Ciencias Matemáticas, Vol. 33, No. 1, Pag. 82-86, 2019

Evaluación de los criptosistemas McEliece y Niederreiter como candidatos post-cuánticos
Evaluation of McEliece and Niederreiter cryptosystems as post-quantum candidates

Ernesto Dominguez Fiallo[1]*, Frank E. Acosta Fonseca[1], Luis R. Piñeiro Díaz[1]

Resumen En el presente trabajo se analizan los criptosistemas basados en códigos correctores de errores McEliece y Niederreiter, así como sus variantes. Mostramos también los principales ataques que han llevado a la evolución de los parámetros y la utilización de uno u otro código. También revisamos los parámetros recomendados en la literatura para una fortaleza de los criptosistemas contra ataques cúanticos y clásicos.

Abstract In the present paper we analize McEliece and Niederreiter error-correcting code-based cryptosystems and their variants. Also we show the main attacks which brought to them to new parameters and to the use of diferents codes. We review as well the recommended parameters in literature for a strongness of the cryptosystems against quantum and classic attacks.

Palabras Clave
McEliece, Niederreiter, criptografía post-cuántica, criptoanálisis

Keywords
McEliece, Niederreiter, post-quantum cryptography, cryptanalysis

[1] *Instituto de Criptografía, Universidad de La Habana, La Habana, Cuba, edominguezfiallo@nauta.cu, frankorazonero@nauta.cu, lrp@matcom.uh.cu*
*Autor para Correspondencia, Corresponding Author

Introducción

Recientemente se han producido grandes avances en la construcción de los ordenadores cuánticos [9]. En 1994, Peter Shor [24] mostró un algoritmo cuántico de complejidad polinomial que resuelve el problema de factorizar enteros y el problema del logaritmo discreto en un grupo abeliano. Por tanto, los esquemas asimétricos basados en los problemas de factorizar enteros y del logaritmo discreto en general y en particular en curvas elípticas, quedan completamente vulnerables. Con el fin de remediar tal situación, el NIST, a propuesta de la NSA, inició un proceso de búsqueda y estandarización de un esquema asimétrico para encriptación, firma digital e intercambio de llaves, resistente a los ataques en ordenadores cuánticos. Este proceso comenzó en enero de 2016 y debe finalizar entre el 2021 y 2023 [9].

Dentro de los esquemas asimétricos propuestos a analizar como posibles esquemas post cuánticos, se encuentran el criptosistema McEliece [21] y su variante Niederreiter [22], los cuales se basan en Códigos Correctores de Errores. La seguridad de ambos radica en la complejidad computacional de resolver el Problema General de Decodificación en Campos Finitos el cual fue probado NP-completo [3]. Estos esquemas tienen como principal desventaja que los tamaños de llave son muy grandes.

Con el objetivo de reducir los tamaños de llave en el McEliece, se ha intentado cambiar el código sobre el que subyace el esquema, sin embargo, en la práctica esto ha sido funesto pues se han encontrado ataques denominados estructurales, los cuales han criptoanalizado casi todas las variantes propuestas excepto la versión original (aunque modificando los parámetros originales) y otras variantes recientes. Este esquema se encuentra actualmente bajo fuerte análisis con el fin de eliminar sus deficiencias y poder utilizarlo como estándar resistente a los ataques en ordenadores cuánticos.

1. Preliminares

Esta sección fue confeccionada tomando como referencia [16], [13], [12], [2] y [26].

Definición 1 *Sea $\mathbb{F}$ un campo finito. Un código lineal $[n,k]$, al cual denotaremos por $\mathscr{C}$, es un subespacio lineal $k-$dimensional de $\mathbb{F}^n$.*

Definición 2 *Para un código lineal $[n,k]$ $\mathscr{C}$ sobre $\mathbb{F}$, su matriz generadora G es una matriz $k \times n$ sobre $\mathbb{F}$ cuyas filas forman una base de $\mathscr{C}$.*

Definición 3 *Sea $\mathscr{C}$ un código lineal $[n,k]$ sobre $\mathbb{F}$. Una matriz de chequeo de paridad H de $\mathscr{C}$ es una matriz $(n-k) \times n$ sobre $\mathbb{F}$ tal que $\forall c \in \mathbb{F}^n$*

$$c \in \mathscr{C} \iff cH^T = \boldsymbol{0}.$$

Definición 4 *La distancia mínima de $\mathscr{C}$ es la mínima distancia (distancia Hamming) de cualesquiera dos palabras códigos de $\mathscr{C}$:*

$$d = \min_{c_1,c_2\in\mathscr{C}:\ c_1\neq c_2} d(c_1,c_2).$$

Si $\mathscr{C}$ es un código lineal $[n,k]$ con una distancia mínima d entonces decimos que $\mathscr{C}$ es un código lineal $[n,k,d]$.

Definición 5 *Sea $\mathscr{C}$ un código lineal $[n,k,d]$ sobre $\mathbb{F}$ con una matriz generadora G. Decimos que $\mathscr{C}$ puede corregir t errores, si existe un algoritmo de decodificación $\mathscr{D}:\mathbb{F}^n\to\mathscr{C}$ tal que $\forall\,\boldsymbol{u}\in\mathbb{F}^k$ y $\forall\,\boldsymbol{e}\in\mathbb{F}^n : wt(\boldsymbol{e})\leq t$, la palabra $\boldsymbol{y}=\boldsymbol{u}G+\boldsymbol{e}$ siempre se decodifica como $\mathscr{D}(\boldsymbol{y})=\boldsymbol{u}$.*

La seguridad de los criptosistemas estudiados en este trabajo está basada en el siguiente problema.

Problema. El problema general de decodificación (en campos finitos) para códigos lineales es definido de la siguiente forma:

- Sea $\mathscr{C}$ un código lineal $[n,k]$ sobre $\mathbb{F}$ y $\mathbf{y}\in\mathbb{F}^n$.
- Encontrar $\mathbf{x}\in\mathscr{C}$ donde $d(\mathbf{x},\mathbf{y})$ sea la mínima.

1.1 Criptosistema McEliece

Dos años después del trabajo de Diffie-Hellman de 1976 *New directions in Cryptography* aparece el criptosistema de llave pública propuesto por Robert McEliece [21]. Aunque el trabajo original fue basado en el código binario de Goppa, puede ser utilizado cualquier subclase de la familia de los códigos alternantes.

Este criptosistema ha resistido el criptoanálisis hasta nuestros días. Aunque es bastante eficiente en el cifrado y descifrado ha recibido poca atención debido a su enorme llave pública y por la expansión del mensaje en un factor de n/k. Para los parámetros originales la llave pública tiene un poco más de 2^{19} bits (64 KB) y el mensaje se expande en un factor de casi el doble ($\approx 1{,}95$). Este criptosistema se encuentra en el **Algoritmo 1**.

Algoritmo 1: Criptosistema de llave pública McEliece

- Generación de llaves
  1. Escoger un código lineal $\mathscr{C}$ $[n,k,d]$ sobre $\mathbb{F}_2$ con un eficiente algoritmo de decodificación $\mathscr{D}$ que pueda corregir t errores.
  2. Calcular una matriz generadora G de $k\times n$ para $\mathscr{C}$.
  3. Generar una matriz aleatoria no singular S de $k\times k$.
  4. Generar una matriz aleatoria de permutación P de $n\times n$.
  5. Calcular la matriz $G'=SGP$.

  La llave pública es (G',t) y la llave privada es $(S,G,P,\mathscr{D})$.
- Cifrado
  1. Representar el mensaje como una cadena binaria $\mathbf{m}\in\{0,1\}^k$.
  2. Escoger un vector aleatorio $\mathbf{e}\in\{0,1\}^n : wt(\mathbf{e})=t$.
  3. Calcular $\mathbf{c}=\mathbf{m}G'+\mathbf{e}$.
- Descifrado
  1. Calcular $\mathbf{c}P^{-1}=(\mathbf{m}S)G+\mathbf{e}P^{-1}$.
  2. Aplicar el algoritmo de decodificación $\mathscr{D}$ a la palabra código $\mathbf{c}P^{-1}$ para obtener $\mathbf{c'}=\mathbf{m}S$.
  3. Calcular $\mathbf{m}=\mathbf{c'}S^{-1}$.

1.2 Criptosistema Niederreiter

Una de las variantes más conocidas del criptosistema McEliece es el Niederreiter, que fue propuesto por el científico austríaco H. Niederreiter [22] en 1986. Se le llama variante dual del McEliece dado que utiliza la matriz de chequeo de paridad en vez de la matriz generadora. Para entender mejor este criptosistema, veremos algunas definiciones.

Definición 6 *Sea $\mathscr{C}$ un código lineal $[n,k,d]$ sobre $\mathbb{F}$ y sea H su matriz de chequeo de paridad. El síndrome de una palabra $\boldsymbol{y}\in\mathbb{F}^n$ lo definiremos como*

$$s=\boldsymbol{y}H^T.$$

De acuerdo a la definición de matriz de chequeo de paridad las palabras códigos de $\mathscr{C}$ son exactamente aquellas cuyo síndrome es igual a $\mathbf{0}$. Sean $\mathbf{y}_1,\mathbf{y}_2\in\mathbb{F}^n$. Entonces

$$\mathbf{y}_1-\mathbf{y}_2\in\mathscr{C}\iff(\mathbf{y}_1-\mathbf{y}_2)H^T=\mathbf{0}\iff\mathbf{y}_1H^T=\mathbf{y}_2H^T.$$

El hecho de que $\mathbf{y}_1-\mathbf{y}_2$ sea una palabra código de $\mathscr{C}$ si y solo si los síndromes de $\mathbf{y}_1$ y $\mathbf{y}_2$ son iguales es la base para implementar eficientemente la decodificación de la palabra código más cercana, el cual es llamado *decodificación de síndrome*.

Definición 7 *Dada una palabra código $\boldsymbol{y}\in\mathbb{F}^n$ un algoritmo de decodificación de síndrome $\mathscr{D}$ encuentra una palabra de mínimo peso $\boldsymbol{e}\in\mathbb{F}^n$:*

$$\boldsymbol{y}H^T=\boldsymbol{e}H^T.$$

El criptosistema Niederreiter es presentado en el **Algoritmo 2**.

El Niederreiter original utilizaba códigos generalizados Reed-Solomon, pero este criptosistema cuando emplea los códigos binarios de Goppa fue demostrado [3] que su seguridad

Algoritmo 2: Criptosistema de llave pública Niederreiter

- Generación de llaves
  1. Escoger un código lineal $\mathscr{C}$ $[n,k,d]$ sobre $\mathbb{F}_2$ con un eficiente algoritmo de decodificación de síndromes $\mathscr{D}$ que pueda corregir t errores.
  2. Calcular una matriz de chequeo de paridad H de $(n-k)\times n$ para $\mathscr{C}$.
  3. Generar una matriz aleatoria no singular S de $(n-k)\times(n-k)$.
  4. Generar una matriz aleatoria de permutación P de $n\times n$.
  5. Calcular la matriz $H' = SHP$.

  La llave pública es (H',t) y la llave privada es $(S,H,P,\mathscr{D})$.
- Cifrado
  1. Representar el mensaje como una cadena binaria $\mathbf{m}\in\{0,1\}^k : wt(\mathbf{m}\leq t)$.
  2. Calcular $\mathbf{c} = \mathbf{m}H'$.
- Descifrado
  1. Calcular $S^{-1}\mathbf{c}^T = HP\mathbf{m}^T$.
  2. Aplicar el algoritmo de decodificación de síndromes $\mathscr{D}$ al síndrome $HP\mathbf{m}^T$ para obtener $P\mathbf{m}^T$.
  3. Calcular $\mathbf{m}^T = P^{-1}P\mathbf{m}^T$.

era equivalente a la del McEliece, igualmente haciendo uso de los códigos de Goppa.

2. Criptoanálisis de los criptosistemas McEliece y Niederreiter

Luego de su primera propuesta, un gran número de artículos aparecieron en la literatura reportando posibles ataques al criptosistema McEliece y a sus variantes. A pesar de los varios intentos de ataques, el criptosistema McEliece se considera no roto, en el sentido de que ningún algoritmo capaz de realizar una ruptura total (donde el atacante deduce la llave secreta) en tiempo polinomial ha sido presentado hasta ahora.

A continuación se muestra un resumen de los ataques contra los criptosistemas McEliece y Niederreiter. Para los ataques algorítmicos se estiman además el factor de trabajo (*work factor, WF*), que no es más que el número promedio de operaciones elementales (binarias) necesarias para realizar un ataque exitoso. El nivel de seguridad de un sistema es definido como el mínimo *WF* alcanzado por cualquier ataque en su contra.

2.1 Ataques por fuerza bruta

Ya en el primer trabajo de R. McEliece [21] fueron reportados dos ataques básicos por fuerza bruta a la seguridad del sistema: el primero consiste en tratar de recuperar G a partir de G' con el fin de utilizar el algoritmo de Patterson [23](ruptura total del criptosistema), el segundo trata de intentar recuperar $\mathbf{m}$ a partir de $\mathbf{c}$ sin conocer G (deducciones locales). Como reporta R. McEliece, el primer ataque parece desesperanzador si n y t son lo suficientemente grandes. El segundo ataque está estrictamente relacionado con el problema de la decodificación de un código lineal desconocido, con longitud n y dimensión k, en presencia de t errores. E. R. Berlekamp y otros autores demuestran en [3] que el problema general de decodificación de los códigos lineales es NP-completo; por lo tanto, si los parámetros del código son elegidos lo suficientemente grandes, este segundo ataque de fuerza bruta es también inviable. Basado en estos argumentos, podemos decir que, cualquier enfoque de fuerza bruta contra el criptosistema McEliece es demasiado complejo para tener éxito.

2.2 Ataques clásicos de Decodificación del Conjunto de Información

Un conjunto de información para un bloque de código lineal dado se define como un conjunto de valores $l\in\{1,\ldots,n\}$, de manera que dos palabras código difieren en al menos una de esas posiciones. Un conjunto de l índices es un conjunto de información si y sólo si las columnas correspondientes a la matriz generadora del código G son linealmente independientes. Los algoritmos de decodificación que usan conjuntos de información son conocidos como algoritmos de decodificación de conjuntos de información (*Information Set Decoding*, ISD).

Un primer ataque ISD al McEliece fue mencionado en [21]. Para los parámetros originales del McEliece este ataque requeriría $2^{80,4}$ operaciones binarias (*WF*). En [19] se propone utilizar un procedimiento determinístico, cuyo *WF* mínimo es de $2^{73,4}$ para el caso $n = 1024$ y $t = 37$. En la última mejora de este algoritmo, [18], fue propuesto una solución para reducir su complejidad, obteniendo así un *WF*=2^{59} para el McEliece original.

2.3 Ataques modernos de Decodificación del Conjunto de Información

Una clase más reciente y eficiente de algoritmos ISD utiliza la paradoja del cumpleaños para buscar palabras código de bajo peso en un código lineal. Un algoritmo probabilístico propuesto por J. Leon [20] está enfocado en encontrar palabras códigos de poco peso en códigos lineales grandes utilizando para ello la matriz generadora pública. Por otra parte, J. Stern [27] realiza una variante de este algoritmo haciendo uso de la matriz de chequeo de paridad. Para los parámetros originales del McEliece su *WF* mínimo es aproximadamente 2^{64}.

El algoritmo de J. Stern ha sido estudiado y mejorado en ([7], [5], [6]). Específicamente en [6] se sugiere el uso de los códigos de Goppa con $n = 2048, k = 1608, t = 40$ para lograr un *WF* en el orden de 2^{100}.

2.4 Distinguidor de códigos Goppa con alta tasa

Una de las premisas de la seguridad del McEliece es que su matriz generadora pública sea indistinguible de otra (matriz generadora) de un código lineal aleatorio. Es por esto que la única vía para que un atacante decodifique el texto cifrado a través de la llave pública es utilizar algoritmos genéricos de decodificación de códigos aleatorios, como los algoritmos ISD. En [14] se muestra que esta indistinguibilidad es falsa, al menos para algunos parámetros del código, y que existe un método para distinguir un código Goppa de un código lineal aleatorio. Este distinguidor solo es aplicable cuando la tasa del código es cercana a 1. El mismo no representa una amenaza para la mayoría de los criptosistemas McEliece utilizados en la literatura, pero si afecta otros que utilizan códigos Goppa con alta tasa como el esquema de firma CFS [10].

2.5 Ataques de mensajes reenviados y mensajes relacionados

El McEliece original es inseguro contra ataques adaptivos de textos cifrados escogidos (IND-CCA2) [29]. Sin embargo, la seguridad IND-CCA2 puede ser restaurada aplicando una adecuada conversión del criptosistema [17]. En este último trabajo se establece también que esta conversión inside positivamente en el tamaño de la llave pública, pues al llevar la misma a forma estándar o sistemática, se reduce su tamaño de $k \times n$ a $k \times (n-k)$ bits. Por otra parte, el Niederreiter permite utilizar matrices públicas en la forma estándar incluso sin ninguna conversión.

2.6 Otros ataques

Dentro de los ataques de canal colateral (side-channel attacks) encontramos un ataque por sincronización (timing attack) [28] contra el algoritmo de decodificación algebraica de Patterson [23], el cual utiliza la dependencia entre el grado del polinomio localizador de errores y el vector de error. Este ataque puede funcionar incluso si se hace uso de una conversión IND-CCA2 y ha sido mejorado significativamente en [25] y [1]. Otras referencias a otros ataques de canal colateral pueden ser encontrados en (SPA [15], DPA [8]).

3. Parámetros recomendados para McEliece y Niederreiter

Como hemos visto, una buena selección de parámetros define la fortaleza del criptosistema estudiado. A día de hoy los parámetros recomendados por la literatura para los códigos Goppa, tanto para el McEliece como para el Niederreiter, son para un código $[n,k,t] = [6960, 5413, 119]$. Estos parámetros fueron propuestos por D. Bernstein y otros autores en [4] y ratificados por el proyecto europeo PQCRYPTO en [11]. Para estos valores se logra $2^{240,4}$ bits de seguridad clásica y $2^{153,1}$ de seguridad postcuántica [30]. En este último trabajo se disminuyen estos parámetros $[n,k,t] = [5542, 4242, 100]$ con el objetivo de obtener $2^{128,0}$ bits de seguridad postcuántica, mientras que alcanza $2^{198,7}$ de seguridad clásica. Por otra parte PQCRYPTO recomienda los siguientes parámetros para los códigos QC-MDPC, aún bajo evaluación, $n = 2^{16}+6$; $k = 2^{15}+3$; $d = 274$, $t = 264$.

Conclusiones

El McEliece y su variante Niederreiter son grandes candidatos para reemplazar a los algoritmos explotados hoy en día (RSA, Diffie-Hellman, etc.). Como prueba de ello, en este trabajo hemos resumido el estado actual de estos criptosistemas, desde la teoría en la que se basan hasta los ataques que han llevado a una revisión de los parámetros utilizados. Hemos expuesto también los parámetros recomendados por la literatura, los cuales, aunque todavía están bajo estudio, son previstos para una larga duración. Esperamos que este trabajo tribute a otras investigaciones en esta área y pueda llevar a la implementación de estos criptosistemas para su evaluación en los sistemas más utilizados como OpenVPN, IPSec, etc., así también como en la creación de certificados y firmas digitales.

Referencias

[1] Avanzi, Roberto, Simon Hoerder, Dan Page y Michael Tunstall: *Side-channel attacks on the McEliece and Niederreiter public-key cryptosystems*. Journal of Cryptographic Engineering, 1(4):271–281, 2011.

[2] Baldi, Marco: *QC-LDPC code-based cryptography*. Springer Science & Business, 2014.

[3] Berlekamp, Elwyn, Robert McEliece y Henk Van Tilborg: *On the inherent intractability of certain coding problems (Corresp.)*. IEEE Transactions on Information Theory, 24(3):384–386, 1978.

[4] Bernstein, Daniel J, Tung Chou y Peter Schwabe: *McBits: fast constant-time code-based cryptography*. En *International Workshop on Cryptographic Hardware and Embedded Systems*, páginas 250–272. Springer, 2013.

[5] Canteaut, Anne y Florent Chabaud: *A new algorithm for finding minimum-weight words in a linear code: application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511*. IEEE Transactions on Information Theory, 44(1):367–378, 1998.

[6] Canteaut, Anne y Nicolas Sendrier: *Cryptanalysis of the original McEliece cryptosystem*. En *International Conference on the Theory and Application of Cryptology and Information Security*, páginas 187–199. Springer, 1998.

[7] Chabaud, Florent: *On the security of some cryptosystems based on error-correcting codes*. En *Workshop on the Theory and Application of of Cryptographic Techniques*, páginas 131–139. Springer, 1994.

[8] Chen, Cong, Thomas Eisenbarth, Ingo Von Maurich y Rainer Steinwandt: *Differential power analysis of a McEliece cryptosystem*. En *International Conference on*

Applied Cryptography and Network Security, páginas 538–556. Springer, 2015.

[9] Chen, Lily, Lily Chen, Stephen Jordan, Yi Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner y Daniel Smith-Tone: *Report on post-quantum cryptography*. US Department of Commerce, National Institute of Standards and Technology, 2016.

[10] Courtois, Nicolas T, Matthieu Finiasz y Nicolas Sendrier: *How to achieve a McEliece-based digital signature scheme*. En *International Conference on the Theory and Application of Cryptology and Information Security*, páginas 157–174. Springer, 2001.

[11] Daniel, Augot, B Lejla *y cols.*: *Initial recommendations of long-term secure post-quantum systems*. PQCRYPTO. EU. Horizon, 2020, 2015.

[12] Eisenbarth, Thomas, Tim Güneysu, Stefan Heyse y Christof Paar: *MicroEliece: McEliece for embedded devices*. En *Cryptographic Hardware and Embedded Systems-CHES 2009*, páginas 49–64. Springer, 2009.

[13] Engelbert, Daniela, Raphael Overbeck y Arthur Schmidt: *A summary of McEliece-type cryptosystems and their security*. Journal of Mathematical Cryptology JMC, 1(2):151–199, 2007.

[14] Faugere, Jean Charles, Valérie Gauthier-Umana, Ayoub Otmani, Ludovic Perret y Jean Pierre Tillich: *A distinguisher for high-rate McEliece cryptosystems*. IEEE Transactions on Information Theory, 59(10):6830–6844, 2013.

[15] Heyse, Stefan, Amir Moradi y Christof Paar: *Practical power analysis attacks on software implementations of McEliece*. En *International Workshop on Post-Quantum Cryptography*, páginas 108–125. Springer, 2010.

[16] Jochemsz, Ellen: *Goppa Codes & the McEliece Cryptosystem*. Doktorarbeit, Universiteit van Amsterdam, 2002.

[17] Kobara, Kazukuni y Hideki Imai: *Semantically secure McEliece public-key cryptosystems-conversions for McEliece PKC*. En *International Workshop on Public Key Cryptography*, páginas 19–35. Springer, 2001.

[18] Kruk, Evgenii Avramovich: *Decoding complexity bound for linear block codes*. Problemy Peredachi Informatsii, 25(3):103–107, 1989.

[19] Lee, Pil Joong y Ernest F Brickell: *An observation on the security of McElieceâs public-key cryptosystem*. En *Workshop on the Theory and Application of of Cryptographic Techniques*, páginas 275–280. Springer, 1988.

[20] Leon, Jeffrey S: *A probabilistic algorithm for computing minimum weights of large error-correcting codes*. IEEE Transactions on Information Theory, 34(5):1354–1359, 1988.

[21] Mceliece, Robert J: *A public-key cryptosystem based on algebraic*. Coding Thv, 4244:114–116, 1978.

[22] Niederreiter, Harald: *Knapsack-type cryptosystems and algebraic coding theory*. Prob. Control and Inf. Theory, 15(2):159–166, 1986.

[23] Patterson, Nicholas: *The algebraic decoding of Goppa codes*. IEEE Transactions on Information Theory, 21(2):203–207, 1975.

[24] Shor, Peter W: *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*. SIAM review, 41(2):303–332, 1999.

[25] Shoufan, Abdulhadi, Falko Strenzke, H Gregor Molter y Marc Stöttinger: *A timing attack against Patterson algorithm in the McEliece PKC*. En *International Conference on Information Security and Cryptology*, páginas 161–175. Springer, 2009.

[26] Siim, Sander: *Study of McEliece cryptosystem*. 2015.

[27] Stern, Jacques: *A method for finding codewords of small weight*. En *International Colloquium on Coding Theory and Applications*, páginas 106–113. Springer, 1988.

[28] Strenzke, Falko, Erik Tews, H Gregor Molter, Raphael Overbeck y Abdulhadi Shoufan: *Side channels in the McEliece PKC*. En *International Workshop on Post-Quantum Cryptography*, páginas 216–229. Springer, 2008.

[29] Sun, Hung Min: *Further cryptanalysis of the McEliece public-key cryptosystem*. IEEE communications letters, 4(1):18–19, 2000.

[30] Vries, SHS: *Achieving 128-bit security against quantum attacks in OpenVPN*. Tesis de Licenciatura, University of Twente, 2016.