Cryptanalysis of HK17

Haoyu Li[1,2], Renzhang Liu[3], Yanbin Pan[1], Tianyuan Xie[1,2]

[1]Key Laboratory of Mathematics Mechanization, NCMIS,
Academy of Mathematics and Systems Science, Chinese Academy of Sciences
Beijing 100190, China
[2] School of Mathematical Sciences, University of Chinese Academy of Sciences,
Beijing 100049, China
[3] State Key Laboratory of Information Security, Institute of Information Engineering,
Chinese Academy of Sciences, Beijing, China.

Abstract. Very recently, a key exchange scheme called HK17 was submitted to NIST as a candidate of the standard of post-quantum cryptography. The HK17 scheme employs some hypercomplex numbers as the basic objects, such as quaternions and octonions. In this paper, we show that HK17 is insecure since a passive adversary can recover the shared key in polynomial time.

1 Introduction

In December of 2017, NIST published the Round 1 submissions for the Post-Quantum Cryptography. Among all the candidate schemes, a key exchange called HK17 was proposed by Hecht and Kamlofsky [1]. Different from most of the popular schemes, the HK17 scheme uses hypercomplex numbers, such as quanternions and octonions.

Some strong points of HK17 were also pointed out in [1], such as: using ordinary modular arithmetic but without big number libraries, relatively fast operation, non-associativity of products and powers, parametric security levels, no classical nor quantum attack at sight, possible resistance to side-channel attacks, easy firmware migration and conjectured semantical security IND-CCA2 compliance.

However, in this paper, we will show that the HK17 scheme is not secure. More precisely, any passive adversary can recover the shared key very efficiently.

2 Preliminaries

2.1 Quaternions and Octonions

In mathematics, Quaternions and Octonions are generalization of the complex numbers. Quaternions are the noncommutative generalization of the complex numbers. In general, a quaternion can be represented in the following form:

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

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

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

The octonions are nonassociative generalization of quaternions. Generally speaking, an octonions $\boldsymbol{o}$ 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. Furthermore, the product of each pair of terms can be given by multiplication of the coefficients and a multiplication table of the unit octonions, like the following:

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

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

2.2 HK17

The HK17 Key Exchange scheme uses some hypercomplex numbers such as quaternions and octonions. We take the octonions version as an example to describe this scheme.

* Initialization:
  1) Alice choose two non-zero octonions $\boldsymbol{o}_A$, $\boldsymbol{o}_B$ with each coordinate uniformly in $\mathbb{Z}_p$ with some prime p;
  2) Alice choose 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 send $\boldsymbol{o}_A$ and $\boldsymbol{o}_B$ to Bob;
  4) Bob choose 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 Alice's private key.
* Computing the tokens:
  1) Alice compute the value $\boldsymbol{r}_A = f(\boldsymbol{o}_A)^m\boldsymbol{o}_B f(\boldsymbol{o}_A)^n$ and send it to Bob;
  2) Bob compute the value $\boldsymbol{r}_B = h(\boldsymbol{o}_A)^r\boldsymbol{o}_B h(\boldsymbol{o}_A)^s$ and send it to Alice.
* Computing Session Keys:
  1) Alice compute her key: $K_A = f(\boldsymbol{o}_A)^m\boldsymbol{r}_B f(\boldsymbol{o}_A)^n$;
  2) Bob compute his key: $K_B = h(\boldsymbol{o}_A)^r\boldsymbol{r}_A h(\boldsymbol{o}_A)^s$.

It can be verified that

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

Finally, Alice and Bob share the common key $K_A = K_B$.

3 Our Attack against the Octonions Version of HK17

3.1 The key observation

We have the following key observations.

Lemma 1. *For any octonion $\boldsymbol{o}$, we can find α, β in polynomial time such that*

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

Furthermore, when all the coordinates of $\boldsymbol{o}$ are in $\mathbb{Z}_p$, for any polynomial $g(x) \in \mathbb{Z}_p[x]$, there exist a, $b \in \mathbb{Z}_p$, such that

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

Proof. Given an octonion $\boldsymbol{o} = a_0\boldsymbol{e}_0 + a_1\boldsymbol{e}_1 + \cdots + a_7\boldsymbol{e}_7$, we have

$$\begin{aligned}&(a_0\boldsymbol{e}_0 + a_1\boldsymbol{e}_1 + \cdots + a_7\boldsymbol{e}_7)^2\\ =&(a_0^2 - a_1^2 - \cdots - a_7^2)\boldsymbol{e}_0 + 2a_0a_1\boldsymbol{e}_1 + \cdots + 2a_0a_7\boldsymbol{e}_7\\ =&2a_0(a_0\boldsymbol{e}_0 + \cdots + a_7\boldsymbol{e}_7) - (a_0^2 + \cdots + a_7^2)\boldsymbol{e}_0\end{aligned}$$

Let

$$\alpha = -2a_0, \beta = a_0^2 + \cdots + a_7^2.$$

Then $\boldsymbol{o} = a_0\boldsymbol{e}_0 + a_1\boldsymbol{e}_1 + \cdots + a_7\boldsymbol{e}_7$ is a solution of

$$x^2 + \alpha x + \beta = 0.$$

Then for any polynomial $g(x) \in \mathbb{Z}_p[x]$, we can write

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

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*

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

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

$$f(\boldsymbol{o}_A)^m = a\boldsymbol{o}_A + b, \text{ and } f(\boldsymbol{o}_A)^n = c\boldsymbol{o}_A + d.$$

Therefore, we can write

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

By comparing every corresponding coordinate of $\boldsymbol{r}_A$ and $ac\boldsymbol{o}_A\boldsymbol{o}_B\boldsymbol{o}_A + ad\boldsymbol{o}_A\boldsymbol{o}_B + bc\boldsymbol{o}_B\boldsymbol{o}_A + bd\boldsymbol{o}_B$, we will have eight linear equations with four unknowns ac, ad, bc, bd. 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).

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. Without loss of generality, assume $a \neq 0$, $c \neq 0$, then we can set $a = 1$, and

$$(1, s_1^{-1}s_3, s_1, s_2)$$

must be a solution, since

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

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

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

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

Proof. 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.

3.2 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

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

by Lemma 2.

Step 2 Compute

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

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

3.3 Experimental Result

We take the example on Page 11 in [1] to verify our attack. In the example, we have

- $p = 251$;
- $\boldsymbol{o}_A = (157, 188, 177, 188, 203, 149, 217, 148)$;
- $\boldsymbol{o}_B = (40, 207, 6, 33, 75, 79, 98, 54)$;
- $\boldsymbol{r}_A = (121, 3, 110, 243, 184, 230, 202, 171)$;
- $\boldsymbol{r}_B = (90, 42, 17, 119, 150, 23, 110, 182)$.

After Step 1 in our attack, we find the solution $(1, 142, 75, 187)$ such that

$$\boldsymbol{r}_A = (\boldsymbol{o}_A + 142)\boldsymbol{o}_B(75\boldsymbol{o}_A + 187).$$

After Step 2, we recover the shared key

$$K = (\boldsymbol{o}_A + 142)\boldsymbol{r}_B(75\boldsymbol{o}_A + 187) = (84, 242, 130, 31, 84, 244, 45, 20),$$

which is exactly the shared key established in [1].

4 Our Attack against the Quaternions Version of HK17

In [1], 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 for any quaternions $\boldsymbol{q} = a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}$, it also satisfied a quadratic equation

$$x^2 - 2ax + (a^2 + b^2 + c^2 + d^2) = 0.$$

References

1. Hecht, Kamlofsky: HK17: Post Quantum Key Exchange Protocol Based on Hypercomplex Numbers. Available at https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/submissions/HK17.zip