Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 130-135

Tipo de artículo: Artículos cortos
Temática: Seguridad informática
Recibido: 23/11/2022 | Aceptado: 28/12/2022 | Publicado: 29/01/2023

Sobre un nuevo ataque a esquemas de firma digital de tipo mCFS$_c$ basados en códigos

About a new attack on code-based mCFS$_c$-type digital signature schemes

Ernesto Dominguez Fiallo 0000-0003-3831-2889[1*]
Luis Ramiro Piñeiro 0000-0002-7807-2624[1]
Pablo Freyre Arrozarena 0000-0000-0000-0000[1]

[1]Instituto de Criptografía. Facultad de Matemática y Computación. Universidad de La Habana.
edominguezfiallo@nauta.cu

[*]Autor para correspondencia: (edominguezfiallo@nauta.cu)

Resumen

Recientemente fue publicado un nuevo ataque de falsificación de firma digital sobre esquemas post-cuánticos basados códigos de tipo mCFS$_c$. En este artículo se demuestra que el ataque no es aplicable cuando el código secreto y el código público no son equivalentes mediante permutación. En particular, el ataque no es aplicable al esquema mCFS$^{QC-LDPC}$.

Palabras clave: Firma Digital; Falsificación; Criptografía basada en códigos; mCFS$^{QC-LDPC}$.

Abstract

A new signature forgery attack on post-quantum code-based digital signature schemes of mCFS$_c$-type was recently published. This paper prove that the attack is not applicable when the secret code and the public code are not equivalent by permutation. In particular, the attack is not applicable to the scheme mCFS$^{QC-LDPC}$.

Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 130-135

Keywords: Digital Signature; Forgery; code-base Cryptography; mCFS$^{QC-LDPC}$.

Introducción

La búsqueda de nuevos estándares asimétricos post-cuánticos es una de las áreas de investigación criptográfica de mayor interés en la actualidad (Das and Sadhu, 2022). La criptografía basada en códigos es una de las principales alternativas que se consideran en ese sentido (Weger et al., 2022). Sin embargo, diseñar un esquema de firma digital post-cuántico basado en códigos es uno de los problemas más difíciles de resolver (Balamurugan et al., 2021). Ninguno de los estándares post-cuánticos para firma digital, serán construido sobre los códigos (Alagic et al., 2020).

Los esquemas de tipo CFS son una de las principales líneas de diseño de esquemas de firma digital basados en códigos (Vysotskaya and Chizhov, 2021). Su principal dificultad radica, además de los tamaños de llaves públicas, en la cantidad de hash que se aplican al mensaje hasta obtener un síndrome decodificable. Esto es costoso computacionalmente pues el número es considerablemente grande y aumenta en gran medida también cuando se aumentan los niveles de seguridad. En (Ren et al., 2017) se propuso una idea para resolver tal desventaja. Usando esta misma idea, (Fiallo, 2021) propuso el empleo de códigos QC-LDPC para reducir los tamaños de llave pública sin costo computacional adicional y sin perder seguridad.

Recientemente, en formato preprint se propuso un nuevo ataque sobre los esquemas de tipo mCFS$_c$ que compromete la seguridad de los mismos (DÁlconzo et al., 2021). El ataque permite la falsificación de mensajes aprovechando la forma en que se construye la función hash a partir de la llave pública. En este breve trabajo se demuestra que el ataque no es aplicable al esquema propuesto por (Fiallo, 2021), por lo que no compromete la seguridad del mismo.

Función hash y función de compresión

La función hash usada en los esquemas de tipo mCFS$_c$ usa como base la aplicación iterativa de una función de compresión. Sean r la longitud de salida del hash y $f : \mathbb{F}_2^s \to \mathbb{F}_2^r,\ s > r$ la función de compresión. Se define la función hash del siguiente modo:

1. el mensaje m se asume, una vez que se le aplicó un padding, de longitud múltiplo de $s - r$, por lo que se

Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 130-135

descompone en $Length(m)/(s-r)$ bloques $m_1, m_2, \ldots, m_{Length(m)/(s-r)}$ cada uno de longitud $s-r$.

2. el estado inicial lo compone la concatenación de m_1 con un vector inicial (IV) de longitud r, es decir, $S_1 = m_1||IV$.
3. la ronda i es la salida de $f(m_i||f(S_{i-1}))$.
4. la salida de la función hash será $f(S_{m/(s-r)})$.

Sea H una matriz de control de un código binario con tamaño $r \times n$. Sean w un entero que divide a n, $l = n/w$ y $s = w\log_2 l$. El valor de w se selecciona menor o igual a la capacidad de corregir errores del código. La función de compresión f se define del siguiente modo:

1. la matriz H se descompone en $H = (H_1, H_2, \ldots, H_w)$ submatrices.
2. dado $x \in \mathbb{F}_2^s$, se descompone en w bloques $x = (x_1, x_2, \ldots, x_w)$ de $\log_2 l$ bits cada uno. Cada x_i se convierte en un entero entre 0 y $l-1$.
3. Se selecciona la correspondiente $(x_i + 1)$ columna en cada H_i, es decir $h_{(i-1)l+x_i+1}$ donde h_j denota la columna j de la matriz H, y se calcula $f(x) = \bigoplus_{i=1}^{w} h_{(i-1)l+x_i+1}$.

Si se considera la aplicación $\delta : \mathbb{F}_2^s \to \mathbb{F}_2^n,\ \delta(x) = y$, donde y es un vector de peso de Hamming w cuyo soporte está en las posiciones $(i-1)l + x_i + 1$, con $i = 1, \ldots, w$ y $0 \leq x_i \leq l-1$, entonces f se puede expresar de la forma $f(x) = H \cdot (\delta(x))^T$. Un vector obtenido de aplicar δ se denomina *regular*.

El ataque

Dados f, w, H y el mensaje m' a falsificar su firma, el atacante selecciona aleatoriamente $R' \in \{1, \ldots, 2^{n-k}\}$ y calcula $f\left(f(m' \parallel R')\right)$ pero se detiene antes de la última iteración de f, es decir, en el estado $f(m'_{Length(m')/(s-r)-1})$. Selecciona $y = \delta\left(f(m'_{Length(m')/(s-r)-1})\right)$ y se establece como firma al vector $\sigma = (m', R' \parallel y)$. Cualquiera que desee verificar la validez de la firma comprobará que

$$f\left(f(m') \parallel R'\right) = H \cdot \left(\delta\left(f(m'_{Length(m')/(s-r)-1})\right)\right)^T = H \cdot y^T$$

Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 130-135

Este ataque de falsificación se generaliza al caso de cualquier función hash de este tipo porque a cualquier vector $(f(m) \parallel R')$ al que se le aplique δ, se transformará en un vector regular. El ataque funciona porque aunque el atacante seleccione m' y R' distintos al del firmante, la transformación $\delta((f(m') \parallel R'))$ es una *permutación del vector regular original* que entra a la última iteración de f.

Hecho: Si $(m, R \parallel u)$ es la firma original y $(m', R' \parallel y)$ una falsificación mediante el ataque anterior. Entonces se cumple que $y = uP$ donde P es una matriz de permutación desconocida tal que $H = H_{priv} \cdot P$, siendo H_{priv} la matriz llave secreta.

Caso del esquema mCFS$^{QC-LDPC}$

En el esquema mCFS$^{QC-LDPC}$ (Fiallo, 2021) la relación entre la matriz llave pública y la matriz llave privada está dada por $H = H_{priv} \cdot \left(Q^T\right)^{-1}$ donde la matriz Q es una matriz de transformación (y no de permutación) secreta, sparse, no singular y de tamaño $n \times n$.

La firma en este esquema es como sigue: a) se calcula $d = f(f(m) \parallel R)$, b) se decodifica $v = \text{DEC}_{H_{priv}}(d)$ siendo $\text{DEC}_{H_{priv}}$ un algoritmo eficiente de decodificación de códigos LDPC, y c) se calcula $y = v \cdot Q$. La firma es $\sigma = (m, R \parallel y)$.

Como y y v no están relacionados mediante una permutación, sino a través de la matriz de transformación Q, el peso de Hamming de y es distinto al de v, por lo que la aplicación δ del ataque no es efectiva.

Conclusiones

Se demostró que el ataque de falsificación propuesto por DÁlconzo et al. (2021) a los esquemas de firma digital basados en códigos de tipo mCFS$_c$ es efectivo porque la matriz llave pública es una permutación de la matriz llave privada. Cuando lo anterior no se cumple, el ataque no es aplicable. Un ejemplo de lo anterior es el esquema mCFS$^{QC-LDPC}$.

Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 130-135

Referencias

Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, et al. Status report on the second round of the nist post-quantum cryptography standardization process. *US Department of Commerce, NIST*, 2020.

Chithralekha Balamurugan, Kalpana Singh, Ganeshvani Ganesan, and Muttukrishnan Rajarajan. Post-quantum and code-based cryptography. some prospective research directions. *Cryptography*, 5(4):38, 2021.

Giuseppe DÁlconzo, Alessio Meneghetti, and Paolo Piasenti. Security issues of cfs-like digital signature algorithms. *arXiv preprint arXiv:2112.00429*, 2021.

Kunal Das and Arindam Sadhu. Challenges and trends on post-quantum cryptography. *Internet of Things*, pages 271–293, 2022.

ED Fiallo. A digital signature scheme mcfsˆqc-ldpc based on qc-ldpc codes. *Mathematical Aspects of Cryptography*, 12(4):99–113, 2021.

Fang Ren, Dong Zheng, WeiJing Wang, et al. An efficient code based digital signature algorithm. *Int. J. Netw. Secur.*, 19(6):1072–1079, 2017.

Victoria Vysotskaya and Ivan Chizhov. The security of the code-based signature scheme based on the stern identification protocol. *Cryptology ePrint Archive*, 2021.

Violetta Weger, Niklas Gassner, and Joachim Rosenthal. A survey on code-based cryptography. *arXiv preprint arXiv:2201.07119*, 2022.

Conflicto de interés

Los autores autorizan la distribución y uso de su artículo.

Contribuciones de los autores

1. Conceptualización: Ernesto Dominguez Fiallo

2. Curación de datos: Ernesto Dominguez Fiallo
3. Análisis formal: Ernesto Dominguez Fiallo
4. Adquisición de fondos: no fue necesario
5. Investigación: Ernesto Dominguez Fiallo
6. Metodología: Ernesto Dominguez Fiallo
7. Administración del proyecto: Luis Ramiro Piñeiro y Pablo Freyre Arrozarena
8. Recursos: Ernesto Dominguez Fiallo
9. Software: -
10. Supervisión: Luis Ramiro Piñeiro y Pablo Freyre Arrozarena
11. Validación: Ernesto Dominguez Fiallo
12. Visualización: Ernesto Dominguez Fiallo
13. Redacción - Ernesto Dominguez Fiallo
14. Redacción - Ernesto Dominguez Fiallo

Financiación

No fue necesario

Notes

[1]Notas aclaratorias del texto, estas estarán ubicadas al final del trabajo.

[2]Esta es otra nota al final