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 \( o = a_0 e_0 + \cdots + a_7 e_7 \), when all the coordinates of \( o \) 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 \( g(o) = a o + b \).

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) = $2^{32} = 4,294,967,296$
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.
<table>
<thead>
<tr>
<th><strong>Table 2.</strong> Output of the Mathematica 11.3 code of an interpreted session of HK17+.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ALICE prepares...</strong></td>
</tr>
<tr>
<td><strong>dim=3</strong></td>
</tr>
<tr>
<td>degree exponent = 4294967296</td>
</tr>
</tbody>
</table>
| tensor A = \[
\begin{bmatrix}
60 & 167 & 194 \\
168 & 131 & 56 \\
66 & 16 & 91
\end{bmatrix}
\] |
| tensor B = \[
\begin{bmatrix}
155 & 112 & 101 \\
168 & 204 & 104 \\
90 & 28 & 232
\end{bmatrix}
\] |
| m = 1293503137 |
| n = 2694910038 |
| coefficient list of \( f(x) = (171, 8, 136, 70, 254, 55, 170, 138, 47, 98, 87, 184, 92, 48, 141, 246, 202, 210, 44, 79, 240, 129, 240, 145, 0, 92, 197, 52, 207, 134, 60, 36) \) |
| tensor A power sum = \[
\begin{bmatrix}
0 & 0 & 0 \\
0 & 0 & 0 \\
0 & 0 & 0
\end{bmatrix}
\] |
| tensor A power sum = \[
\begin{bmatrix}
2 & 1 & 4 \\
2 & 1 & 4 \\
2 & 1 & 4
\end{bmatrix}
\] |
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 $\mathbb{Z}_p$. 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:

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

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 $f = \lfloor 2 \log_2 u \rfloor$ 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:

\[
\begin{align*}
    r_A &= f^\otimes m(t_A) \otimes t_B \otimes f^\otimes n(t_A) \quad \text{or} \quad r_B = h^\otimes r(t_A) \otimes t_B \otimes h^\otimes x(t_A) \quad [1] \\
    r_A &= x \otimes t_B \otimes y \quad [2] \\
    K_A &= x \otimes r_A \otimes y \quad [3]
\end{align*}
\]

With equation [2] which 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:

\[
\begin{pmatrix}
    r_{A11} & r_{A12} \\
    r_{A21} & r_{A22}
\end{pmatrix} =
\begin{pmatrix}
    x_{11} & x_{12} \\
    x_{21} & x_{22}
\end{pmatrix} \cdot
\begin{pmatrix}
    t_{B11} & t_{B12} \\
    t_{B21} & t_{B22}
\end{pmatrix} \cdot
\begin{pmatrix}
    y_{11} & y_{12} \\
    y_{21} & y_{22}
\end{pmatrix}
\]  [4]

In expanded form, the $r_A$ matrix become:
As a result, 2-dim attack involves 32 field product and 12 field sum operation. Considering that byte sums and multiplications in $\text{GF}(2^8)$ 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:

\[
\begin{align*}
(tB_{11} x_{11} + tB_{12} x_{12}) y_{11} + (tB_{21} x_{11} + tB_{22} x_{12}) y_{12} \\
(tB_{11} x_{11} + tB_{12} x_{12}) y_{11} + (tB_{21} x_{11} + tB_{22} x_{12}) y_{12} \\
(tB_{11} x_{11} + tB_{12} x_{12}) y_{11} + (tB_{21} x_{11} + tB_{22} x_{12}) y_{12} \\
(tB_{11} x_{11} + tB_{12} x_{12}) y_{11} + (tB_{21} x_{11} + tB_{22} x_{12}) y_{12}
\end{align*}
\]  

As a result, 2-dim attack involves 32 field product and 12 field sum operation. Considering that byte sums and multiplications in $\text{GF}(2^8)$ 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:

\[
\begin{align*}
ra_{11} &= tB_{11} x_{11} y_{11} + tB_{12} x_{12} y_{11} \\
ra_{12} &= tB_{11} x_{11} y_{12} + tB_{12} x_{12} y_{12} \\
ra_{21} &= tB_{21} x_{21} y_{11} + tB_{22} x_{22} y_{11} \\
ra_{22} &= tB_{21} x_{21} y_{12} + tB_{22} x_{22} y_{12}
\end{align*}
\]

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.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>64</td>
<td>32</td>
<td>Insecure</td>
</tr>
<tr>
<td>3</td>
<td>144</td>
<td>72</td>
<td>Category 1</td>
</tr>
<tr>
<td>4</td>
<td>256</td>
<td>128</td>
<td>Category 5</td>
</tr>
<tr>
<td>5</td>
<td>400</td>
<td>200</td>
<td>Category&gt;&gt;5</td>
</tr>
</tbody>
</table>

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 $\text{GF}(2^8)$ 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