The realm of cryptographic security, particularly concerning RSA encryption, has continually evolved to counteract an array of attack vectors, with chosen ciphertext attacks (CCAs) representing a significant threat.[1] This paper delves into the intricate dynamics of CCAs, focusing on the RSA encryption scheme and the pivotal role of Optimal Asymmetric Encryption Padding (OAEP) in bolstering its defenses. Through a detailed examination of Manger's attack, we unveil the vulnerabilities inherent in RSA-OAEP implementations and propose a comprehensive understanding of the mechanisms at play. The discourse is underpinned by a rigorous mathematical framework and an analytical lens, aiming to bridge the gap between theoretical cryptography and the practical challenges posed by CCAs.[2]

RSA encryption, founded on the RSA algorithm's mathematical principles, has been a bedrock of secure digital communication. However, its deterministic nature has exposed it to various attacks, necessitating the development of padding schemes such as OAEP to enhance security. Despite these advancements, RSA-OAEP is not impervious to attacks, as demonstrated by Manger's CCA, which exploits the decryption oracle's behavior to extract plaintext information from a given ciphertext.[3]

OAEP addresses RSA's vulnerabilities to CCAs by incorporating randomness into the encryption process, thus randomizing ciphertexts and obstructing direct decryption attempts without the private key.[3]

Manger's attack illuminates a critical vulnerability in RSA-OAEP implementations by exploiting the decryption oracle's differential responses to specific decryption failures. The attack's essence lies in its ability to conduct a binary search to deduce the plaintext \(m\) from its corresponding ciphertext \(c\), leveraging the oracle's feedback to refine the search space iteratively.[1]

The attack can be conceptualized through a series of methodical steps, beginning with the initialization of variables and progressing through iterative oracle queries. The binary search algorithm underpinning Manger's attack can be summarized as follows:[4]

1. \*\*Initialization\*\*: Define \(B = 2^{8(k-1)}\) where \(k\) is the bit length of the RSA modulus \(n\). The attacker possesses \(c\), aiming to uncover \(m\).

2. \*\*Oracle Queries\*\*: Generate ciphertexts \(c' = c \cdot (2^e)^i \mod n\) for iterative values of \(i\), observing the oracle's decryption responses.

3. \*\*Binary Search\*\*: Utilize the oracle's feedback to adjust the search range for \(m\), employing a binary search methodology to pinpoint the exact plaintext.

This section delves into the nuanced strategies employed in Manger's attack, dissecting the binary search mechanism and the oracle's role in facilitating the decryption of \(c\) without direct access to the private key.

Manger's attack not only showcases the vulnerabilities within RSA-OAEP but also emphasizes the delicate balance between theoretical security measures and their practical implementations. The findings underscore the necessity for a holistic view of cryptographic security, one that encompasses rigorous implementation testing alongside theoretical robustness.

The exploration of CCAs, particularly through the lens of Manger's attack against RSA-OAEP, highlights the ongoing challenges in cryptographic security. It accentuates the imperative for continuous innovation in cryptographic practices, ensuring they remain resilient against evolving attack methodologies. This study reinforces the dialogue between theoretical cryptography and practical application, advocating for a unified approach to secure digital communication.[2][3][4]

# Reference

|  |
| --- |
| 1. Manger, J. (2001). A Chosen Ciphertext Attack on RSA Optimal Asymmetric Encryption Padding (OAEP) as Standardized in PKCS #1 v2.0. In: Kilian, J. (eds) Advances in Cryptology — CRYPTO 2001. CRYPTO 2001. Lecture Notes in Computer Science, vol 2139. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-44647-8\_14 2. Coron, Jean-Sébastien, et al. "Universal padding schemes for RSA." Advances in Cryptology—CRYPTO 2002: 22nd Annual International Cryptology Conference Santa Barbara, California, USA, August 18–22, 2002 Proceedings 22. Springer Berlin Heidelberg, 2002. 3. Pointcheval, David. "How to encrypt properly with RSA." CryptoBytes 5.1 (2002): 10-19. 4. Kiltz, Eike, Adam O’Neill, and Adam Smith. "Instantiability of RSA-OAEP under chosen-plaintext attack." Journal of Cryptology 30.3 (2017): 889-919. |