# R-Propping of HK17: Upgrade for a Detached Proposal of NIST PQC First Round Survey

Pedro Hecht

Information Security Master, School of Economic Sciences,
School of Exact and Natural Sciences and Engineering School (ENAP-FCE),
University of Buenos Aires, Av. Cordoba 2122 2nd Floor,
. CABA C1120AAP, República Argentina
phecht@dc.uba.ar

**Abstract.** NIST is currently conducting the 3rd round of a survey to find post-quantum class asymmetric protocols (PQC) [1]. We participated in a joint-team with a fellow researcher of the Interamerican Open University (UAI) with a Key-Exchange Protocol (KEP) called HK17 [2]. The proposal was flawed because Bernstein [3] found a weakness, which was later refined by Li [4] using a quadratic reduction of octonions and quaternions, albeit no objection about the published non-commutative protocol and the one-way trapdoor function (OWTF). This fact promoted the search for a suitable algebraic platform. HK17 had its interest because it was the only first-round offer strictly based on canonical group theory [5]. At last, we adapted the original protocol with the R-propping solution of 3-dimensional tensors [6], yielding Bernstein attack fruitless. Therefore, an El Gamal IND-CCA2 cipher security using Cao [7] arguments are at hand.

**Keywords:** Post-quantum cryptography, finite fields, rings, combinatorial group theory, R-propping, public-key cryptography, KEP, non-commutative cryptography, semantic security, IND-CCA2.

## 1 Introduction

### 1.1 Goals of the original HK17 proposal

It is noteworthy that besides a couple of described solutions [8], there remains overlooked solutions belonging to Non-Commutative (NCC) and Non-Associative (NAC) algebraic cryptography. The general structure of these solutions relies on protocols defining one-way trapdoor functions (OWTF) extracted from the combinatorial group theory [5].

The main objective was to develop a parametric family of multifunctional asymmetric protocols of the PQC class, based on the use of modular polynomials of hypercomplex numbers (quaternions, octonions) and OWTF derived from abstract algebra.

### 1.2 Flaw of the original HK17 platform

Choosing hypercomplex numbers like quaternions and octonions was a failure. As Bernstein and later Li found, the following theorem lay the basis of the weakness.

***Theorem 1***. For any octonion $\boldsymbol{o} = a_o \boldsymbol{e_0} + \cdots + a_7 \boldsymbol{e_7}$, when all the coordinates of $\boldsymbol{o}$ are in $\mathbb{Z}_p$, for any polynomial $g(x) \in \mathbb{Z}_p[x]$ there exist $(a,b) \in \mathbb{Z}_p{}^2$ such that $g(\boldsymbol{o}) = a\,\boldsymbol{o} + b$ ■

Therefore, every eight unknowns octonion polynomial reduces to a pair of integer unknowns. A similar deduction could be found for the renormalized quaternions version.

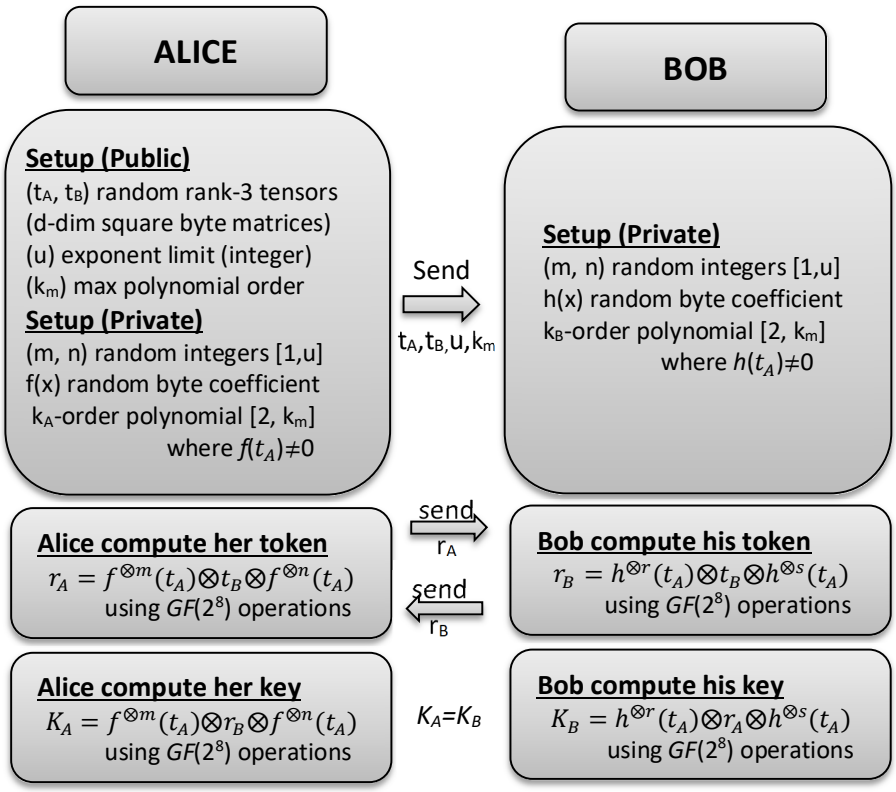
### 1.3 Solution for the HK17 protocol

In this paper, we propose an algebraic patch to HK17 using theoretical well supported combinatorial solutions. Specifically, we switch from hypercomplex numbers to 3-dimensional matrices of AES-field polynomials (bytes) and from numerical operations to field operations [9]. Obviously, this class of matrices are rank-3 tensors [9]. We refer to this version as R-propped [6] HK17 or HK17+.

Essentially R-propping consists of replacing all numerical field operations (arithmetic sum and multiplication), a typical scalar proposal, by algebraic operations using the AES field, a vectorial proposal [9]. This scales up operations complexity foiling classical linearization attacks like AES does and at same time quantum ones. This is a solid way to achieve the best of two worlds, both pointing to cryptographic security

The R-propping solution is described as an Algebraic Extension Ring [9]

## 2 Schematic HK17+ key exchange protocol (KEP)




This is the R-propped version of the original HK17 protocol. The OWTF which protects the KEP, is the generalized symmetric decomposition problem as defined in [[4][6][7].

## 3 Step-by-step numeric example of HK17+

We use as example the following parameters:

$k_m = k_A = k_B$ (polynomial degree) = 31

d (tensor -square matrix- dimension) = 3

u (upper limit for exponents) = $2^{32}$ = 4,294,967,296

```
Print["............................................... HK17+"];
Print["ALICE prepares..."];
dim = 3; Print["dim=", dim];
degree = 31; Print["degree=", degree];
zlimit = 2^32; Print["max exponent=", zlimit];
A = rmat; Print["tensor A=", MatForm[A]];
B = rmat; Print["tensor B=", MatForm[B]];
m = RandomInteger[{1, zlimit}]; Print["m=", m];
n = RandomInteger[{1, zlimit}]; Print["n=", n];
coefA = Table[RandomInteger[255], {k, 0, degree}]; Print["coefficient
list of f(x)=", coefA];
TPowerSet[A, degree]; Print["tensor A power set=",
Table[MatrixForm[TPSet[k]], {k, 0, degree}]];
fA = FieldPolyEval[dim, degree, coefA, A]; Print["f(A)=", fA];
rA = M3[TFastPower[fA, m], B, TFastPower[fA, n]]; Print["rA=", rA];
Print["ALICE sends A, B, rA to BOB"];
Print["................................................."];
Print["BOB prepares..."];
r = RandomInteger[{1, zlimit}]; Print["r=", r];
s = RandomInteger[{1, zlimit}]; Print["s=", s];
coefB = Table[RandomInteger[255], {k, 0, degree}]; Print["coefficient
list of h(x)=", coefB];
TPowerSet[A, degree]; Print["tensor A power set=",
Table[MatrixForm[TPSet[k]], {k, 0, degree}]];
hA = FieldPolyEval[dim, degree, coefB, A]; Print["h(A)=", hA];
rB = M3[TFastPower[hA, r], B, TFastPower[hA, s]]; Print["rB=", rB];
Print["BOB sends rB to ALICE"];
Print["................................................."];
KA = M3[TFastPower[fA, m], rB, TFastPower[fA, n]]; Print["ALICE
session key=", MatrixForm[KA]];
KB = M3[TFastPower[hA, r], rA, TFastPower[hA, s]]; Print["  BOB
session key=", MatrixForm[KB]];
Print["................................................."]
```

**Table 1**. Mathematica 11.3 code of an interpreted session of HK17+. Detailed notebook with full defined functions is available upon request to the author. Here u=zlimit, the upper limit for exponents.

```
.................................................. HK17+
ALICE prepares...
dim=3
degree=31
max exponent=4 294 967 296
tensor A=⎛ 60  167  194 ⎞
         ⎜ 168  131  56  ⎟
         ⎝ 66   16   91  ⎠
tensor B=⎛ 155  112  101 ⎞
         ⎜ 168  204  104 ⎟
         ⎝ 90   28   232 ⎠
m=1 793 503 137
n=2 694 910 638
coefficient list of f(x)={171, 8, 136, 70, 254, 55, 170, 138, 47, 98, 87, 184, 92, 48,
  143, 246, 202, 210, 44, 79, 240, 129, 240, 145, 0, 92, 197, 52, 207, 134, 60, 36}
tensor A power set={⎛ 1  0  0 ⎞, ⎛ 60  167  194 ⎞, ⎛ 42  166  219 ⎞, ⎛ 207  207  191 ⎞, ⎛ 50  156  50 ⎞, ⎛ 150  70   85  ⎞, ⎛ 4    112  42 ⎞,
                    ⎜ 0  1  0 ⎟  ⎜ 168  131  56  ⎟  ⎜ 95  198  94  ⎟  ⎜ 206  251  20  ⎟  ⎜ 4   124  8  ⎟  ⎜ 102  202  158 ⎟  ⎜ 249  80   83 ⎟
                    ⎝ 0  0  1 ⎠  ⎝ 66  16   91  ⎠  ⎝ 8   52   161 ⎠  ⎝ 83   168  234 ⎠  ⎝ 193  190  180 ⎠  ⎝ 24   177  151 ⎠  ⎝ 158  195  42 ⎠,
  ⎛ 219  146  134 ⎞, ⎛ 91  189  72  ⎞, ⎛ 32  110  202 ⎞, ⎛ 139  38   176 ⎞, ⎛ 21  56   58  ⎞, ⎛ 210  73   78  ⎞, ⎛ 131  239  222 ⎞,
  ⎜ 55   161  177 ⎟  ⎜ 113  77   210 ⎟  ⎜ 150  159  160 ⎟  ⎜ 243  42   212 ⎟  ⎜ 90  212  89  ⎟  ⎜ 242  115  180 ⎟  ⎜ 135  187  243 ⎟
  ⎝ 144  54   176 ⎠  ⎝ 41  243  20  ⎠  ⎝ 246  165  50  ⎠  ⎝ 251  234  213 ⎠  ⎝ 29  7    213 ⎠  ⎝ 207  135  41  ⎠  ⎝ 43   198  15  ⎠,
  ⎛ 141  182  133 ⎞, ⎛ 43  83   76  ⎞, ⎛ 78  205  235 ⎞, ⎛ 24   141  205 ⎞, ⎛ 72  121  83  ⎞, ⎛ 77   31   186 ⎞, ⎛ 162  97   125 ⎞,
  ⎜ 201  165  56  ⎟  ⎜ 58  228  24  ⎟  ⎜ 113  69   103 ⎟  ⎜ 114  78   103 ⎟  ⎜ 226  86   169 ⎟  ⎜ 179  156  251 ⎟  ⎜ 154  89   189 ⎟
  ⎝ 174  193  93  ⎠  ⎝ 221  163  158 ⎠  ⎝ 163  121  15  ⎠  ⎝ 209  224  91  ⎠  ⎝ 196  107  213 ⎠  ⎝ 139  43   103 ⎠  ⎝ 248  42   55  ⎠,
  ⎛ 207  186  58  ⎞, ⎛ 26  3    202 ⎞, ⎛ 82  14   2   ⎞, ⎛ 98   246  144 ⎞, ⎛ 171  119  142 ⎞, ⎛ 212  52   99  ⎞, ⎛ 252  149  94  ⎞,
  ⎜ 224  175  179 ⎟  ⎜ 246  42   105 ⎟  ⎜ 99  252  76  ⎟  ⎜ 239  214  234 ⎟  ⎜ 52   131  149 ⎟  ⎜ 41   31   92  ⎟  ⎜ 120  64   10  ⎟
  ⎝ 198  219  101 ⎠  ⎝ 158  169  59  ⎠  ⎝ 157  18   68  ⎠  ⎝ 238  153  110 ⎠  ⎝ 172  225  179 ⎠  ⎝ 45   95   169 ⎠  ⎝ 211  174  128 ⎠,
  ⎛ 76  73   209 ⎞, ⎛ 221  110  167 ⎞, ⎛ 228  133  118 ⎞, ⎛ 138  198  217 ⎞}
  ⎜ 79  149  81  ⎟  ⎜ 254  110  147 ⎟  ⎜ 166  61   61  ⎟  ⎜ 120  87   58  ⎟
  ⎝ 36  255  20  ⎠  ⎝ 96   169  164 ⎠  ⎝ 155  250  104 ⎠  ⎝ 222  163  223 ⎠
f(A)={{238, 175, 147}, {170, 142, 45}, {186, 90, 132}}
rA={{233, 62, 163}, {76, 50, 134}, {167, 131, 205}}
ALICE sends A, B, rA to BOB
.....................................................
BOB prepares...
r=3 791 045 539
s=4 075 263 003
coefficient list of h(x)={174, 13, 217, 229, 100, 171, 120, 190, 79, 192, 190, 25,
  83, 11, 173, 223, 221, 106, 216, 174, 41, 67, 176, 207, 53, 4, 139, 135, 220, 228, 136, 217}
tensor A power set={⎛ 1  0  0 ⎞, ⎛ 60  167  194 ⎞, ⎛ 42  166  219 ⎞, ⎛ 207  207  191 ⎞, ⎛ 50  156  50 ⎞, ⎛ 150  70   85  ⎞, ⎛ 4    112  42 ⎞,
                    ⎜ 0  1  0 ⎟  ⎜ 168  131  56  ⎟  ⎜ 95  198  94  ⎟  ⎜ 206  251  20  ⎟  ⎜ 4   124  8  ⎟  ⎜ 102  202  158 ⎟  ⎜ 249  80   83 ⎟
                    ⎝ 0  0  1 ⎠  ⎝ 66  16   91  ⎠  ⎝ 8   52   161 ⎠  ⎝ 83   168  234 ⎠  ⎝ 193  190  180 ⎠  ⎝ 24   177  151 ⎠  ⎝ 158  195  42 ⎠,
  ⎛ 219  146  134 ⎞, ⎛ 91  189  72  ⎞, ⎛ 32  110  202 ⎞, ⎛ 139  38   176 ⎞, ⎛ 21  56   58  ⎞, ⎛ 210  73   78  ⎞, ⎛ 131  239  222 ⎞,
  ⎜ 55   161  177 ⎟  ⎜ 113  77   210 ⎟  ⎜ 150  159  160 ⎟  ⎜ 243  42   212 ⎟  ⎜ 90  212  89  ⎟  ⎜ 242  115  180 ⎟  ⎜ 135  187  243 ⎟
  ⎝ 144  54   176 ⎠  ⎝ 41  243  20  ⎠  ⎝ 246  165  50  ⎠  ⎝ 251  234  213 ⎠  ⎝ 29  7    213 ⎠  ⎝ 207  135  41  ⎠  ⎝ 43   198  15  ⎠,
  ⎛ 141  182  133 ⎞, ⎛ 43  83   76  ⎞, ⎛ 78  205  235 ⎞, ⎛ 24   141  205 ⎞, ⎛ 72  121  83  ⎞, ⎛ 77   31   186 ⎞, ⎛ 162  97   125 ⎞,
  ⎜ 201  165  56  ⎟  ⎜ 58  228  24  ⎟  ⎜ 113  69   103 ⎟  ⎜ 114  78   103 ⎟  ⎜ 226  86   169 ⎟  ⎜ 179  156  251 ⎟  ⎜ 154  89   189 ⎟
  ⎝ 174  193  93  ⎠  ⎝ 221  163  158 ⎠  ⎝ 163  121  15  ⎠  ⎝ 209  224  91  ⎠  ⎝ 196  107  213 ⎠  ⎝ 139  43   103 ⎠  ⎝ 248  42   55  ⎠,
  ⎛ 207  186  58  ⎞, ⎛ 26  3    202 ⎞, ⎛ 82  14   2   ⎞, ⎛ 98   246  144 ⎞, ⎛ 171  119  142 ⎞, ⎛ 212  52   99  ⎞, ⎛ 252  149  94  ⎞,
  ⎜ 224  175  179 ⎟  ⎜ 246  42   105 ⎟  ⎜ 99  252  76  ⎟  ⎜ 239  214  234 ⎟  ⎜ 52   131  149 ⎟  ⎜ 41   31   92  ⎟  ⎜ 120  64   10  ⎟
  ⎝ 198  219  101 ⎠  ⎝ 158  169  59  ⎠  ⎝ 157  18   68  ⎠  ⎝ 238  153  110 ⎠  ⎝ 172  225  179 ⎠  ⎝ 45   95   169 ⎠  ⎝ 211  174  128 ⎠,
  ⎛ 76  73   209 ⎞, ⎛ 221  110  167 ⎞, ⎛ 228  133  118 ⎞, ⎛ 138  198  217 ⎞}
  ⎜ 79  149  81  ⎟  ⎜ 254  110  147 ⎟  ⎜ 166  61   61  ⎟  ⎜ 120  87   58  ⎟
  ⎝ 36  255  20  ⎠  ⎝ 96   169  164 ⎠  ⎝ 155  250  104 ⎠  ⎝ 222  163  223 ⎠
h(A)={{3, 7, 154}, {140, 34, 117}, {135, 127, 168}}
rB={{179, 70, 197}, {255, 130, 212}, {30, 233, 160}}
BOB sends rB to ALICE
.....................................................
ALICE session key=⎛ 235  96   236 ⎞
                  ⎜ 97   180  81  ⎟
                  ⎝ 235  222  114 ⎠
  BOB session key=⎛ 235  96   236 ⎞
                  ⎜ 97   180  81  ⎟
                  ⎝ 235  222  114 ⎠
.....................................................
```

**Table 2.** Output of the Mathematica 11.3 code of an interpreted session of HK17+.

## 4 Cryptographic security of HK17+

There is no way to adapt Bernstein and Li attacks to this HK17+ instance and other simplifying linear attacks would equally fail because of the field operations involved. There are two brute-force attacks we consider:

### 4.1 First kind brute-force attack

As the private polynomial search space of does not depend on the dimension of public tensors , there are $256^{k+1}$ Field Element Coefficient Polynomial of degree k and coefficients in $\mathbb{Z}_{256}$. To evaluate the computational effort, this cardinal we must the multiplied with the square of the integer exponent upper limit (zlimit) due to the private exponents pair (m, n). Here we present classical and quantum security levels as functions of the private keys polynomial degrees:

| *k-degree* of R-propped private key Polynomial and exponent *factor *f=1* | Conservative Classical Security (bits) | [Grover] Quantum Security (bits) | session time (setup-exchange-key derivation) (sec) | NIST security level for PQC proposals [6] |
|---|---|---|---|---|
| 7 | 64 | 32 | 2.5625 | Insecure |
| 15 | 128 | 64 | 2.7656 | Category 1 |
| 23 | 192 | 96 | 3.1094 | Category 3 |
| 31 | 256 | 128 | 3.3594 | Category 5 |

**Table 3.** Expected security and mean session time (Interpreted Mathematica 11.3) of increasing Polynomial degree used as private keys subject to classical and quantum attacks. To simplify interpretation, we consider here unitary exponents but in general the classical securities must be multiplied with a *factor $f = \lfloor 2log_2 u \rfloor$ for u>1. For the 3rd-round NIST PQC selection, Category 5 parameters must be supplied.

### 4.2 Second kind brute-force attack

This apparently more profitable attack searches directly the two unknown tensors powers replacing:

$$r_A = f^{\otimes m}(t_A) \otimes t_B \otimes f^{\otimes n}(t_A) \text{ or } r_B = h^{\otimes r}(t_A) \otimes t_b \otimes h^{\otimes s}(t_A) \quad [1]$$

$$r_A = x \otimes t_B \otimes y \quad [2]$$

$$K_A = x \otimes r_A \otimes y \quad [3]$$

With equation [2] witch depends on any public tensor r and unknown tensors (x,y) who once solved allow computing [3], the session key. We assume that the $u$ parameter is sufficiently big to foil power set brute-force explorations. This reduces SGDP to the DP problem [5] under field operations. A way to estimate present search difficulty is referring to matrix field operations and overall complexity will be related to dimension of the square matrices.

Suppose we work with 2-dim matrices (tensors), the pair (x,y) involves 8 unknown field elements (bytes) and 8 known field elements, equation [2] against ALICE could be defined as:

$$\begin{pmatrix} \mathrm{rA}_{11} & \mathrm{rA}_{12} \\ \mathrm{rA}_{21} & \mathrm{rA}_{22} \end{pmatrix} = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} . \begin{pmatrix} \mathrm{tB}_{11} & \mathrm{tB}_{12} \\ \mathrm{tB}_{21} & \mathrm{tB}_{22} \end{pmatrix} . \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix} \quad [4]$$

In expanded form, the rA matrix become:

$$\begin{pmatrix} (tB_{11}\,x_{11} + tB_{21}\,x_{12})\,y_{11} + (tB_{12}\,x_{11} + tB_{22}\,x_{12})\,y_{21} & (tB_{11}\,x_{11} + tB_{21}\,x_{12})\,y_{12} + (tB_{12}\,x_{11} + tB_{22}\,x_{12})\,y_{22} \\ (tB_{11}\,x_{21} + tB_{21}\,x_{22})\,y_{11} + (tB_{12}\,x_{21} + tB_{22}\,x_{22})\,y_{21} & (tB_{11}\,x_{21} + tB_{21}\,x_{22})\,y_{12} + (tB_{12}\,x_{21} + tB_{22}\,x_{22})\,y_{22} \end{pmatrix} \quad [5]$$

As a result, 2-dim attack involves 32 field product and 12 field sum operation. Considering that byte sums and multiplications in GF($2^8$) could be hardcoded (like AES does), each field operation involves 44 elementary lookup operations. Expanding the exposed equations, they resume into a set of 4 nonlinear equations:

$$\begin{aligned} rA_{11} &= tB_{11}\,x_{11}\,y_{11} + tB_{21}\,x_{12}\,y_{11} + tB_{12}\,x_{11}\,y_{21} + tB_{22}\,x_{12}\,y_{21} \\ rA_{12} &= tB_{11}\,x_{11}\,y_{12} + tB_{21}\,x_{12}\,y_{12} + tB_{12}\,x_{11}\,y_{22} + tB_{22}\,x_{12}\,y_{22} \\ rA_{21} &= tB_{11}\,x_{21}\,y_{11} + tB_{21}\,x_{22}\,y_{11} + tB_{12}\,x_{21}\,y_{21} + tB_{22}\,x_{22}\,y_{21} \\ rA_{22} &= tB_{11}\,x_{21}\,y_{12} + tB_{21}\,x_{22}\,y_{12} + tB_{12}\,x_{21}\,y_{22} + tB_{22}\,x_{22}\,y_{22} \end{aligned} \quad [6]$$

This non-linear set of four equations in 8 variables could not be linearized so a residual way to solve would be to perform a systematic exploration of 2-dim matrices space for each variable. As a result, each variable takes 256 values giving a total of $256^8$ combinations, a 64-bit space. Similarly, given a greater dimension like 3, there would appear a nonlinear system of 9 equations with 18 unknowns, yielded a search space of 144-bit. Table 4. resumes further security levels.

| *d-degree* of matrices (tensors) | Classical Security (bits) | [Grover] Quantum Security (bits) | NIST security level for PQC proposals [6] |
|---|---|---|---|
| 2 | 64 | 32 | Insecure |
| 3 | 144 | 72 | Category 1 |
| 4 | 256 | 128 | Category 5 |
| 5 | 400 | 200 | Category>>5 |

**Table 4.** Expected security of increasing matrix (tensor) dimension of HK17+ against classical and quantum attacks if the second kind of brute-force attack is used. Clearly any randomized polynomial time attack must find a better algorithm to proceed.

## 5 Conclusions

We present a reasonable way to increase the security of the original HK17 protocol simply switching from hypercomplex numbers to rank-3 tensors and GF($2^8$) operations. For real-life use we recommend using at least k=31 and d=4 to reach NIST Category 5 security. Further works of the author covering PQC can be found at [10].

## References


1. NIST, https://www.nist.gov/news-events/news/2020/07/pqc-standardization-process-third-round-candidate-announcement, 2020
2. P. Hecht, J, Kamlofsky, HK17: Post Quantum Key Exchange Protocol Based on Hypercomplex Numbers, NIST PQC Standarization Proposals, Round 1, https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions, 2017
3. D. Bernstein, T. Lange, HK17 Official Comment, Dec 25., https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/official-comments/HK17-official-comment.pdf, 2017
4. H. Li, R. Liu, Y. Pan, T. Xie, Cryptanalysis of HK17, Cryptology ePrint https://eprint.iacr.org/2017/1259.pdf, 2017
5. A. Myasnikov, V. Shpilrain, A. Ushakov, Non-commutative Cryptography and Complexity of Group-theoretic Problems, Mathematical Surveys and Monographs, AMS Volume 177, 2011

6. P. Hecht, PQC: R-Propping of Public-Key Cryptosystems Using Polynomials over Non-commutative Algebraic Extension Rings, Preprint IACR, https://eprint.iacr.org/2020/1102.pdf
7. Z. Cao, X. Lei, L. Wang, New Public Key Cryptosystems Using Polynomials over Non-commutative Rings, Preprint IACR, http://eprint.iacr.org/2007/009.pdf 1.2
8. D. J. Bernstein, T. Lange, "Post-Quantum Cryptography", Nature, 549:188-194, 2017.
9. P. Hecht, Algebraic Extension Ring Framework for Non-Commutative Asymmetric Cryptography, Preprint ,arXiv https://arxiv.org/ftp/arxiv/papers/2002/2002.08343.pdf 1.2, 2020
10. https://arxiv.org/a/hecht_p_1.html