Breaking HK17 in Practice

Haoyu Li [*†‡], Renzhang Liu[§], Qutaibah M. Malluhi[¶], Yanbin Pan[*], Yongge Wang [||], and Tianyuan Xie[*‡]
[*]Key Laboratory of Mathematics Mechanization, NCMIS, Academy of Mathematics and Systems Science,
Chinese Academy of Sciences, Beijing, 100190, China
panyanbin@amss.ac.cn
[†]State Key Laboratory of Cryptology, P.O. Box 5159, Beijing, 100878, China
[‡]School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing, 100049, China
[§]Westone Cryptologic Research Center, Westone Information Industry INC. Beijing, 100070, China
[¶]Department of Computer Science, Qatar University, Qatar
[||]Department of SIS, UNC Charlotte, USA
yongge.wang@gmail.com

***Abstract*—In November 2017, Hecht and Kamlofsky submitted HK17, a quaternion(octonion)-based Diffie-Hellman key exchange protocol, to NIST post-quantum cryptography project, and thought that at least $O(p^8)$ arithmetic operations are needed for a passive adversary to recover the shared key where p is the modulo used in the scheme. Later, Bernstein and Lange pointed out that the shared key can be recovered with $O(p)$ arithmetic operations, which implies that HK17 with small p is not secure. However, their attack does not work in practice for the scheme with sufficiently large p, although the scheme is still efficient. In this paper, we propose an attack to show that just constant arithmetic operations, or $\tilde{O}(\log p)$ bit operations, are enough to recover the shared key for a passive adversary. Note that even the legal party in the protocol needs at least $\tilde{O}(\log p)$ bit operations to establish the shared key. We break HK17 completely in the practical sense.**

I. Introduction

Due to Shor's algorithms [10], [11], the cryptographic protocols based on integer factorization and discrete logarithm problem can be efficiently broken with practical quantum computers. Besides, the improvements of some quantum algorithms like Grover's algorithm [7] demand us to reevaluate the security of classical cryptographic protocols. The parameters should be no doubt selected carefully to resist the attack from quantum computers, which will make the protocols less efficient. Therefore, it become more and more urgent to construct cryptographic primitives that can resist quantum attacks since more and more people believed that the practical quantum computers move to reality closer and closer.

Under such a circumstance, NIST initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms since 2016. It called for proposals of post quantum cryptosystems including public key encryption, digital signature and key encapsulation. Later in November of 2017, NIST published the Round 1 submissions for the Post-Quantum Cryptography. Among all the candidate schemes, a key exchange protocol called HK17 was proposed by Hecht and Kamlofsky [8].

Key exchange (KE) protocol is a fundamental cryptographic primitive, which allows two communicators to establish a common key so that they can do the further communication securely. Since KE protocol can establish a common key securely over an insecure channel, it is widely used in building communication protocols, such as SSL/TLS. The first KE protocol was proposed by Diffie and Hellman [5]. It is based on the discrete logarithm problem, and obviously insecure under the quantum attacks. Therefore post-quantum key exchange protocol constitutes a substantial part of the NIST post-quantum cryptography project.

So far, plenty of post-quantum KE protocols have been proposed these years, such as [1], [3], [6]. Most of them are based on the lattice problems. However, HK17 employs an interesting mathematical object called hypercomplex numbers like quaternions and octonions as the basic elements in their protocol, which is very different from most of the other KE protocols.

Quaternions are noncommutative generalization of the complex numbers, and octonions are nonassociative generalization of quaternions. Using the noncommutativity of quaternions and octionions, HK17 employs the DH structure [5] to implement the key exchange protocol.

Roughly speaking, when establishing the shared key, Alice first generates two octonions (or quaternions) $\boldsymbol{o}_A$ and $\boldsymbol{o}_B$ over $\mathbb{Z}_p$, and chooses two random polynomials f_1, f_2, then computes $\boldsymbol{r}_A = f_1(\boldsymbol{o}_A)\boldsymbol{o}_B f_2(\boldsymbol{o}_A)$ and sends $\boldsymbol{o}_A$, $\boldsymbol{o}_B$, $\boldsymbol{r}_A$ to Bob. After receiving Alice's message, Bob chooses two random polynomials h_1, h_2, and computes $\boldsymbol{r}_B = h_1(\boldsymbol{o}_A)\boldsymbol{o}_B h_2(\boldsymbol{o}_A)$, then sends $\boldsymbol{r}_B$ back to Alice. Finally, Alice computes $K_A = f_1(\boldsymbol{o}_A)\boldsymbol{r}_B f_2(\boldsymbol{o}_A)$ and Bob computes $K_B = h_1(\boldsymbol{o}_A)\boldsymbol{r}_A h_2(\boldsymbol{o}_A)$. They will share the common key $K_A = K_B$.

Hecht and Kamlofsky [8] claimed that HK17 has some strong points, such as: using ordinary modular arithmetic but without big number libraries since they can choose p not very big, relatively fast operation, non-associativity of products and powers, parametric security levels, no classical nor quantum attacks at sight, possible resistance to side-channel attacks, easy firmware migration and conjectured semantical security IND-CCA2 compliance.

However, Bernstein and Lange [2] pointed out that the shared key can be recovered with $O(p)$ arithmetic operations, which implies that HK17 with small p is not secure.

We have to point out that the Bernstein-Lange attack does not work in practice for HK17 with p sufficiently large, although the scheme with large p is still efficient. For example, the Bernstein-Lange attack on a PC failed to recover the shared key for HK17 with parameter $p = 184467440737$ recommended in [8], since it will need about 2^{64} operations. Hence, a natural question is whether the scheme could be secure if p is sufficiently large.

Almost at the same time, we independently propose an attack to show that HK17 is insecure. We go further than Bernstein and Lange by showing that just constant arithmetic operations, or $\tilde{O}(\log p)$ bit operations, are enough to recover the shared key for a passive adversary. Note that even the legal party in the protocol needs at least $\tilde{O}(\log p)$ bit operations to establish the shared key. We break HK17 completely in the practical sense.

More precisely, both our attack and Bernstein-Lange attack are based on the following key observation: given a polynomial f and an octonion (resp. quaternion) $\boldsymbol{o}$, there exists some $a, b \in \mathbb{Z}_p$ such that $f(\boldsymbol{o}) = a \cdot \boldsymbol{o} + b$. Hence, the task to recover the shared key can be reduced to the question of finding a, b, c, d such that $\boldsymbol{r}_A = (a \cdot \boldsymbol{o}_A + b)\boldsymbol{o}_{\boldsymbol{B}}(c \cdot \boldsymbol{o}_A + d)$. Bernstein and Lange used a clever exhaustive search method to solve this problem which needs $O(p)$ arithmetic operations, whereas we employ the method of solving a system of linear equations to solve this problem which needs just constant arithmetic operations. Note that $\boldsymbol{r}_A = (a \cdot \boldsymbol{o}_A + b)\boldsymbol{o}_B(c \cdot \boldsymbol{o}_A + d) = ac \cdot \boldsymbol{o}_A \boldsymbol{o}_B \boldsymbol{o}_A + ad \cdot \boldsymbol{o}_A \boldsymbol{o}_B + bc \cdot \boldsymbol{o}_B \boldsymbol{o}_A + bd \cdot \boldsymbol{o}_B$. We will obtain a system of linear equations with 8 linear equations but just 4 unknowns ac, ad, bc, bd. Hence we can efficiently find a set of solutions for ac, ad, bc, bd. Moreover, we can show a set of solution of a, b, c, d can also be obtained efficiently from the solution for ac, ad, bc, bd.

Roadmap. The remainder of the paper is organized as follows. In Section II, we give some preliminaries needed. In Section III, we describe the HK17 key exchange scheme. We present our attack in Section IV and a short conclusion is given in Section V.

II. Preliminaries

There are four famous 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 whereas the complex numbers are not ordered. The quaternions are not commutative and the octonions are neither commutative nor associative.

A. Quaternions

Quaternions $\mathbb{H}$ were invented by Hamilton in 1843. In general, a quaternion $\boldsymbol{q}$ can be represented in the following form:

$$\boldsymbol{q} = a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}$$

where a, b, c, d are all real numbers and $\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$ are the fundamental quaternion units, which satisfy the following identities:

$$\boldsymbol{i}^2 = \boldsymbol{j}^2 = \boldsymbol{k}^2 = \boldsymbol{ijk} = -1.$$

TABLE I
Multiplication Table of the Unit Octonions

$\boldsymbol{e}_i\boldsymbol{e}_j$		$\boldsymbol{e}_j$							
		$\boldsymbol{e}_0$	$\boldsymbol{e}_1$	$\boldsymbol{e}_2$	$\boldsymbol{e}_3$	$\boldsymbol{e}_4$	$\boldsymbol{e}_5$	$\boldsymbol{e}_6$	$\boldsymbol{e}_7$
$\boldsymbol{e}_i$	$\boldsymbol{e}_0$	$\boldsymbol{e}_0$	$\boldsymbol{e}_1$	$\boldsymbol{e}_2$	$\boldsymbol{e}_3$	$\boldsymbol{e}_4$	$\boldsymbol{e}_5$	$\boldsymbol{e}_6$	$\boldsymbol{e}_7$
	$\boldsymbol{e}_1$	$\boldsymbol{e}_1$	$-\boldsymbol{e}_0$	$\boldsymbol{e}_3$	$-\boldsymbol{e}_2$	$\boldsymbol{e}_5$	$-\boldsymbol{e}_4$	$-\boldsymbol{e}_7$	$\boldsymbol{e}_6$
	$\boldsymbol{e}_2$	$\boldsymbol{e}_2$	$-\boldsymbol{e}_3$	$-\boldsymbol{e}_0$	$\boldsymbol{e}_1$	$\boldsymbol{e}_6$	$\boldsymbol{e}_7$	$-\boldsymbol{e}_4$	$-\boldsymbol{e}_5$
	$\boldsymbol{e}_3$	$\boldsymbol{e}_3$	$\boldsymbol{e}_2$	$-\boldsymbol{e}_1$	$-\boldsymbol{e}_0$	$\boldsymbol{e}_7$	$-\boldsymbol{e}_6$	$\boldsymbol{e}_5$	$-\boldsymbol{e}_4$
	$\boldsymbol{e}_4$	$\boldsymbol{e}_4$	$-\boldsymbol{e}_5$	$-\boldsymbol{e}_6$	$-\boldsymbol{e}_7$	$-\boldsymbol{e}_0$	$\boldsymbol{e}_1$	$\boldsymbol{e}_2$	$\boldsymbol{e}_3$
	$\boldsymbol{e}_5$	$\boldsymbol{e}_5$	$\boldsymbol{e}_4$	$-\boldsymbol{e}_7$	$\boldsymbol{e}_6$	$-\boldsymbol{e}_1$	$-\boldsymbol{e}_0$	$-\boldsymbol{e}_3$	$\boldsymbol{e}_2$
	$\boldsymbol{e}_6$	$\boldsymbol{e}_6$	$\boldsymbol{e}_7$	$\boldsymbol{e}_4$	$-\boldsymbol{e}_5$	$-\boldsymbol{e}_2$	$\boldsymbol{e}_3$	$-\boldsymbol{e}_0$	$-\boldsymbol{e}_1$
	$\boldsymbol{e}_7$	$\boldsymbol{e}_7$	$-\boldsymbol{e}_6$	$\boldsymbol{e}_5$	$\boldsymbol{e}_4$	$-\boldsymbol{e}_3$	$-\boldsymbol{e}_2$	$\boldsymbol{e}_1$	$-\boldsymbol{e}_0$

Denote $\boldsymbol{q}^* = a - b\boldsymbol{i} - c\boldsymbol{j} - d\boldsymbol{k}$ the conjugate of $\boldsymbol{q}$ and

$$\|\boldsymbol{q}\| = \sqrt{\boldsymbol{q} \cdot \boldsymbol{q}^*} = \sqrt{\boldsymbol{q}^* \cdot \boldsymbol{q}} = \sqrt{a^2 + b^2 + c^2 + d^2}$$

the norm of $\boldsymbol{q}$.

Using the same approach of interpreting a complex number $a + b\boldsymbol{i}$ as a pair $[a, b]$ of real numbers, $\boldsymbol{q}$ can be written into $[a, b, c, d]$.

B. Octonions

The octonions $\mathbb{O}$ were invented by Graves in 1844 and Cayley in 1845 independently. Generally speaking, an octonion $\boldsymbol{o}$ can be represented as a real linear combination of the unit octonions:

$$\boldsymbol{o} = a_0\boldsymbol{e}_0 + a_1\boldsymbol{e}_1 + \cdots + a_7\boldsymbol{e}_7$$

where $\boldsymbol{e}_0$ is the real number 1 and $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_7$ are fundamental octonion units, which satisfy

$$\boldsymbol{e}_i\boldsymbol{e}_j = \begin{cases} \boldsymbol{e}_j & i = 0, \\ \boldsymbol{e}_i & j = 0, \\ -\delta_{ij}\boldsymbol{e}_0 + \epsilon_{ijk}\boldsymbol{e}_k & \text{otherwise,} \end{cases}$$

where δ_{ij} is the Kronecker delta and $\epsilon_{ijk} = 1$ when $ijk = 123$, 145, 176, 246, 257, 357, 347, 365.

Equivalently, the product of each pair of terms can also be given by multiplication of the coefficients and a multiplication table of the unit octonions, like the following table.

Similar to complex numbers and quaternions,

$$\boldsymbol{o}^* = a_0\boldsymbol{e}_0 - a_1\boldsymbol{e}_1 - a_2\boldsymbol{e}_2 - \cdots - a_7\boldsymbol{e}_7$$

is the conjugate of $\boldsymbol{o}$, and

$$\|\boldsymbol{o}\| = \sqrt{\boldsymbol{o} \cdot \boldsymbol{o}^*} = \sqrt{\boldsymbol{o}^* \cdot \boldsymbol{o}} = \sqrt{a_0^2 + a_1^2 + \cdots + a_7^2}$$

is the norm of $\boldsymbol{o}$. Throughout the paper, we will use the following notations for real and imaginary part of an octonion $\boldsymbol{o} \in \mathbb{O}$,

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

Similarly, each octonion $\boldsymbol{o}$ can be written as a vector $\boldsymbol{o} = [a_0, \cdots, a_7] \in \mathbb{R}^8$. The norm of $\boldsymbol{o}$ is just $\|\boldsymbol{o}\| = \sqrt{a_0^2 + \cdots + a_7^2}$, the conjugate is $\boldsymbol{o}^* = [a_0, -a_1, \cdots, -a_7]$ and the inverse is $\boldsymbol{o}^{-1} = \boldsymbol{o}^*/\|\boldsymbol{o}\|^2$.

Theorem 1: For $\boldsymbol{o} \in \mathbb{O}$, we have $\boldsymbol{o}^2 = 2\mathrm{Re}(\boldsymbol{o})\boldsymbol{o} - \|\boldsymbol{o}\|^2$.

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

Different from the quaternions and complex numbers, the octonions do not satisfy the associative law, but the Moufang identities.

Theorem 2: (Moufang identities [4]) Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in \mathbb{O}$, then we have

$$\begin{aligned} \boldsymbol{c}(\boldsymbol{a}(\boldsymbol{c}\boldsymbol{b})) &= (((\boldsymbol{c}\boldsymbol{a})\boldsymbol{c})\boldsymbol{b}), \\ \boldsymbol{a}(\boldsymbol{c}(\boldsymbol{b}\boldsymbol{c})) &= (((\boldsymbol{a}\boldsymbol{c})\boldsymbol{b})\boldsymbol{c}), \\ (\boldsymbol{c}\boldsymbol{a})(\boldsymbol{b}\boldsymbol{c}) &= (\boldsymbol{c}(\boldsymbol{a}\boldsymbol{b}))\boldsymbol{c}, \\ (\boldsymbol{c}\boldsymbol{a})(\boldsymbol{b}\boldsymbol{c}) &= \boldsymbol{c}((\boldsymbol{a}\boldsymbol{b})\boldsymbol{c}). \end{aligned}$$

The Moufang identities imply the alternative law for octonions immediately. That is,

Corollary 1: For $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{O}$, we have

$$\begin{aligned} (\boldsymbol{a}\boldsymbol{a})\boldsymbol{b} &= \boldsymbol{a}(\boldsymbol{a}\boldsymbol{b}), \\ (\boldsymbol{a}\boldsymbol{b})\boldsymbol{a} &= \boldsymbol{a}(\boldsymbol{b}\boldsymbol{a}), \\ \boldsymbol{a}(\boldsymbol{b}\boldsymbol{b}) &= (\boldsymbol{a}\boldsymbol{b})\boldsymbol{b}. \end{aligned}$$

This property will make the HK17 work correctly.

C. Quaternions and Octonions over $\mathbb{Z}_p$

In the following, we will only take the octonions to state the process, and the quaternions will be similar.

From the definition of octonions, we can consider the octonions $\mathbb{O}$ as a vector space over $\mathbb{R}$, together with some special multiplication operation of vectors. More precisely, we have the following map:

$$\begin{aligned} \mathbb{O} &\longrightarrow \mathbb{R}^8 \\ \boldsymbol{o} = [a_0, a_1, \ldots, a_7] &\mapsto (a_0, a_1, \ldots, a_7) \end{aligned}$$

and the multiplication of two vectors is given before.

Based on such observation, we can construct "octonions" over $\mathbb{Z}_p$, which will be denoted $\mathbb{O}(\mathbb{Z}_p)$. First $\mathbb{Z}_p^8$ is a vector space over $\mathbb{Z}_p$, which can also be seen as a linear space over a finite field. Then we can define a multiplication operation of two vectors in $\mathbb{Z}_p^8$ using the multiplication of octonions. More precisely, given two vectors $\boldsymbol{a} = (a_0, a_1, \ldots, a_7)$ and $\boldsymbol{b} = (b_0, b_1, \ldots, b_7)$, we define the multiplication of $\boldsymbol{a}$ and $\boldsymbol{b}$ as

$$\begin{aligned} \boldsymbol{a} \cdot \boldsymbol{b} = (a_0, a_1, \ldots, a_7) \cdot (b_0, b_1, \ldots, b_7) := \\ (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4 - a_5b_5 - a_6b_6 - a_7b_7, \\ a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2 + a_4b_5 - a_5b_4 - a_6b_7 + a_7b_6, \\ a_0b_2 - a_1b_3 + a_2b_0 + a_3b_1 + a_4b_6 + a_5b_7 - a_6b_4 - a_7b_5, \\ a_0b_3 + a_1b_2 - a_2b_1 + a_3b_0 + a_4b_7 - a_5b_6 + a_6b_5 - a_7b_4, \\ a_0b_4 - a_1b_5 - a_2b_6 - a_3b_7 + a_4b_0 + a_5b_1 + a_6b_2 + a_7b_3, \\ a_0b_5 + a_1b_4 - a_2b_7 + a_3b_6 - a_4b_1 + a_5b_0 - a_6b_3 + a_7b_2, \\ a_0b_6 + a_1b_7 + a_2b_4 - a_3b_5 - a_4b_2 + a_5b_3 + a_6b_0 - a_7b_1, \\ a_0b_7 - a_1b_6 + a_2b_5 + a_3b_4 - a_4b_3 - a_5b_2 + a_6b_1 + a_7b_0), \end{aligned}$$

where all the operations involved are those defined for $\mathbb{Z}_p$.

As the discussion before, we know that this multiplication operation satisfies the alternative law.

Similarly, we can also construct "octonions" over any field $\mathbb{F}_q$ with $q = p^m$ or over any ring $\mathbb{Z}_q$ with $q = p_1^{r_1} \cdots p_m^{r_m}$. Generally, all theorems except division-related results for octonions hold in $\mathbb{O}(\mathbb{Z}_q)$, since it is not a division algebra.

For more related discussion, the reader is referred to [12].

III. The HK17 Key Exchange Scheme

A. The Octonions Version of HK17

The HK17 Key Exchange scheme uses some hypercomplex numbers such as quaternions and octonions over $\mathbb{Z}_p$ as defined before. We take the octonions version as an example to describe it.

Initialization:

1) Alice chooses two non-zero octonions $\boldsymbol{o}_A$, $\boldsymbol{o}_B$ with each coordinate uniformly in $\mathbb{Z}_p$ with some prime p;
2) Alice chooses two integers m, n and a non-zero polynomial $f(x) \in \mathbb{Z}_p[x]$ with degree d such that $f(\boldsymbol{o}_A) \neq 0$, and (f, m, n) is Alice's private key;
3) Alice sends $\boldsymbol{o}_A$ and $\boldsymbol{o}_B$ to Bob;
4) Bob chooses two integers r, s and a non-zero polynomial $h(x) \in \mathbb{Z}_p[x]$ with degree d such that $h(\boldsymbol{o}_A) \neq 0$, and (h, r, s) is Bob's private key.

Computing the tokens:

1) Alice computes the value $\boldsymbol{r}_A = f(\boldsymbol{o}_A)^m \boldsymbol{o}_B f(\boldsymbol{o}_A)^n$ and sends it to Bob;
2) Bob computes the value $\boldsymbol{r}_B = h(\boldsymbol{o}_A)^r \boldsymbol{o}_B h(\boldsymbol{o}_A)^s$ and sends it to Alice.

Computing Session Keys:

1) Alice computes her key: $K_A = f(\boldsymbol{o}_A)^m \boldsymbol{r}_B f(\boldsymbol{o}_A)^n$;
2) Bob computes his key: $K_B = h(\boldsymbol{o}_A)^r \boldsymbol{r}_A h(\boldsymbol{o}_A)^s$;
3) Finally Alice and Bob share the common key $K_A = K_B$.

It can be easily verified that

$$\begin{aligned} K_A &= f(\boldsymbol{o}_A)^m \boldsymbol{r}_B f(\boldsymbol{o}_A)^n \\ &= f(\boldsymbol{o}_A)^m (h(\boldsymbol{o}_A)^r \boldsymbol{o}_B h(\boldsymbol{o}_A)^s) f(\boldsymbol{o}_A)^n \\ &= h(\boldsymbol{o}_A)^r f(\boldsymbol{o}_A)^m \boldsymbol{o}_B f(\boldsymbol{o}_A)^n h(\boldsymbol{o}_A)^s \\ &= h(\boldsymbol{o}_A)^r \boldsymbol{r}_A h(\boldsymbol{o}_A)^s \\ &= K_B. \end{aligned}$$

B. Parameter Sets and Security

Hecht and Kamlofsky [8] thought that the best attack against HK17 was to enumerate all possible values for the shared key, which needs p^8 operations. Hence, with parameter p, they thought HK17 can achieve the $8 \log p$-bit security.

The parameter sets and the conjectured security in [8] are listed in the following table.

d	p	pre-quantum security (bits)	post-quantum security (bits)
16	251	64	32
32	65521	128	64
64	4294967291	256	128
128	184467440737	512	256

However, Bernstein and Lange [2] pointed out that the shared key can be recovered with just $O(p)$ arithmetic operations. For $p = 251, 65521$, their attack succeeded to recover the shared key on a PC. For $p = 4294967291$, we believe their attack will work if it is implemented properly. However, on a PC, the attack failed to recover the shared key for HK17 with parameter $p = 184467440737$, since it will need about 2^{64} operations.

IV. Break HK17 Completely

We will show that HK17 can be broken completely with just constant arithmetic operations, or $\tilde{O}(\log p)$ bit operations. The octonions version of HK17 is taken as an example to explain our attack.

A. The key observation

We have the following key observations.

Lemma 1: For any octonion $\boldsymbol{o} \in \mathbb{O}(\mathbb{Z}_p)$, there exist α, $\beta \in \mathbb{Z}_p$ such that

$$\boldsymbol{o}^2 + \alpha \boldsymbol{o} + \beta = 0.$$

Furthermore, for any polynomial $g(x) \in \mathbb{Z}_p[x]$, there exist a, $b \in \mathbb{Z}_p$, such that

$$g(\boldsymbol{o}) = a \cdot \boldsymbol{o} + b.$$

Proof 1: Suppose $\boldsymbol{o} \in \mathbb{O}(\mathbb{Z}_p)$. The first statement follows from Theorem 1, in which $\alpha = -2\mathrm{Re}(\boldsymbol{o}) \bmod p$ and $\beta = \|\boldsymbol{o}\|^2 \bmod p$.

For the second statement, given any polynomial $g(x) \in \mathbb{Z}_p[x]$, it can be written into

$$g(x) = (x^2 + \alpha x + \beta)q(x) + (ax + b),$$

with $q(x) \in \mathbb{Z}_p[x]$ and $a, b \in \mathbb{Z}_p$, which implies immediately that

$$g(\boldsymbol{o}) = a\boldsymbol{o} + b.$$

Lemma 2: For HK17, given $\boldsymbol{o}_A$, $\boldsymbol{o}_B$, $\boldsymbol{r}_A$, there exists a polynomial time (in $\log p$) algorithm to find $a, b, c, d \in \mathbb{Z}_p$ such that

$$\boldsymbol{r}_A = (a \cdot \boldsymbol{o}_A + b)\boldsymbol{o}_B(c \cdot \boldsymbol{o}_A + d). \qquad (1)$$

Proof 2: By Lemma 1, we know that there exist $a, b, c, d \in \mathbb{Z}_p$, such that

$$\begin{aligned} f(\boldsymbol{o}_A)^m &= a \cdot \boldsymbol{o}_A + b, \\ f(\boldsymbol{o}_A)^n &= c \cdot \boldsymbol{o}_A + d. \end{aligned}$$

Therefore, we can write

$$\begin{aligned} \boldsymbol{r}_A &= f(\boldsymbol{o}_A)^m \boldsymbol{o}_B f(\boldsymbol{o}_A)^n \\ &= (a \cdot \boldsymbol{o}_A + b)\boldsymbol{o}_B(c \cdot \boldsymbol{o}_A + d) \\ &= ac \cdot \boldsymbol{o}_A\boldsymbol{o}_B\boldsymbol{o}_A + ad \cdot \boldsymbol{o}_A\boldsymbol{o}_B + bc \cdot \boldsymbol{o}_B\boldsymbol{o}_A + bd \cdot \boldsymbol{o}_B \end{aligned}$$

By comparing every corresponding coordinate of $\boldsymbol{r}_A$ and $ac \cdot \boldsymbol{o}_A\boldsymbol{o}_B\boldsymbol{o}_A + ad \cdot \boldsymbol{o}_A\boldsymbol{o}_B + bc \cdot \boldsymbol{o}_B\boldsymbol{o}_A + bd \cdot \boldsymbol{o}_B$, we will have eight linear equations with four unknowns ac, ad, bc, bd. More precisely, to find ac, ad, bc, bd, we need to solve the following system of linear equations:

$$\boldsymbol{r}_A = (s_1, s_2, s_3, s_4) \cdot \boldsymbol{A}$$

over $\mathbb{Z}_p^4$, where $\boldsymbol{A} = \begin{pmatrix} \boldsymbol{o}_A\boldsymbol{o}_B\boldsymbol{o}_A, \\ \boldsymbol{o}_A\boldsymbol{o}_B, \\ \boldsymbol{o}_B\boldsymbol{o}_A, \\ \boldsymbol{o}_B \end{pmatrix} \in \mathbb{Z}_p^{4\times 8}$. By the existence of a, b, c, d, we can always solve the system of the eight linear equations to get a solution (s_1, s_2, s_3, s_4) for (ac, ad, bc, bd). There are two cases to be considered.

1) $\boldsymbol{A}$ has full row rank.
A solution (s_1, s_2, s_3, s_4) can be directly obtained by solving the linear equations. Moreover $(s_1, s_2, s_3, s_4) = (ac, ad, bc, bd)$ in this case. Note that since a, b can not be zero at the same time if $\boldsymbol{r}_A \neq 0$, so we can tell from which is nonzero. For example if $s_1 = 0$ and $s_2 = 0$, then b must not be zero. Similarly, we can also know that if c or d is zero or not.
All these cases are presented in the following and can be easily verified to satisfy the Equation (1).

   a) If $s_1 \neq 0$, then $a, c \neq 0$, and we set $(a, b, c, d) = (1, s_1^{-1}s_3, s_1, s_2)$.
   It can be easily verified that $(a, b, c, d) = (1, s_1^{-1}s_3, s_1, s_2)$ must be a solution, since

   $$\begin{aligned} \boldsymbol{r}_A &= (a \cdot \boldsymbol{o}_A + b)\boldsymbol{o}_B(c \cdot \boldsymbol{o}_A + d) \\ &= a(\boldsymbol{o}_A + a^{-1}b)\boldsymbol{o}_B(c \cdot \boldsymbol{o}_A + d) \\ &= (\boldsymbol{o}_A + a^{-1}b)\boldsymbol{o}_B(ac \cdot \boldsymbol{o}_A + ad). \end{aligned}$$

   Note that we can also set a to be any nonzero element in $\mathbb{Z}_p$ and solve the other corresponding b, c, d.
   Similarly, we have

   b) If $s_1 = s_2 = 0$, then $a = 0$, and we set $b = 1$, $c = s_3$, $d = s_4$;

   c) If $s_1 = s_3 = 0$, then $c = 0$, and we set $a = s_1$, $b = s_2$, $d = 1$;

2) $\boldsymbol{A}$ does not have full row rank.
It is obvious that a specific solution (s_1, s_2, s_3, s_4) can be obtained efficiently.
Note that if one of a, b, c, d is zero, at least two of ac, ad, bc, bd are zero. Hence we try to find a solution (s'_1, s'_2, s'_3, s'_4) with all $s'_i \neq 0$ for $i = 1, 2, 3, 4$ or at least two of s'_i are zero. If the specific solution (s_1, s_2, s_3, s_4) satisfies such property, we simply set $s'_i = s_i$. Otherwise, there is exactly one of s_i, which equals to 0. Without loss of generality, we suppose $s_1 = 0$ and $s_2, s_3, s_4 \neq 0$. In such case, we first find a nontrivial solution (t_1, t_2, t_3, t_4) such that $(t_1, t_2, t_3, t_4) \cdot \boldsymbol{A} = \boldsymbol{0}$.

   a) If $t_1 = 0$, note that at most one of t_2, t_3, t_4 is zero, then either t_2 or t_3 is nonzero. Without loss of generality, we can assume $t_2 \neq 0$. We first compute $r = -s_2 \cdot t_2^{-1} \in \mathbb{Z}_p$, then set $(s'_1, s'_2, s'_3, s'_4) = (0, 0, s_3 + r \cdot t_3, s_4 + r \cdot t_4)$;

   b) If $t_1 \neq 0$, we find an $r \in \mathbb{Z}_p$, such that all $s_i + r \cdot t_i (i = 1, 2, 3, 4)$ are not zero, which can be done since $p > 4$ is big enough. Then we set $(s'_1, s'_2, s'_3, s'_4) = (r \cdot t_1, s_2 + r \cdot t_2, s_3 + r \cdot t_3, s_4 + r \cdot t_4)$.

Hence, in both cases, we can efficiently find a solution (s'_1, s'_2, s'_3, s'_4) with all $s'_i \neq 0$ for $i = 1, 2, 3, 4$ or at least two of s'_i are zero. What we will do is to solve (a, b, c, d) using the same way as in the full-rank case.

Lemma 3: For HK17 key exchange scheme, if we can find any two polynomial $g_1(x), g_2(x) \in \mathbb{Z}_p[x]$, such that

$$\boldsymbol{r}_A = g_1(\boldsymbol{o}_A)\boldsymbol{o}_B g_2(\boldsymbol{o}_A),$$

then the shared key is

$$K = g_1(\boldsymbol{o}_A)\boldsymbol{r}_B g_2(\boldsymbol{o}_A).$$

Proof 3: Note that

$$\begin{aligned} K_B &= h(\boldsymbol{o}_A)^r \boldsymbol{r}_A h(\boldsymbol{o}_A)^s \\ &= h(\boldsymbol{o}_A)^r (g_1(\boldsymbol{o}_A)\boldsymbol{r}_B g_2(\boldsymbol{o}_A)) h(\boldsymbol{o}_A)^s \\ &= g_1(\boldsymbol{o}_A) h(\boldsymbol{o}_A)^r \boldsymbol{r}_B h(\boldsymbol{o}_A)^s g_2(\boldsymbol{o}_A) \\ &= g_1(\boldsymbol{o}_A)\boldsymbol{r}_B g_2(\boldsymbol{o}_A) \\ &= K. \end{aligned}$$

The lemma follows.

B. Our Attack

Based on the lemmas above, we present our attack.

Step 1. When the adversary gets $\boldsymbol{o}_A$, $\boldsymbol{o}_B$, $\boldsymbol{r}_A$ by eavesdropping, he can compute $a, b, c, d \in \mathbb{Z}_p$ such that

$$\boldsymbol{r}_A = (a \cdot \boldsymbol{o}_A + b)\boldsymbol{o}_B(c \cdot \boldsymbol{o}_A + d),$$

by Lemma 2.

Step 2. Compute

$$K = (a \cdot \boldsymbol{o}_A + b)\boldsymbol{r}_B(c \cdot \boldsymbol{o}_A + d).$$

By Lemma 3, we know K is exactly the shared key established by Alice and Bob.

Remark 1: In [8], a quaternions version was also proposed, which has the same framework to the octonions version, but with an additional normalization. It can be easily concluded that our attack can be extended to the quaternions version of HK17, since any quaternion $\boldsymbol{q}$ satisfies

$$\boldsymbol{q}^2 - 2\mathrm{Re}(\boldsymbol{q})\boldsymbol{q} + \|\boldsymbol{q}\|^2 = 0.$$

Remark 2: Another natural idea to generalize HK17 is to replace the octonions (or quaternions) with some matrices over finite field. However, it seems the matrix-version will still be insecure since any matrix satisfies its characteristic polynomial by the famous Cayley-Hamilton theorem, and then our attack still works. However, we would like to point out that if the octonions (or quaternions) are replaced with the elements in some non-commutative (semi)groups, the corresponding scheme may be secure (see [9] for some examples).

C. Experimental Result

We implemented our attack with SageMath on a PC with *Intel(R)_Core(TM)_i5-5200U_CPU_@_2.20GHz*, 8G RAM and Windows 7 OS. We randomly generated several instances with the recommended parameters in [8] and all shared key can be recovered efficiently, not only for the instances with small p which were already broken in [2], but also for the instances with the largest parameter $p = 184467440737 \approx 2^{64}$ which can not be broken practically on a PC before.

TABLE II
TIME OF OUR ATTACK FOR LARGE PARAMETERS

$\log_2(p)$	64	128	256	512	1024
Time(in second)	0.175	0.179	0.202	0.875	1.472

Furthermore, we replaced $p = 184467440737$ with random p with 128, 256, 512 and 1024 bits for HK17 and tested our attack against the randomly generated instances with such p's. We found that even with 1024-bits p, the running time for the protocol HK17 was still reasonable. However, our attacks can also be completed in around one second and always succeeded. The detailed time for our attacks is listed as in Table II.

V. CONCLUSION

In this paper, we present a practical attack for HK17 key exchange protocol, by which we find that HK17 is not secure even with large parameters for a passive adversary.

ACKNOWLEDGMENT

Y. Pan was supported by the NNSF of China (No. 61572490) and by the National Center for Mathematics and Interdisciplinary Sciences, CAS.

REFERENCES

[1] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, *Post-quantum key exchange-a new hope,* USENIX Security Symposium, pages 327–343, 2016.

[2] NIST webpage: *Comments for HK17*. Available at https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/official-comments/HK17-official-comment.pdf

[3] 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,* Security and Privacy (SP), 2015 IEEE Symposium on, pages 553–570, IEEE, May 2015.

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

[5] W. Diffie, M. Hellman. *New directions in cryptography,* IEEE Transactions on Information Theory, 22(6):644–654, Nov 1976.

[6] J. Ding, X. Xie, and X. Lin, *A simple provably secure key exchange scheme based on the learning with errors problem,* IACR Cryptology EPrint Archive, 2012:688, 2012.

[7] L. K. Grover, *A fast quantum mechanical algorithm for database search,* Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing, STOC '96, pages 212–219, New York, NY, USA, 1996. ACM.

[8] J. P. Hecht, J. A. Kamlofsky, *HK17: Post quantum key exchange protocol based on hypercomplex numbers,* 2017.

[9] A. G. Myasnikov, V. Shpilrain, A. Ushakov, *Non-commutative cryptography and complexity of group-theoretic problems,* No. 177. American Mathematical Soc., 2011.

[10] P. W. Shor, *Algorithms for quantum computation: discrete logarithms and factoring,* Proceedings 35th Annual Symposium on Foundations of Computer Science, pages 124–134, Santa Fe, NM, USA, November 1994. IEEE.

[11] P. W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,* SIAM J. Comput., 26(5):1484–1509, October 1997.

[12] Y. Wang, Q. M. Malluhi, *Privacy preserving computation in cloud using noise-free fully homomorphic encryption (FHE) schemes,* ESORICS, pages 301–323. Springer, 2016.