}(\mathbf{a})\mathbf{a} - \|\mathbf{a}\|^2\mathbf{1}$ where $\mathbf{1} = [1, 0, 0, 0, 0, 0, 0, 0]$. It follows that there exist $x_0, x_1, x_2, x_3, y_0, y_1, y_2, y_3 \in \mathbb{Z}_p$ such that

$$\begin{array}{c} f_1(\mathbf{o}_A) = x_0\mathbf{o}_A + x_1\mathbf{1} \\ f_2(\mathbf{o}_A) = x_2\mathbf{o}_A + x_3\mathbf{1} \\ g_1(\mathbf{o}_A) = y_0\mathbf{o}_A + y_1\mathbf{1} \\ g_2(\mathbf{o}_A) = y_2\mathbf{o}_A + y_3\mathbf{1} \end{array}$$

Since $\mathbf{r}_A = f_1(\mathbf{o}_A)\mathbf{o}_B f_2(\mathbf{o}_A)$ and $\mathbf{r}_B = g_1(\mathbf{o}_A)\mathbf{o}_B g_2(\mathbf{o}_A)$, we have

$$\begin{array}{c} \mathbf{r}_A = (x_0\mathbf{o}_A + x_1\mathbf{1})\mathbf{o}_B(x_2\mathbf{o}_A + x_3\mathbf{1}) \\ \mathbf{r}_B = (y_0\mathbf{o}_A + y_1\mathbf{1})\mathbf{o}_B(y_2\mathbf{o}_A + y_3\mathbf{1}) \end{array} \tag{10}$$

Let the observed (transmitted over public channels) values $\mathbf{o}_A, \mathbf{o}_B, \mathbf{r}_A, \mathbf{r}_B$ be as follows:

$$\begin{array}{c} \mathbf{o}_A = [o_0^A, o_1^A, o_2^A, o_3^A, o_4^A, o_5^A, o_6^A, o_7^A] \\ \mathbf{o}_B = [o_0^B, o_1^B, o_2^B, o_3^B, o_4^B, o_5^B, o_6^B, o_7^B] \\ \mathbf{r}_A = [r_0^A, r_1^A, r_2^A, r_3^A, r_4^A, r_5^A, r_6^A, r_7^A] \\ \mathbf{r}_B = [r_0^B, r_1^B, r_2^B, r_3^B, r_4^B, r_5^B, r_6^B, r_7^B] \end{array}$$

By the first identity of (10), one can establish a homogeneous quadratic equation system of eight equations in four unknowns x_0, x_1, x_2, x_3 as follows.

$$
\begin{array}{l}
[r_0^A, r_1^A, r_2^A, r_3^A, r_4^A, r_5^A, r_6^A, r_7^A] = (x_0\mathbf{o}_A + x_1\mathbf{1})\mathbf{o}_B(x_2\mathbf{o}_A + x_3\mathbf{1}) \\
= [x_0o_0^A + x_1, x_0o_1^A, x_0o_2^A, x_0o_3^A, x_0o_4^A, x_0o_5^A, x_0o_6^A, x_0o_7^A]\mathbf{o}_B[x_2o_0^A + x_3, x_2o_1^A, x_2o_2^A, x_2o_3^A, x_2o_4^A, x_2o_5^A, x_2o_6^A, x_2o_7^A] \\
= [x_0o_0^A + x_1, x_0o_1^A, x_0o_2^A, x_0o_3^A, x_0o_4^A, x_0o_5^A, x_0o_6^A, x_0o_7^A] \\
\quad \times \begin{pmatrix}
o_0^B & o_1^B & o_2^B & o_3^B & o_4^B & o_5^B & o_6^B & o_7^B \\
-o_1^B & o_0^B & -o_4^B & -o_7^B & o_2^B & -o_6^B & o_5^B & o_3^B \\
-o_2^B & o_4^B & o_0^B & -o_5^B & -o_1^B & o_3^B & -o_7^B & o_6^B \\
-o_3^B & o_7^B & o_5^B & o_0^B & -o_6^B & -o_2^B & o_4^B & -o_1^B \\
-o_4^B & -o_2^B & o_1^B & o_6^B & o_0^B & -o_7^B & -o_3^B & o_5^B \\
-o_5^B & o_6^B & -o_3^B & o_2^B & o_7^B & o_0^B & -o_1^B & -o_4^B \\
-o_6^B & -o_5^B & -o_7^B & -o_4^B & o_3^B & o_1^B & o_0^B & -o_2^B \\
-o_7^B & -o_3^B & -o_6^B & o_1^B & -o_5^B & o_4^B & o_2^B & o_0^B
\end{pmatrix} \\
\quad \times [x_2o_0^A + x_3, x_2o_1^A, x_2o_2^A, x_2o_3^A, x_2o_4^A, x_2o_5^A, x_2o_6^A, x_2o_7^A] \\
= \begin{pmatrix}
x_0o_0^Ao_0^B + x_1o_0^B - x_0o_1^Ao_1^B - x_0o_2^Ao_2^B - x_0o_3^Ao_3^B - x_0o_4^Ao_4^B - x_0o_5^Ao_5^B - x_0o_6^Ao_6^B - x_0o_7^Ao_7^B \\
x_0o_0^Ao_1^B + x_1o_1^B + x_0o_1^Ao_0^B + x_0o_2^Ao_4^B + x_0o_3^Ao_7^B - x_0o_4^Ao_2^B + x_0o_5^Ao_6^B - x_0o_6^Ao_5^B - x_0o_7^Ao_3^B \\
x_0o_0^Ao_2^B + x_1o_2^B - x_0o_1^Ao_4^B + x_0o_2^Ao_0^B + x_0o_3^Ao_5^B + x_0o_4^Ao_1^B - x_0o_5^Ao_3^B - x_0o_6^Ao_7^B - x_0o_7^Ao_6^B \\
x_0o_0^Ao_3^B + x_1o_3^B - x_0o_1^Ao_7^B - x_0o_2^Ao_5^B + x_0o_3^Ao_0^B + x_0o_4^Ao_6^B + x_0o_5^Ao_2^B - x_0o_6^Ao_4^B + x_0o_7^Ao_1^B \\
x_0o_0^Ao_4^B + x_1o_4^B + x_0o_1^Ao_2^B - x_0o_2^Ao_1^B - x_0o_3^Ao_6^B + x_0o_4^Ao_0^B + x_0o_5^Ao_7^B + x_0o_6^Ao_3^B - x_0o_7^Ao_5^B \\
x_0o_0^Ao_5^B + x_1o_5^B - x_0o_1^Ao_6^B + x_0o_2^Ao_3^B - x_0o_3^Ao_2^B - x_0o_4^Ao_7^B + x_0o_5^Ao_0^B + x_0o_6^Ao_1^B + x_0o_7^Ao_4^B \\
x_0o_0^Ao_6^B + x_1o_6^B + x_0o_1^Ao_5^B - x_0o_2^Ao_7^B + x_0o_3^Ao_4^B - x_0o_4^Ao_3^B - x_0o_5^Ao_1^B + x_0o_6^Ao_0^B + x_0o_7^Ao_2^B \\
x_0o_0^Ao_7^B + x_1o_7^B + x_0o_1^Ao_3^B + x_0o_2^Ao_6^B - x_0o_3^Ao_1^B + x_0o_4^Ao_5^B - x_0o_5^Ao_4^B - x_0o_6^Ao_2^B + x_0o_7^Ao_0^B
\end{pmatrix}^T \\
\times \begin{pmatrix}
x_2o_0^A + x_3 & x_2o_1^A & x_2o_2^A & x_2o_3^A & x_2o_4^A & x_2o_5^A & x_2o_6^A & x_2o_7^A \\
-x_2o_1^A & x_2o_0^A + x_3 & -x_2o_4^A & -x_2o_7^A & x_2o_2^A & -x_2o_6^A & x_2o_5^A & x_2o_3^A \\
-x_2o_2^A & x_2o_4^A & x_2o_0^A + x_3 & -x_2o_5^A & -x_2o_1^A & x_2o_3^A & -x_2o_7^A & x_2o_6^A \\
-x_2o_3^A & x_2o_7^A & x_2o_5^A & x_2o_0^A + x_3 & -x_2o_6^A & -x_2o_2^A & x_2o_4^A & -x_2o_1^A \\
-x_2o_4^A & -x_2o_2^A & x_2o_1^A & x_2o_6^A & x_2o_0^A + x_3 & -x_2o_7^A & -x_2o_3^A & x_2o_5^A \\
-x_2o_5^A & x_2o_6^A & -x_2o_3^A & x_2o_2^A & x_2o_7^A & x_2o_0^A + x_3 & -x_2o_1^A & -x_2o_4^A \\
-x_2o_6^A & -x_2o_5^A & -x_2o_7^A & -x_2o_4^A & x_2o_3^A & x_2o_1^A & x_2o_0^A + x_3 & -x_2o_2^A \\
-x_2o_7^A & -x_2o_3^A & -x_2o_6^A & x_2o_1^A & -x_2o_5^A & x_2o_4^A & x_2o_2^A & x_2o_0^A + x_3
\end{pmatrix}
\end{array}
\tag{11}
$$

Similarly, by the second identity of (10), one can establish a homogeneous quadratic equation system of eight equations in four unknowns y_0, y_1, y_2, y_3 as follows:

$$
\begin{array}{l}
[r_0^B, r_1^B, r_2^B, r_3^B, r_4^B, r_5^B, r_6^B, r_7^B] \\
= \begin{pmatrix}
y_0o_0^Ao_0^B + y_1o_0^B - y_0o_1^Ao_1^B - y_0o_2^Ao_2^B - y_0o_3^Ao_3^B - y_0o_4^Ao_4^B - y_0o_5^Ao_5^B - y_0o_6^Ao_6^B - y_0o_7^Ao_7^B \\
y_0o_0^Ao_1^B + y_1o_1^B + y_0o_1^Ao_0^B + y_0o_2^Ao_4^B + y_0o_3^Ao_7^B - y_0o_4^Ao_2^B + y_0o_5^Ao_6^B - y_0o_6^Ao_5^B - y_0o_7^Ao_3^B \\
y_0o_0^Ao_2^B + y_1o_2^B - y_0o_1^Ao_4^B + y_0o_2^Ao_0^B + y_0o_3^Ao_5^B + y_0o_4^Ao_1^B - y_0o_5^Ao_3^B - y_0o_6^Ao_7^B - y_0o_7^Ao_6^B \\
y_0o_0^Ao_3^B + y_1o_3^B - y_0o_1^Ao_7^B - y_0o_2^Ao_5^B + y_0o_3^Ao_0^B + y_0o_4^Ao_6^B + y_0o_5^Ao_2^B - y_0o_6^Ao_4^B + y_0o_7^Ao_1^B \\
y_0o_0^Ao_4^B + y_1o_4^B + y_0o_1^Ao_2^B - y_0o_2^Ao_1^B - y_0o_3^Ao_6^B + y_0o_4^Ao_0^B + y_0o_5^Ao_7^B + y_0o_6^Ao_3^B - y_0o_7^Ao_5^B \\
y_0o_0^Ao_5^B + y_1o_5^B - y_0o_1^Ao_6^B + y_0o_2^Ao_3^B - y_0o_3^Ao_2^B - y_0o_4^Ao_7^B + y_0o_5^Ao_0^B + y_0o_6^Ao_1^B + y_0o_7^Ao_4^B \\
y_0o_0^Ao_6^B + y_1o_6^B + y_0o_1^Ao_5^B - y_0o_2^Ao_7^B + y_0o_3^Ao_4^B - y_0o_4^Ao_3^B - y_0o_5^Ao_1^B + y_0o_6^Ao_0^B + y_0o_7^Ao_2^B \\
y_0o_0^Ao_7^B + y_1o_7^B + y_0o_1^Ao_3^B + y_0o_2^Ao_6^B - y_0o_3^Ao_1^B + y_0o_4^Ao_5^B - y_0o_5^Ao_4^B - y_0o_6^Ao_2^B + y_0o_7^Ao_0^B
\end{pmatrix}^T \\
\times \begin{pmatrix}
y_2o_0^A + y_3 & y_2o_1^A & y_2o_2^A & y_2o_3^A & y_2o_4^A & y_2o_5^A & y_2o_6^A & y_2o_7^A \\
-y_2o_1^A & y_2o_0^A + y_3 & -y_2o_4^A & -y_2o_7^A & y_2o_2^A & -y_2o_6^A & y_2o_5^A & y_2o_3^A \\
-y_2o_2^A & y_2o_4^A & y_2o_0^A + y_3 & -y_2o_5^A & -y_2o_1^A & y_2o_3^A & -y_2o_7^A & y_2o_6^A \\
-y_2o_3^A & y_2o_7^A & y_2o_5^A & y_2o_0^A + y_3 & -y_2o_6^A & -y_2o_2^A & y_2o_4^A & -y_2o_1^A \\
-y_2o_4^A & -y_2o_2^A & y_2o_1^A & y_2o_6^A & y_2o_0^A + y_3 & -y_2o_7^A & -y_2o_3^A & y_2o_5^A \\
-y_2o_5^A & y_2o_6^A & -y_2o_3^A & y_2o_2^A & y_2o_7^A & y_2o_0^A + y_3 & -y_2o_1^A & -y_2o_4^A \\
-y_2o_6^A & -y_2o_5^A & -y_2o_7^A & -y_2o_4^A & y_2o_3^A & y_2o_1^A & y_2o_0^A + y_3 & -y_2o_2^A \\
-y_2o_7^A & -y_2o_3^A & -y_2o_6^A & y_2o_1^A & -y_2o_5^A & y_2o_4^A & y_2o_2^A & y_2o_0^A + y_3
\end{pmatrix}
\end{array}
\tag{12}
$$

For a system of $n(n+1)/2$ homogeneous quadratic equations with n variables $x_0, \cdots, x_{n-1}$, the folklore linearization technique replaces each quadratic monomial x_ix_j with a new variable y_{ij} and obtains $n(n+1)/2$ linear equations with $n(n+1)/2$ variables. The resulting equation system could be efficiently solved using Gauss elimination algorithm. The value of the original variable x_i can be recovered as one of the square roots of y_{ii}. Kipnis and Shamir [4] introduced a relinearization algorithm to solve quadratic equation systems with $l \geq 0.09175n^2$ linearly independent homogeneous quadratic equations in n variables. This is achieved by adding additional nonlinear equations. In the simplest form, we have $(x_{i_0}x_{i_1})(x_{i_2}x_{i_3}) = (x_{i_0}x_{i_2})(x_{i_1}x_{i_3}) = (x_{i_0}x_{i_3})(x_{i_1}x_{i_2})$. Thus we can add $y_{i_0i_1}y_{i_2i_3} = y_{i_0i_2}y_{i_1i_3} = y_{i_0i_3}y_{i_1i_2}$. Kipnis and Shamir [4] showed that 5 homogeneous quadratic equations in 4 variables could be solved using their relinearization techniques.

In a summary, the relinearization technique could be used to obtain the values of x_0, x_1, x_2, x_3 from the equation system (11) and obtain the values of y_0, y_1, y_2, y_3 from the equation system (12). In other words, one can obtain the values of $f_1(\mathbf{o}_A), f_2(\mathbf{o}_A), g_1(\mathbf{o}_A), g_2(\mathbf{o}_A)$ from the publicly observed values $\mathbf{o}_A, \mathbf{o}_B, \mathbf{r}_A, \mathbf{r}_B$. Armed with the values of $f_1(\mathbf{o}_A), f_2(\mathbf{o}_A), g_1(\mathbf{o}_A), g_2(\mathbf{o}_A)$, one can obtain $k_A (= k_B) = f_1(\mathbf{o}_A)\mathbf{r}_B f_2(\mathbf{o}_A)$.

In case that the protocol HK17 is based on quaternions, the homogeneous quadratic equation system (11) (respectively, (12)) contains four equations in four unknowns. Thus relinearization techniques could not be used to solve the equation system. However, the resulting equation system could be solved using Buchberger's Gröbner basis algorithm (see, e.g., [6]) or Faugere's F4 and F5 algorithms.

5 HK17 over $\mathbb{O}(\mathbb{Z}_q)$?

In the preceding section, we show that HK17 could not be secure on any $\mathbb{O}(\mathbb{F}_p)$. We may expect that HK17 is secure(?) over $\mathbb{O}(\mathbb{Z}_q)$ for large enough $q = p_1p_2$. But is it not quantum resistant.

References

[1] J. Baez. The octonions. *Bullet. American Mathematical Society*, 39(2):145–205, 2002.

[2] J. Conway and D. Smith. On quaternions and octonions. *AMC*, 10:12, 2003.

[3] Juan edro Hecht and Jorge Alejandro Kamlofsky. Hk17: lgorithm specifications and supporting documentation. Submission to NIST PQC Project, 2017.

[4] A. Kipnis and A. Shamir. Cryptanalysis of the HFE public key cryptosystem. In *Proc. Crypto*, 1999.

[5] R. Lidl and H. Niederreiter. *Finite fields*, volume 20. Cambridge university press, 1997.

[6] B. Sturmfels. What is a Gröbner basis. *Notices Amer. Math. Soc*, 52(10):1199–1200, 2005.

[7] Yongge Wang and Qutaibah M Malluhi. Privacy preserving computation in cloud using noise-free fully homomorphic encryption (FHE) schemes. In *ESORICS*, pages 301–323. Springer, 2016.