Tamper Resistance of AES

—

Models, Attacks and Countermeasures

Volker Krummel

27. Dezember 2007

Zusammenfassung

Die Blockchiffre Rijndael wurde im Jahre 2001 vom U.S. amerikanischen National Institute for Standards and Technology (NIST) zum neuen Standard, dem sogenannten Advanced Encryption Standard (AES) ausgewählt. Schon seit dem Beginn des Auswahlprozesses im Jahre 1997 wurde die Sicherheit von Forschern auf der ganzen Welt im Hinblick auf verschiedene Aspekte untersucht.

In dieser Dissertation analysieren wir die Sicherheit von AES gegen sogenannte Manipulationsangriffe bzw. Seitenangriffe, eine der größten Bedrohungen für kryptographische Algorithmen. Im ersten Teil stellen wir ein allgemeines aber dennoch starkes Sicherheitsmodell zur Analyse der Sicherheit kryptographischer Algorithmen bezüglich Seitenangriffen vor. In diesem Modell nehmen wir an, daß ein Angreifer in der Lage ist, die Werte einiger Zwischenergebnisse von AES-Verschlüsselungen mit einem festen Schlüssel zu erhalten. Ein Algorithmus wird sicher genannt, falls diese Werte keinerlei Informationen über den geheimen Schlüssel preisgeben. Ein Algorithmus der in unserem Modell sicher ist, bietet Sicherheit gegenüber den meisten Seitenangriffen. Weiterhin geben wir eine Methode an, mit der jeder Algorithmus über einem endlichen Körper in einen sicheren Algorithmus überführt werden kann. Insbesondere geben wir einen Algorithmus an, der sichere AES-Verschlüsselungen ermöglicht.

Im zweiten Teil analysieren wir eine auf Sicherheits-Smartcards weit verbreitete Gegenmaßnahme, die sogenannte Speicherverschlüsselung. Wir entwickeln eine neue Klasse von Fehlerangriffen die in der Lage sind, den geheimen AES-Schlüssel auch dann zu bestimmen, falls Speicherverschlüsselung eingesetzt wird. Unsere Angriffe benötigen nur eine geringe Anzahl an Fehlern und zeigen damit, daß Speicherverschlüsselung keine effektive Gegenmaßnahme ist, Seitenangriffe zu vereiteln.

Im letzten Teil analysieren wir eine spezielle Art von Seitenangriffen, die sogenannten cache-basierten Angriffe (CBA). In einem CBA kann ein Angreifer Informationen über das Cache-Verhalten von AES-Verschlüsselungen erhalten und damit Rückschlüsse auf den geheimen Schlüssel ziehen. Wir zeigen, daß zufällige Permutationen, wie in der Literatur vorgeschlagen, keine effektive Gegenmaßnahme gegen CBAs darstellen. Wir stellen eine Verbesserung dieser Gegenmaßnahme vor, indem wir eine neuer Klasse von Permutationen einführen, die sogenannten "ausgezeichneten Permutationen". Ausgezeichnete Permutationen können Teile des geheimen Schlüssels beweisbar schützen. Wir analysieren auch die Sicherheit von verschiedenen Algorithmen für AES-Verschlüsselungen gegen CBAs. Wir entwickeln neue Algorithmen, die eine größere Sicherheit gegen CBAs bieten.