Public Key Encryption #1

Sara Nohemi Zavala (carné No. 18893)
Ricardo Antonio Valenzuela (carné No. 18762)
Jose Amado Garcia (carné No. 181469)
Juan Fernando De Leon Quezada (carné No. 17822)
Edgar Andree Toledo Torres (carné No. 18439)

OAEP

¿Qué es? ¿Cómo se relaciona con RSA?

Es un esquema de relleno que usualmente es utilizado en conjunto con el modelo de encripción RSA. OAEP esencialmente es una red Feistel que utiliza dos Random Oracles, G y H, para procesar el texto sin formato antes del cifrado simétrico.

Al ser implementado junto con RSA se crea un esquema simétricamente seguro ante ataques de texto cifrado elegido y de texto plano elegido

Un Random Oracle es una función matemática elegida aleatoriamente, esto quiere decir que es una función que asigna cada consulta posible a una respuesta aleatoria de su dominio de salida.

¿Cuáles son los beneficios de su correcto uso?

- Utilizado para evitar ataques de texto cifrado elegido y de texto plano elegido.
- Convierte un esquema de cifrado determinista en un esquema probabilístico, ya que agrega aleatoriedad.
- Evita fuga de información y descifrado parcial de textos ya cifrados.
- Se puede construir una transformación de todo o nada, esto quiere decir que para recuperar el mensaje se realizar una recuperación completa.

¿Existen aplicaciones actualmente? ¿Cuáles?

Actualmente no cuenta con muchas implementaciones ya que existen modelos ya más desarrollados, de sus aplicaciones actuales podemos resaltar:

- Es utilizado en la red de anonimato TOR.
- También es utilizado en PKCS#1

OAEP+

¿Qué es? ¿Cómo se relaciona con RSA?

Optimal Asymmetric Encryption Padding (OAEP+) tomar cualquier *trapdoor permutation* y lo convierte en un cifrado de clave pública.

Este se relaciona con RSA, ya que dentro de su proceso utiliza el algoritmo RSA. Esto permite tener una mejor expansión del mensaje.

OAEP+

¿Qué aspecto mejora de la OAEP? ¿Cómo plantea las mejoras?

La diferencia principal es que en OAEP se utiliza dos Random Oracles, G y H, para procesar el texto sin formato antes del cifrado simétrico, mientras que en OAEP+ se agrega un Random Oracle más

Esto nos permite decir que el OAEP+ es seguro contra el ataque de texto cifrado elegido adaptativo.

OAEP+

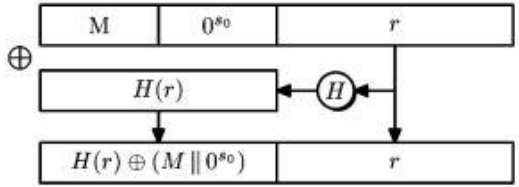
¿Existen aplicaciones actualmente? ¿Cuáles?

En la actualidad se puede encontrar variantes de OAEP+ en sistemas como NTRU. NTRU es un criptosistema de clave pública de código abierto. Este es utilizado para cifrado y firmas digitales.

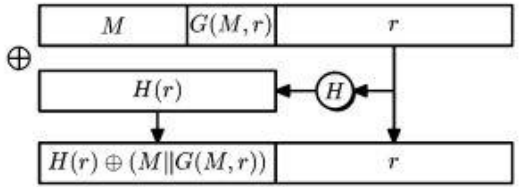
SAEP+

¿Qué es? ¿Cómo se relaciona con RSA?

El relleno de cifrado asimétrico óptimo es una técnica para convertir la permutación de la trampilla RSA en un sistema seguro de texto cifrado elegido en el modelo de oráculo aleatorio.



SAEP padding



SAEP+ padding

Fig. 1. SAEP and SAEP$^+$ padding

¿Cuáles son los beneficios de su correcto uso?

- El Simplificado OAEP puede visto como dos rondas de una red Feistel. Mostramos eso para el Rabin y las funciones de trampilla RSA un esquema de relleno mucho más simple es suficiente para la seguridad del texto cifrado elegido en el modelo de Oracle aleatorio

- Demostramos que solo una ronda de una red Feistel es suficiente. La prueba de seguridad utiliza las propiedades algebraicas de las funciones RSA y Rabin.

¿Existen aplicaciones actualmente? ¿Cuáles?

La principal aplicación es sin duda el famoso RSA – OAEP, que se ha utilizado para actualizar el estándar PKCS # 1 . En su artículo , Shoup pudo reparar el resultado de seguridad para un exponente pequeño, e = 3, utilizando el algoritmo de Coppersmith de . Sin embargo, nuestro resultado se puede aplicar para reparar RSA-OAEP, independientemente del exponente; Gracias a la autorreductibilidad aleatoria de RSA, la dirección unitaria de dominio parcial de RSA es equivalente a la de todo el problema de RSA, tan pronto como una fracción constante de los bits más significativos (o los bits menos significativos) de los la imagen se puede recuperar

Bibliografía

- https://es.qwe.wiki/wiki/Optimal_asymmetric_encryption_padding
- https://eprint.iacr.org/2000/060.pdf
- https://www.math.uni-frankfurt.de/~dmst/teaching/WS2013/Vorlesung/Boneh.OAEP.pdf
- https://crypto.stackexchange.com/questions/59017/whats-the-point-of-oaep
- M. Bellare, P. Rogaway, “Random oracles are practical: a paradigm for designing efficient protocols”, In ACM conference on Computers and Communication Security, pp. 62–73, 1993.
- M. Bellare, P. Rogaway, “Optimal asymmetric encryption”, Eurocrypt ’94, pp. 92–111, 1994.
- M. Bellare, A. Desai, D. Pointcheval, P. Rogaway, “Relations among notions of security for public-key encryption schemes”, in proc. Crypto ’98, pp. 26–45, 1998.
- D. Boneh, R. Venkatesan, “Hardness of computing the most significant bits of secret keys in Diffie-Hellman and related schemes”, in proc. Crypto ’96, pp. 129–142, 1996.