Cifrado homomórfico de clave pública basado en Residuosidad Cuadrática

Javier Herranz
Dept. de Matemàtica Aplicada IV
Universitat Politècnica de Catalunya
Email: jherranz@ma4.upc.edu

Juan Ramón Sisternes
Conselleria d'Educació, Formació i Ocupació
Generalitat Valenciana
Email: juanrasisternes@gmail.com

***Abstract*—Los esquemas de cifrado de clave pública con propiedades homomórficas tienen muchas utilidades en aplicaciones reales. Entre los esquemas con propiedades homomórficas aditivas existentes, hay una familia (desde el esquema de Goldwasser-Micali hasta el esquema de Paillier) cuya seguridad se basa en problemas computacionalmente difíciles relacionados con el problema de factorizar un número grande N. Los esquemas de esta familia tienen diferentes propiedades tanto en lo referente a la eficiencia, como al problema de teoría de números concreto en el que basan su seguridad.**

En este artículo proponemos un nuevo esquema a añadir a esta familia. La hipótesis computacional en la que se basa la seguridad de nuestro esquema es la hipótesis de la Residuosidad Cuadrática módulo N. En términos de eficiencia, por un lado nuestro esquema mejora todos los esquemas anteriores cuya seguridad se basa en la hipótesis de la Residuosidad d-ésima módulo N, para $d \geq 2$; por otro lado, nuestro esquema es en general menos eficiente (tiempo de descifrado) que algunos esquemas como el de Paillier, cuya seguridad se basa en otra hipótesis (Residuosidad N-ésima módulo N^2). Sin embargo, si los mensajes a cifrar son cortos, la eficiencia de nuestro esquema es esencialmente la misma que la del esquema de Paillier.

I. Introducción

Los sistemas criptográficos de cifrado son una primitiva esencial en el mundo de la seguridad en comunicaciones digitales, porque son los encargados de proporcionar confidencialidad a la comunicación. En los sistemas de cifrado *simétricos*, la misma clave secreta se usa para cifrar y para descifrar, y por tanto debe ser compartida de manera segura entre emisor y receptor. En los sistemas de cifrado *asimétricos* (o de clave pública), cualquier emisor puede usar la clave pública del receptor parar cifrar, y esa clave es diferente de la clave secreta, que sólo conoce el receptor y que debe usar para descifrar.

Los sistemas simétricos son más eficientes que los asimétricos, pero presentan el problema de la generación y gestión de las claves. De hecho, ésa fue la causa de la aparición de los sistemas asimétricos. Además, los sistemas asimétricos permiten otras funcionalidades, como por ejemplo la capacidad de realizar operaciones aritméticas entre textos cifrados que se traduzcan en operaciones aritméticas entre los mensajes en claro subyacentes. Este tipo de operaciones se encuentran en varias aplicaciones de la vida real que necesitan confidencialidad de la información. Explicamos aquí dos ejemplos ilustrativos:

- *Votación electrónica:* cada votante envía un voto (0 o 1, si es una votación de tipo *referendum*) cifrado, para preservar la confidencialidad de su voto. Cuando todos los votos cifrados se han recibido, se aplica una operación a los cifrados que resulta en un cifrado de la suma de todos los votos. Sólo en ese momento, la entidad competente procede a descifrar el cifrado global, obteniendo el resultado final de la votación.
- *Computación en la nube:* una empresa o usuario particular que almacene cantidades my grandes de información confidencial, puede contratar los servicios de alguna empresa de *cloud computing*, y enviarles esa información cifrada. Más tarde, si el cliente quiere recuperar una cierta función de alguna parte de esa información (por ejemplo, el promedio de algún subconjunto de datos), puede enviar a la empresa esa petición, la empresa hará algunos cálculos sobre datos cifrados, enviará el cifrado resultante al cliente, quién deberá sólo descifrar ese cifrado final para recuperar el valor deseado.

Los sistemas de cifrado que permiten realizar este tipo de operaciones reciben el nombre de *homomórficos*. Si las operaciones entre cifrados se traducen en sumas (resp., multiplicaciones) entre mensajes, se dice que el sistema es *aditivamente* (resp., *multiplicativamente*) homomórfico. Un sistema que permita realizar algunas operaciones entre cifrados que se traduzcan en sumas entre mensajes y otras operaciones entre cifrados que se traduzcan en multiplicaciones entre mensajes, recibe el nombre de *completamente homomórfico*.

Durante más de 30 años, desde 1978 hasta 2009, la existencia de sistemas completamente homomórficos ha sido un problema abierto. En esos años, sí que se propusieron sistemas homomórficos respecto a una de las operaciones: suma [5], [2], [6], [7], [8], [9] o multiplicación [10], [3]. De ésos, algunos como RSA [10] son deterministas y por tanto no puede conseguir el mínimo nivel de seguridad requerido, la seguridad semántica (ver Sección II-B). El resto de sistemas aditivos, excepto [9], basan su seguridad en la dificultad de algunos problemas computacionales relacionados con la dificultad de factorizar números grandes $N = pq$, con p y q primos. El sistema aditivo en [9] utiliza retículos de enteros (*lattices*); la criptografía basada en retículos es actualmente uno de los temas más estudiados en criptografía, y una de

las razones es la posibilidad de obtener buenas propiedades homomórficas a partir de ellos. No sólo se pueden combinar cifrados para obtener sumas de mensajes, como en [9], sino que se puede iterar esa idea para obtener un número limitado de multiplicaciones de mensajes [1]. Además, usando retículos se han diseñado por fin los primeros sistemas completamente homomórficos [4].

Sin embargo, la criptografía basada en retículos es aún muy reciente y tiene algunas desventajas, como el gran tamaño de las claves públicas. Por eso, en aplicaciones reales que sólo requieran operaciones homomórficas aditivas (como las votaciones electrónicas, sistemas de recuperación anónima de información, etc.) se siguen utilizando esquemas de la familia basada en el problema de la factorización, en particular el esquema de Paillier [8]. Dentro de esta familia, algunos esquemas tienen mejor eficiencia que otros (en cuanto al coste de cifrar y descifrar, o en cuanto a la relación entre la longitud de un mensaje y la longitud de su texto cifrado). En ese sentido, los esquemas más eficientes son los de [7], [8]. Además, los esquemas también se diferencian en el problema computacional de teoría de números concreto en el que basan su seguridad. Algunos esquemas [5] basan su seguridad en la dificultad del problema de la Residuosidad Cuadrática módulo N, otros [2], [6] en la dificultad del problema de la Residuosidad d-ésima módulo N, para $d > 2$, el esquema en [7] basa su seguridad en la dificultad de factorizar números del tipo $N = p^2q$, y el esquema en [8] en el problema de la residuosidad N-ésima módulo N^2, siendo $N = pq$. Se conjetura que todos estos problemas son computacionalmente muy difíciles, para valores muy grandes de N. Desafortunadamente, no se conocen relaciones de comparación entre estos problemas de teoría de números, y por tanto no se puede afirmar que algún esquema en esta familia sea "más seguro" que otro.

En este artículo proponemos un nuevo esquema de cifrado a añadir a esta familia de sistemas de cifrado aditivamente homomórficos con seguridad relacionada con el problema de la factorización; en concreto, demostramos formalmente la seguridad semántica de nuestro esquema si se supone que el problema de la Residuosidad Cuadrática módulo $N = pq$ es difícil. Esta hipótesis es una de las más estándar entre las relacionadas con el problema de la factorización. Nuestro esquema es más eficiente que todos los esquemas cuya seguridad se basa en la hipótesis de la Residuosidad d-ésima módulo $N = pq$, para $d \geq 2$. Es decir, es más eficiente que los esquemas en [5], [2], [6]. Sin embargo, nuestro esquema es menos eficiente que los esquemas en [7], [8], que basan su seguridad en hipótesis que tal vez no son tan estándar. Queremos remarcar aquí, no obstante, que si los mensajes a cifrar son bastante cortos (cosa que pasa en aplicaciones reales como referendums o recuperación privada de información), entonces la eficiencia de nuestro esquema es esencialmente la misma que la eficiencia de los esquemas en [7], [8]. Por todo eso, consideramos que nuestro esquema puede tener un interés tanto teórico (es el primer sistema que permite cifrar de manera eficiente más de un bit y cuya seguridad reside en la hipótesis de la Residuosidad Cuadrática) como práctico (para aplicaciones reales como un referéndum digital).

El resto del trabajo se organiza de la siguiente manera. En la Sección II repasamos los protocolos que forman un sistema de cifrado de clave pública, la definición de seguridad semántica y el problema de la Residuosidad d-ésima (en particular, cuadrática). En la Sección III describimos el nuevo sistema de cifrado. Analizamos formalmente la seguridad de este nuevo esquema en la Sección IV y lo comparamos con otros esquemas similares en la Sección V. Finalmente, en la Sección VI presentamos un resumen de las contribuciones de este trabajo y mencionamos algunos problemas abiertos relacionados.

II. Preliminares

A. Cifrado de Clave Pública

Un *esquema de cifrado de clave pública* $\mathsf{PKE} = (\mathsf{PKE.KG}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ consta de tres algoritmos probabilísticos y de tiempo polinómico:

- El algoritmo de generación de claves, $\mathsf{PKE.KG}$, toma como entrada un parámetro de seguridad λ y devuelve una pareja $(\mathsf{sk}, \mathsf{pk})$ de claves secreta y pública. Escribiremos $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{PKE.KG}(1^\lambda)$.
- El algoritmo de cifrado, $\mathsf{PKE.Enc}$, toma como entrada una clave pública pk y un mensaje m. La salida es un texto cifrado c. Escribiremos $c \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}, m)$.
- El algoritmo de descifrado, $\mathsf{PKE.Dec}$, toma como entrada una clave secreta sk y un texto cifrado c. La salida es un mensaje $\tilde{m}$. Escribiremos $\tilde{m} \leftarrow \mathsf{PKE.Dec}(\mathsf{sk}, c)$.

Se requiere la siguiente propiedad para que el esquema funcione correctamente: $\mathsf{PKE.Dec}(\mathsf{sk}, \mathsf{PKE.Enc}(\mathsf{pk}, m)) = m$, para toda pareja de claves $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{PKE.KG}(1^\lambda)$.

El esquema PKE tiene propiedades *homomórficas* si existen una operación $\otimes$ entre textos cifrados y una operación $\oplus$ entre mensajes tales que $\mathsf{PKE.Dec}\big(\mathsf{sk}, \mathsf{PKE.Enc}(\mathsf{pk}, m) \otimes \mathsf{PKE.Enc}(\mathsf{pk}, m_2)\big) = m_1 \oplus m_2$, para toda pareja de claves $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{PKE.KG}(1^\lambda)$ y todo par de mensajes m_1, m_2.

B. Seguridad Semántica

Recordamos aquí la noción estándar de seguridad para esquemas de cifrado de clave pública en términos de *indistinguibilidad*, o *seguridad semántica*. Consideramos ataques de tipo CPA (*chosen plaintext attacks*), porque un esquema con propiedades homomórficas no puede nunca alcanzar seguridad contra ataques de tipo CCA (*chosen ciphertext attacks*). Para definir la seguridad semántica, usamos los experimentos $\mathbf{Exp\text{-}CPA}^{b,\mathsf{PKE}}_{\mathcal{A}}(\lambda)$, para $b = 0, 1$, que implican a un adversario $\mathcal{A}$ y un retador, y que se definen de la siguiente manera:

1) **Inicialización.** El retador ejecuta $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{PKE.KG}(1^\lambda)$. La clave pública pk se envía al adversario $\mathcal{A}$.
2) **Reto.** El adversario $\mathcal{A}$ escoge dos mensajes $m^0 \neq m^1$ de la misma longitud. El retador calcula $c = \mathsf{PKE.Enc}(\mathsf{pk}, m^b)$, y lo envía a $\mathcal{A}$.
3) **Apuesta final.** El adversario $\mathcal{A}$ devuelve un bit $b' \in \{0, 1\}$.

Sea Ω_b el suceso donde $\mathcal{A}$ devuelve $b' = 1$ en el experimento $\textbf{Exp-CPA}_{\mathcal{A}}^{b,\mathsf{PKE}}(\lambda)$, para $b = 0, 1$. La ventaja de ese adversario $\mathcal{A}$ se define como

$$\textbf{Adv-CPA}_{\mathcal{A}}^{\mathsf{PKE}}(\lambda) = \left|\Pr[\Omega_1] - \Pr[\Omega_0]\right|.$$

Un esquema de cifrado de clave pública se dice que es indistinguible contra ataques CPA si $\textbf{Adv-CPA}_{\mathcal{A}}^{\mathsf{PKE}}(\lambda)$ es una función despreciable (*negligible*, en inglés) de λ, para cualquier adversario $\mathcal{A}$ que corra en tiempo polinómico (en λ). Despreciable quiere decir que decrece más rápido que el inverso de cualquier polinomio.

C. El Problema de la Residuosidad Cuadrática

Sea $N = pq$ un producto de dos números primos, cada uno con $\lambda/2$ bits. Dentro del grupo $\mathbb{Z}_N^*$ de unidades de $\mathbb{Z}_N$, intuitivamente el problema de la residuosidad cuadrática consiste en adivinar, dados N y un elemento aleatorio $z \in \mathbb{Z}_N^*$, si es un cuadrado módulo N o no; es decir, si existe algún número entero $a \in \mathbb{Z}_N$ tal que $z = a^2 \bmod N$. Hay que remarcar aquí que el símbolo de Jacobi de $z \in \mathbb{Z}_N^*$, que puede ser calculado de manera eficiente conociendo sólo N, ya actúa parcialmente como discriminador entre residuos y no-residuos cuadráticos, puesto que el símbolo de Jacobi de todos los residuos cuadráticos es siempre 1, mientras que el símbolo de Jacobi de la mitad de los no-residuos cuadráticos es 0. Por tanto, si definimos el problema con $z \in \mathbb{Z}_N^*$ aleatorio, existiría una probabilidad no-despreciable de solucionar el problema usando el símbolo de Jacobi.

Por tanto, restringiremos la definición del problema a elementos $z \in \mathbb{Z}_N^*$ que tengan símbolo de Jacobi igual a 1. Por tanto, definimos los subconjuntos $QR(N) \subset JS_1(N) \subset \mathbb{Z}_N^*$ de la siguiente manera: $JS_1(N)$ contiene todos los elementos de $\mathbb{Z}_N^*$ con símbolo de Jacobi igual a 1, y $QR(N)$ contiene todos los elementos de $JS_1(N)$ que son residuos cuadráticos módulo N.

El problema de la Residuosidad Cuadrática (*QR problem*) se define de manera formal mediante los dos experimentos de probabilidad siguientes, entre un retador y un algoritmo $\mathcal{D}$. El experimento $\textbf{Exp-QR}_{\mathcal{D}}^{\beta}(\lambda)$ se define de la siguiente manera, para $\beta \in \{0, 1\}$.

1) El retador escoge aleatoriamente dos números primos p, q, cada uno con $\lambda/2$ bits, y calcula $N = pq$.
2) El retador escoge $z \in \mathbb{Z}_N^*$ de la siguiente manera:
   - si $\beta = 0$, entonces $z \in_R QR(N)$,
   - si $\beta = 1$, entonces $z \in_R JS_1(N) - QR(N)$.
3) La pareja (N, z) se envía al algoritmo $\mathcal{D}$.
4) $\mathcal{D}$ devuelve un bit $\beta' \in \{0, 1\}$.

Sea Ω_β^{QR} el suceso en el que $\mathcal{D}$ devuelve $\beta' = 1$ en el experimento $\textbf{Exp-QR}_{\mathcal{D}}^{\beta}(\lambda)$, para $\beta \in \{0, 1\}$. La ventaja de ese algoritmo $\mathcal{D}$ en resolver el problema de la Residuosidad Cuadrática se define como

$$\textbf{Adv-QR}_{\mathcal{D}}(\lambda) = \left|\Pr[\Omega_1^{QR}] - \Pr[\Omega_0^{QR}]\right|.$$

La *hipótesis de la Residuosidad Cuadrática* dice que $\textbf{Adv-QR}_{\mathcal{D}}(\lambda)$ es una función despreciable de λ, para cualquier algoritmo $\mathcal{D}$ que corra en tiempo polinómico (en λ).

El problema de la residuosidad cuadrática puede extenderse para valores $d \geq 2$ del exponente. Hablamos entonces del problema de la *Residuosidad d-ésima*, que consiste en adivinar, dado un elemento $z \in \mathbb{Z}_N^*$, si existe un entero $a \in \mathbb{Z}_N$ tal que $z = a^d \bmod N$ o no. Si se conoce la factorización de $N = pq$, entonces el problema es fácil de resolver, puesto que z es un residuo d-ésimo si y sólo si $z^{(p-1)/d} = 1 \bmod p$ y $z^{(q-1)/d} = 1 \bmod q$. En general, podemos definir, para $d \geq 2$, el bit $HQR_N(d, z)$ que es igual a 0 si z es un residuo d-ésimo módulo N, e igual a 1 si no. El coste de calcular $HQR_N(d, z)$ si se conocen p, q es de dos exponenciaciones modulares, mientras que la hipótesis de la Residuosidad d-ésima afirma que calcular $HQR_N(d, z)$ conociendo sólo N es un problema computacionalmente difícil.

III. El Nuevo Esquema

Generación de claves, $\mathsf{PKE.KG}(1^\lambda)$. Escoger dos números primos p, q de $\lambda/2$ bits cada uno, y calcular $N = pq$. Escoger un entero positivo ℓ para la longitud admitida de los mensajes a cifrar. Escoger un no-residuo cuadrático de manera aleatoria, $x \in_R JS_1(N) - QR(N)$.

La clave pública es $\mathsf{pk} = (N, x, \ell)$, mientras que la clave secreta es $\mathsf{sk} = (p, q)$.

Cifrado, $\mathsf{PKE.Enc}(\mathsf{pk}, m)$. Sea $m \in \mathbb{Z}^+, m < 2^\ell$ un mensaje a cifrar; escribimos $m = (m_{\ell-1}, \ldots, m_1, m_0)$ para la representación en bits de m, de manera que $m = \sum_{i=0}^{\ell-1} m_i 2^i$. El protocolo de cifrado funciona de la siguiente manera.

1) Escoger $y \in_R \mathbb{Z}_N^*$ aleatoriamente.
2) Calcular y devolver el texto cifrado $c = y^{2^{\ell+1}} \cdot x^m \bmod N$.

Descifrado, $\mathsf{PKE.Dec}(\mathsf{sk}, c)$. Recordemos que el bit $HQR_N(d, c)$ que nos indica si c es un residuo d-ésimo módulo N o no puede calcularse de manera eficiente (dos exponenciaciones modulares) si los factores p, q de N son conocidos (ver Sección II-C).

Para descifrar un texto cifrado $c \in \mathbb{Z}_N$, se procede de la siguiente manera, para i desde 0 hasta $\ell - 1$.

1) Calcular y definir $m_i = HQR_N(2^{i+1}, c)$.
2) Actualizar: $c \longleftarrow \frac{c}{x^{m_i 2^i}} \bmod N$

El protocolo de descifrado da como salida el texto en claro resultante: $m = \sum_{i=0}^{\ell-1} m_i 2^i \equiv (m_{\ell-1}, \ldots, m_1, m_0)$.

A. Propiedad Homomórfica

Es fácil verificar que, para cualquier par de mensajes $m, m' \in \{0, 1, \ldots, 2^\ell - 1\}$ tales que $m + m' < 2^\ell$, se cumple que al multiplicar un cifrado de m por un cifrado de m', y reducir módulo N, obtenemos un cifrado válido de $m + m'$. En particular, esa propiedad permite re-aleatorizar textos cifrados: si $c = y^{2^{\ell+1}} \cdot x^m \bmod N$ es un texto cifrado para el mensaje m, cualquiera puede obtener un nuevo texto cifrado c' para el mismo mensaje m, sin necesidad de conocer ni m ni la clave secreta. Para ello, basta con multiplicar c por un cifrado aleatorio $(y')^{2^{\ell+1}}$ del mensaje 0, y obtener así $c' = (y \cdot y')^{2^{\ell+1}} \cdot x^m \bmod N$.

Esta propiedad homomórfica *aditiva* (manipular textos cifrados permite obtener un texto cifrado de la *suma* de los mensajes subyacentes) es la misma que disfrutan otros esquemas como Goldwasser-Micali [5], Benaloh [2], Naccache-Stern [6], Okamoto-Uchiyama [7], Paillier [8]. En cambio, otros esquemas clásicos como RSA [10] o ElGamal [3] tienen una propiedad homomórfica *multiplicativa*. La propiedad aditiva parece tener más utilidad en aplicaciones reales como sistemas de voto electrónico, subhastas digitales, computación multiparte, etc.

Por último, destacar que en los últimos años el tema de los criptosistemas con propiedades homomórficas ha vuelto con gran fuerza a la actualidad de la comunidad criptográfica, debido a la aparición de esquemas de cifrado que tienen a la vez propiedades homomórficas aditivas y multiplicativas, el primero de ellos debido a Gentry [4]. Estos esquemas *completamente homomórficos* son bastante complicados teóricamente y de momento su eficiencia es muy precaria, pero se están obteniendo avances de manera muy rápida. Las aplicaciones de los esquemas completamente homomórficos son potencialmente muy amplias, desde la delegación de computaciones costosas de manera privada (*cloud computing*) hasta protocolos de consultas seguras sobre bases de datos cifradas.

IV. Análisis de Seguridad

Para demostrar que nuestro esquema tiene la propiedad de seguridad semántica suponiendo que el problema de la Residuosidad Cuadrática es difícil, utilizaremos un argumento híbrido, muy común para este tipo de demostraciones. En nuestro caso, en el que podemos aprovechar además la propiedad homomórfica del esquema, ese argumento nos da el siguiente resultado.

Lema 1. *Si existe algún adversario $\mathcal{A}$ contra la seguridad CPA de nuestro esquema con ventaja* $\textbf{Adv-CPA}_{\mathcal{A}}^{PKE}(\lambda)$*, entonces existe algún adversario $\mathcal{A}_i$ que elige siempre los mensajes $m^0 = 0$ y $m^1 = 2^i$, para algún $i \in \{0, 1, \ldots, \ell-1\}$, con ventaja* $\textbf{Adv-CPA}_{\mathcal{A}_i}^{PKE}(\lambda) \geq \frac{1}{\ell} \cdot \textbf{Adv-CPA}_{\mathcal{A}}^{PKE}(\lambda)$.

Demostración. El retador ejecuta $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{PKE.KG}(1^\lambda)$ y envía pk al adversario $\mathcal{A}$, que escoge dos mensajes $m^0 \neq m^1$ de igual longitud ℓ. Escribimos la representación en bits de dichos mensajes como $m^0 = (m^0_{\ell-1}, \ldots, m^0_1, m^0_0)$ y $m^1 = (m^1_{\ell-1}, \ldots, m^1_1, m^1_0)$. Tomamos las posiciones en las que los bits son diferentes, es decir $J = \{j | m^0_j \neq m^1_j\}$. Si ordenamos esos índices de mayor a menor, obtendremos $J = \{j_1, j_2, \ldots, j_t\}$ con $\ell - 1 \geq j_1 > j_2 > \ldots > j_t \geq 0$, y por tanto $t \leq \ell$.

Consideramos ahora los siguientes $t+1$ mensajes en claro: $\tilde{m}^0 = m^0$, y para $k = 1, \ldots, t$, definimos $\tilde{m}^k$ como el resultado de cambiar el bit t_k-ésimo al mensaje $\tilde{m}^{k-1}$ anterior. Obtenemos de esta manera una lista ordenada de mensajes, $\tilde{m}^0, \tilde{m}^1, \ldots, \tilde{m}^t$, que cumplen que dos mensajes consecutivos se diferencian sólo en un bit, y además $\tilde{m}^0 = m^0$ y $\tilde{m}^t = m^1$.

Definimos ahora $t+1$ experimentos CPA modificados, $\textbf{mExp-CPA}_{\mathcal{A}}^{k,\mathsf{PKE}}(\lambda)$, exactamente como el experimento $\textbf{Exp-CPA}_{\mathcal{A}}^{b,\mathsf{PKE}}(\lambda)$ definido en la Sección II-B, pero ahora el cifrado que se envía al adversario es $c = \mathsf{PKE.Enc}(\mathsf{pk}, \tilde{m}^k)$. Sea $\tilde{\Omega}_k$ el suceso donde $\mathcal{A}$ devuelve $b' = 1$ en el experimento $\textbf{mExp-CPA}_{\mathcal{A}}^{k,\mathsf{PKE}}(\lambda)$, para $k = 0, 1, \ldots, t$.

Tenemos ahora $\textbf{mExp-CPA}_{\mathcal{A}}^{0,\mathsf{PKE}}(\lambda) = \textbf{Exp-CPA}_{\mathcal{A}}^{0,\mathsf{PKE}}(\lambda)$ y $\textbf{mExp-CPA}_{\mathcal{A}}^{t,\mathsf{PKE}}(\lambda) = \textbf{Exp-CPA}_{\mathcal{A}}^{1,\mathsf{PKE}}(\lambda)$, por tanto $\left|\Pr[\tilde{\Omega}_t] - \Pr[\tilde{\Omega}_0]\right| = |\Pr[\Omega_1] - \Pr[\Omega_0]| = \textbf{Adv-CPA}_{\mathcal{A}}^{\mathsf{PKE}}(\lambda)$. Por otro lado, tenemos que $\left|\Pr[\tilde{\Omega}_t] - \Pr[\tilde{\Omega}_0]\right| \geq \left|\Pr[\tilde{\Omega}_t] - \Pr[\tilde{\Omega}_{t-1}]\right| + \ldots + \left|\Pr[\tilde{\Omega}_1] - \Pr[\tilde{\Omega}_0]\right|$. Por tanto, por un razonamiento básico de desigualdades, debe haber alguna de estas t diferencias que sea mayor o igual que $\frac{1}{t} \cdot \textbf{Adv-CPA}_{\mathcal{A}}^{\mathsf{PKE}}(\lambda)$. Sea $k^* \in \{1, \ldots, t\}$ el índice tal que

$$\left|\Pr[\tilde{\Omega}_{k^*}] - \Pr[\tilde{\Omega}_{k^*-1}]\right| \geq \frac{1}{t} \cdot \textbf{Adv-CPA}_{\mathcal{A}}^{\mathsf{PKE}}(\lambda)$$

y sea $i = t_{k^*}$. Tenemos pues que $\tilde{m}^{k^*-1}$ y $\tilde{m}^{k^*}$ difieren sólo en el bit i-ésimo. Sin pérdida de generalidad, supongamos que $\tilde{m}_i^{k^*-1} = 0$ y $\tilde{m}_i^{k^*} = 1$. Viendo los mensajes como números enteros, eso se traduce en $\tilde{m}^{k^*} = \tilde{m}^{k^*-1} + 2^i$.

Ahora ya podemos construir un adversario $\mathcal{A}_i$ que cumple las condiciones enunciadas en el lema: $\mathcal{A}_i$ escoge los mensajes $m^0 = 0$ y $m^1 = 2^i$ y recibe un texto cifrado $c = \mathsf{PKE.Enc}(\mathsf{pk}, m^b)$. Usando las propiedades homomórficas del sistema, $\mathcal{A}_i$ opera c con un cifrado aleatorio del mensaje $\tilde{m}^{k-1}$ para obener un cifrado $\tilde{c} = \mathsf{PKE.Enc}(\mathsf{pk}, m^b + \tilde{m}^{k-1})$. Y ahora $\mathcal{A}_i$ ejecuta el experimento $\textbf{mExp-CPA}_{\mathcal{A}}^{\cdot,\mathsf{PKE}}(\lambda)$ con el adversario $\mathcal{A}$, enviándole en la fase de Reto el texto cifrado $\tilde{c}$.

Es inmediato ver que cuando $b = 0$, el experimento que ejecutan $\mathcal{A}_i$ y $\mathcal{A}$ es $\textbf{mExp-CPA}_{\mathcal{A}}^{k^*-1,\mathsf{PKE}}(\lambda)$ y cuando $b = 1$, el experimento que ejecutan $\mathcal{A}_i$ y $\mathcal{A}$ es $\textbf{mExp-CPA}_{\mathcal{A}}^{k^*,\mathsf{PKE}}(\lambda)$. Por tanto, tenemos que

$$\textbf{Adv-CPA}_{\mathcal{A}_i}^{\mathsf{PKE}}(\lambda) = \left|\Pr[\tilde{\Omega}_{k^*}] - \Pr[\tilde{\Omega}_{k^*-1}]\right| \geq$$

$$\geq \frac{1}{t} \cdot \textbf{Adv-CPA}_{\mathcal{A}}^{\mathsf{PKE}}(\lambda) \geq \frac{1}{\ell} \cdot \textbf{Adv-CPA}_{\mathcal{A}}^{\mathsf{PKE}}(\lambda)$$

como queríamos demostrar. □

Lema 2. *Si existe algún adversario $\mathcal{A}_i$ contra la seguridad CPA de nuestro esquema, para $i \in \{0, 1, \ldots, \ell-1\}$, que elige siempre los mensajes $m^0 = 0$ y $m^1 = 2^i$ y tiene ventaja* $\textbf{Adv-CPA}_{\mathcal{A}_i}^{PKE}(\lambda)$*, entonces existe un algoritmo $\mathcal{D}$ que resuelve el problema de la Residuosidad Cuadrática con ventaja* $\textbf{Adv-QR}_{\mathcal{D}}(\lambda) \geq \frac{1}{2(\ell-i+1)} \cdot \textbf{Adv-CPA}_{\mathcal{A}_i}^{PKE}(\lambda)$.

Demostración. Para $b \in \{0, 1\}$, y $j = 1, 2, \ldots, \ell - i + 1$, definimos el experimento $\textbf{Exp-CPA}_{\mathcal{A}_i}^{(b,j),\mathsf{PKE}}(\lambda)$ como el experimento que define la seguridad CPA (ver Sección II-B), modificado de la siguiente manera. Al generar el par de claves $(\mathsf{sk}, \mathsf{pk})$, el retador escoge el elemento x de la clave pública se define tomando primero un elemento aleatorio $\tilde{x} \in_R \mathbb{Z}_N^*$ y calculando después $x = \tilde{x}^{2^j}$. En lo que refiere al texto cifrado que se entrega a $\mathcal{A}_i$ en la fase de Reto, si $b = 0$ se le da un cifrado $c = \mathsf{PKE.Enc}(\mathsf{pk}, 0)$ de $m^0 = 0$, y si $b = 1$ se le da un cifrado $c = \mathsf{PKE.Enc}(\mathsf{pk}, 2^i)$ de $m^1 = 2^i$. Para $j = 0$, definimos $\textbf{Exp-CPA}_{\mathcal{A}_i}^{(0,0),\mathsf{PKE}}(\lambda) = \textbf{Exp-CPA}_{\mathcal{A}_i}^{0,\mathsf{PKE}}(\lambda)$ y $\textbf{Exp-CPA}_{\mathcal{A}_i}^{(1,0),\mathsf{PKE}}(\lambda) = \textbf{Exp-CPA}_{\mathcal{A}_i}^{1,\mathsf{PKE}}(\lambda)$.

Sea $\tilde{\Omega}_{(b,j)}$ el suceso donde $\mathcal{A}_i$ devuelve $b' = 1$ en el experimento $\mathbf{Exp\text{-}CPA}_{\mathcal{A}_i}^{(b,j),\mathsf{PKE}}(\lambda)$, para $b \in \{0,1\}$ y $j = 0, 1, \ldots, \ell - i + 1$. Por tanto tenemos

$$\mathbf{Adv\text{-}CPA}_{\mathcal{A}_i}^{\mathsf{PKE}}(\lambda) = |\Pr[\Omega_1] - \Pr[\Omega_0]| = \left|\Pr[\tilde{\Omega}_{(0,0)}] - \Pr[\tilde{\Omega}_{(1,0)}]\right|$$

Veamos ahora que $\Pr[\tilde{\Omega}_{(0,\ell-i+1)}] = \Pr[\tilde{\Omega}_{(1,\ell-i+1)}]$. En efecto, en esos dos experimentos el elemento x de la clave pública es $x = \tilde{x}^{2^{\ell-i+1}}$. Por tanto un cifrado de $m^0 = 0$ tendrá la forma $c^0 = y^{2^{\ell+1}} \bmod N$ para un elemento aleatorio $y \in \mathbb{Z}_N^*$, mientras que un cifrado de $m^1 = 2^i$ tendrá la forma $c^1 = y^{2^{\ell+1}} \cdot x^{2^i} \bmod N = y^{2^{\ell+1}} \cdot \tilde{x}^{2^{\ell-i+1} \cdot 2^i} \bmod N = (y \cdot \tilde{x})^{2^{\ell+1}} \bmod N$. Como $y \cdot \tilde{x}$ es también un elemento aleatorio en $\mathbb{Z}_N^*$, tenemos que la distribución de probabilidad de c^0 es exactamente la misma que la de c^1. Por tanto, el adversario $\mathcal{A}_i$ tiene el mismo comportamiento en los experimentos $\mathbf{Exp\text{-}CPA}_{\mathcal{A}_i}^{(0,\ell-i+1),\mathsf{PKE}}(\lambda)$ y $\mathbf{Exp\text{-}CPA}_{\mathcal{A}_i}^{(1,\ell-i+1),\mathsf{PKE}}(\lambda)$.

A continuación, veremos que para cada $b \in \{0,1\}$ y cada $j = 1, \ldots, \ell - i + 1$, podemos construir un algoritmo $\mathcal{D}$ que resuelve el problema de la Residuosidad Cuadrática con ventaja $\mathbf{Adv\text{-}QR}_{\mathcal{D}}(\lambda) = \left|\Pr[\tilde{\Omega}_{(b,j)}] - \Pr[\tilde{\Omega}_{(b,j-1)}]\right|$. En efecto, cuando $\mathcal{D}$ recibe la entrada (N, z) del problema de la Residuosidad Cuadrática, $\mathcal{D}$ ejecuta el experimento $\mathbf{Exp\text{-}CPA}_{\mathcal{A}_i}^{(b,\cdot),\mathsf{PKE}}(\lambda)$ con $\mathcal{A}_i$, definiendo el elemento x de la clave pública del esquema PKE como $x = z^{2^{j-1}} \bmod N$, y el texto cifrado como $c = \mathsf{PKE.Enc}(\mathsf{pk}, m^b)$. Si $\mathcal{D}$ está en el experimento de residuosidad cuadrática $\mathbf{Exp\text{-}QR}_{\mathcal{D}}^0(\lambda)$, entonces $z \in JS_1(N) - QR(N)$ y por tanto el experimento que están ejecutando $\mathcal{D}$ y $\mathcal{A}_i$ es en realidad $\mathbf{Exp\text{-}CPA}_{\mathcal{A}_i}^{(b,j-1),\mathsf{PKE}}(\lambda)$. Por otro lado, si $\mathcal{D}$ está en el experimento de residuosidad cuadrática $\mathbf{Exp\text{-}QR}_{\mathcal{D}}^1(\lambda)$, entonces $z \in QR(N)$ y por tanto el experimento que están ejecutando $\mathcal{D}$ y $\mathcal{A}_i$ es en realidad $\mathbf{Exp\text{-}CPA}_{\mathcal{A}_i}^{(b,j),\mathsf{PKE}}(\lambda)$. Por tanto, tenemos $\Omega_0^{QR} = \tilde{\Omega}_{(b,j-1)}$ y $\Omega_1^{QR} = \tilde{\Omega}_{(b,j)}$, y obtenemos el resultado deseado: $\mathbf{Adv\text{-}QR}_{\mathcal{D}}(\lambda) = \left|\Pr[\Omega_1^{QR}] - \Pr[\Omega_0^{QR}]\right| = \left|\Pr[\tilde{\Omega}_{(b,j)}] - \Pr[\tilde{\Omega}_{(b,j-1)}]\right|$.

Por último, podemos utilizar la desigualdad triangular y los dos resultados parciales descritos en los dos párrafos previos, para obtener el resultado enunciado en el lema. En efecto, tenemos

$$\begin{aligned}
\mathbf{Adv\text{-}CPA}_{\mathcal{A}_i}^{\mathsf{PKE}}(\lambda) &= \left|\Pr[\tilde{\Omega}_{(0,0)}] - \Pr[\tilde{\Omega}_{(1,0)}]\right| \leq \\
&\leq \sum_{j=1}^{\ell-i+1} \left(\left|\Pr[\tilde{\Omega}_{(0,j)}] - \Pr[\tilde{\Omega}_{(0,j-1)}]\right|\right) + \\
&+ \left|\Pr[\tilde{\Omega}_{(0,\ell-i+1)}] - \Pr[\tilde{\Omega}_{(1,\ell-i+1)}]\right| + \\
&+ \sum_{j=1}^{\ell-i+1} \left(\left|\Pr[\tilde{\Omega}_{(1,j)}] - \Pr[\tilde{\Omega}_{(0,j-1)}]\right|\right) = \\
&= 2(\ell - i + 1)\mathbf{Adv\text{-}QR}_{\mathcal{D}}(\lambda).
\end{aligned}$$

□

Combinando los resultados en los Lemas 1 y 2, y teniendo en cuenta que $i \geq 0$, se obtiene directamente el siguiente teorema que nos da la seguridad semántica del nuevo esquema de cifrado, bajo la hipótesis que el problema de la Residuosidad Cuadrática es difícil.

Teorema 1. *Si existe algún adversario $\mathcal{A}$ contra la seguridad CPA de nuestro esquema con ventaja* $\mathbf{Adv\text{-}CPA}_{\mathcal{A}}^{\mathsf{PKE}}(\lambda)$*, entonces existe un algoritmo $\mathcal{D}$ que resuelve el problema de la Residuosidad Cuadrática con ventaja* $\mathbf{Adv\text{-}QR}_{\mathcal{D}}(\lambda) \geq \frac{1}{2\ell(\ell+1)} \cdot \mathbf{Adv\text{-}CPA}_{\mathcal{A}}^{\mathsf{PKE}}(\lambda)$.

El teorema anterior nos da una relación concreta entre la dificultad de romper la seguridad CPA del nuevo esquema y la dificultad de solucionar el problema de la Residuosidad Cuadrática (QR). Dicha relación permite escoger de manera segura la longitud de claves y la longitud de mensajes para el esquema de cifrado, dependiendo del estado de arte en cuanto a algoritmos conocidos para resolver el problema QR. Por ejemplo, si la mejor manera conocida de resolver el problema QR es factorizar el número N, y se asume (los datos no son necesariamente reales) que el mejor algoritmo para factorizar un número de $\lambda = 2048 = 2^{11}$ bits tiene probabilidad de éxito 2^{-100} (o, lo que es equivalente, tiempo de ejecución 2^{100}), y buscamos proteger nuestro esquema de cifrado contra ataques que tengan probabilidad de éxito como mucho 2^{-80}, entonces para que el resultado del teorema sea significativo y nos dé seguridad real, podemos tomar ℓ tal que $2\ell(\ell+1) \leq 2^{20}$, por ejempmlo $\ell = 2^9$. En este ejemplo concreto, nuestro esquema permitiría cifrar mensajes de $\ell = 2^9 = 512$ bits mediante textos cifrados de $\lambda = 2^{11} = 2048$ bits. Por tanto, el *factor de expansión* entre la longitud de un texto cifrado y la longitud del mensaje sería en este caso $\lambda/\ell = 4$.

V. Comparación con Otros Esquemas Homomórficos Aditivos

El esquema que proponemos en este trabajo es bastante similar a otros esquemas de cifrado homomórficos, en particular los de Benaloh [2] y Naccache-Stern [6]. De hecho, el protocolo de cifrado de nuestro esquema es exactamente igual que el protocolo de cifrado de esos esquemas. La diferencia está en el protocolo de descifrado, que es más eficiente en nuestro caso, puesto que requiere $\mathcal{O}(\ell)$ exponenciaciones modulares. En la siguiente tabla presentamos un resumen con las características de varios esquemas de cifrado de clave pública homomórficos cuya seguridad se basa en hipótesis computacionales relacionadas de alguna manera con el problema de factorizar un número N producto de primos grandes.

En la tabla, λ es el parámetro de seguridad (la longitud en bits de N), y el coste de descifrado se deriva del hecho que una exponenciación modular del tipo $z^{(p-1)/d} \bmod N$ tiene coste $\mathcal{O}(\lambda^3)$. El primer esquema de esta familia, propuesto por Goldwasser y Micali [5], sólo podía cifrar un bit; si se cifran ℓ bits con dicho esquema, los costes de cifrar y descifrar son similares a nuestro esquema, pero la longitud total del cifrado sería ℓ veces mayor. Nuestro esquema mejora a los esquemas en [2] y [6] en lo que refiere al coste de descifrado. En cambio,

Esquema	$\|m\|$	$\|c\|$	coste de descifrado (caso peor)	Hipótesis de seguridad
GoMi84 [5]	1	λ	$\mathcal{O}(\lambda^3)$	Res. cuad. módulo N
Ben88 [2]	ℓ	λ	$\mathcal{O}(\ell 2^{\ell/2})$	Res. d-ésima módulo N
NaSt98 [6]	ℓ	λ	$\mathcal{O}(\lambda^5 \log(\lambda))$	Res. d-ésima módulo N
OkUc98 [7]	$\lambda/3$	λ	$\mathcal{O}(\lambda^3)$	Factorizar $N = p^2q$
Pai99 [8]	λ	2λ	$\mathcal{O}(\lambda^3)$	Res. N-ésima módulo N^2
Nuestro esquema	ℓ	λ	$\ell \cdot \mathcal{O}(\lambda^3)$	Res. cuad. módulo N

TABLE I
COMPARACIÓN ENTRE ESQUEMAS PKE HOMOMÓRFICOS.

nuestro esquema puede ser peor que los esquemas en [7] y [8] en lo que refiere a factor de expansión entre las longitudes de texto cifrado y mensaje, y es definitivamente peor que ellos en lo que refiere al coste de descifrado (ℓ veces peor). Sin embargo, en aplicaciones reales como votación electrónica o búsqueda anónima en bases de datos, los mensajes a cifrar (y por tanto ℓ en nuestro esquema) son pequeños, y en ese caso nuestro esquema sería realmente comparable en términos de eficiencia a los esquemas en [7] y [8].

Una posible ventaja de nuestro esquema respecto a los esquemas en [7] y [8] es la hipótesis de seguridad en la cual se basan, puesto que la hipótesis de la Residuosidad Cuadrática módulo $N = pq$ parece más estándar, mejor estudiada, que hipótesis que utilizan módulos como $N = p^2q$ o $N^2 = p^2q^2$.

En cualquier caso, es un problema abierto (y aparentemente muy difícil) encontrar relaciones entre todos estos problemas. Nuestro nuevo esquema ganaría mucho interés e impacto si, por ejemplo, se pudiese demostrar que el problema de la Residuosidad Cuadrática módulo N es estrictamente más difícil que el problema de la residuosidad N-ésima módulo N^2.

VI. CONCLUSIÓN

En este trabajo hemos propuesto un nuevo esquema de cifrado de clave pública con propiedades homomórficas aditivas. El nuevo esquema puede situarse en una posición intermedia dentro de la familia de esquemas de este tipo cuya seguridad se basa en la dificultad de algún problema computacional relacionado con la factorización de números grandes. Por un lado, nuestro esquema es más eficiente que el resto de esquemas existentes que basan su seguridad en el mismo problema computacional (la residuosidad d-ésima módulo $N = pq$, para $d \geq 2$). Por otro lado, los esquemas que tienen mejor eficiencia (en el algoritmo de descifrado, y sólo en el caso en que los mensajes cifrados sean largos) que el nuestro basan su seguridad en otros problemas computacionales diferentes, como factorizar números del tipo $N = p^2q$ o bien decidir la residuosidad N-ésima módulo N^2, cuando $N = pq$.

Como línea futura de investigación, sería muy interesante intentar encontrar relaciones entre todos estos problemas computacionales de teoría de números, para aclarar qué esquemas de esta familia disfrutan de mejores propiedades de eficiencia y seguridad, globalmente. Por ejemplo, si fuese posible demostrar que un algoritmo que resuelva el problema de la Residuosidad Cuadrática módulo N puede ser usado para resolver el problema de la Residuosidad N-ésima módulo N^2, y no al revés, entonces nuestro esquema tendría mejor seguridad que el esquema de Paillier, que es el mejor considerado y más utilizado en aplicaciones reales, dentro de esta familia.

REFERENCES

[1] C. Aguilar, P. Gaborit, J. Herranz, "Additively homomorphic encryption with d-operand multiplications". *Proceedings of Crypto'10*, LNCS **6223**, Springer-Verlag, pp. 138–154, 2010.

[2] J. Benaloh, "Verifiable secret-ballot elections". Ph-D thesis, Yale University, 1988.

[3] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms". *IEEE Transactions on Information Theory*, vol. 31, pp. 469–472, 1985.

[4] C. Gentry, "Fully homomorphic encryption using ideal lattices". *Proceedings of STOC'09*, ACM Press, pp. 169–178, 2009.

[5] S. Goldwasser, S. Micali, "Probabilistic encryption". *Journal of Computer and System Sciences*, vol. 28, no. 2, pp. 270–299, 1984.

[6] D. Naccache, J. Stern, "A new public-key cryptosystem based on higher residues". *Proccedings of CCS'88*, ACM Press, pp. 59–66, 1998.

[7] T. Okamoto, S. Uchiyama, "A new public-key cryptosystem as secure as factoring". *Proceedings of Eurocrypt'98*, LNCS **1403**, Springer-Verlag, pp. 308–318, 1998.

[8] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes". *Proceedings of Eurocrypt'99*, LNCS **1592**, Springer-Verlag, pp. 223–238, 1999.

[9] O. Regev, "New lattice-based cryptographic constructions". *Journal of the ACM*, vol. 51, no. 6, pp. 899–942, 2004.

[10] R. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems". *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.