Integrale Angriffe auf die PRESENT-Blockchiffre mit praktischer Komplexität

Tuesday 25th March, 2025 - 10:03

Ivaylo Krumov
University of Luxembourg
Email: ivaylo.krumov.001@student.uni.lu

Dieser Bericht wurde unter der Aufsicht von:
Baptiste Lambin
University of Luxembourg
Email: baptiste.lambin@uni.lu

1. Einleitung

Dieses Projekt zielt darauf ab, das Ausmaß inwieweit die PRESENT-Blockchiffre durch kryptoanalytische Angriffe unter Verwendung effizienter mathematischer Techniken angreifbar ist. Um dies herauszufinden, konzentriert sich das Projekt auf den Bereich der integralen Kryptoanalyse.

Dieser Bericht gibt eine gründliche Antwort auf die Frage wie verwundbar eine Blockchiffre, insbesondere die PRESENT Blockchiffre, unter Berücksichtigung praktischer Beschränkungen ist. Um zu bestimmen, wurde eine Handvoll kryptoanalytischer Angriffe Angriffe auf die Blockchiffre durchgeführt, die effiziente mathematische ausnutzen. Zusätzlich liefert ein wissenschaftlicher Text den Kontext für diese Angriffe und für das Thema des Projekts insgesamt. Die in diesem Bericht präsentierten Informationen sollen einen Einblick in die Verwendung mathematischer Werkzeuge zur effiziente Durchführung kryptoanalytischer Angriffe auf Blockchiffren.

2. Projektbeschreibung und Voraussetzungen

Dieses Projekt besteht aus einem wissenschaftlichen und einem technischen Arbeitsergebnis. Das wissenschaftliche Arbeitsergebnis ist ein Text, der versucht, eine Antwort auf die wissenschaftliche Frage ”Wie viele Runden der PRESENT-Blockchiffre können mit integralen Angriffen mit praktischer Komplexität angegriffen werden?” zu geben. Zu diesem Zweck erforscht der Text das Thema der integralen Kryptoanalyse und nutzt die gesammelten Informationen, um die Frage gründlich zu beantworten.

Das technische Arbeitsergebnis nutzt das Gebiet der mixed integer linear programming (MILP), um effiziente integrale Angriffe auf PRESENT durchzuführen. Es wurde vollständig in Python erstellt und nutzt das MILP-Tool Gurobi, während die Programmierumgebung der Wahl Visual Studio Code ist.

Die wichtigste Voraussetzung für die wissenschaftliche Arbeit ist die Fähigkeit, wissenschaftliche Texte kompetent zu schreiben. Die wichtigsten technischen Voraussetzungen sind allgemeine Erfahrung mit der Programmierung in mehreren Programmiersprachen und angemessene Kenntnisse der Programmierung in Python.

3. Wissenschaftliches Arbeitsergebnis - Wie viele Runden der PRESENT-Blockchiffre können mit integralen Angriffen mit praktischer Komplexität angegriffen werden?

3.1. Anforderungen und Gestaltung

Die wichtigsten funktionalen Anforderungen an das wissenschaftliche Arbeitsergebnis sind die gründliche Beantwortung der wissenschaftlichen Frage durch Analyse der Schlüsselbegriffe und deren korrekte Definition zum besseren Verständnis des Themas, die Verwendung anderer wissenschaftlicher Quellen zur Unterstützung bestimmter Ideen des wissenschaftlichen Arbeitsergebnisses und schließlich die Kombination aller gewonnenen Informationen zur Formulierung einer kohärenten Antwort auf die wissenschaftliche Frage. Was die nicht-funktionalen Anforderungen betrifft, so wird erwartet, dass das Arbeitsprodukt leicht zu verstehen ist, einen guten logischen Fluss hat und referenziertes Material korrekt zitiert.

Das wissenschaftliche Arbeitsergebnis ist als Text gestaltet, der den Kontext zu den wissenschaftlichen Ideen hinter dem erstellten technischen Arbeitsergebnis liefert. Es stützt sich auf glaubwürdige wissenschaftliche Quellen mit nützlichen Informationen, um seine Ideen zu untermauern. Das wissenschaftliche Arbeitsergebnis lässt sich logisch in zwei Teile gliedern, wobei der erste Teil die Schlüsselbegriffe im Zusammenhang mit der wissenschaftlichen Frage analysiert und der zweite Teil die Antwort auf die Frage liefert.

3.2. Produktion und Bewertung

Das wissenschaftliche Arbeitsergebnis beschreibt verschiedene Begriffe und Konzepte im Zusammenhang mit der wissenschaftlichen Fragestellung. Insbesondere enthält er eine Definition der Begriffe Blockchiffre, integraler Angriff, Unterscheidungsmerkmal und Teilungsmerkmal. Außerdem wird die Funktionsweise der PRESENT-Blockchiffre eingehend erläutert. Am Ende kommt der Text zu dem Schluss, dass mindestens 5 Runden von PRESENT mit Sicherheit innerhalb einer praktischen Zeitspanne angegriffen werden können, und kündigt an, dass das technische Arbeitsergebnis bestimmen wird, wie hoch diese Zahl sein kann.

Insgesamt legt das wissenschaftliche Arbeitsergebnis die Grundlage für das technische Arbeitsergebnis, indem es die definierten Anforderungen erfüllt und die erwarteten Ergebnisse liefert, so dass davon ausgegangen werden kann, dass es seine Ziele erfolgreich erreicht hat.

4. Technisches Arbeitsergebnis - Integrale Angriffe auf die PRESENT-Blockchiffre

4.1. Anforderungen und Gestaltung

Das technische Arbeitsergebnis, insbesondere der Satz integraler Angriffe, muss außerdem bestimmte funktionale und nicht-funktionale Anforderungen erfüllen. Zu den funktionalen Anforderungen gehören die Suche nach einem Unterscheidungsmerkmal mit Hilfe von MILP, die Reduzierung der möglichen Schlüssel auf ein Minimum und die Verwendung eines Brute-Force-Ansatzes zur Ermittlung des echten Schlüssels. Zu den nichtfunktionalen Anforderungen gehört, dass so viele Runden von PRESENT wie praktisch möglich angestrebt werden und die wichtigen Ergebnisse bequem im Terminalfenster angezeigt werden.

Das technische Arbeitsergebnis ist in 5 verschiedene Programme unterteilt, die jeweils einem bestimmten Zweck dienen. Außerdem weicht die Implementierung von PRESENT leicht von den ursprünglichen Spezifikationen ab, da ein 64-Bit-Geheimschlüssel anstelle eines 80-Bit-Schlüssels verwendet wird. Schließlich wurde der anfängliche integrale Angriff auf 5 Runden von PRESENT und der endgültige Angriff im Rahmen praktischer Beschränkungen auf 7 Runden festgelegt.

4.2. Produktion und Bewertung

Das Arbeitsergebnis besteht aus 5 Programmen - der Implementierung von PRESENT, einem Programm für die Suche nach einem Unterscheidungsmerkmal für eine bestimmte Anzahl von Runden unter Verwendung des MILP-Tools Gurobi und 3 integralen Angriffen - jeweils einer für 5, 6 und 7 Runden. Der Erfolg jedes der integralen Angriffe hängt von dem Unterscheidungsmerkmal ab, das für jeden von ihnen gefunden wird. Sobald für jeden Angriff ein geeigneter Distinguisher identifiziert ist, wird er verwendet, um alle Kandidaten für den richtigen Schlüssel zu erhalten, gefolgt von einem Brute-Force-Algorithmus, der den Schlüsselplan der Blockchiffre umkehrt, um herauszufinden, welcher Kandidat in der Lage ist, eine Nachricht zu verschlüsseln und den erwarteten Chiffretext zu erzeugen. Der Schlüsselkandidat, dem dies gelingt, ist der richtige Schlüssel, er wurde also gefunden.

Insgesamt erfüllt das technische Arbeitsergebnis seine Anforderungen und schafft es einwandfrei, eine konkrete Antwort auf die zuvor definierte wissenschaftliche Frage zu geben. Sie kann daher als Erfolg gewertet werden.

5. Schlussfolgerung

Im Großen und Ganzen hat das Projekt seine Ziele erreicht. Es ist gelungen, die Widerstandsfähigkeit von PRESENT gegen ausgeklügelte integrale Angriffe zu testen und einen Einblick in die Verwendung von MILP zur Durchführung solcher Angriffe zu geben.