A. Mana, et al., "Incremento de la Seguridad del Estandar de Cifrado de Datos basado en la Combinación de Datos y Clave", *III Jornadas de Informática y Automática*, pp. 423-432, 1997.
NICS Lab. Publications: https://www.nics.uma.es/publications

# Incremento de la Seguridad del Estándar de Cifrado de Datos basado en la combinación de datos y clave

*Antonio Maña, Javier López, Lucia Pino, Juan J. Ortega, Carlos Maraval*

*Departamento de Lenguajes y Ciencias de la Computación.*

*Universidad de Málaga.*

***Resumen***

*A pesar del gran esfuerzo investigador llevado a cabo, el ataque al DES ha sido infructuoso desde que a mediados de los setenta fue adoptado como estándar por el U. S. National Bureau of Standards. El criptoanálisis diferencial constituye la base de las primeras técnicas capaces de acabar con tal invulnerabilidad. Las técnicas de criptoanálisis basadas en modelos de fallos y su adaptación a DES, el criptoanálisis de fallos diferencial, son dos de esas técnicas que han conseguido recientemente romper sistemas DES (aunque el ataque está limitado a ciertos casos especiales, en particular implementaciones hardware). En este artículo se presenta un punto débil de DES sobre el cual puede aumentarse la seguridad y se propone una modificación de la estructura interna de DES con objeto de mejorar su resistencia ante el criptoanálisis diferencial y por ende de los ataques derivados de este. La modificación introducida no supone un coste adicional elevado.*

## 1. Introducción

En la actualidad uno de los ataques más conocidos a DES es el cripotoanálisis diferencial. Este sistema ha conseguido reducir la complejidad del análisis por debajo de la de la búsqueda exhaustiva bajo determinadas condiciones. El ataque mediante criptoanálisis diferencial es un ataque sobre criptograma elegido (aunque puede adaptarse para ser sobre criptograma conocido) aplicable a cualquier cifrado de bloques iterativo que se basa en la estructura de estos y en la observación de que la frecuencia con que aparecen ciertos criptogramas puede revelar información sobre la clave usada.

DES (Data Encription Standard) es una versión mejorada de *Lucifer* que fué desarrollada por IBM y certificada por el U.S. NBS (National Bureau of Standards) [1] como criptosistema estandar para datos reservados. Desde ese momento DES se ha convertido en un sistema muy usado y conocido. DES trabaja sobre bloques de 64 bits bajo el control de una clave de 56 bits. En cada pasada los 64 bits de entrada se dividen en dos partes de igual

longitud que se combinan como muestra la figura. Puede verse que la transformación principal la produce la función F, que combina la parte derecha de la entrada con una subclave de 48 bits.

La función F utiliza ocho cajas-S de seis bits de entrada y cuatro de salida para combinar la subclave con la parte derecha de la entrada a ese nivel produciendo una salida de 32 bits. La XOR de esta salida de la función F y de la parte izquierda de la entrada constituye la parte derecha de la salida, mientras que la parte izquierda de la salida es igual a la parte derecha de la entrada. Puede consultarse la especificación completa de DES en casi la totalidad de los libros sobre criptografía general o en [1].

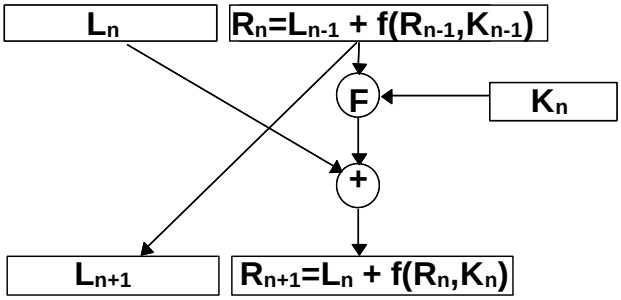


**Fig. 1. Función base de DES**

Desde su aparición DES ha sido el reto más importante para los criptoanalistas. En el intento de criptoanalizar el DES se han probado muchos caminos sin que hasta la aparición del cripoanálisis diferencial se publicasen técnicas o medios de reducir la complejidad de la búsqueda a menos de la mitad de la complejidad de la búsqueda exhaustiva. La mayoría de los métodos se han topado con que sus soluciones eran más complejas que la propia búsqueda exaustiva y algunos, no encontrando otra salida, se han limitado a sugerir o diseñar hardware dedicado para romper por búsqueda exhaustiva este criposistema. Muchos análisis se han basado en versiones simplificadas de DES con menos pasadas que las 16 del estandar.

Desde la certificación de DES, no obstante, se han ido realizando avances y hoy parece claro que, dada la evolución de la tecnología harware, un espacio de claves de $2^{56}$ no será seguro por mucho tiempo incluso sin contar con técnicas para reducir el tamaño de la búsqueda exhaustiva. Algunos autores [2] siempre han tenido claro que este no sería un estandar duradero, incluso antes de que fuese certificado.

En 1987 Donald W. Davies publica un ataque sobre criptograma conocido que se basa en la XOR de el texto en claro y el criptograma para encontrar 16 relaciones lineales entre los bits de la clave cifrando $10^{26}$ textos en claro, con lo que el coste de una búsqueda exhaustiva se reduciría a $2^{40}$. Este ataque se basa en la correlación encontrada por Davies en la salida de las cajas-S que se debe a que sus entradas se derivan de bits iguales que se generan en la operación de expansión de bits.

| | | | | | |
|---|---|---|---|---|---|
| 32 | 1 | 2 | 3 | 4 | 5 |
| 4 | 5 | 6 | 7 | 8 | 9 |
| 8 | 9 | 10 | 11 | 12 | 13 |
| 12 | 13 | 14 | 15 | 16 | 17 |
| 16 | 17 | 18 | 19 | 20 | 21 |
| 20 | 21 | 22 | 23 | 24 | 25 |
| 24 | 25 | 26 | 27 | 28 | 29 |
| 28 | 29 | 30 | 31 | 32 | 1 |

**Fig. 2. Operación de expansión E**

Este método es pues más costoso que la búsqueda exhaustiva. Sin embargo, el análisis es efectivo para DES reducido a 8 pasadas, lo que significa que el ataque de Davies era capaz de romper más pasadas de DES que ningún otro ataque hasta esa fecha.

Finalmente en 1990 Eli Biham y Adi Shamir desarrollan el criptoanálisis diferencial [3] y en 1992 publican el primer ataque conocido [4] cuya complejidad es inferior a la de la búsqueda exhaustiva en el DES completo de 16 pasadas. Posteriormente han aparecido otros ataques, como el criptoanálisis lineal [5][6], pero ninguno ha demostrado ser efectivo en la práctica hasta el desarrollo del criptoanálisis basado en modelos de fallos y el criptoanálisis de fallos diferencial. De hecho DES fue diseñado específicamente para resistir este tipo de ataques [7].

# 2. Criptoanálisis Diferencial.

El criptoanálisis diferencial es un ataque sobre criptograma elegido que se basa en lo que se denomina una *pareja de criptogramas* que esta constituido por dos criptogramas cuyos textos en claro tienen una diferencia particular (que para los sistemas derivados de DES es expresada por su XOR). Los textos en claro no son útiles al ataque y pueden elegirse aleatoriamente siempre que cumplan que su XOR es la deseada. La naturaleza estadística del ataque hace que no siempre tenga éxito, aunque son escasas las ocasiones en que falla.

Una vez fijada una diferencia en el texto en claro, las diferencias en los criptogramas pueden usarse para asignar probabilidades a las claves posibles y extraer la más probable. El método requiere usar muchos pares de textos en claro con una diferencia fija y considera sólo las parejas de criptogramas correspondientes. Veamos como podemos obtener el conocimiento de la clave partiendo de esas diferencias.

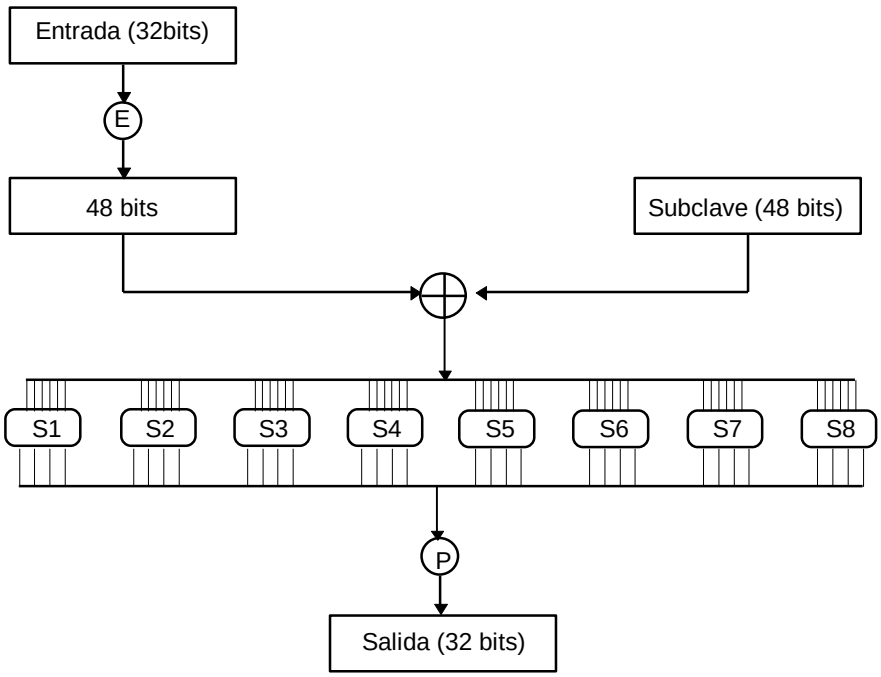


**Fig. 3. Esquema de la función F**

En la descripción que sigue nos centraremos en el funcionamiento en una de las pasadas, ya que el criptoanálisis diferencial de más de una pasada es simplemente una extensión del que se realiza en una pasada.

En cada pasada de DES la función F toma como entrada 32 bits de la pasada anterior y 48 de la clave. La entrada se expande a 48 bits mediante la función de expansión E y su resultado se combina mediante XOR con la clave. El resultado de la XOR se utiliza como entrada a las cajas-S y la salida de esta se permuta.

La XOR de la salida de una pasada de DES es fácilmente calculable conociendo la XOR de las entradas y las transformaciones mencionadas. La única parte de la definición de DES que no permite extender el conocimiento de la XOR de la entrada a la salida son las cajas-S que se definen mediante tablas no lineales. El conocimiento de la XOR de dos entradas a una caja-S no garantiza que se pueda conocer la XOR de las salidas de esas cajas.

Para atacar las cajas-S se utiliza el hecho de que para cada una de ellas podemos obtener una distribución de probabilidad que relaciona cada posible XOR de las entradas con las XOR de las salidas que pueden producirse con esa XOR de las entradas aún sin conocer los valores concretos de las entradas. Las distribuciones de probabilidad indican que dada una XOR de las entradas y una XOR de las salidas existen algunos pares de entradas con esa XOR que provocan salidas cuya XOR es la deseada mientras que otros pares de entradas nunca pueden producirla.

Esta propiedad es un arma útil para identificar bits de la clave. Supongamos que conocemos la XOR de las salidas de la función F de la última pasada. Conociendo los dos criptogramas es posible conocer la XOR de las entradas y la de las salidas de la función F. Esto lleva a conocer la XOR de las entradas y la de las salidas de las cajas-S. El conocimiento de la XOR de entrada nos permite, viendo las tablas de las cajas-S, encontrar los posibles pares de entradas con dicha XOR de entrada que provocan la XOR de salida dada. Si existen *n* de tales pares de entradas cuya XOR sea la deseada y que produzcan esa XOR de salida habrá *n* valores de la subclave posibles, ya que la clave puede conocerse debido a que conocemos la entrada a las cajas-S y la salida de la expansión E y la XOR de estos valores es precisamente la clave. Si se registran todos los valores sugeridos de la clave, tras un número suficientemente alto de pruebas, el valor real aparece muchas más veces que los demás. El hecho de que la clave se derive de forma inmediata de estos valores es básico para que el criptoanálisis diferencial tenga éxito y será uno de los puntos clave de nuestra propuesta. Para una descripción más detallada ver [8] cap. 3.

# 3. Nuestra Variante de DES.

## *3.1. Introducción*

El primer paso de este trabajo consistió en estudiar el funcionamiento del criptoanálisis diferencial para encontrar puntos donde reforzar DES, o lo que es lo mismo, cual es el punto débil de DES que permite que el criptoanálisis diferencial tenga éxito. Debido a que el criptoanálisis diferencial se centra en el análisis del funcionamiento de las cajas-S y a que el diseño de las mismas fue desde un principio un punto controvertido del DES se han desarrollado numerosas investigaciones sobre la seguridad de las cajas-S desde diferentes puntos de vista y se han publicado varias alternativas [9][10][11][12]. Casi la totalidad de los estudios realizados coinciden en valorar la calidad criptográfica de las cajas-S del DES original y en resaltar la dificultad de encontrar otras mejores. A pesar de que esa posibilidad de mejora existe, se ha demostrado que dicha capacidad de mejora está limitada de forma que incluso la mejor caja-S posible debe tener una probabilidad diferencial de $1/2^{m-1}$ (siendo m el tamaño del bloque)[13]. De todo lo anterior se desprende que la modificación de las cajas-S no mejorará en mucho la seguridad del DES original ante un ataque mediante criptoanálisis diferencial.

En lo que sigue vamos a denominar las entradas a cada función con el subíndice *in* y las salidas con *out*, por ejemplo $E_{out}$ será la salida de la operación de expansión E. Por otra parte vamos a denominar función f a la transformación compuesta por las cajas S y la permutación P (por tanto, desde ahora, la entrada de las cajas S se denominará $f_{in}$).

El criptoanálisis diferencial permite obtener varias posibles entradas a la función f a partir de la XOR de sus entradas y la de sus salidas y descartar un buen número de entradas imposibles. La importancia de este hecho radica en que el conocimiento de la entrada $f_{in}$ de la función f permite fácilmente (puesto que se conoce $E_{out}$ a partir de $L_{i+1}$) obtener la subclave $K_i$. Aún más, el conocimiento parcial de $f_{in}$ también revela información parcial sobre $K_i$. De hecho el método de criptoanálisis diferencial lo que hace es descubrir mediante los análisis estadísticos citados algunos bits de la clave para posteriormente realizar una busqueda exhaustiva del resto de la clave.

El siguiente diagrama muestra como se propaga la información en el criptoanálisis diferencial de una pasada del DES:

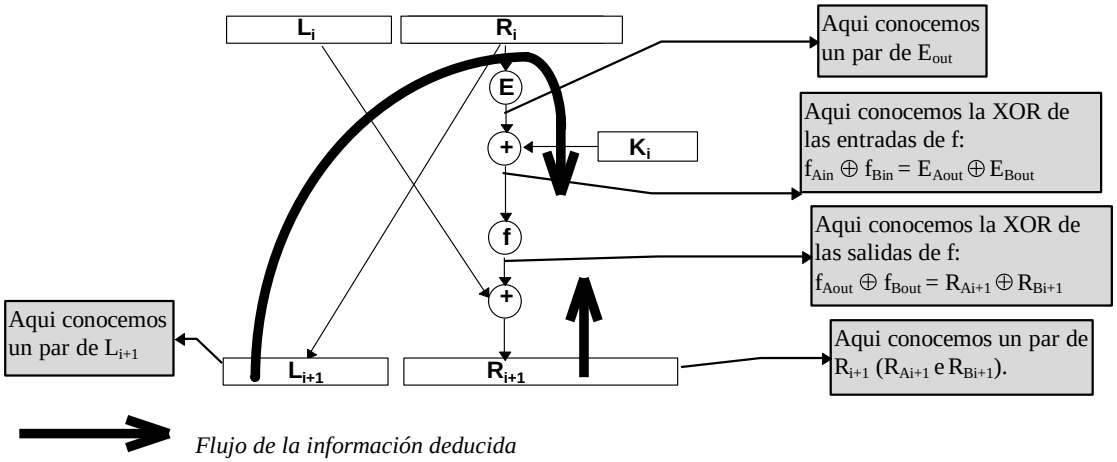


**Fig. 4. Propagación de la información necesaria para el Criptoanálisis Diferencial**

Según se observa, la solución a la debilidad comentada puede consistir en "bloquear" uno de los dos caminos de deducción. El siguiente diagrama muestra como se utiliza esa información y como se obtienen resultados.

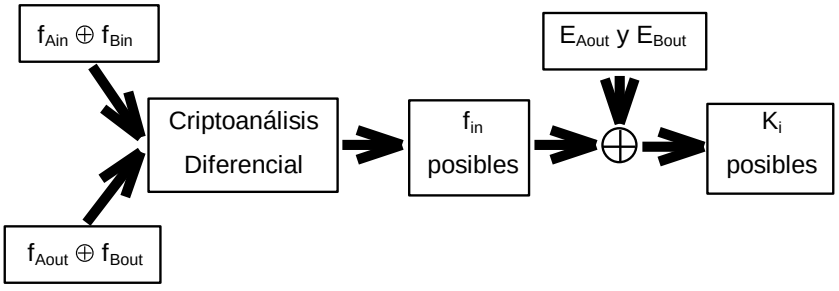


**Fig. 5. Información Procesada por el Criptoanálisis Diferencial**

Nuestra propuesta estudia dos alternativas: bloquear los caminos de deducción mostrados en la fig. 4 y evitar que los resultados del criptoanálisis diferencial sean útiles para obtener información de la subclave $K_i$ como se ve en la fig. 5.

De ambas figuras se obtiene una conclusión: Hay un punto común en ambos diagramas: el modo en el cual la subclave $K_i$ se combina con la salida de la operación de expansión E (a la que denominaremos $E_{out}$ a partir de ahora) para producir la entrada de las cajas S.

Como primera aproximación a las ideas presentadas podemos incluir una función irreversible i que no conserve la operación XOR antes de la función f original, pero podríamos considerar esta modificación como la definición de una nueva función f' compuesta de las dos mencionadas a la cual probablemente podríamos aplicar el criptoanálisis diferencial. En este caso deberíamos considerar la probabilidad diferencial conjunta de la función f' resultante de la unión de la nueva función i con la f primitiva. Consecuentemente habríamos avanzado poco en nuestro intento de reforzar la estructura de DES ante ataques de tipo diferencial.

Por tanto, centrándonos en ese punto común de ambas figuras podríamos modificar el método de combinación de $E_{out}$ y $K_i$, de forma que el conocimiento de la XOR de las $E_{out}$ no permita conocer la XOR de las $f_{in}$ y además el conocimiento de las $f_{in}$ posibles no revele información sobre $K_i$ o, al menos, una de estas dos cosas sea computacionalmente poco rentable. Se han presentado en la literatura varias formas de derivar las subclaves $K_i$ a partir de la clave original, pero no se ha dedicado suficiente esfuerzo al estudio de métodos de combinar la subclave con $E_{out}$, en particular, se ha propuesto sustituir la operación XOR por adiciones, lo cual, al ser la suma una operación reversible no aporta nada en cuanto evitar el conocimiento de $K_i$ a partir de $f_{in}$. Por otra parte, el resultado de la suma siempre coincide con el de la XOR para el bit menos significativo y en más de la mitad de los casos para los demás bits, y por tanto, a pesar de que la suma con una constante no conserva la XOR en todos los casos podemos elegir valores que si lo hacen, en consecuencia la seguridad añadida es escasa.

# 4. NPDES

## *4.1. Introducción.*

Si sustituimos la operación XOR por una operación L de dos argumentos no reversible como se muestra en la figura siguiente, o una cuya inversión sea de gran complejidad (pertenezca a la clase NP) podemos evitar que se extraiga información sobre $K_i$ dados $E_{out}$ y $f_{in}$. Llamaremos NPDES a los sistemas que sustituyan la XOR de $E_{out}$ y $K_i$ por una función perteneciente a la clase P cuya inversa pertenezca a la clase NP. Por tanto, esta especificación deja abierta la elección de la función irreversible a utilizar, aunque se proponen dos ejemplos, ya que el incremento de la resistencia al criptoanálisis diferencial bajo las condiciones mencionadas se asegura por la estructura y no por la función en sí misma.

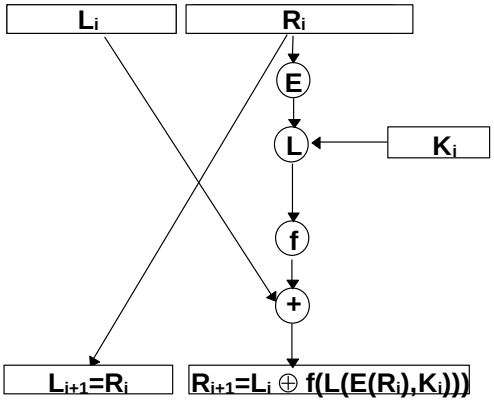


**Fig. 6. Función base de NPDES**

Las funciones irreversibles que se han utilizado en criptografía son un subconjunto de las conocidas puesto que se necesitaban funciones que tuviesen una puerta trampa (trapdoor one way functions) para poder ser invertidas fácilmente con algún conocimiento adicional, esto no es necesario en este sistema ya que la función siempre será utilizada en el mismo sentido. En cualquier caso es importante hacer notar que no es necesario que el proceso de invertir la función sea intratable computacionalmente (de hecho, estará limitado superiormente por la complejidad de la búsqueda exhaustiva -$2^{48}$ encriptaciones como máximo-), sino que será suficiente con que el proceso sea muy costoso.

Supongamos ahora que :

- El coste de invertir L es *x ;*
- se conoce un algoritmo *A* que es capaz de encontrar *n* bits de $f_{in}$ con un coste *y(n)* ;

Esto no nos proporcionará *n* bits de la clave "gratis" como sucede en el DES estandar sino $2^{48-n}$ posibles valores de $K_i$, lo cual es en cierto modo equivalente, con la salvedad de que el cálculo de cada uno de esos valores implica una complejidad extra *x* (en el DES *x*=1). Esto es, si no se conoce $f_{in}$ completamente (por ejemplo, supongamos que conocemos n bits), deberemos invertir la función L para cada uno de los valores posibles de $f_{in}$, o sea $2^{48-n}$ veces. Por tanto, El coste de descubrir $K_i$ es:

$$C = min\ C(n),\ 1 \leq n \leq 48$$

donde *C(n),* el coste del proceso cuando se usa *A* para encontrar n bits y el resto se descubren mediante búsqueda exhaustiva, es:

$$C(n) = y(n) + (2^{48-n} \bullet x)$$

Si *C* es mayor que el coste de la busqueda exhaustiva ($2^{48}$) habremos frustrado un ataque mediante criptoanálisis diferencial a nuestro sistema. Si atendemos a cuestiones de eficiencia, el resultado es que la velocidad de nuestro sistema se verá afectada por un factor polinomial mientras que la complejidad para romperlo se verá afectada por un factor exponencial.

### *4.2. Un ejemplo: NPDES Logarítmico.*

Como ejemplo, basándonos en la dificultad de cálculo de logaritmos en un campo finito G(q) con un nº primo de elementos trabajando módulo q. podemos obtener un sistema NPDES en el cual $f_{in}$ se calcula del siguiente modo:

$$f_{in} = L(E_{out}, K_i) = (\alpha^{E_{out} \oplus \beta^{K_i} \bmod q}) \bmod q$$

donde $\alpha$ y $\beta$ son elemetos primitivos de G(q). En este caso:

$$K_i = log_{\beta}(E_{out} \oplus log_{\alpha} f_{in}) \qquad (1)$$

Si *q* es un nº primo cercano a $2^{48}$ (tamaño de la subclave), la complejidad del proceso de calcular su logaritmo es de $\approx q^{1/2} \approx 2^{24}$. Dado que la fórmula anterior requiere el cálculo de dos logaritmos la complejidad de resolverla es de $\approx 2 \bullet q^{1/2} \approx 2 \bullet 2^{24} \approx 2^{25}$. Por tanto, si hemos averiguado *n* bits de $f_{in}$ con un coste *y(n)* deberemos resolver la ecuación (1) $2^{48-n}$ veces, con un coste cada vez de $\approx 2^{25}$. Por consiguiente, el coste total del criptoanálisis será de $y(n) + 2^{73-n}$, que probablemente será mayor que $2^{48}$.

Este sistema se basa en evitar el conocimiento de la subclave a partir de la $f_{in}$ pero al mismo tiempo evita que se conozca la XOR de las $f_{in}$ a partir de las $E_{out}$ que son conocidas. La siguiente figura (en la que hemos dividido la función L en dos potencias $L_1$ y $L_2$) muestra como se consigue esto:

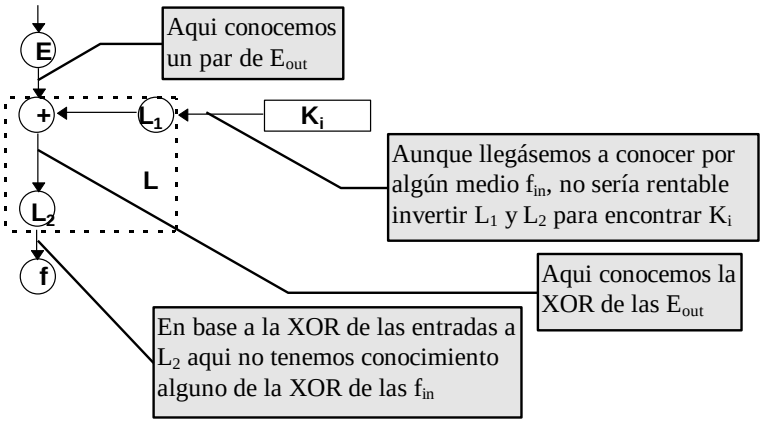


**Fig. 7. Propagación de la información en el NPDES Logarítmico.**

La velocidad del sistema, por otra parte, no se ve afectada negativamente en demasía, ya que el cálculo de cada potencia requiere un máximo de $2 \bullet \log_2 q$ [14] operaciones, lo cual supone (puesto que calculamos dos potencias) menos de $2 \bullet 2 \bullet 48$ operaciones en nuestro caso. Por tanto, el aumento de la complejidad de cifrado es pequeño comparado al aumento de la seguridad.

### *4.3. Un segundo ejemplo: Hash NPDES.*

Utilizaremos una función irreversible para transformar un valor de 96 bits (la concatenación de $K_i$ y $E_{out}$) en $f_{in}$, un valor de 48 bits.

$$H : G(2^{96}) \rightarrow G(2^{48})$$

Muchas funciones hash pueden ser adecuadas, siempre que produzcan salidas pseudoaleatorias. Como se ha mencionado anteriormente, no hay necesidad de que sea completamente imposible invertir la función. Basta con que sea computacionalmente costoso. Dos posibles funciones a usar son :

A. Basándonos de nuevo en la dificultad de calcular logaritmos discretos podemos obtener:

$$H(m) = \alpha^{m} \bmod q$$

donde *m* es la concatenación de $K_i$ y $E_{out;}$ *q* es un número primo cercano a $2^{48}$, y $\alpha$ es un elemento primitivo de $G(2^{96})$, $\alpha \in G(2^{48})$.

B. Una variante de la función hash del compilador de C de P. J. Weinberger [15] que posea el rango y el dominio mencionados.

### *4.4. Respecto a la implementación.*

Al ser DES un sistema diseñado originalmente para implementarse en circuitos digitales, todas las operaciones son operaciones binarias básicas. Nuestra variante, NPDES, y en particular el ejemplo propuesto puede asimismo implementarse mediante software o hardware, en este segundo caso podemos trabajar más eficientemente en $G(2^{48})$ en vez de G(q).

### *4.5. El ataque a nuestro sistema.*

La función base de NPDES contiene dos elementos: la función L y las cajas-S, que proporcionan la seguridad y se complementan. No obstante el sistema no es seguro *per se* y puede ser vulnerable si la función L o sus parámetros no se escogen cuidadosamente.

En el ejemplo propuesto se produce una reducción del espacio de claves válidas. Esta reducción del espacio de claves puede llegar a ser importante si q no es muy cercano a $2^{48}$ (aunque también es posible trabajar en $G(2^{48})$ como se indica en el apartado siguiente) . Además es necesario que $\alpha$ y $\beta$ sean elemetos primitivos de G(q) y que ni la factorización de $\alpha$-1 ni la de $\beta$-1 contengan únicamente factores primos pequeños [16]. Es importante que los exponentes sean números grandes ya que, de otro modo, es fácil calcular el logaritmo [17]. Es por ello que se ha escogido un orden de las operaciones que no permite a un criptoanalista forzar la aparición de exponentes pequeños.

Al igual que en la primera aproximación en la que incluíamos una función irreversible antes de la función f, en este caso podemos dividir la función L en dos funciones $L_1$ y $L_2$ y podemos considerar que hemos definido una nueva función $f'(x)=f(L_2(x))$ de forma que podríamos aplicar el criptoanálisis diferencial a esta nueva función f'. Por otra parte, la subclave original se transforma mediante la función $L_1$ en una nueva subclave $K'_i$ que, si el criptoanálisis diferencial de la función f' tiene éxito, será parcialmente descubierta. Supongamos que esta es la situación, en tal caso un ataque que trate de descubrir la subclave $K_i$ debería invertir $L_1$, con un coste adicional que haría poco eficiente el criptoanálisis, pero tambien sería posible diseñar una versión en la que las $K_i$ no sufriesen transformación alguna y utilizarla para cifrar textos con la $K'_i$ descubierta. La consecuencia inmediata de esto consiste en que tal sistema sería equivalente a un sistema de subclaves independientes, al cual el criptoanálisis diferencial tal como aparece en [4] no puede ser aplicado.

La figura siguiente muestra la descomposición conceptual de la función base del NPDES Logarítmico:

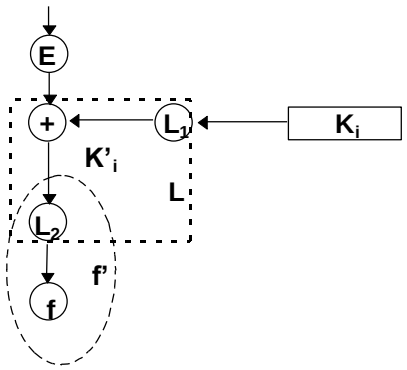


**Fig. 8. Descomposición de la función base del NPDES Logarítmico**

El criptoanálisis diferencial podría ser utilizado directamente si la función L posee una probabilidad diferencial suficientemente alta. No obstante, al tener este análisis un coste adicional las posibilidades de éxito de un ataque tipo diferencial respecto al DES original serían más reducidas.

# 5. Conclusiones y Trabajo Futuro.

Para nosotros la contribución más importante de este trabajo es la de presentar un punto débil de DES sobre el cual puede aumentarse la seguridad. La concepción abstracta o genérica

de NPDES es el centro del mismo. El trabajo muestra dos ejemplos, elegidos con objeto de ilustrar la idea genérica y de mostrar que, incluso en el caso más simple, la eficiencia del criptoanálisis diferencial se ve reducida. Los efectos en otros tipos de ataques están siendo considerados.

Se están implementando varias versiones prácticas de NPDES. Está previsto disponer de resultados en Junio/Julio de 1997. Por último, también se está considerando el efecto de incluir parámetros en la función *L*, lo cual puede incrementar la longitud efectiva de la clave o añadir nuevas capacidades funcionales al sistema.


[1] National Bureau of Standards. *Data Encription Standard*, U.S. Department of Commerce, FIPS pub. 46, January 1977.

[2] Diffie W., Hellman M. E. *A critique of the proposed Data Encription Standard.* Communications of the ACM, v. 19, 1976.

[3] Biham E., Shamir A.. *Differential Cryptanalysis of DES-like Cryptosystems*. Advances in Cryptology Proceedings of Crypto '90. Springer-Verlag. 1991.

[4] Biham E., Shamir A.. *Differential Cryptanalysis of the Full 16-Round DES.* Advances in Cryptology. Proceedings of Crypto '92. Springer-Verlag. 1993

[5] Matsui, M. *Linear Cryptanalysis method for DES cipher.* Advances in Cryptology. Proceedings of Eurocrypt '93. Springer-Verlag. 1993.

[6] Matsui, M. *Linear The First Experimental Cryptanalysis of the Data Encryption Standard.* Advances in Cryptology. Proceedings of Crypto '94. Springer-Verlag. 1994

[7] Coppersmith, D. *The Data Encryption standard and its Strength Against Attacks.* IBM Research Report 18613 (81421). 1992.

[8] Biham E., Shamir A.. *Differential Cryptanalysis of the Data Encription Standard.* Springer-Verlag. 1993.

[9] Nyberg K., Knudsen L. R. *Provable security against Differential Cryptanalysis.* Advances in Cryptology. Proceedings of Crypto '92. Springer-Verlag. 1993.

[10] Pieprzyk. J. *On Bent Permutations.* Technical Report CS91/11. The University of New South Wales.

[11] Adams C.A., Tavares S.E. *The Structured Design of Criptographically Good S-Boxes.* Journal of Cryptology. v. 3 1990.

[12] Adams C. A. *On inmunity against Biham and Shamir's Differential Cryptanalysis.* Information Processing Letters. v 41. 1992.

[13] Sivabalan M., Tavares S. E., Peppard. L. E. *On the design of SP Networks From an Information Theoretic Point of View.* Advances in Cryptology. Proceedings of Crypto '92. Springer-Verlag. 1993.

[14] Knuth D E. *The art of computer programming Vol. 2. Semi-numerical algorithms.* Second Edition. Addison-Wesley. 1981.

[15] Aho A., Setti R., Ullman J. *Compilers. Principles, techniques and tools*. Addison-Wesley. 1986.

[16] Pohlig S. C., Hellman M. E. *An improved algorithm for computing logarithms over GF(p) and its cryptographic significance.* IEEE Trans. Inf. Theory. v. 24. 1978

[17] Van Oorschot P. C., Wiener M. J. *On Diffie-Hellman key agreement with short exponents.* Advances in Cryptology. Proceedings of Eurocryp '96. Springer-Verlag. 1996.