

AES - Eine Analyse der Sicherheit des Rijndael-Algorithmus

Elisabeth.Oswald@iaik.at*



30. Oktober 2002

*Dieser Artikel ist die Übersetzung von „AES - The State of the Art of Rijndael's Security“ der gemeinsam von Elisabeth Oswald, Vincent Rijmen und Joan Daemen geschrieben wurde.

1 Einleitung

Im Oktober 2000 verkündete das US National Institut of Standards and Technology (NIST) die Auswahl des Algorithmus mit dem Namen „Rijndael“ als Advanced Encryption Standard (AES). In diesem Artikel beschreiben wir die wichtigsten Angriffe, die für den Algorithmus Rijndael gefunden werden konnten.

Dieser Artikel beinhaltet keine Beschreibung des Algorithmus Rijndael. Für eine solche verweisen wir den interessierten Leser auf [DR02]. In diesem Artikel bieten wir einen Überblick über die Attacken auf den Algorithmus Rijndael und über Ideen, die potenziell zu neuen Attacken führen könnten. Tabelle 1 gibt vorweg schon einen Überblick über diejenigen Attacken, die rundenreduzierte Versionen des Algorithmus Rijndael brechen können. Unter einer rundenreduzierten Version versteht man eine Version von Rijndael, die weniger Runden als die spezifizierte Anzahl von Runden berechnet. In Tabelle 1 sind die Attacken mit ihren üblichen Namen, dem Publikationsjahr in der zweiten Spalte, den Autoren (bzw. der Referenz auf den Artikel) in der dritten Spalte und der Anzahl der Runden in den letzten Spalten aufgelistet. Zum Beispiel bricht eine Attacke basierend auf dem Konzept der „Impossible Differentials“ 6 von 10 Runden des Rijndael Algorithmus mit einer Schlüssellänge von 128 Bits.

Attacke	Jahr	Autor	AES-128 10 Runden	AES-192 12 Runden	AES-256 14 Runden
Impossible Differential	2001	[CKK ⁺ 01]	6 Runden		
Square Attacks	2000	[Luc00]		7 Runden	7 Runden
	2000	[FKL ⁺ 00]	7 Runden	7 Runden	9 Runden
Collision Attack	2000	[GM00]	7 Runden	7 Runden	7 Runden

Tabelle 1: Shortcut Attacken auf rundenreduzierte Versionen von Rijndael

Wie man der Tabelle entnehmen kann, waren alle (bis auf die Attacke, die im Jahre 2001 publiziert wurde) dem NIST bereits bekannt, als die Entscheidung zur Auswahl des Algorithmus für den AES getroffen wurde.

Eine Schlussfolgerung die man ziehen kann ist, dass es zur Zeit keine Attacke gibt, die den Rijndael Algorithmus brechen kann. Keine der publizierten Attacken oder Ideen hat zu einer Attacke mit einer geringerer Komplexität als der des vollständigen Durchsuchens des gesamten Schlüsselraumes geführt.

Für eine detailliertere Erläuterung der Attacken und eine Diskussion einiger neuer Ideen laden wir den Leser ein auch den restlichen Teil des Artikels, der wie folgt aufgebaut ist, zu lesen. In Abschnitt 2 erläutern wir die gebräuchlichsten Ausdrücke und Konzepte die in der Kryptoanalyse verwendet werden. In Abschnitt 3 diskutieren wir die bekannten Attacken auf den Rijndael Algorithmus und in Abschnitt 4 behandeln wir die neuen Ideen (algebraischen Methoden) die kürzlich vorgeschlagen wurden und nun diskutiert werden.

2 Kryptoanalyse im Allgemeinen

Exhaustive key search (das vollständige Durchsuchen des Schlüsselraumes) ist die triviale Technik des sequenziellen Ausprobierens aller möglichen Schlüssel bis zum Auffinden des korrekten Schlüssels. Man braucht nur eine geringe Menge an Eingabetexten und deren Chiffraten

um den korrekten Schlüssel zu identifizieren. Wenn der Eingabetext eine bekannte Form von Redundanz aufweist, wie beispielsweise eine ASCII Kodierung, dann genügt auch schon eine geringe Menge vom Chiffretext. Das vollständige Durchsuchen des Schlüsselraumes benötigt keinerlei Information über die Struktur der Chiffre.

Im folgenden Abschnitt behandeln wir Angriffe die solche strukturellen Eigenschaften einer Chiffre ausnützen. Solche Angriffe bezeichnet man üblicherweise als *Kryptoanalyse*. Eine kryptoanalytische Attacke *bricht* eine Chiffre im akademischen Sinn, wenn ihr erwarteter Aufwand geringer ist als der Aufwand des vollständigen Durchsuchens des gesamten Schlüsselraumes. Eine solche Attacke wird im Englischen auch als *Shortcut-Attacke*¹ bezeichnet. Das vollständige Durchsuchen des Schlüsselraumes braucht also nur wenige Eingabetext-Chiffretext Paare. Die meisten Shortcut-Attacken jedoch brauchen eine wesentlich größere Menge an Eingabetext-Chiffretext Paaren. Shortcut-Attacken mit dieser Anforderung werden als *known plaintext* (bekannter Eingabetext) Attacken bezeichnet. Andere Attacken benötigen Chiffretexte zu ausgewählten Eingabetexten. Solche Attacken werden dann als *chosen-plaintext* Attacken bezeichnet. In sogenannten *related-key* Attacken, muss der Angreifer in der Lage sein, ausgewählte Eingabetexte mit verschiedenen (unbekannten) Schlüsseln, die gewissen Beziehungen genügen, zu verschlüsseln.

Trotzdem ist das Nichtvorhandensein von Shortcut-Attacken ein wichtiges Qualitätskriterium und ist in der wissenschaftlichen Gemeinschaft akzeptiert. Tatsächlich war dieses Kriterium das ausschlaggebende Kriterium im AES Auswahlverfahren.

Für viele moderne Chiffren sind bis dato keine Shortcut-Attacken bekannt. Trotzdem kann man die Resistenz von Chiffren gegenüber einer speziellen kryptoanalytischen Methode testen, indem man diese Methode nur auf eine rundenreduzierte Version der Chiffre einsetzt. Solche Attacken auf rundenreduzierte Versionen erlauben es Rückschlüsse auf den sogenannten *security margin* der Chiffre zu ziehen. Existiert für eine Chiffre mit R Runden eine Shortcut-Attacke gegen eine rundenreduzierte Version mit $R - r$ Runden, dann hat die Chiffre einen absoluten security margin von r Runden, oder einen relativen security margin von r/R Runden. Das bedeutet aber nicht dass eine Chiffre für die es eine Shortcut-Attacke auf $R/2$ Runden gibt, zur Hälfte gebrochen ist. Es ist hingegen so, dass die Komplexität der bekannten Attacken **exponentiell** mit der Anzahl der Runden ansteigt.

3 Kryptoanalyse von Rijndael

3.1 Differentielle und lineare Kryptoanalyse

Die heutzutage wirksamsten und allgemein anwendbaren Angriffe auf symmetrische Chiffren sind die differentielle und lineare Kryptoanalyse. Die Berechnung von unteren Schranken für die Komplexität dieser beider Attacken war das wichtigste Kriterium im Design von Rijndael.

Für den Algorithmus Rijndael konnten eine obere Schranke von 2^{-150} für die Wahrscheinlichkeit eines über 4 Runden gehenden differentiellen Trails, und eine Wahrscheinlichkeit von 2^{-75} für die Korrelation eines über 4 Runden gehenden linearen Trails, bewiesen werden. Gemeinsam mit der Anzahl der Runden in Rijndael, bieten diese Schranken eine hohe Sicherheit gegen differentielle und lineare Attacken. Für eine genauere Beschreibung dieser Attacken und der Entwurfsstrategie von Rijndael verweisen wir den Leser auf [DR02].

¹Begriffe, für die es keine sinnvolle deutsche Analogie gibt, übersetzen wir in diesem Artikel nicht.

3.2 Varianten

Nach ihrer Publikation wurden lineare und differentielle Attacken erweitert, und neue, an sie angelehnte Attacken publiziert. Die effizienteste bekannte Erweiterung wird als *truncated differential attack* (abgeschnittene differentielle Attacke) bezeichnet, und wurde bereits in den Entwurf von Rijndael miteinbezogen (siehe [DR02]). Andere Attacken benutzen die Eigenschaften der Fortpflanzung von Eingabedifferenzen und der Korrelation verschiedener Bits auf eine andere Art und Weise.

Impossible Differentials. Die Attacke, basierend auf impossible differentials (unmöglichen Differenzen), bricht 5 von 10 Runden von Rijndael definiert für 128 Bits, mit $2^{29.5}$ ausgesuchten Eingabetexten [BK00], 2^{31} Verschlüsselungen, 2^{42} Bytes Speicher und 2^{26} Zeit für Vorberechnungen. Diese Attacke wurde in [CKK⁺01] verbessert und bricht nun 6 von 10 Runden.

Square attacks. Die stärkste Attacke auf den Rijndael Algorithmus ist zur Zeit die *square Attack* (Quadratattacke). Sie benutzt ausgewählte Eingabetexte und benutzt die Byte orientierte Struktur von Rijndael. Prinzipiell kann diese Attacke auf jede Chiffre angewendet werden deren Struktur ähnlich zu Rijndael ist. Die Attacke wurde erstmals in einem Artikel präsentiert, der einen der Vorgänger des Rijndael Algorithmus beschreibt. Dieser Algorithmus trägt den Namen „Square“ und ist somit der Namensgeber für diese Attacke. Es gibt jedoch auch einige andere Namen für ein und dieselbe Attacke (und ihrer Variationen). Zum Beispiel den Namen „saturation attack“ (Sättigungsattacke), vorgeschlagen von Lucks in [Luc00]. Seine Variante bricht 7 Runden von 12 bzw. 14 Runden von Rijndael definiert für 192 und 256-bit Schlüssel (d. h. AES-192 und AES-256). Oder der Name „integral cryptanalysis“ vorgeschlagen von Knudsen und Wagner [KW02] und der Name „structural attacks“ vorgeschlagen von Biryukov und Shamir [BS01]. Keiner der beiden letztgenannten Artikel beschäftigt sich mit dem Rijndael Algorithmus.

Die ursprüngliche Quadratattacke kann eine rundenreduzierte Version von Rijndael bis zu 7 Runden (für Rijndael definiert für eine 128-bit Schlüssel) brechen. Ferguson et al. [FKL⁺00] schlugen einige Optimierungen für diese Attacke vor. Mit diesen Verbesserungen kann man 9 Runden (von 14) von Rijndael definiert für 256-bit Schlüsseln brechen. Dies erfordert dann 2^{77} Eingabetexte, 256 Schlüssel die in einer speziellen Beziehung stehen, und 2^{224} Verschlüsselungen.

Collision Attacks. Diese Attacke wurde von Gilbert und Minier in [GM00] präsentiert und ist im Prinzip die stärkste Attacke, die es momentan für Rijndael gibt. Sie kann 7 Runden für alle Versionen von Rijndael brechen. Im Fall von Rijndael-128 ist die Attacke aber nur wenig aufwendiger als das vollständige Durchsuchen des Schlüsselraumes.

4 Ideen und Beobachtungen

Während die im vorigen Abschnitt vorgestellten Methoden zu Attacken gegen rundenreduzierten Versionen von Rijndael geführt haben, haben die Methoden die wir in diesem Abschnitt diskutieren bis jetzt zu keiner Attacke gegen Rijndael geführt. Die meisten dieser Ideen werden sogenannten *algebraic attacks* (algebraischen Attacken) zugeordnet und können folgendermassen grob skizziert werden:

1. Sammlungsphase: Der Kryptoanalytiker drückt die Chiffre als Menge *einfacher* Gleichungen in einer bestimmten Anzahl von Variablen aus. Diese Variablen beinhalten Bits oder Bytes des Eingabetextes, des Chiffrats und des Schlüssels und typischerweise auch Bits von anderen Berechnungsschritten und Rundenschlüsseln. Die Definition von *einfach* für die Gleichungen kann dabei meist nur sehr ungenau gegeben werden, und heißt meistens *verwendbar für den nächsten Schritt*.
2. Lösungsphase: Der Kryptoanalytiker substituiert Daten wie Eingabetext-Chiffretext Paare für die entsprechenden Variablen der Gleichungen, die er in Phase eins gesammelt hat. Damit versucht er die resultierende Menge von Gleichungen zu lösen und somit den geheimen Schlüssel zu errechnen.

Wegen seiner Entwurfskriterien kann Rijndael *elegant* in Gleichungsform dargestellt werden. Der wichtige Aspekt jedoch ist: Sind Gleichungssysteme, die für einen Mathematiker *elegant* aussehen auch *einfach* lösbar? Vielerlei Versuche wurden bis dato gestartet um algebraische Attacken für Rijndael zu entwerfen. Bis dato waren aber alle diese Attacken erfolglos, d.h. sie haben zu keinerlei Shortcut-Attacke auf Rijndael geführt. In den folgenden Paragraphen diskutieren wir einige dieser Versuche.

Continued fractions. Ferguson, Schroepel und Whiting [FSW01] beschreiben Rijndael in einer geschlossenen Form, welche als eine Art von Kettenbruch angesehen werden kann. Jedes Byte eines Zwischenergebnisses nach fünf Runden kann wie folgt ausgedrückt werden:

$$x = K + \sum \frac{C_1}{K^* + \sum \frac{C_2}{K^* + \sum \frac{C_3}{K^* + \sum \frac{C_4}{K^* + \sum \frac{C_5}{K^* + p^*}}}}} \quad (1)$$

In dieser Formel ist jedes K ein Key-Byte, jedes C_i eine bekannte Konstante und jedes $*$ ein bekannter Exponent oder Index. Jeder dieser Werte hängt allerdings von den Summationsvariablen ab, die das Summensymbol umschließen. Eine ausmultiplizierte Version von (1) hat 2^{25} Terme. Um eine 10-Runden Version von Rijndael (d.h. AES-128) zu brechen, würde ein Kryptoanalytiker zwei solcher Gleichungen benutzen. Eine davon beschreibt die Zwischenvariablen nach fünf Runden als Funktion des Eingabetextes, während die andere Gleichung die Runden sechs bis zehn als Funktion des Chiffretextes beschreibt. Eine Kombination beider Gleichungen resultiert somit in eine Gleichung mit 2^{26} Unbekannten. Eine wiederholte Anwendung dieser Gleichung für alle $2^{26}/16$ bekannten Eingabetext-Chiffretext Paare würde im informationstheoretischen Sinn genügend Informationen für alle Variablen beinhalten. Allerdings ist keinerlei Lösungsmethode für Gleichungen dieser Gestalt bekannt.

XSL. Courtois und Pieprzyk [CP02a] bemerken, dass die S-box von Rijndael durch eine Anzahl von impliziten quadratischen booleschen Gleichungen beschrieben werden kann. Bezeichnet man die Eingabebits mit x_1, \dots, x_8 , und die Chiffrebits mit y_1, \dots, y_8 , dann gibt es Gleichungen der Form

$$f(x_1, \dots, x_8, y_1, \dots, y_8) = 0, \quad (2)$$

wobei der algebraische Grad von f gleich zwei ist.

Prinzipiell genügen acht Gleichungen dieses Typs um die S-box vollständig zu beschreiben. Courtois und Pieprzyk aber beobachten, dass es mehr Gleichungen dieses Typs für die S-box

gibt. Zusätzlich behaupten sie, dass diese zusätzlichen Gleichungen die Komplexität in der Lösungsphase reduzieren. Diese Behauptung impliziert, dass für spezielle Instanzen des normalerweise NP-harten Problems des Lösens multivariater quadratischer Gleichungen (kurz das MQ-Problem), ein Algorithmus existiert welcher dieses Problem in sub-exponentieller Zeit löst. Aber einige Wissenschaftler zweifeln die Korrektheit der Abschätzungen von Courtois und Pieprzyk an. Zum Beispiel sagt Don Coppersmith² in [Cop02b]: „I believe that the Courtois-Pieprzyk work is flawed. They overcount the number of linearly independent equations. The result is that they do not in fact have enough linear equations“. Zusätzlich fügt er noch in einem Brief der in [Cop02a] abgedruckt ist hinzu: „The method has some merits, and is worth investigating, but it does not break Rijndael as it stands“. Auch T. Moh³ zweifelt die Korrektheit der Ergebnisse an [Moh02]. Lässt man all die berechtigten Zweifel beiseite und nimmt man an dass all die Abschätzungen korrekt sind, dann ist die Komplexität der Attacke im optimistischen Fall 2^{255} . Dies gilt unter bestimmten Annahmen für Parameter der Attacke, welche in Abschnitt 8.1 des Artikels [CP02a] gefunden werden können. Das bedeutet, dass diese Attacke nur Rijndael mit 256-bit Schlüssel brechen kann, da für kürzere Schlüssel das vollständige Durchsuchen des gesamten Schlüsselraumes eine geringere Komplexität als die Attacke hat. Man weiss auch nicht welche Eigenschaften von Rijndael, oder einer beliebigen anderen Blockchiffre, die Komplexität der Attacke beeinflussen.

Embedding. Murphy und Robshaw [MR02] definieren die Blockchiffre BES, welche anstatt auf Datenbits auf Datenblöcke von 128 bytes arbeitet. Nach den Aussagen von Murphy und Robshaw, ist die algebraische Struktur von BES noch eleganter und einfacher als die von Rijndael. Zusätzlich kann Rijndael in BES *eingebettet* werden. Mathematisch gesehen bedeutet das, dass es ein Abbildung ϕ gibt, sodass:

$$Rijndael_K(x) = \phi^{-1} \left(BES_{\phi(K)}(\phi(x)) \right). \quad (3)$$

In dieser Gleichung bezeichnet K den Schlüssel und x den Eingabetext. Murphy und Robshaw machen dann einige Beobachtungen für den BES, die sich aber nicht auf Rijndael übertragen lassen können.

Murphy und Robshaw merken in ihrem Artikel an, dass die Anwendung der XSL-Methode auf BES zu einer Verminderung der Komplexität in der Lösungsphase führen könnte.

Dual Cipher. In [BB02] wird das Konzept der dualen Chiffre vorgestellt. Dieses Konzept ist prinzipiell eine Erweiterung des Konzepts der Einbettungstechnik. Das bedeutet, nimmt man umkehrbare Abbildungen f, g und h , dann gibt es eine duale Chiffre *DUAL*, sodass:

$$Rijndael_K(x) = f^{-1} DUAL_{g(K)}(h(P)). \quad (4)$$

In dieser Gleichung bezeichnet K den Schlüssel und x den Eingabetext. Diese Gleichung sagt aus, dass die duale Chiffre equivalent zur originale Chiffre ist, in dem Sinn dass sie das selbe Chifftrat für denselben Eingabetext und denselben Schlüssel produziert, indem sie zuerst Abbildungen auf den Eingabetext, den Schlüssel und dann dem Chifftrat anwendet. Daraus folgt, dass man die duale Chiffre anstatt der originalen Chiffre implementieren und

²Er erhielt sein Doktorat in reiner Mathematik, arbeitet für IBM und war Ko-Entwickler des Data Encryption Standard DES.

³Auch er hat sein Doktorat in reiner Mathematik und forscht aktiv auf dem Gebiet der Algebra.

analysieren kann. In [BB02] werden 240 duale Chiffren für Rijndael identifiziert. Es werden keinerlei Schwächen dieser Chiffren berichtet.

Ein ähnliches Konzept, das Rijndael-GF genannt wird, ist in [DR02] definiert. Es wird damit demonstriert, dass alle Chiffren der Rijndael-GF Familie die selbe Resistenz gegenüber differentieller und linearer Kryptoanalyse aufweisen.

5 Konklusion

In diesem Artikel haben wir einen Überblick über die publizierten Attacken und Beobachtungen zum Rijndael Algorithmus gegeben. Zusätzlich haben wir die Ideen diskutiert, die zu neuen Attacken führen könnten. Zur Zeit des Abfassens dieses Artikels sind keine Shortcut-Attacken für den Rijndael Algorithmus bekannt.

Literatur

- [BB02] Elad Barkan and Eli Biham. In how many ways can you write Rijndael? In Yuliang Zheng, editor, *Proceedings of Asiacrypt'02*, Lecture Notes in Computer Science. Springer-Verlag, 2002. Also a NESSIE report.
- [BK00] Eli Biham and Nathan Keller. Cryptanalysis of reduced variants of RIJNDAEL. In *Proceedings of the Third Advanced Encryption Standard Conference*. NIST, April 2000.
- [BS01] Alex Biryukov and Adi Shamir. Structural cryptanalysis of SASAS. In Birgit Pfitzmann, editor, *Proceedings of Eurocrypt'01*, number 2045 in Lecture Notes in Computer Science, pages 394–405. Springer-Verlag, 2001.
- [CKK⁺01] Jung Hee Cheon, MunJu Kim, Kwangjo Kim, Jung-Yeun Lee, and SungWoo Kang. Improved Impossible Differential Cryptanalysis of Rijndael and Crypton. In K. Kim, editor, *Information Security and Cryptology - ICISC 2001*, number 2288 in Lecture Notes in Computer Science, pages 39–49. Springer, 2001.
- [Cop02a] D. Coppersmith. Xsl against rijndael. CRYPTO-GRAM, Oktober 2002.
- [Cop02b] Don Coppersmith. Impact of Courtois and Pieprzyk results. NIST AES Discussion Forum, September 2002. Available from <http://www.nist.gov/aes>.
- [CP02a] Nicolas T. Courtois and Josef Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. In Yuliang Zheng, editor, *Proceedings of Asiacrypt'02*, Lecture Notes in Computer Science. Springer-Verlag, 2002. Different version of the preprint [CP02b].
- [CP02b] Nicolas T. Courtois and Josef Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. IACR eprint server, 2002. Available at <http://eprint.iacr.org/2002/044/>.
- [DKR97] Joan Daemen, Lars Ramkilde Knudsen, and Vincent Rijmen. The block cipher Square. In Eli Biham, editor, *Proceedings of Fast Software Encryption – FSE'97*, number 1267 in Lecture Notes in Computer Science, pages 149–165. Springer-Verlag, 1997.

- [DR02] Joan Daemen and Vincent Rijmen. *The Design of Rijndael*. Information Security and Cryptography. Springer Verlag, 2002.
- [FKL⁺00] N. Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, M. Stay, D. Wagner, David Wagner, and Doug Whiting. Improved cryptanalysis of Rijndael. In Bruce Schneier, editor, *Proceedings of Fast Software Encryption – FSE’00*, number 1978 in Lecture Notes in Computer Science, pages 213–230. Springer-Verlag, 2000.
- [FSW01] Niels Ferguson, Richard Schroepel, and Doug Whiting. A simple algebraic representation of Rijndael. In Serge Vaudenay and Amr M. Youssef, editors, *Proceedings of Selected Areas in Cryptography – SAC’01*, number 2259 in Lecture Notes in Computer Science, pages 103–111. Springer-Verlag, 2001.
- [GM00] Henri Gilbert and Marine Minier. A collision attack on seven rounds of Rijndael. In *Proceedings of the Third Advanced Encryption Standard Conference*, pages 230–241. NIST, April 2000.
- [KW02] Lars Ramkilde Knudsen and David Wagner. Integral cryptanalysis (extended abstract). In Joan Daemen and Vincent Rijmen, editors, *Proceedings of Fast Software Encryption – FSE’02*, number 2365 in Lecture Notes in Computer Science, pages 112–127. Springer-Verlag, 2002.
- [Luc00] Stefan Lucks. Attacking seven rounds of Rijndael under 192-bit and 256-bit keys. In *Proceedings of the Third Advanced Encryption Standard Conference*. NIST, April 2000.
- [Moh02] T. Moh. On the Courtois-Pieprzyk’s attack on Rijndael. University of San Diego Web-Site, September 2002. Available from <http://www.usdsi.com/aes.html>.
- [MR02] Sean Murphy and Matthew J. B. Robshaw. Essential algebraic structure within the AES. In Moti Yung, editor, *Proceedings of Crypto’02*, number 2442 in Lecture Notes in Computer Science, pages 17–38. Springer-Verlag, 2002.