Diss. ETH No. 13076

On the Validity of Certain Hypotheses Used in Linear Cryptanalysis

A dissertation submitted to the
SWISS FEDERAL INSTITUTE OF TECHNOLOGY
ZURICH

for the degree of
Doctor of Technical Sciences

presented by
ZSOLT KUKORELLY
dipl. Math. ETH
born April 23, 1970
citizen of Thônex GE

accepted on the recommendation of
Prof. Dr. James L. Massey, examiner
Prof. Dr. Ueli Maurer, co-examiner

1999

Abstract

Linear cryptanalysis and its generalisations are possible ways to attack an iterated block cipher. Their success relies on a certain number of assumptions made by the attacker. In this thesis, the validity of some of these assumptions is investigated.

According to Matsui's Piling-up Lemma, the imbalance of a sum of independent binary random variables is equal to the product of the imbalances of these random variables. One uses this fact in linear cryptanalysis to compute a lower bound on the probability of success of one's attack. It is shown that, on average, the imbalance of the sum is at least as large as the product of the imbalances and that for large sample spaces, both expressions are almost always approximately equal. It is deduced that, at least as an approximation, the Piling-up Lemma is applicable in a linear cryptanalysis attack to linked threefold sums even if they are not independent.

The validity of the hypothesis of fixed-key equivalence is investigated. The hypothesis asserts that for any effective input/output sum (I/O sum) virtually all key-dependent imbalances are approximately equal to their average, the average-key imbalance of the I/O sum. A counter-example is given. It is further proved that, for one round of encryption, the average and the variance of the key-dependent imbalances are approximately the same for virtually all I/O sums. Whether the key-dependent imbalances of an I/O sum can then be considered as "approximately equal" is subjective and therefore no conclusion about it is drawn. Finally, the average, over all I/O sums, of the average-key imbalances is computed for any number of rounds. Based on this result, a new quantitative definition of effective I/O sums is given.

The validity of the piling-up hypothesis is studied. This hypothesis is an m-ary analogue to Matsui's Piling-up Lemma. It says that (for certain imbalance measures) the imbalance of a product of independent m-ary random variables is in virtually all cases approximately equal to

the product of the imbalances of these random variables. The family of all imbalance measures that are convex-$\cup$ on the set of m-ary probability distributions, equal to 1 for a constant random variable and equal to 0 for a uniformly distributed random variable, is considered. It is argued that they are all equally appropriate for measuring the goodness of an expression used in the group generalisation of linear cryptanalysis attack. For the measure I_2^2, which belongs to this family, it is shown that the imbalance of a product of two random variables is on average equal to the product of the imbalances of the two random variables. It is inferred that the piling-up hypothesis holds for two random variables when m is large enough. By induction, it is shown that the hypothesis also holds for any number of random variables when m is large enough. Finally, it is argued that I_2^2 is an appropriate imbalance measure to use in the group generalisation of linear cryptanalysis.

Keywords. Iterated block cipher, linear cryptanalysis, imbalance, Piling-up Lemma, hypothesis of fixed-key equivalence, piling-up hypothesis.

Zusammenfassung

Die lineare Kryptoanalyse und ihre Verallgemeinerungen sind mögliche Methoden, um ein iteriertes Blockverschlüsselungsverfahren anzugreifen. Ihr Erfolg basiert auf einer Anzahl Annahmen, welche vom Angreifer (Kryptoanalysten) gemacht werden. In dieser Doktorarbeit wird die Gültigkeit einiger dieser Annahmen untersucht.

Nach Matsuis Auftürmlemma (Piling-up Lemma) ist die Unausgeglichenheit einer Summe von binären, unabhängigen Zufallsvariablen gleich dem Produkt der einzelnen Unausgeglichenheiten dieser Zufallsvariablen. Diese Tatsache kann in der linearen Kryptoanalyse benutzt werden, um eine untere Schranke der Erfolgswahrscheinlichkeit eines Angriffs zu berechnen. Für allgemeine Zufallsvariablen wird gezeigt, dass im Durchschnitt die Unausgeglichenheit der Summe mindestens so gross ist wie das Produkt der Unausgeglichenheiten, sowie dass für grosse Ergebnisräume beide Ausdrücke in der Regel gut übereinstimmen. Daraus wird geschlossen, dass in einem Angriff mit linearer Kryptoanalyse das Auftürmlemma auf zusammengekettete Dreifachsummen als Approximation anwendbar ist, selbst wenn diese Dreifachsummen nicht unabhängig sind.

Die Gültigkeit der Hypothese der Gleichartigkeit fester Schlüssel (hypothesis of fixed-key equivalence) wird erforscht. Die Hypothese behauptet, dass für jede wirksame Eingangs-/Ausgangssumme (E/A-Summe) die schlüsselabhängigen Unausgeglichenheiten fast alle ungefähr gleich ihrem Durchschnitt, der mittleren Unausgeglichenheit der E/A-Summe sind. Dazu wird ein Gegenbeispiel gegeben. Des weiteren wird gezeigt, dass für eine Verschlüsselungsrunde der Durchschnitt und die Varianz der schlüsselabhängigen Unausgeglichenheiten für fast alle E/A Summen beinahe gleich sind. Ob man die schlüsselabhängigen Unausgeglichenheiten einer E/A Summe dann als "ungefähr gleich" betrachten darf, ist subjektiv; aus diesem Grund wird auf einen solchen Schluss verzichtet. Schliesslich wird der Durchschnitt der mittleren Unausgeglichenheiten über alle E/A-Summen für eine beliebige Anzahl

von Runden berechnet. Beruhend auf diesem Resultat wird eine neue quantitative Definition einer wirksamen E/A-Summe gegeben.

Die Gültigkeit der Auftürmhypothese (piling-up hypothesis) wird studiert. Diese Hypothese ist ein Analogon zu Matsuis Auftürmlemma im m-wertigen Fall. Sie besagt, dass (für gewisse Unausgeglichenheitsmaße) die Unausgeglichenheit eines Produktes von m-wertigen, unabhängigen Zufallsvariablen in praktisch allen Fällen ungefähr gleich dem Produkt der Unausgeglichenheiten dieser Zufallsvariablen ist. Die Familie der Unausgeglichenheitsmaße, welche auf der Menge der m-wertigen Wahrscheinlichkeitsverteilungen konvex sind, sowie für konstante Zufallsvariablen den Wert 1 und für gleichverteilte Zufallsvariablen den Wert 0 haben, wird betrachtet. Es wird behauptet, dass sie alle für die Messung der Güte eines in einem Angriff mittels der Gruppenverallgemeinerung der linearen Kryptoanalyse gebrauchten Ausdrucks gleich gut sind. Für das Maß I_2^2 aus dieser Familie wird gezeigt, dass die Unausgeglichenheit des Produktes zweier Zufallsvariablen im Durchschnitt gleich dem Produkt der Unausgeglichenheiten beider Zufallsvariablen ist. Es wird bewiesen, dass die Auftürmhypothese für zwei Zufallsvariablen gültig ist, falls m groß genug ist. Mittels vollständiger Induktion wird dann gezeigt, dass bei genug großem m die Hypothese auch für eine beliebige Anzahl von Zufallsvariablen gültig ist. Schließlich wird dargelegt, dass I_2^2 in einem Angriff mittels Gruppenverallgemeinerung der linearen Kryptoanalyse ein geeignetes Unausgeglichenheitsmaß ist.

Schlüsselwörter. Iterierte Blockverschlüsselungsverfahren, lineare Kryptoanalyse, Unausgeglichenheit, Auftürmlemma, Hypothese der Gleichartigkeit fester Schlüssel, Auftürmhypothese.