NIST Post-Quantum Cryptography

HK17: Algorithm Specifications and Supporting Documentation

Buenos Aires city, November 29th, 2017

National Institute of Standards and Technology,
Information Technology Laboratory,
100 Bureau Drive – Stop 8930, Gaithersburg, Maryland.
Attention: Post-Quantum Cryptographic Algorithm Submissions – Mr. Dustin Moody

Ref.: Executive Sumary of the proppoased algorithm: HK17

This document contains all the documentation to be able to offer a complete proposal of our cryptographic algorithm called HK17 as required in the CFP published in: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography.

HK17 consists broadly in a Key Exchange Protocol (KEP) based on non-commutative algebra of hypercomplex numbers limited to quaternions and octonions. In particular, this proposal is based on non-commutative and non-associative algebra using octonions.

Originally, tests and developments of the algorithm were made in Python 2.7. The technical description of the algorithm was made based on data and tests performed using this language. In order to fulfill the requirements of the NIST, the algorithms were coded optimized in Ansi C. However, since Python is a language in clear evolution present in multiple platforms, a sketch version in Python is also included.

HK17 has several parameters. We present here those that we consider to present the best compromise solution between security and performance, but HK17 is not limited to them. We hope and wish that throughout the evaluation process we can find better combinations of parameters.

The algorithm is parameterizable: just seting two parameters: p (platform – modulo) and d (degree of polynomials), the algorithm could be implemented in different platforms. We are proposing 4 profiles: 8 bits (with d = 16), 16 bits (with d = 32), 32 bits (with d = 64) and 64 bits (with d = 128). Together, it can cover a very wide range of devices. The profile for 8 bits platform called HK17-O-64 can provide security to very small devices such as memories, smart cards, small prototyping boards; the 16-bits profile called HK17-O-128 would provide security to medium size processors as included on industrial controllers; The 32-bits profile called HK17-O-256 offers security for devices with medium computing capacity. Finally, the 64 bits profile called HK17-O-256 offers security to larger processors. To comply with the requirements, the "reference" implementation will be the 8-bits profile (HK17-O-64). The implementation called "optimized" will be the 32 bits profile (HK17-O-256). Include a test version using the KAT files.

The strong points of our HK17 proposal are: (1) ordinary modular arithmetic, (2) no big number libraries needed, (3) relatively fast operation, (4) non-associativity of products and powers, (5) strong security even with small parameter sets, (6) no classical nor quantum attack at sight, (7) non-associativity of powers blocks side-channel attacks, (8) conjectured semantical security IND-CCA2 compliance, and (9) easy implementation in hardware.

In this document you can find: a complete written specification, a detailed performance and memory use analysis, a thorough description of the expected security strength, an analysis of the algorithm with respect to known attacks, a statement of advantages and limitations, and acknowledgements and a sheet about us.

We hope that the present work is pleasantly received.

…..

Hecht, Juan Pedro
Principal Submitter

…..

Kamlofsky, Jorge Alejandro
Auxiliar Submitter

HK17: Post Quantum Key Exchange Protocol Based on Hypercomplex Numbers

Juan Pedro Hecht[1] – Jorge Alejandro Kamlofsky[2]

[1] University of Buenos Aires, Economical Sciences Faculty, Exact and Natural Sciences Faculty, Engineering Faculty.
Master in IT Security, 2122 Córdoba Av. Buenos Aires, Argentina.
phecht@dc.uba.ar

[2] CAETI - Interamerican Open University (UAI)
725 Montes de Oca Av. Buenos Aires, Argentina.
Jorge.Kamlofsky@uai.edu.ar

Abstract. Encrypted communications are performed using symmetric ciphers, which require asymmetric cryptography for safe initiation. Asymmetric cryptography was seriously weakened after the presentation of Shor's algorithm for quantum computers. Supposedly quantum resistant algorithms are classified as post-quantum cryptography (PQC). Asymmetric cryptography based on non-commutative and non-associative algebraic systems is a growing trend arising as a solid PQC choice. Hyper-complex numbers generated from complex numbers by the Cayley-Dickson construction forms non-commutative and non-associative algebraic structures. This paper presents a PQC key exchange system performing operations with these numbers. Non-associativity of quaternions grants additional security features like blocking side-channel attacks i.e. those based on square and multiply routines. Finally, we conjecture for octonions, the pretended semantic security level IND-CCA2.

Keywords: octonion's cipher, quaternion's cipher, non-commutative cryptography, post-quantum cryptography, IND-CCA2.

1 Introduction

Post-quantum cryptography (PQC) collectively represents a branch of study in the current cryptology [1,2] and has recently been brought into focus by NIST [3,4]. The central objective is to generate protocols that resist quantum attacks such as that proposed by Shor [5]. It refers to the development of asymmetric cryptography since the mentioned attack breaks in polynomial time the problem of the discrete logarithm (DLP) in simple numerical and algebraic fields and consequently other ones linked as the integer factorization problem (IFP) [6]. Main lines belong to code-based encryption, lattice-based encryption, multivariate public key cryptography, and Merkle trees using hashing functions [1]. However, these variants do not exclude another class of protocols, including essentially algebraic solutions that do not focus their security on the use of extended precision libraries, numerical fields [7] and large prime numbers. In this sense, it is worth noting what is collectively known as non-commutative cryptography (NCC) since the last decade of the last century [8,9,10,11,12] and as an alternative non-associative cryptography (NAC) [13].

Our team has focused on the study of PQC solutions of an algebraic nature [14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24]. Particularly in the last three references, a generalized Diffie-Hellman key exchange protocol based on hypercomplex numbers were presented, which, in our view, offer a significant cryptographic potential. In this work, this path is deepened, applying algebra of octonions [25].

The present protocol is simple, secure and easily adaptable to all kinds of solutions pursued by asymmetric cryptography, such as key transport, generalized ElGamal encryption, digital signature and ZKP knowledge authentication [10].

The family of protocols here presented do not require the use of extended precision libraries. Therefore they can be implemented in small processors. The implementation of the protocol by quaternions (HK17-Q) achieves the generation of keys very quickly in comparison with similar implementations using matrices [14]. The implementation with octonions [24] (HK17-O), allows its implementation in elementary processors because the whole protocol is achieved with sum-product operations, with an additional security plus.

The security of an asymmetric protocol inevitably lies in some one-way (OWF) function which is modified to act as a one-way trap function (OWTF) [6]. Our protocol uses the generalized decomposition (DP) or the generalized symmetric decomposition (GSDP) and in some cases the double coset problem (DCP) [8,9,10]. These complex problems for which a probabilistic solution in polynomial time either classical or quantum is generally unknown would belong to the quantum complexity class in AWPP time, though outside the BQP set [26]. If this conjecture was true, it would force the adversary and as their best option, to perform a brute-force attack on the private key space. By carefully designing such space, a high computational security is achieved that operates in reasonable computational time. The rationale for safety focuses on ensuring that the octonions protocol conforms to the standard IND-CCA2 [27, 33].

Hypercomplex numbers are an extension of complex numbers constructed using abstract algebra tools. Hypercomplex numbers are ternions, quaternions, tesarins, octonions, sedenions, and so on. They have more than one complex component. Many of them build algebras that lack interest in our analysis. However, those which can be shaped by the Cayley-Dickson construction [25] can be of great cryptographic interest, which is what is proposed here.

Such construction produces a sequence of algebras over the field of real numbers. Each algebra produced has a double size of the previous one. At each stage, when a new algebra is generated, a specific algebraic property is lost [25]. Complex numbers can be understood as a pair of real numbers. The complex numbers are obtained from the real numbers. Similarly, quaternions can be defined from the complex numbers [31]. That is, they can be thought of as a pair of complex numbers and obtain the sum, product, conjugation, and norm. By repeating the process, the algebras of higher dimension can be found.

By applying the Cayley-Dickson process over the field of the real numbers and obtaining complex numbers, the relation of order is lost. The application over the field of the complex numbers forms the algebra of quaternions: it causes them to lose the commutative property. Then, the quaternions [31] form a division ring structure. Applying the process on the quaternions ring, the algebra of octonions is generated: the associative property is lost. The octonions form a normed division algebra. The structure of the algebra of sedenions (16 components) removes the property of being a division algebra, which is inherited to the later superior algebras generated after successive applications of the process, making them not interesting for its use in cryptography in general, and particularly in PQC.

Finally, the use of hypercomplex numbers that form non-commutative algebras for using in PQC is therefore limited to quaternions and octonions.

2 Objectives

This project has the following objectives:

2.1. To develop a parametric family of multifunctional asymmetric protocols of the PQC class, based on the use of modular polynomials of hypercomplex numbers and one-way functions derived from GSD / DP / DCP complex algebraic problems, with safety conjectured for octonions at the IND-CCA2 level. While it is not demonstrated that the protocol adhere to this standard, they provide all the necessary arguments to be able to arrive at the concrete demonstration in a continuation of the present project.

2.2. This presentation addresses the application of the protocol to the key exchange function, but its direct adaptation to other functionalities such as key transport, encryption, digital signatures and interactive authentication tests of zero knowledge is considered.

2.3. To obtain a set of parameters that provide balanced solutions between security and computational performance, both in unrestricted platforms in their capacities and in those of small size.

3 Proposed Key Exchange Protocol

3.1 HK17-Q: Implementation of the HK17 protocol with quaternions

Initialization:

(a) ALICE choose two non-zero quaternions A and B with elements in Z_p, where p is the maximum prime in 4, 8, 16 and 32 bits: p = 13, 251, 65521 and 4294967279.

(b) ALICE compute q_A, q_B: the normalization of A and B.

(c) ALICE choose as a private key, two non-zero elements m, n in Z and a non-zero polynomial f(x) of degree d with coefficients in Z_p with d = 16, 32 or 64 such that $f(q_A) \neq 0$.

(d) BOB choose as a private key, two non-zero elements r, s in Z and a non-zero polynomial h(x) of degree d with coefficients in Z_p with d = 16, 32 or 64 such that $h(q_A) \neq 0$.

(e) ALICE send to BOB q_A, q_B over the insecure channel.

Computing the tokens:

(f) ALICE compute her token: With $f'(q_A)$ the normalization of $f(q_A)$, then: $r_A = f'(q_A)^m . q_B . f'(q_A)^n$ and send it to BOB over the insecure channel.

(g) BOB compute his token: With $h'(q_A)$ the normalization of $h(q_A)$, then: $r_B = h'(q_A)^r . q_B . h(q_A)^s$ and send it to ALICE over the insecure channel.

Computing Session Keys:

(h) ALICE compute her key: $k_A = f'(q_A)^m . r_B . f'(q_A)^n$.

(i) BOB compute his key: $k_B = h'(q_A)^r . r_A . h'(q_A)^s$.

Can be verified that: $k_A = f'(q_A)^m . h'(q_A)^r . q_B . h'(q_A)^s . f'(q_A)^n = h'(q_A)^r . f'(q_A)^m . q_B . f'(q_A)^n . h'(q_A)^s = k_B$

(j) ALICE compute: $K_A = (k_A.p)(mod\ p)$

(k) BOB compute: $K_B = (k_B.p)(mod\ p)$

Finally: $K_A = K_B$.

Figure 1 shows a diagram of the working of the protocol HK17-Q.

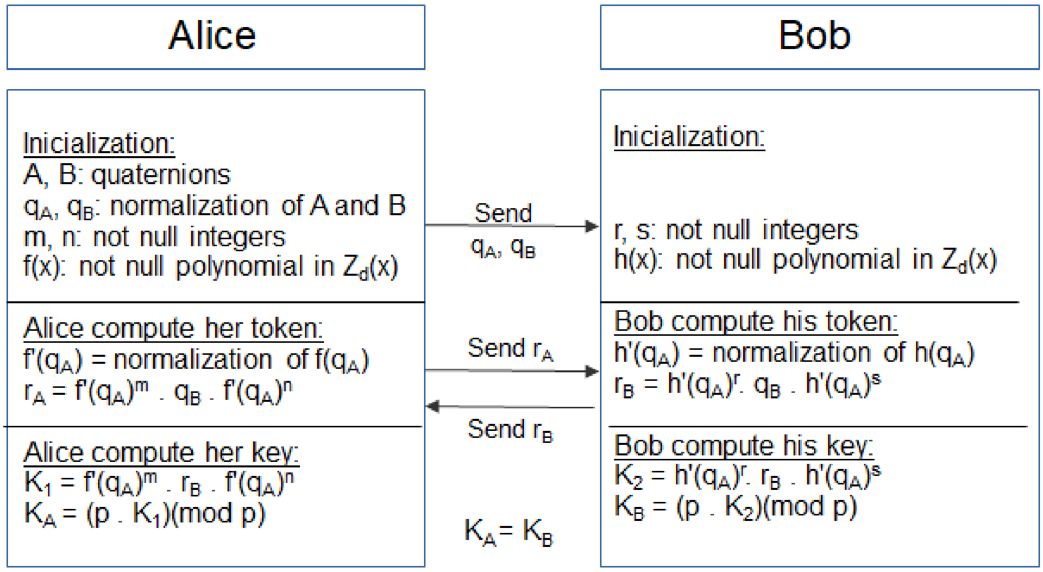

Alice
Bob
Inicialization:
A, B: quaternions
q_A, q_B: normalization of A and B
m, n: not null integers
f(x): not null polynomial in $Z_d(x)$
Send
q_A, q_B
Inicialization:
r, s: not null integers
h(x): not null polynomial in $Z_d(x)$
Alice compute her token:
$f'(q_A)$ = normalization of $f(q_A)$
$r_A = f'(q_A)^m . q_B . f'(q_A)^n$
Send r_A
Send r_B
Bob compute his token:
$h'(q_A)$ = normalization of $h(q_A)$
$r_B = h'(q_A)^r . q_B . h'(q_A)^s$
Alice compute her key:
$K_1 = f'(q_A)^m . r_B . f'(q_A)^n$
$K_A = (p . K_1)(mod\ p)$
$K_A = K_B$
Bob compute his key:
$K_2 = h'(q_A)^r . r_B . h'(q_A)^s$
$K_B = (p . K_2)(mod\ p)$

Figure 1. Diagram of the working of the protocol HK17 using quaternions (HK17-Q).

Observation:

The result obtained consists of a vector of four components, with elements in Z_p. Therefore, depending on the required key length, the process must be repeated as many times as necessary. It is suggested to limit (m,n,r,s) to Z^*_{257}.

3.2 HK17-O: Implementation of the HK17 protocol with Octonions

Initialization:

(a) ALICE choose two non-zero octonions o_A and o_B with elements in Z_p, where p is the maximum prime in 4, 8, 16 and 32 bits: p = 13, 251, 65521 and 4294967279.

(b) ALICE choose as the private key, two non-zero elements m, n in Z and a non-zero polynomial $f(x)$ of degree d with coefficients in Z_p, with $d = 16$ *and* 32 such that $f(o_A) \neq 0$.

(c) BOB choose as the private key, two non-zero elements r, s in Z and a non-zero polynomial $h(x)$ of degree d with coefficients in Z_p, with $d = 16$ *and* 32 such that $h(o_A) \neq 0$.

(d) ALICE send to BOB o_A , o_B over the insecure channel.

Computing the tokens:

(e) ALICE compute her token: $r_A = f(o_A)^m . o_B. f(o_A)^n$ and send it to BOB over the insecure channel.

(f) BOB compute his token: $r_B = h(o_A)^r . o_B . h(o_A)^s$ and send it to ALICE over the insecure channel.

Computing Session Keys:

(g) ALICE compute her key: $K_A = f(o_A)^m . r_B . f(o_A)^n$

(h) BOB compute his key: $K_B = h(o_A)^r . r_A . h(o_A)^s$

Can be verified that: $K_A = f(o_A)^m . h(o_A)^r . o_B. h(o_A)^s . f(o_A)^n = h(o_A)^r . f(o_A)^m . o_B . f(o_A)^n . h(o_A)^s = K_B$

Finally: $K_A = K_B$.

Figure 2. shows a diagram of the working scheme of the protocol HK17-O.

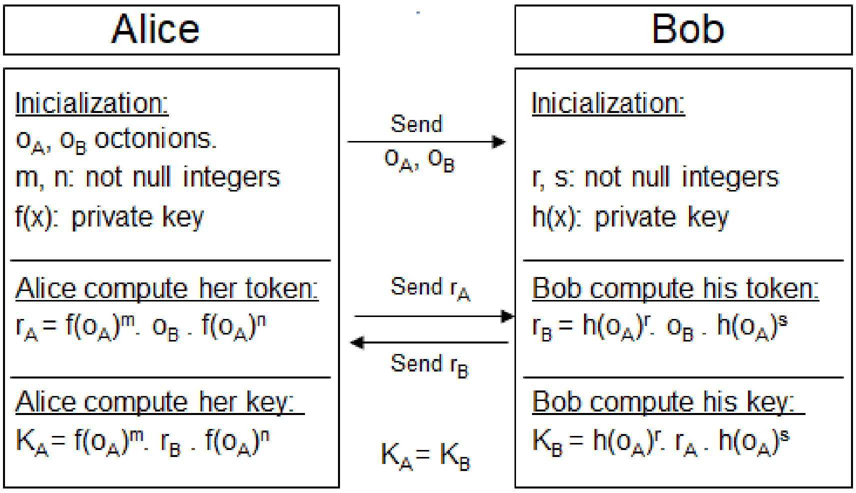


Figure 2. Diagram of the working scheme of the protocol HK17 using octonions (HK17-O).

Observation:

The result obtained consists of an eight-component vector, with elements in Zp. Therefore, depending on the required key length, the process must be repeated as many times as necessary or alternatively expand the random key using a cryptographically secure Hashing function. It is suggested to limit *(m,n,r,s)* to Z^*_{257}.

4 Protocol Security Analysis

4.1 General Considerations

The security analysis is focused on the protocol based on the use of octonions, although it is applied similarly to the protocol that operates with quaternions. This decision is reasonable for two reasons, firstly because of both base the protection of private keys on the same one-way function (GSDP / DP) and secondly because the security of the protocol using octonions exceeds significantly that based on quaternions.

This presentation of a Diffie-Hellman protocol is not limited to it and it is easily translatable to other asymmetric protocols such as key transport (Baumslag) [10], Encryption (ElGamal) [15], Digital Signature (ElGamal) and Zero Knowledge Proof (ZKP) authentication [16]. For this reason, the security analysis is not limited to the present example and can be extended in new contexts. In order with proceeding to this analysis, two conjectures which will be later justified more formally, are taken as starting point.

DEFINITION (D1): ***interactive challenge-response game by a verifier against an active adversary.***
In this three-phase protocol, two entities, an adversary and a verifier (or challenger) are involved. The verifier has a secret key that he tries to hide from the adversary and allows the adversary to pose questions to him that answers truthfully like an Oracle. In a first phase, the adversary can raise all the questions that he wants to try to obtain information about the secret key. In a second phase, the verifier presents the secret key (k) to the adversary next to another of equal length and format (k) randomly generated. Even during the second phase, the adversary may continue to consult the verifier, except for questions linked to the disclosure of the secret itself. In the third phase, the adversary has a polynomial time stochastic algorithm and must distinguish whether the secret is k or * k, with probability negligibly greater than ½ (defined in* [27, 33]*). If the opponent achieves the distinction with that probability, he wins the game and loses it in the opposite case.*

CONJECTURE (C1): Indistinguishability of polynomial transformed random octonions.
The octonions (or) are vectors of uniformly random integers of prime modulus and dimension eight. The modular polynomials f (x) of parametric (fixed) degree also have coefficients of uniformly random integer values of prime modulus. Such polynomials are monotonic, not trivial, and not necessarily irreducible. Since applying the polynomial f(x) to an octonion (o) implies modular sum and product (and power) on that argument, the result f(o) is another random octonion, although statistically, f(o) behaves differently to (o). Something equivalent happens with the powers of the value f(o). Given that non-biased cryptographically secure bitwise cryptographically secure bit generators (NBCSPRBG [6]*) are used, the transformation f(o) is indistinguishable from another similar g(*o) corresponding to another random polynomial g(x) of the same structure and applied on another octonion (*o). What can be concluded is that both f(o) and g(*o) are statistically distributed identically, as well as their respective powers. The consequence is that in an interactive challenge-response protocol (Definition D1), an adversary does not achieve the distinction raised with the required probability.*

CONJECTURE (C2): the octonion protocol adheres to semantical security under IND-CCA2.
The One-Way Function (OWF) [4] *Generalized Symmetric Decomposition Problem o simply Decomposition Problem (GSDP/DP)* [14,15,16] *with which the private key is protected are not weakened by attacks of probabilistically polynomial time, whether classical or quantum and that are in the public domain until today, forcing the potential attacker of the octonion protocol, or equivalent, to perform a systematic exploration of the private key space. Under this assumption and considering the indistinguishability of randomly generated octonions, it is reasonable to assign to the algorithm using it a (provisional) security mark equivalent to IND-CCA2* [27, 33] *(semantical security under IND-CCA2) which would be evident if the agreed key is used as a secret key of a symmetric cipher IND-CCA2 or by adapting the key exchange protocol to a generalized ElGamal encryption format secured by the same OWF* [15, 17].

To proceed to analyze the safety of the octonion protocol, the reasoning formalized in [27, 33] is followed and summarized here. A key exchange protocol will be secure if the shared key is totally unknown to a spy who has the public elements and values exchanged. This requires that the active adversary is unable to distinguish between the key generated by the protocol of any other session generated entirely randomly and of the same format. This requirement is stronger than the first stated condition and is necessary if the participating entities (Alice / Bob) proceed to perform some cryptographic task derived from the exchange of keys, such as the use of any symmetric encryption that is probably safe. As expected, the protocol will be secure if the adversary (definition D1) fails to successfully specify the contemplated distinction, with probability negligibly greater than ½. If this is the case, the protocol under study belongs to the class IND-CCA2.

It is clear that the key obtained is not a binary string but an element of an algebraic structure. However, this is not an impediment, as there are numerous uniform mapping procedures for transforming that element into a string through randomness extractors.

For the present protocol, it is not known probabilistic algorithm in polynomial time to proceed to the previously mentioned distinction and that is essentially what the Conjecture C2 expresses. Obviously, it is necessary that there is no algorithm of the stated kind of temporal complexity capable of solving the generalized discrete logarithm problem posed by GSDP / SDP. The only weakness assumed by the present protocol is the *man-in-the-middle* attack (MITM) [6, 27] although this impact is outside of this security analysis.

4.2 Security in detail

First, the statistical quality of the octonions generated is analyzed. In this sense, we start with the statistical distribution of the components of 1000 octonions randomly obtained and compare it with the corresponding powers of random polynomials of octonions, both for the case d = 32, p = 251.

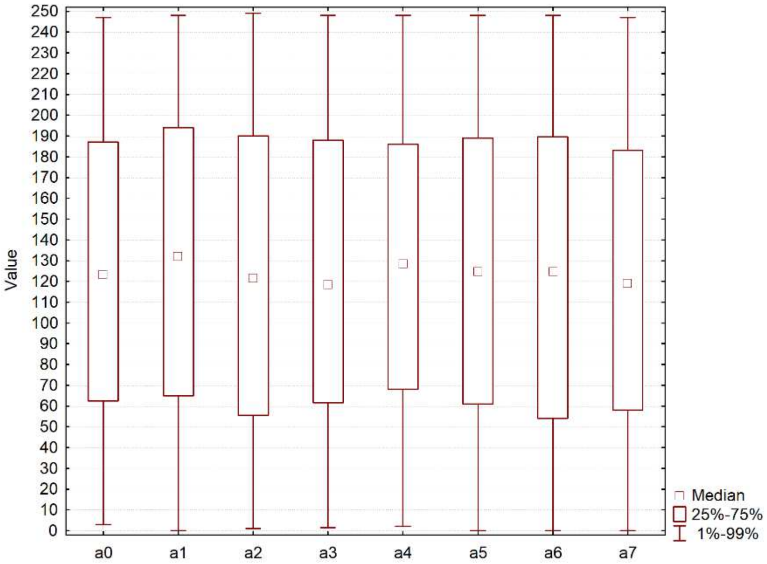


Figure 3. Distribution of the components of 1000 random octonions for the parameters: d=32, p=251.

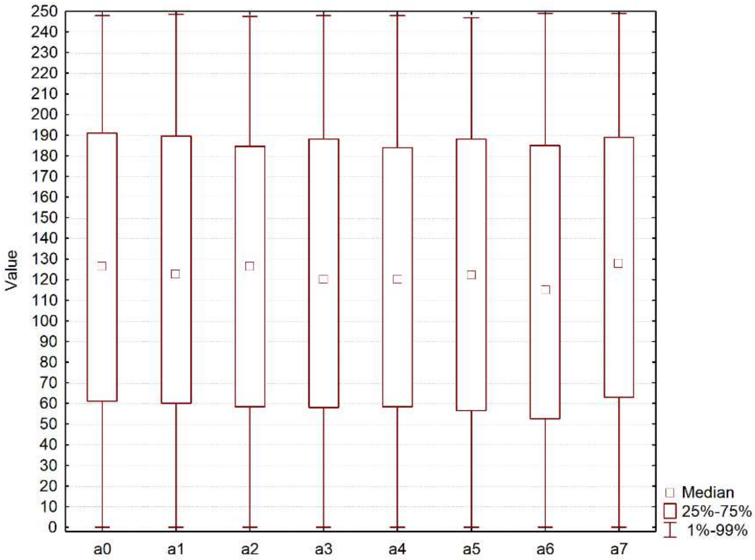


Figure 4. Distribution of the components of the 1000 successive powers of random polynomials of randomly generated octonions for parameters d = 32, p = 251.

Figure 3 shows the distribution of the components of 1000 randomly generated octonions. In Figure 4, we present the distribution of 1000 components of successive powers of a random polynomial applied to a random octonion and whose multiplicative order is 1800 not to repeat values. In all cases, the uniform and unbiased distribution of values throughout the range is qualitatively appreciated. The comparison between both distributions is not significant, indicating that it is not possible to distinguish the original random octonion from its powers, a necessary condition to support the hypothesis of indistinguishability required by the Conjecture C1.

Figure 4 shows the chaotic sequence of each of the eight modular components of 100 successive random octonions. Table 1 presents the non-parametric comparison of the eight components of the 100 randomly generated successive octonions presented in Figure 5. The result of a Friedman ANOVA and the Kendall Concordance Coefficient [28], indicates the uniform distribution and absence of correlation between these components.

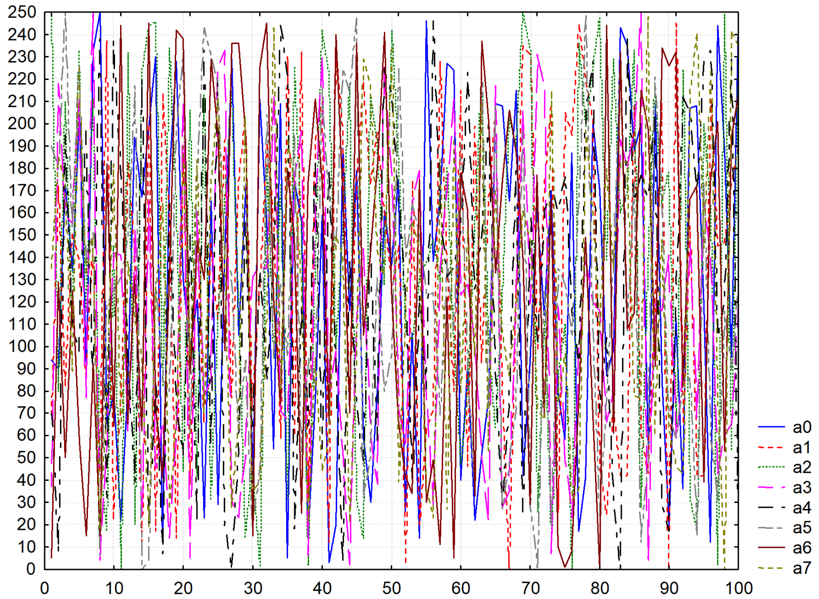


Figure 5. Chaotic distribution of the eight components of 100 successive random octonions for the parameters d = 32, p = 251

Friedman ANOVA and Kendall Coeff. of Concordance
ANOVA Chi Sqr. (N = 100, df = 7) = 4.631372 p = .70485
Coeff. of Concordance = .00662 Aver. rank r = -.0034

	Average Rank	Sum of Ranks	Mean	Std.Dev.
a0	4.480000	448.0000	127.8700	74.11998
a1	4.620000	462.0000	130.0200	73.67770
a2	4.860000	486.0000	138.5100	79.42018
a3	4.185000	418.5000	113.1400	68.90354
a4	4.510000	451.0000	124.8500	72.87534
a5	4.580000	458.0000	123.3700	69.42050
a6	4.385000	438.5000	131.1400	77.51299
a7	4.380000	438.0000	123.1500	67.15223

Table 1. Comparison statistics among the modular components corresponding to the 100 random octonions of Figure 2.

The monic polynomials forming private keys are of degree $d=2^s$ (*were* $s=2, 3, 4, 5,\ldots$) with coefficients and octonion terms in Z^*_p, where p is the greatest prime fitting in 4, 8, 16, 32, … bits. Values of polynomial degree (d) and prime module (p) are unrelated and should be set according to any situation.

Under these conditions [7, 25]:

(a) The quantity of non-zero octonions is

$$N_o = p^8 - 1 \qquad (1)$$

(b) The quantity of non-trivial (null and unitary) monic polynomials of degree d in the field $F_p[x]$ is

$$N_{tot} = p^d \ - \ 2 \qquad (2)$$

(c) Using the Möbius function μ, number of non-reducible polynomials of degree d in the field $F_p[x]$ is

$$N_p(d) = \frac{1}{d}\sum_{r|d} \ \ (d)p^{d/r} = \frac{p^d-2}{d} = \frac{N_{tot}}{d} \qquad (3)$$

(d) The multiplicative order of a polynomial randomly selected in $F_p[x]$ is empirically obtained studying the distribution of experimental periods.

The lower bound of the cardinal of private keys, using non-trivial monic polynomials and using unit exponents (the smallest possible multiplicative order), is

$$N_{pri}(d,p,s) \geq \big((p^8-1).(p^d-2)\ ^{2};\ p \approx 2^s\ ,\ d\ = 2^s \tag{4}$$

In this case of unit exponents, the GSDP / DP problem is transformed into an instance of the *Double Coset Problem* (DCP) described in [8, 9, 10, 17] and of which it is reasonable to suppose that is of less complexity than the first.

The distribution of power periods of random polynomials of random octonions was obtained empirically by Monte-Carlo simulation through 5000 tests of each configuration, using octonions, polynomials and evenly random powers within their natural range. This is the situation for which the operating speed is maximum since it is not controlled if the random polynomial is primitive or even irreducible. The computation of the median power periods (π) leads to the estimation of average security based on the cardinal of private keys.

$$\overline{N}_{pri}(d,p,s) = \big((p^8-1).(p^d-2)\ ^{2\pi};\ p \approx 2^s\ ,\ d\ = 2^s \tag{5}$$

The period π of each case is obtained with the lowest power of the random polynomial applied to a random octonion leading to the unit octonion, that is to say, its multiplicative order modulo p. The periods correspond to the predicted by the theory [7] and their values are respectively divisors of φ(p) and their multiples. The results of the simulation (Tables 2 and 3) are difficult to represent and can reach high values of periods, in fact, 16% of *d* = 16, p = 13 and 42% of d = 32, p = 251 exceeds arbitrary upper bound 8φ(p). The real upper bound of the periods is estimated at π. It is reasonable to use the median value of the computed periods as an average value, considering that even this parameter represents a significant underestimation and therefore leads to prudent safety values. Only lower bound security values are included Table 4.

We define the security levels until here described as the theoretical security against private key space attack. But it must be considered another kind of attack, much stronger, against HK17. We call it the empirical attack against the generated session keys. This kind of brute-force attack depends on the cardinal of session keys and forces a much lower and realistic security level. This empirical and real level of security is also shown in Table 4. We depict real security of single-pass session keys. Obviously, they could be increased in a multi-pass scenario, but this would be an artificial and inconvenient use of the protocol. We emphasize that every set of parameters selected, otherwise arbitrary, should be aiming obviously to the goal of attaining the highest security level with the fastest operational throughput.

Period	Count	Period	Count	Period	Count
1	69	13	18	52	55
2	123	14	98	56	323
3	182	21	159	78	45
4	247	24	143	84	304
6	421	26	28	> 8φ(p)	805
7	73	28	159	**All**	**5000**
8	51	39	54		
12 (*)	**1492**	42	151		

Table 2. Numerical distribution of power periods of 5000 random polynomials of (non-zero) octonions randomly chosen for the parameters (d = 16, p = 13). The median of the periods obtained is highlighted (*).

Period	Count	Period	Count	Period	Count	Period	Count	Period	Count	Period	Count
1	1	60	2	126	1	280	3	525	7	1125	17
10	2	63	2	150	1	300	4	600	9	1255	1
25	28	72	1	168	1	315	2	630	4	1260	8
28	2	75	2	175	5	350	5	700	10	1400	16
30	1	84	1	180	2	360	3	750	12	1500	16
35	1	90	1	200	4	375	12	840	8	1575	26
36	2	100	2	210	2	420	4	875	32	1750	18
45	2	105	2	225	7	450	5	900	11	1800	21
50	90	120	1	**250 (*)**	1815	500	10	1000	21	> $8\varphi(p)$	2114
56	1	125	612	252	1	504	3	1050	3	**All**	**5000**

Table 3. Numerical distribution of power periods of 5000 random polynomials of octonions (non-null) randomly chosen for the parameters (d = 32, p = 251). The median of the periods obtained is highlighted (*).

Set	d	p	Lower bound of the theoretical security level (bits)	Real pre-quantum security level of a single-pass protocol ([5]) (bits)	Real post-quantum security level of a single-pass protocol ([6]) (bits)	Unoptimized mean key generation time ([7]) (ms)
([1])	16	251	383	64	32	30
([2])	32	65521	1280	128	64	50
([3])	64	4294967291	4608	256	128	170
([4])	128	18446744073709551557	17408	512	256	1209

Table 4. Theoretical and real security bounds for the HK17-O protocol against private key and session-keys attacks in pre and post-quantum scenarios under conjecture C2 (IND-CCA2)

Table 4.: combination ([1]) works as reference implementation. Combination ([2]) would fit successfully on limited platforms. Combination ([3]) provides an interesting compromise solution between cryptographic security and operational speed on unrestricted platforms and combination ([4]) for high-security requirements. Irrespective of these limit parameter sets, alternatives could be applied to achieve solutions that best suit the case in question. ([5])([6]) Safety levels are on the same scale as any strong symmetric algorithm (AES). ([6]) This level is calculated taking into account Grover algorithm [34, 35]. Informed times ([7]) refer to means of 1000 runs.

Some concern about security in algebraic protocols was risen by Roman'kov [36]. He presents three different attacks to ElGamal type encryption schemes of such algebraic platforms cryptosystems and proposes that under some natural assumptions (but not detailed by the author), they are vulnerable to at least one of those algebraic attacks. In our protocol, we could not find any ways to proceed with any abelianization of our octonions non-associative Moufang loop [29] or reducing of the GSDP problem of polynomial powers of octonions to a finitely generated nilpotent image of the given free group in the cryptosystem and a further nonlinear decomposition attack. We simply conclude that Roman'kov attacks do not affect our proposal.

4.3. Summary

As indicated, the present analysis serves both quaternions and octonions. However, operating with octonions gives an advantage thanks to the dimension of the numerical vectors involved. In another order, it is necessary to emphasize the fact that the algebra of octonions, by forming a non-associative loop of Moufang [29], prevents to associate the powers [30] by which its computation cannot be accelerated using the square-and-multiply algorithm [6]. The powers must be obtained in a microscopically recursive form and that makes difficult the task of a potential systematic exploration and gives the using of octonions, a safety differential against the using of quaternions, that do have non-commutative ring structures [7]. This feature blocks many described side-channel attacks [32].

5 Numerical Examples and Performance Analysis

5.1 Platform Independence

The protocol has been tested on different platforms and operating systems, obtaining in all cases coincident values, which suggests that it does not functionally dependent on the specific characteristics of the platform used.

5.2 Numerical Example of HK17-Q: The Implementation of the HK17 Protocol with Quaternions.

An example of the implementation of the HK17 protocol with quaternions (HL17-Q) for p = 251 and d = 16 is presented. For presenting demonstrative simplicity, only four decimal places are used. As previously expressed, the four secret values *(m, n, r, s)* are arbitrarily chosen integers, here belonging to Z^*_{251}.

Initialization:

(a) ALICE choose quaternions: $A = (111, 248, 213, 109)$, $B = (99, 162, 164, 37)$.

(b) ALICE Normalizes quaternions A and B: $q_A = (0.3066, 0.6850, 0.5883, 0.3011)$, $q_B = (0.3904, 0.6388, 0.6467, 0.1459)$

(c) ALICE choose as private key the elements $m = 135$, $n = 245$, and the polynomial: $f(x) = 194x^{15} + 241x^{14} + 101x^{13} + 87x^{12} + 200x^{11} + 15x^{10} + 153x^9 + 58x^8 + 60x^7 + 148x^6 + 80x^5 + 175x^4 + 9x^3 + 242x^2 + 11x + 212.$

(d) Bob choose as private key the elements $r = 183$, s = 180, and the polynomial $h(x) = 62x^{15} + 124x^{14} + 196x^{13} + 236x^{12} + 238x^{11} + 113x^{10} + 58x^9 + 127x^8 + 185x^7 + 160x^6 + 175x^5 + 191x^4 + 223x^3 + 202x^2 + 243x + 103.$

(e) Alice sent to Bob: *(0.3066, 0.6850, 0.5883, 0.3011), (0.3904, 0.6388, 0.6467, 0.1459)* over the insecure channel.

Computing Tokens:

(f) Alice compute her token:

$f(0.3066, 0.6850, 0.5883, 0.3011) = 194.(0.3066, 0.6850, 0.5883, 0.3011)^{15} + 241.(0.3066, 0.6850, 0.5883, 0.3011)^{14} + 101.(0.3066, 0.6850, 0.5883, 0.3011)^{13} + 87.(0.3066, 0.6850, 0.5883, 0.3011)^{12} + 200.(0.3066, 0.6850, 0.5883, 0.3011)^{11} + 15.(0.3066, 0.6850, 0.5883, 0.3011)^{10} + 153.(0.3066, 0.6850, 0.5883, 0.3011)^9 + 58.(0.3066, 0.6850, 0.5883, 0.3011)^8 + 60.(0.3066, 0.6850, 0.5883, 0.3011)^7 + 148.(0.3066, 0.6850, 0.5883, 0.3011)^6 + 80.(0.3066, 0.6850, 0.5883, 0.3011)^5 + 175.(0.3066, 0.6850, 0.5883, 0.3011)^4 + 9.(0.3066, 0.6850, 0.5883, 0.3011)^3 + 242.(0.3066, 0.6850, 0.5883, 0.3011)^2 + 11.(0.3066, 0.6850, 0.5883, 0.3011) + 212.(1.0000, 0.0000, 0.0000, 0.0000) =(342.4786, -42.4031, -36.4188, -18.6369)$. Their normalization: $f'(q_A) = (0.9855, -0.1220, -0.1048, -0.0536)$

$r_A = (0.9855, -0.1220, -0.1048, -0.0536)^{135} . (0.3904, 0.6388, 0.6467, 0.1459) . (0.9855, -0.1220, -0.1048, -0.0536)^{245}$ ==> r_A = (0.2663, 0.1556, 0.1643, 0.0190) and send it to Bob.

(g) Bob compute his token:

$h(0.3066, 0.6850, 0.5883, 0.3011) = 62.(0.3066, 0.6850, 0.5883, 0.3011)^{15} + 124.(0.3066, 0.6850, 0.5883, 0.3011)^{14} + 196.(0.3066, 0.6850, 0.5883, 0.3011)^{13} + 236.(0.3066, 0.6850, 0.5883, 0.3011)^{12} + 238.(0.3066, 0.6850, 0.5883, 0.3011)^{11} + 113.(0.3066, 0.6850, 0.5883, 0.3011)^{10} + 58.(0.3066, 0.6850, 0.5883, 0.3011)^9 + 127.(0.3066, 0.6850, 0.5883, 0.3011)^8 + 185.(0.3066, 0.6850, 0.5883, 0.3011)^7 + 160.(0.3066, 0.6850, 0.5883, 0.3011)^6 + 175.(0.3066, 0.6850, 0.5883, 0.3011)^5 + 191.(0.3066, 0.6850, 0.5883, 0.3011)^4 + 223.(0.3066, 0.6850, 0.5883, 0.3011)^3 + 202.(0.3066, 0.6850, 0.5883, 0.3011)^2 + 243.(0.3066, 0.6850, 0.5883, 0.3011) + 103.(1.0000, 0.0000, 0.0000, 0.0000) = (-181.7140, 202.0317, 173.5191, 88.7962)$. Their normalization: $h'(q_A) = (-0.5434, 0.6041, 0.5189, 0.2655)$.

$r_B = (-0.5434, 0.6041, 0.5189, 0.2655)^{183}.(0.3904, 0.6388, 0.6467, 0.1459).(-0.5434, 0.6041, 0.5189, 0.2655)^{180}$ ==> r_B = (0.6509, 0.4941, 0.5453, 0.1005) and send it to Alice.

Computing Session Keys:

(h) Alice compute her key:
$K_A = (0.9855, -0.1220, -0.1048, -0.0536)^{135}.(0.6509, 0.4941, 0.5453, 0.1005).(0.9855, -0.1220, -0.1048, -0.0536)^{245}$ = (0.3184, 0.0799, 0.1076, -0.0081). $K_A = ((0.3184, 0.0799, 0.1076, -0.0081).251) \ (mod\ 251)$
$K_A = (79, 20, 27, 249)$

(i) Bob compute his key:
$K_B = (-0.5434, 0.6041, 0.5189, 0.2655)^{183}.(0.2663, 0.1556, 0.1643, 0.0190) .(-0.5434, 0.6041, 0.5189, 0.2655)^{180} = (0.3184, 0.0799, 0.1076, -0.0081)$. $K_B = ((0.3184, 0.0799, 0.1076, -0.0081).251) \ (mod\ 251)$
$K_B = (79, 20, 27, 249)$

Finally: $K_A = (79, 20, 27, 249) = K_B$.

5.3 Numeric Example of HK17-O: The Implementation of the HK17 Protocol with Octonions.

An example of the implementation of the HK17 protocol with octonions (HL17-O) is presented for p = 251 and d = 16. As previously expressed, the four secret values *(m, n, r, s)* are arbitrarily chosen integers, here belonging to Z^*_{251}.

Initialization:

(a) ALICE choose octonions o_A = (157, 188, 177, 188, 203, 149, 217, 148) and o_B = (40, 207, 6, 33, 75, 79, 98, 54).

(b) ALICE choose as private key the elements $m = 4$, $n = 122$ and the polynomial $f(x) = 97x^{15} + 98x^{14} + 6x^{13} + 136x^{12} + 238x^{11} + 150x^{10} + 5x^9 + 135x^8 + 186x^7 + 83x^6 + 168x^5 + 90x^4 + 238x^3 + 249x^2 + 150x + 180.$

(c) BOB choose as private key the elements $r = 17$, $s = 177$ and the polynomial $h(x) = 157x^{15} + 48x^{14} + 53x^{13} + 124x^{12} + 76x^{11} + 33x^{10} + 166x^9 + 76x^8 + 150x^7 + 52x^6 + 50x^5 + 40x^4 + 114x^3 + 58x^2 + 97x + 5.$

(d) ALICE send to BOB the octonions o_A = (157, 188, 177, 188, 203, 149, 217, 148) and o_B = (40, 207, 6, 33, 75, 79, 98, 54) over the insecure channel.

Computing Tokens:

(e) ALICE compute her token:

$f(157, 188, 177, 188, 203, 149, 217, 148) = 97.(157, 188, 177, 188, 203, 149, 217, 148)^{15} + 98.(157, 188, 177, 188, 203, 149, 217, 148)^{14} + 6.(157, 188, 177, 188, 203, 149, 217, 148)^{13} + 136.(157, 188, 177, 188, 203, 149, 217, 148)^{12} + 238.(157, 188, 177, 188, 203, 149, 217, 148)^{11} + 150.(157, 188, 177, 188, 203, 149, 217, 148)^{10} + 5.(157, 188, 177, 188, 203, 149, 217, 148)^9 + 135.(157, 188, 177, 188, 203, 149, 217, 148)^8 + 186.(157, 188, 177, 188, 203, 149, 217, 148)^7 + 83.(157, 188, 177, 188, 203, 149, 217, 148)^6 + 168.(157, 188, 177, 188, 203, 149, 217, 148)^5 + 90.(157, 188, 177, 188, 203, 149, 217, 148)^4 + 238.(157, 188, 177, 188, 203, 149, 217, 148)^3 + 249.(157, 188, 177, 188, 203, 149, 217, 148)^2 + 150.(157, 188, 177, 188, 203, 149, 217, 148) + 180.(1, 0, 0, 0, 0, 0, 0, 0) = (161, 14, 128, 14, 178, 190, 147, 246).$

$r_A = (161, 14, 128, 14, 178, 190, 147, 246)^4 . (40, 207, 6, 33, 75, 79, 98, 54) . (161, 14, 128, 14, 178, 190, 147, 246)^{122}$ = (121, 3, 110, 243, 184, 230, 202, 171). Alice send to BOB r_A over the insecure channel.

(f) BOB compute his token:

$h(157, 188, 177, 188, 203, 149, 217, 148) = 157.(157, 188, 177, 188, 203, 149, 217, 148)^{15} + 48.(157, 188, 177, 188, 203, 149, 217, 148)^{14} + 53.(157, 188, 177, 188, 203, 149, 217, 148)^{13} + 124.(157, 188, 177, 188, 203, 149, 217, 148)^{12} + 76.(157, 188, 177, 188, 203, 149, 217, 148)^{11} + 33.(157, 188, 177, 188, 203, 149, 217, 148)^{10} + 166.(157, 188, 177, 188, 203, 149, 217, 148)^9 + 76.(157, 188, 177, 188, 203, 149, 217, 148)^8 + 150.(157, 188, 177, 188, 203, 149, 217, 148)^7 + 52.(157, 188, 177, 188, 203, 149, 217, 148)^6 + 50.(157, 188, 177, 188, 203, 149, 217, 148)^5 + 40.(157, 188, 177, 188, 203, 149, 217, 148)^4 + 114.(157, 188, 177, 188, 203, 149, 217, 148)^3 + 58.(157, 188, 177, 188, 203, 149, 217, 148)^2 + 97.(157, 188, 177, 188, 203, 149, 217, 148) + 5.(1, 0, 0, 0, 0, 0, 0, 0) = (112, 177, 184, 177, 99, 179, 227, 134).$

$r_B = (112, 177, 184, 177, 99, 179, 227, 134)^{17} . (40, 207, 6, 33, 75, 79, 98, 54) . (112, 177, 184, 177, 99, 179, 227, 134)^{177}$ = (90, 42, 17, 119, 150, 23, 110, 182). Bob send to ALICE r_B over the insecure channel.

Computing session keys:

(g) ALICE compute her key: $K_A = (161, 14, 128, 14, 178, 190, 147, 246)^{4} \,.\, (90, 42, 17, 119, 150, 23, 110, 182) \,.\, (161, 14, 128, 14, 178, 190, 147, 246)^{122} = (84, 242, 130, 31, 84, 244, 45, 20)$

(h) BOB compute his key: $K_B = (112, 177, 184, 177, 99, 179, 227, 134)^{17} \,.\, (121, 3, 110, 243, 184, 230, 202, 171) \,.\, (112, 177, 184, 177, 99, 179, 227, 134)^{177} = (84, 242, 130, 31, 84, 244, 45, 20)$.

Finally: $\boldsymbol{K_A = (84, 242, 130, 31, 84, 244, 45, 20) = K_B}$.

5.4 Performance Analysis

Equipment Used. The used computer has an Intel® Core ™ i3-2328M CPU @ 2.20GHz × 4 and 3.7 GiB RAM. Kali GNU / Linux 64-bit operating system, with a Debian kernel. The algorithms were programmed and interpreted in Python 2.7.10.

Experimental Results. A comparison of the execution times for the obtaining of 1000 keys of 256 bits between different configurations of the protocol is presented. Table 5 shows the experimental results.

	CPU Time (s)			
	HK17-Q		HK17-O	
# Test	**d=16 – p=13**	**d=32 – p=251**	**d=16 – p=13**	**d=32 – p=251**
1	11.2096	9.2007	159.8864	145.5201
2	11.0282	9.1331	159.5625	147.3274
3	10.9511	9.1616	156.4030	148.5692
4	10.7975	9.1604	156.3475	146.6056
5	10.6980	9.6835	157.6077	147.6849
6	10.7913	9.1055	163.3307	146.4674
7	11.1125	9.1385	160.9185	149.1146
8	11.1388	9.2798	156.9379	159.9235
9	10.7496	9.3992	162.3867	144.9810
10	10.7799	8.9372	159.0211	150.9912
Average	**10.9257**	**9.2200**	**159.2402**	**148.7185**
Std. Deviation	**0.1858**	**0.2014**	**2.4586**	**4.3157**

Table 5: Execution times for obtaining 1000 256-bit keys in different configurations.

For each configuration, the reproducibility of the simulations is high. This confirms that the generation of random parameters produces unbiased values (see Figures 3, 4 and 5). It remains to demonstrate whether this uniform behavior contributes to the resilience of protocols to lateral channel attacks [32].

It is assumed that the results obtained can be improved since the code has not been yet optimized.

6 Conclusions

In the present project a family of asymmetric protocols of the PQC class was presented, from which it was conjectured that adheres to the safety standard IND-CCA2 [33]. This conjecture was empirically analyzed and substantiated. The minimum and average security bounds measured in bits for a couple of sets of reasonable parameters, at least one for non-limited platforms and other for reduced platforms. From the analysis executed and the computational behavior of the protocol, the potential utility of the protocol is deduced even in computational environments of scarce capacities like smartcards, USB cryptographic tokens, cellular telephones or any firmware migration. This is a direct consequence of the fact that the protocol does not make use of extended precision libraries and only uses sums and modular products with 8-bit representable primes.

7 The strong points of our proposal

In synthesis, the strong points of our HK17 proposal are: (1) ordinary modular arithmetic, (2) no big number libraries needed, (3) relatively fast operation, (4) non-associativity of products and powers, (5) parametric security levels, (6) no classical nor quantum attack at sight, (7) non-associativity of powers blocks side-channel attacks, (8) easy firmware migration and (9) conjectured semantical security IND-CCA2 compliance.

References

[1] D. Bernstein, J. Buchmann, E. Dahmen, Post-Quantum Cryptography, Springer Verlag, 2009

[2] Ç. Kaya Koç, Open Problems in Mathematics and Computational Science, Springer Verlag, 2014

[3] L. Chen et al, NISTIR 8105, Report on Post-Quantum Cryptography, NIST, 2006. http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf (consulted April 20, 2017)

[4] D. Moody, Update on the NIST Post-Quantum Cryptography Project, 2016 http://csrc.nist.gov/groups/SMA/ispab/ (consulted April 20, 2017)

[5] P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", SIAM J. Comput., no. 5, pp. 1484-1509, 1997.

[6] A. Menezes, P. van Oorschot and S.Vanstone, "Handbook of Applied Cryptography", CRC Press, 1997

[7] R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1997

[8] A. Myasnikov, V. Shpilrain, A. Ushakov, Non-commutative Cryptography and Complexity of Group-theoretic Problems, Mathematical Surveys and Monographs, AMS Volume 177, 2011

[9] M. I. González Vasco, R. Steinwandt, Group Theoretic Cryptography, CRC Press, 2015

[10] L. Gerritzen et al (Editors), Algebraic Methods in Cryptography, Contemporary Mathematics, AMS, Vol. 418, 2006

[11] B. Tsaban, Polynomial time solutions of computational problems in non-commutative algebraic crypto, 2012. http://arxiv.org/abs/1210.8114v2, (consulted April 20, 2017)

[12] D. Grigoriev and I. Ponomarenko, "Constructions in public-key cryptography over matrix groups", Preprint arXiv/math, no. 0506180v1, 2005. (consulted April 20, 2017)

[13] A. Kalka, Non-associative public-key cryptography, 2012. arXiv:1210.8270 [cs.CR] (consulted April 20, 2017)

[14] P. Hecht, Un modelo compacto de criptografía asimétrica empleando anillos no conmutativos, V Euromerican Congress of IT Security (CIBSI'09), 188-201, 2009.

[15] P. Hecht, Post-Quantum Cryptography(PQC): Generalized ElGamal Cipher over GF(251^8), ArXiv Cryptography and Security (cs.CR) http://arxiv.org/abs/1702.03587 6pp, 2017

[16] P. Hecht, Post-Quantum Cryptography: A Zero-Knowledge Authentication Protocol, ArXiv Cryptography and Security (cs.CR) https://arxiv.org/abs/1703.08630, 3pp, 2017

[17] P. Hecht, Post-Quantum Cryptography: S_{381} Cyclic Subgroup of High Order, ArXiv Cryptography, and Security (cs.CR) http://arxiv.org/abs/1704.07238 (preprint) & International Journal of Advanced Engineering Research and Science (IJAERS) 4:6, pp 78-86, 2017 https://dx.doi.org/10.22161/ijaers.4.6.10

[18] P. Hecht, A Zero-Knowledge authentication protocol using non-commutative groups, VI Euromerican Congress of IT Security (CIBSI'11), 96-102, 2011.

[19] P. Hecht, Criptografía no conmutativa usando un grupo general lineal de orden primo de Mersenne, VII Euromerican Congress of IT Security (CIBSI'13), 147-153, 2013.

[20] P. Hecht, A Post-Quantum Set of Compact Asymmetric Protocols using a General Linear Group, VIII Euromerican Congress of IT Security (CIBSI'15), 96-101, 2015.

[21] P. Hecht, Zero-Knowledge Proof Authentication using Left Self Distributive Systems: a Post-Quantum Approach, VIII Euromerican Congress of IT Security (CIBSI'15), 113-116, 2015.

[22] J. Kamlofsky and P. Hecht, O. A. Hidalgo Izzi, S. Abdel Masih, A Diffie-Hellman Compact Model over Non-Commutative Rings Using Quaternions, VIII Euromerican Congress of IT Security (CIBSI'15), 218-222, 2015.

[23] J. Kamlofsky, P. Hecht, and Samira Abdel Masih. Post-Quantum Cryptography: An Elementary and Compact Key Exchange Scheme Based on Octonions. IX Euromerican Congress of IT Security (CIBSI'17), 2017.

[24] J. Kamlofsky and P. Hecht. Post-Quantum Cryptography Using Hyper-Complex Numbers, XXIII Argentinean Congress of Computer Sciences (CACIC'17), 2017

[25] J. Baez, The Octonions, Bulletin of the American Mathematical Society, 39:2, 145-205, 2001.

[26] L. Fortnow, J. Rogers, Complexity Limitations on Quantum Computation, arXiv:cs/9811023 [cs.CC], 1998

[27] J. Katz, Y. Lindell, Introduction to Modern Cryptography, Chapman & Hall/CRC, 2008.

[28] G.W. Corder, D.I. Foreman, "Nonparametric Statistics: A Step-by-Step Approach", J. Wiley & Sons, 2014.

[29] V.D. Belousov: "Moufang loops", Hazewinkel, Michiel, Encyclopedia of Mathematics, Springer, 2001

[30] W.B. Vasantha Kandasamy, “Smarandache near-rings”, American Research Press, Rehoboth, 2002.

[31] W.R. Hamilton, Lectures on Quaternions: Containing a Systematic Statement of a New Mathematical Method. Hodges and Smith, 1853.

[32] Lawson, N.: Side-Channel Attacks on Cryptographic software, IEEE computer and reliability societies, https://www.computer.org/csdl/mags/sp/2009/06/msp2009060065.html, 2009.

[33] M. Bellare, A. Dessai, D. Pointcheval, P. Rogaway, Relations Among Notions of Security for Public-Key Encryption Schemes, Advances in Cryptology (CRYPTO '98), Lecture Notes in Computer Science Vol. 1462, H. Krawczyk ed., Springer-Verlag, 1998.

[34] L. K. Grover,A fast quantum mechanical algorithm for database search. In Proc. 28th Ann. ACM Symp. on Theory of Computing (ed. Miller, G. L.) 212–219, ACM, 1996.

[35] D. J. Bernstein, T. Lange, Post-quantum cryptography, Nature, 549:188, pp 188-194, 2017.

[36] V. Roman’kov, Cryptanalysis of a combinatorial public key cryptosystem, De Gruyter, Groups Complex. Cryptol. 2017

Juan Pedro Hecht received an MSc in Information Technology at Escuela Superior de Investigación Operativa (ESIO-DIGID) and a Ph.D. degree from Universidad de Buenos Aires (UBA). Currently, he is a researcher and full professor of cryptography at Information Security Graduate School at UBA, EST (Army Engineering School), ENI (National Intelligence School) and IUPFA (Federal Police University), he is research fellow UBACyT and Director of EUDEBA editorial board of UBA.
https://www.linkedin.com/in/juan-pedro-hecht-a6b52516/

Jorge Kamlofsky. Graduated with a degree in Mathematics in the Universidad Abierta Interamericana (UAI) and a Specialist in Cryptography and IT Security in the Faculty of Engineering of the Argentinean Army (EST-IUE). He is finishing a Master in IT in the UAI and doing a Doctorate in Engineering in the Faculty of Engineering of the National University of Lomas de Zamora (UNLZ). He is a professor of Discrete Mathematics in the UAI and Professor of Algebra and Analytic Geometry in the National Technological University (UTN). Also, he is a researcher in the Center for high studies on Information Technology (CAETI).
https://www.linkedin.com/in/jorgekamlofsky/

Buenos Aires city, November 29th, 2017

National Institute of Standards and Technology,
Information Technology Laboratory,
100 Bureau Drive – Stop 8930, Gaithersburg, Maryland.
Attention: Post-Quantum Cryptographic Algorithm Submissions – Mr. Dustin Moody

Ref.: Statement 2.b.2. Estimated Computational efficiency and memory requirements

As required in point 2.b.2, here we present an estimated computational efficiency and memory requirements for the “NIST PQC Reference Platform” as specified in Section 5.B.

Reference Equipment used:

Brand	Dell
Model	XPS 12 9Q33
Processor	Intel(R) Core(TM) i7-4510U CPU @ 2.00GHz, 2601 Mhz, 2 Core(s), 4 Logical Processor(s)
Installed Physical Memory (RAM)	8,00 GB
Full Specification	https://www.cnet.com/products/dell-xps-12-9q33-12-5-core-i7-4500u-8-gb-ram-256-gb-ssd/specs/
OS Name	Microsoft Windows 10 Home
Version	10.0.15063 Build 15063
Manufacturer	Microsoft Corporation

Computational efficiency:

The following table shows medium times in mili-seconds of the complete key generation process, based on averages of 1000 executions, in Ansi C compared with the implementation programmed in Python 2.7 presented in Table 4 of the Technical Description.

Profiles	Name	Degree of Polynomials	Minimum Platform	Key lenght	Key Generation Time (ms)	
					Ansi C	Python 2.7
Profile 1	HK17-O-64	16	8 bits	64 bits	2,25	19
Profile 2	HK17-O-128	32	16 bits	128 bits	4,42	38
Profile 3	HK17-O-256	64	32 bits	256 bits	13,4	189
Profile 4	HK17-O-512	128	64 bits	512 bits	85,64 (*)	1208

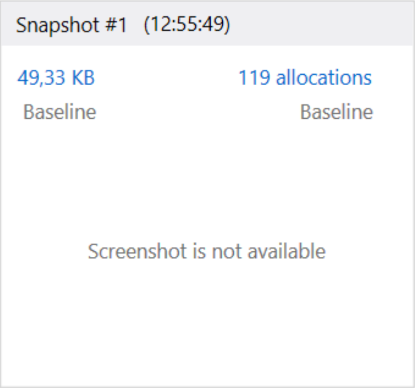
(*) Projected value

Memory requirement and consumption analysis:

Memory snapshots:

The following figures show memory allocation before, during and after algorithm execution.

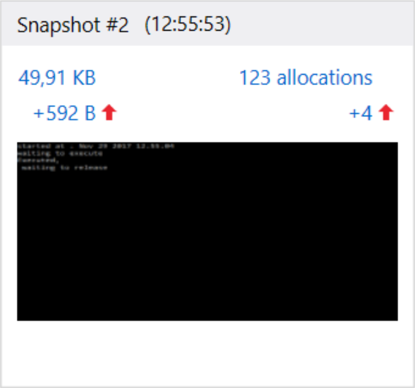
Profile 1 (8 bits):



Snapshot #1 (12:55:49)

49,33 KB
119 allocations
Baseline
Baseline

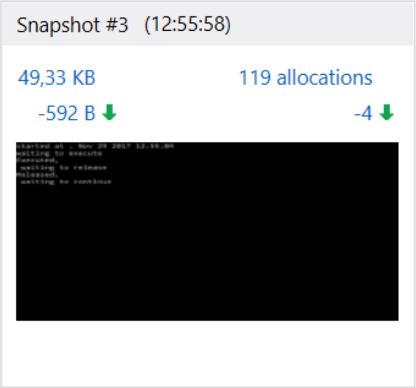
Screenshot is not available



Snapshot #2 (12:55:53)

49,91 KB
123 allocations
+592 B ⬆
+4 ⬆

```
started at : Nov 29 2017 12.55.04
waiting to execute
Executed,
 waiting to release
```

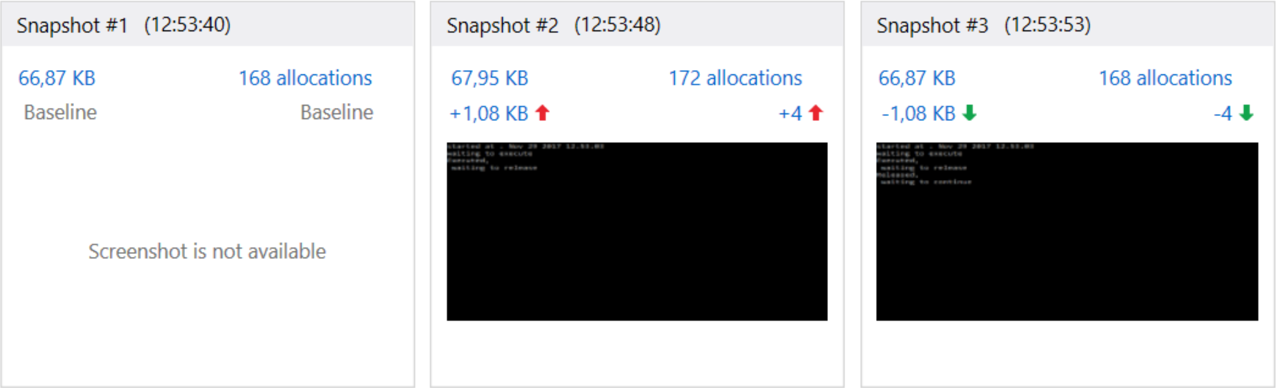


Snapshot #3 (12:55:58)

49,33 KB
119 allocations
-592 B ⬇
-4 ⬇

```
started at : Nov 29 2017 12.55.04
waiting to execute
Executed,
 waiting to release
Released,
 waiting to continue
```

Profile 2 (16 bits):



Snapshot #1 (12:53:40)
66,87 KB 168 allocations
Baseline Baseline
Screenshot is not available

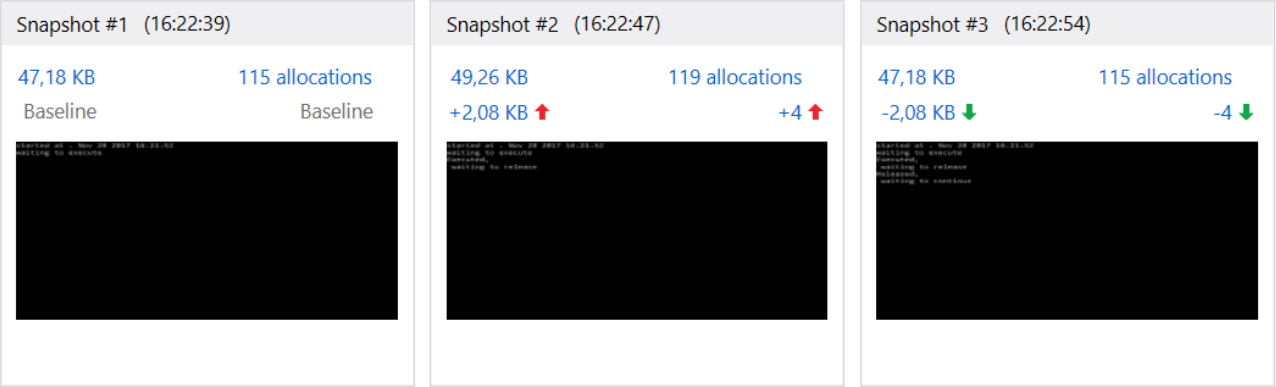
Snapshot #2 (12:53:48)
67,95 KB 172 allocations
+1,08 KB ↑ +4 ↑

```
started at : Nov 28 2017 12.53.03
waiting to execute
Executed,
 waiting to release
```

Snapshot #3 (12:53:53)
66,87 KB 168 allocations
-1,08 KB ↓ -4 ↓

```
started at : Nov 28 2017 12.53.03
waiting to execute
Executed,
 waiting to release
Released,
 waiting to continue
```

Profile 3 (32 bits):



Snapshot #1 (16:22:39)
47,18 KB 115 allocations
Baseline Baseline

```
started at : Nov 28 2017 16.21.52
waiting to execute
```

Snapshot #2 (16:22:47)
49,26 KB 119 allocations
+2,08 KB ↑ +4 ↑

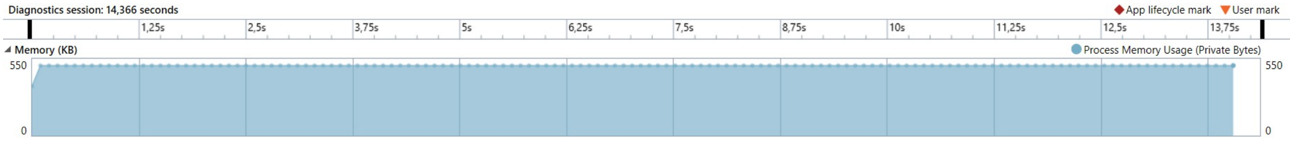
```
started at : Nov 28 2017 16.21.52
waiting to execute
Executed,
 waiting to release
```

Snapshot #3 (16:22:54)
47,18 KB 115 allocations
-2,08 KB ↓ -4 ↓

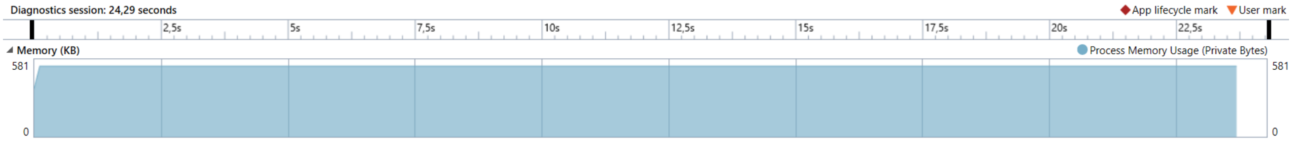
```
started at : Nov 28 2017 16.21.52
waiting to execute
Executed,
 waiting to release
Released,
 waiting to continue
```

<u>Total memory allocation over time:</u>

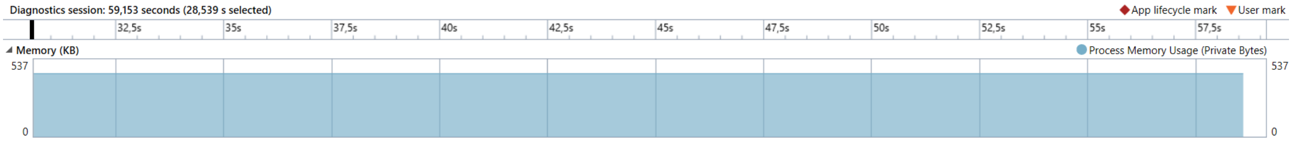
Profile 1 (8 bits):



Profile 2 (16 bits):



Profile 3 (32 bits):



The following table present details of memory consumption:

Memory analysis	**Profile 1**	**Profile 2**	**Profile 3**
Memory allocated (*)	596 B	1,08kB	2.08kB
Memory used in-calculation (*)	320B	320B	320B
Private Key:			
Component sizes			
Private key Structure	40 B	40 B	40 B
PolynomialTerm Size	16 B	16 B	16 B
PolynomialTerm count	16	32	64
Total PrivateKeySize		552 B	1064 B
Public key:			
Octonion size	64 B	64 B	64 B
Octonions present in Public information	4	4	4
Total Public information size	256 B	256 B	256 B

(*) Empyric values

…..

Hecht, Juan Pedro
Principal Submitter

…..

Kamlofsky, Jorge Alejandro
Auxiliar Submitter

Buenos Aires city, November 29th, 2017

National Institute of Standards and Technology,
Information Technology Laboratory,
100 Bureau Drive – Stop 8930, Gaithersburg, Maryland.
Attention: Post-Quantum Cryptographic Algorithm Submissions – Mr. Dustin Moody

Statement 2.b.4: Security Strength Expected Statement

As required in point 2.b.4 and following the guidelines suggested in point 4.a.5. we can expect the following categories of security for the proposed algorithm. Different profiles are presented depending of parameters as showed in the following table:

Profile	Name	Minimum Platform	Expected Pre-Quantum Security Classification	Expected Post-Quantum Security Classification (*)
Profile 1: 8-bits – d=16	HK17-O-64	8-bits	AES 64 bits	AES 32 bits
Profile 2: 16-bits – d=32	HK17-O-128	16-bits	AES 128 bits	AES 64 bits
Profile 3: 32-bits – d=64	HK17-O-256	32-bits	AES 256 bits	AES 128 bits
Profile 4: 64-bits – d=128	HK17-O-512	64-bits	AES 512 bits	AES 256 bits

(*) Considering Grover's algorithm

More causes and details that justify the assignment of expectations of security levels shown previously can be found in section 4.2 of the Technical Description of the algorithm.

Regarding Semantical Security as defined in 4.a.2, we can assign a conjectured and provisional security level of IND-CCA2. Justification and more details can be found in point 4.1 of the Technical Description of the algorithm.

....

Hecht, Juan Pedro
Principal Submitter

....

Kamlofsky, Jorge Alejandro
Auxiliar Submitter

Buenos Aires city, November 29th, 2017

National Institute of Standards and Technology,
Information Technology Laboratory,
100 Bureau Drive – Stop 8930, Gaithersburg, Maryland.
Attention: Post-Quantum Cryptographic Algorithm Submissions – Mr. Dustin Moody

Statement 2.b.5: Known criptanalytic attacks

Requirements of point 2.b.5, ask for a list of references of published materials describing or analyzing the security of the submitted algorithm or cryptosystem.

In this way, our study is focused on cryptographic solutions of algebraic nature: Non Commutative Criptografía (NCC) and specifically Non Commutative and Non Asociative Cryptography (NAC). In the Technical Description, references 8 to 24 (listed bellow) enumerate arguments of the security of these lines of study.

List of published references related NCC and NAC:

- A. Myasnikov, V. Shpilrain, A. Ushakov, Non-commutative Cryptography and Complexity of Group-theoretic Problems, Mathematical Surveys and Monographs, AMS Volume 177, 2011.
- M. I. Gonzalez Vasco, R. Steinwandt, Group Theoretic Cryptography, CRC Press, 2015
- L. Gerritzen et al (Editors), Algebraic Methods in Cryptography, Contemporary Mathematics, AMS, Vol. 418, 2006.
- B. Tsaban, Polynomial time solutions of computational problems in non-commutative algebraic crypto, 2012. http://arxiv.org/abs/1210.8114v2, (consulted April 20, 2017)
- D. Grigoriev and I. Ponomarenko, "Constructions in public-key cryptography over matrix groups", Preprint arXiv/math, no. 0506180v1, 2005. (consulted April 20, 2017)
- A. Kalka, Non-associative public-key cryptography, 2012. arXiv:1210.8270 [cs.CR] (consulted April 20, 2017)
- P. Hecht, Un modelo compacto de criptografía asimetrica empleando anillos no conmutativos, V Euromerican Congress of IT Security (CIBSI'09), 188-201, 2009.
- P. Hecht, Post-Quantum Cryptography(PQC): Generalized ElGamal Cipher over GF(251^8), ArXivCryptography and Security (cs.CR) http://arxiv.org/abs/1702.03587 6pp, 2017.
- P. Hecht, Post-Quantum Cryptography: A Zero-Knowledge Authentication Protocol, ArXiv Cryptography and Security (cs.CR) https://arxiv.org/abs/1703.08630, 3pp, 2017.
- P. Hecht, Post-Quantum Cryptography: S_{381} Cyclic Subgroup of High Order, ArXiv Cryptography, and Security (cs.CR) http://arxiv.org/abs/1704.07238 (preprint) & International Journal of Advanced Engineering Research and Science (IJAERS) 4:6, pp 78-86, 2017 https://dx.doi.org/10.22161/ijaers.4.6.10.
- P. Hecht, A Zero-Knowledge authentication protocol using non-commutative groups, VI Euromerican Congress of IT Security (CIBSI'11), 96-102, 2011.
- P. Hecht, Criptografia no conmutativa usando un grupo general lineal de orden primo de Mersenne, VII Euromerican Congress of IT Security (CIBSI'13), 147-153, 2013.
- P. Hecht, A Post-Quantum Set of Compact Asymmetric Protocols using a General Linear Group, VIII Euromerican Congress of IT Security (CIBSI'15), 96-101, 2015.
- P. Hecht, Zero-Knowledge Proof Authentication using Left Self Distributive Systems: a Post-Quantum Approach, VIII Euromerican Congress of IT Security (CIBSI'15), 113-116,

2015.

- J. Kamlofsky and P. Hecht, O. A. Hidalgo Izzi, S. Abdel Masih, A Diffie-Hellman Compact Model over Non-Commutative Rings Using Quaternions, VIII Euromerican Congress of IT Security (CIBSI'15), 218-222, 2015.
- J. Kamlofsky, P. Hecht, and Samira Abdel Masih. Post-Quantum Cryptography: An Elementary and Compact Key Exchange Scheme Based on Octonions. IX Euromerican Congress of IT Security (CIBSI'17), 2017.
- J. Kamlofsky and P. Hecht. Post-Quantum Cryptography Using Hyper-Complex Numbers, XXIII Argentinean Congress of Computer Sciences (CACIC'17), 2017
- V. Roman'kov, Cryptanalysis of a combinatorial public key cryptosystem, De Gruyter, Groups Complex. Cryptol. 2017

Regarding attacks to the proposed cryptosystem we can state that:

- No effective classical nor quantum based attack is known to any of these lines.
- With classical resources, no sub-exponential attack is known for our non-commutative/non-associative cryptosystem. We discuss in our Technical Description the non-applicability of algebraic attacks like the referenced Roman'kov cryptanalysis to our non-associative Moufang loop.
- With quantum resources, no known polynomic time algorithm could efficiently attack our non-commutative/non-associative cryptosystem. We discuss this point in detail in our Technical Description.
- Because powers of octonions can only be obtained in recursive way, no square-and-multiply algorithm could simplify polynomial powers of octonions, thus blocking known side-channel attacks.

More information can be found in point 4.3 of the Technical Description.

....

Hecht, Juan Pedro
Principal Submitter

....

Kamlofsky, Jorge Alejandro
Auxiliar Submitter

Buenos Aires city, November 29th, 2017

National Institute of Standards and Technology,
Information Technology Laboratory,
100 Bureau Drive – Stop 8930, Gaithersburg, Maryland.
Attention: Post-Quantum Cryptographic Algorithm Submissions – Mr. Dustin Moody

Statement 2.b.6: Advantages and limitations of the cryptosystem.

Advantages of the cryptosystem:

The strong advantages of our HK17 proposal are:

- Design simplicity: The overall design is very simple and easily understandable.
- Ordinary modular arithmetic: All the algorithm is performed just with modular sum-product operations, making possible its implementation in very elementary devices.
- Hardware implementations could be developed: because of the use of elementary operations (sum and product) in all the protocol, a logical circuit with logical “and” and “or” gates could be designed, leading to an easy firmware migration.
- No big number libraries needed: giving the potential utility of the protocol in computational environments of scarce capacities like smartcards, USB cryptographic tokens, basic cellular telephones or simple firmware devices.
- Relatively fast operation: makes possible cryptographic implementation without noticing significant delay.
- Power computation cannot be accelerated by square-and-multiply algorithm: because of the use of octonion’s non-associative Moufang loop. As a consequence, the polynomial powers of octonions must be obtained in a microscopically recursive form and that makes difficult the task of a potential systematic exploration and gives the using of octonions, a safety differential against the use of other non-commutative algebras. This feature, hinders the applicability of Shor’s algorithm.
- Parametric Crypto-System for a wide range of devices: Changing just two parameters (modulo and degree of polynomials) it is possible to implement post-quantum cryptography in very elementary devices or to give and also in highly demanding environments as compromise solution between security and performance.
- High Security Scheme: There are no classical or quantum attacks in sight: about non-commutative cryptography. Even less on structures that besides not fulfilling the commutative property, do not fulfill the associative property, as is the case of the algebra of octonions. Conjectured semantical security IND-CCA2 compliance. No possible side-channel attacks because of non-associative of powers. No sub-exponential attacks possible in non-commutative cryptosystems.

Limitations of the proposal:

In the other hand, we detected a solvable limitation:

- Fast propagation of zeros: Quaternions and octonions form division algebras. However, after the appearance of a zero in some component of quaternions and octonions, the propagation of inside zeros in polynomial powers occurs fast. This kind of limitation could be easily avoided, the probability of a random apparition of a zero component is 1/(p-1) which not only decreases with the prime value, should it appear and consequently propagate to a zero hypercomplex value, it would be dismissed and replaced by our protocols.

....

Hecht, Juan Pedro
Principal Submitter

....

Kamlofsky, Jorge Alejandro
Auxiliar Submitter

Acknowledgement:

We would like to specifically thank the Engineer and Ph.D. student Matias Ivan Teragni for his great contribution in the programming of our algorithm HK17 in ANSI C, in both implementations: reference and optimized, and in the test of the KAT data.

Not only did he manage to fine-tune our thoughts in ANSI C code, but he already considers future improvements to make it even more efficient.

During these weeks Matias was temporally stopped in his thesis topic. But we hope that this experience has been pleasant and valuable for him.

About us:

Hecht, Juan Pedro
https://www.linkedin.com/in/juan-pedro-hecht-a6b52516/

He has a MSc in biochemistry at the University of Buenos Aires (UBA). He also graduated in Systems Analysis at the Higher School of Operations Research (ESIO-DIGID). Finally, he graduated as Ph.D. at the UBA.

Currently he is Professor of Cryptography I and II of the Master in Information Technology Security dependent on the Faculties of Economic Sc., Exact and Natural Sc. and Engineering of the UBA. He is also Professor of Cryptography and Advanced Cryptography in the School of Engineering of the Army (EST-IUE), Professor of Cryptography of the University Institute of the Argentine Federal Police and Professor of Cryptography of the National Intelligence School (AFI).

He is also the Academic Coordinator of the aforementioned Master (UBA), Consultant Professor of Biophysics (UBA), Project Director and researcher in mathematical models of UBACyT and Director of EUDEBA (Editorial Board of UBA).

He is a member of Criptored (Polytechnic University of Madrid, Spain), IEEE, ACM SIGCSE, ACM SIGITE and others.

Kamlofsky, Jorge Alejandro

https://www.linkedin.com/in/jorgekamlofsky/

Graduated with a degree in Mathematics in the Interamerican Open University (UAI) and a Specialization in Cryptography and Information Technology Security in the Faculty of Engineering of the Argentinean Army (EST-IUE). He is finishing a Master in Information Technology in the UAI and doing a Ph.d in the Faculty of Engineering of the National University of Lomas de Zamora (UNLZ).

Actually he is professor of Discrete Mathematics in the UAI and Professor of Algebra and Analytic Geometry in the National Technological University (UTN).

Also he is researcher and project director in the Center of high studies on Information Technology (CAETI) of the UAI: he is managing the project "Ciber-security on industrial networks". The aim is to find out compact and elementary (and post-quantum) asymmetric protocols in order to try to provide cryptography onto industrial devices.