Unforgeable Encryption and Chosen Ciphertext Secure Modes of Operation

Seminararbeit

von

Thomas King

Schramberg

vorgelegt bei

Dr. Stefan Lucks

Juni 2002

Inhaltsverzeichnis

1 Motivation

Die selben Definitionen von Sicherheit werden für die Private-Key Kryptographie und Public-Key Kryptographie verwendet. Dies, obwohl beide Verfahren sehr unterschiedlich sind:

- in der Public-Key Kryptographie ist Verschlüsselung für jeden durchführbar
- Public-Key Kryptographie wird normalerweise für kleine Datenmengen verwendet (z.B. Sessionschlüssel)
- Private-Key Kryptographie wird oft bei grossen Datenmengen verwendet
- Private-Key Kryptographie ist die Basis für viele Authentifikations- und Sicherheitsprotokolle

Aus den oben genannten Gründen wird hier ein höherer Sicherheitsstandard für die Private-Key Kryptographie eingeführt: *encryption unforgeability*. Encryption unforgeability garantiert Sicherheit für:

- Authentifikationsprotokolle
- Nachrichtenintegrität ohne zusätzliche Kryptographie
- manche Chosen Ciphertext Angriffe

Es wird hier eine Betriebsart für Blockchiffren (engl.: mode of operation) präsentiert und analysiert, der die oben genannten Ziele erreicht: *Related Plaintext Chaining*.

2 Unfälschbarkeit (engl.: unforgeability)

Es werden hier drei Arten von Unfälschbarkeit (engl.: unforgeability) für Verschlüsselung definiert. Diese Definitionen beinhaltet die Fälle, in denen der Angreifer versucht:

- den Ciphertext mit einem vorherigen Ciphertext zu erweitern
- zwei Ciphertexte zusammen zuwürfeln
- einen Ciphertextblock aus einem gültigen Ciphertext zu löschen

um einen Ciphertext zu fälschen.

2.1 Unfälschbarkeit bei zufälligem Plaintext (engl.: Random Plaintext Unforgeability)

Ein Plaintext wird zufällig aus dem Plaintext-Raum gewählt. Der Angreifer gewinnt, wenn er einen Ciphertext y angeben kann, der die Verschlüsselung von x ist.
Sei $\Pi = (K, E, D)$ ein Private-Key Schema und A ein Angreifer.

$$Adv^{random}_{A,\Pi} \quad = \quad Pr[sk \leftarrow K; x \leftarrow M; y \leftarrow A^{E_{sk}(\cdot)}(x) : D_{sk}(y) = x]$$

Natürlich darf A nicht das Orakel nach x fragen.

2.2 Unfälschbarkeit bei gewähltem Plaintext (engl.: Chosen Plaintext Unforgeability)

Bei diesem Angriff ist das Ziel des Angreifers einfacher. Der Angreifer gewinnt, wenn er einen Ciphertext zu einem Plaintext ausgeben kann, den er selber gewählt hat. Der Angreifer muss aber den Plaintext zu dem Ciphertext kennen, den er ausgibt.
Sei $\Pi = (K, E, D)$ ein Private-Key Schema und A ein Angreifer.

$$Adv^{chosen}_{A,\Pi} \quad = \quad Pr[sk \leftarrow K; (x, y) \leftarrow A^{E_{sk}(\cdot)} : D_{sk}(y) = x]$$

Natürlich darf A den Ciphertext y nicht von seinem Orakel erhalten haben.

2.3 Existentielle Unfälschbarkeit (engl.: Existential Unforgeability)

Dieser Angriff repräsentiert die stärkste Idee von Unfälschbarkeit (engl.: unforgeability) und ist gleichzeitig der einfachste Angriff für einen Angreifer. Der Angreifer gewinnt, wenn er irgendeinen gültigen Ciphertext erzeugen kann. Dazu muss er den dazugehörigen Plaintext nicht kennen.
Sei $\Pi = (K, E, D)$ ein sicheres private-Key Schema und A ein Angreifer.

$$Adv^{exist}_{A,\Pi} \quad = \quad Pr[sk \leftarrow K; y \leftarrow A^{E_{sk}(\cdot)} : D_{sk}(y) \neq \perp]$$

Wie bei "Unfälschbarkeit bei gewähltem Plaintext" darf der Angreifer den Ciphertext y nicht von einem Orakel erhalten haben.

3 Unfälschbare Betriebsart (engl.: Unforgeable Modes of Operation)

Die Variable crt ist eine r-Bit Zahl. Additionen mit crt sind modulo 2^r.
Der Verschlüsselungsalgorythmus von RPC:

$E - RPC_{n,r}(ctr,\ M)$
  parse M as $M_1, \ldots, M_l$ where $\mid M_i \mid = n - r$
  $C_0 = F_{sk}(start, ctr)$
  for $i = 1, \ldots, l$ do
    $C_i = F_{sk}(M_i, ctr + i)$
  $C_{l+1} = F_{sk}(end, ctr + l + 1)$
  $ctr := ctr + l + 1$
  return $(ctr,\ \mathrm{C} = C_0, \ldots, C_{l+1})$

Der Entschlüsselungsalgorythmus von RPC:

$D - RPC_{n,r}(C)$
  parse C as $C_0, \ldots, C_{l+1}$ where $\mid C_i \mid = n$
  for $i = 0, \ldots, l + 1$ do
    $(M_i, ctr_i) = F_{sk}^{-1}(C_i)$
  if $(M_0 \neq start) \vee (M_{l+1} \neq end)$ **return** $\perp$
  for $i = 1, \ldots, l$ do
    if $ctr_i \neq ctr_0 + i$ **return** $\perp$
    if $(M_i = start) \vee (M_i = end)$ **return** $\perp$
  if $ctr_{l+1} \neq ctr_0 + l + 1$ **return** $\perp$
  return $\mathrm{M} = M_1, \ldots, M_l$

Theorem 1.

Sei Π ein kryptographisches Schema, dass $RPC_{n,r}$ mit einer Blockchiffre verwendet. Dann ist Π sicher im Sinne von existentieller Unfälschbarkeit (engl.: existential forgeability) und es gilt:

$$Adv_{A,\Pi}^{exist} \leq \frac{2^{n-r-1}}{2^n - b - 2q}$$

b gibt die Anzahl der n-Bit Block Anfragen ans Orakel an. q steht für die Anzahl der Anfragen ans Orakel (die *start* und *end* Blöcke können nicht mehr verwendet werden).

Beweisskizze

Es gibt höchstens 2^{n-r-1} Blocke, die verschlüsselt werden können ($n-r$ Datenbits und die Tags *start* und *end*). Weiterhin sind es $2^n - b - 2q$ Ciphertextblöcke, die der Angreifer auswählen kann.

Theorem 2.

Sei Π ein kryptographisches Schema, dass $RPC_{n,r}$ mit einer Blockchiffre verwendet. Dann ist Π sicher im Sinne von IND-P2-C2 und es gilt:

$$Adv_{A,\Pi}^{IND-P2-C2} = \frac{q_d 2^{n-r-1}}{2^n - b_e - 2q_e}$$

Beweisskizze

Der Vorteil eines Angreifers A auf Π im Sinne von IND-P2-C0 ist 0. Anwendung des Hilfs-Theorem (hier ohne Beweis) ergibt den Beweis.

Hilfs-Theorem

Sei Π ein kryptographisches Schema, dass im Sinne von existentieller Unfälschbarkeit (engl.: existential forgeability) ($Adv = \epsilon$) und IND-PX-C0 (für X $\in \{0,1,2\}$) ($Adv = \grave{\epsilon}$) sicher ist. Dann ist Π im Sinne von IND-PX-C2 sicher und es gilt:

$$Adv_{A,\Pi}^{IND-PX-C2} = \epsilon + q_d \grave{\epsilon}$$

Theorem 3.

Sei Π ein kryptographisches Schema, dass $PRC_{n,r}$ mit einer Blockchiffre F verwendet, deren $Adv \leq \epsilon$ ist. Dann ist Π sicher im Sinne von existentieller Unfälschbarkeit (engl.: existential forgeability) und es gilt:

$$Adv_{A,\Pi}^{exit} = \epsilon + \frac{2^{n-r-1}}{2^n - b - 2q}$$

Beweisskizze

A sei ein Angreifer im Sinne von existential forgeability. Wir konstruieren einen Unterscheider D für die Blockchiffre F, der A als Unterfunktion verwendet. D simuliert für A das encryption Orakel (*ctr* Variable verwalten, ...) und gibt den so erhaltenen String an das eigene Orakel f (für F) weiter. Gibt A einen (gefälschten) ciphertext zurück, den D vorher nicht von seinem Orakel erhalten hat, dann übergibt D diesen ciphertext an sein Orakel $f^{(-1)}$. Passt die *ctr* Variable vom ciphertext zu den anderen ciphertext Blöcken (die D kennt), so gibt D 1 aus, sonst 0.

Theorem 4.

Sei Π ein kryptogaphisches Schema, dass $PRC_{n,r}$ mit einer Blockchiffre F verwendet, deren $Adv \leq \epsilon$ ist. Dann ist Π sicher im Sinne von IND-P2-C2 und es gilt:

$$Adv_{A,\Pi}^{IND-P2-C2} \quad = \quad \epsilon + \frac{q_d 2^{n-r-1}}{2^n - b_e - 2q_e}$$

Beweisskizze

Siehe Beweis von Theorem 3.

4 Diskussion

Es wurde gezeigt, dass der RPC einfach ist und kryptographisch leicht zu analysieren. Die Ziele

- zuverlässige Authentifikation - für RPC wird nur ein geheimer Schlüssel benötigt
- Nachrichtenintegrität - durch das spezielle Plaintextformat von RPC
- Sicherheit gegen gewiesse Chosen Ciphertext Angriffe - wurde oben bewiesen

wurden erreicht.
Leider hat RPC auch Nachteile. Der grösste Nachteil ist die Ciphertextexpansion. Um praktikable Sicherheit zu erreichen, sollte man $r \geq 32$ wählen. Somit steigt bei einer 64-Bit Blockchiffre der Ciphertext um über 50%, bei einer 128-Bit Blockchiffre immerhin noch um über 33%. Aber aufgrund der stänidigen Zunahme der Bandbreite und Speicherkapazität dürfte dies leicht zu verkraften sein.

5 Literatur

[1] Jonathan Katz, Moti Yung: *Unforgeable Encryption and Chosen Ciphertext Secure Modes of Operation*

[2] Jonathan Katz, Moti Yung: *Complete Characterization of Security Notions for Probabilistic Private-Key Encryption*