La herramienta criptográfica Maude-NPA es un verificador de modelos especializado para protocolos de seguridad criptográficos que tienen en cuenta las propiedades algebraicas de un sistema criptográfico. En la literatura, las propiedades criptográficas adicionales han descubierto debilidades de los protocolos de seguridad y, en otros casos, son parte de los supuestos de seguridad del protocolo para funcionar correctamente. Maude-NPA tiene una base teórica en la rewriting logic, la unificación ecuacional y el narrowing para realizar una búsqueda hacia atrás desde un patrón de estado inseguro para determinar si es alcanzable o no. Maude-NPA se puede utilizar para razonar sobre una amplia gama de propiedades criptográficas, incluida la cancelación del cifra- do y descifrado, la exponenciación de Diffie-Hellman, el exclusive-or y algunas aproximaciones del cifrado homomórfico.

En esta tesis consideramos nuevas propiedades criptográficas, ya sea como parte de protocolos de seguridad o para descubrir nuevos ataques. También hemos modelado diferentes familias de protocolos de seguridad, incluidos los Distance Bounding Protocols or Multi-party key agreement protocolos. Y hemos desarrollado nuevas técnicas de modelado de protocolos para reducir el coste de análisis de espacio y tiempo. Esta tesis contribuye de varias maneras al área de análisis de protocolos criptográficos y muchas de las contribuciones de esta tesis pueden ser útiles para otras herramientas de análisis criptográfico.