Zur Fehlererkennungsfähigkeit von Random Codes am Beispiel des Message Authentication Code

Dr. Bernd Friedrichs, ANT Nachrichtentechnik GmbH, D-71522 Backnang

Übersicht: Der Message Authentication Code ist ein kryptographisches Verfahren zur Gewährleistung der Integrität und Authentizität, das gleichzeitig auch zur Erkennung stochastischer Fehler eingesetzt werden kann. In der codierungstheoretischen Interpretation resultiert ein systematischer nichtlinearer Random Code zur Fehlererkennung. Für das BSC-Kanalmodell wird die Wahrscheinlichkeit unerkannter Fehler berechnet und mit den informationstheoretischen Grenzen verglichen, wobei lediglich das Shannon'sche Diffusions-Prinzip vorausgesetzt wird.

1 Einführung

Der Message Authentication Code (MAC) ist ein kryptographisches schlüsselgesteuertes Verfahren zur Gewährleistung der *Integrität* (Unversehrtheit) und *Authentizität* (Echtheit bezüglich des Absenders) einer Nachricht, dessen Leistungsfähigkeit bei der Erkennung kryptographischer Manipulationen wohlbekannt ist [3, 10]. Gleichzeitig kann der MAC aber auch zur Erkennung stochastischer Fehler benutzt werden und dies führt auf eine Reihe neuartiger Fragestellungen. Als Anwendungsbeispiel für diese Zwitterrolle des MAC-Verfahrens zwischen Kryptographie und Kanalcodierung wird in [1, 3] ein System zur sicherheitsrelevanten Kommunikation behandelt.

In der codierungstheoretischen Interpretation erweist sich das MAC-Verfahren als ein systematischer, nichtlinearer, parametrisierter Fehlererkennungscode, der aufgrund des kryptographisch motivierten *Shannon'schen Diffusionsprinzips* als ein Code mit zufällig gewählten und näherungsweise binomialverteilten Codewörtern (*Random Code*) interpretiert werden kann. Ziel ist die Bestimmung der Fehlererkennungsfähigkeit, wobei als Kanalmodell der *binäre symmetrische Kanal* (BSC) angenommen wird. Jeder einzelne vom kryptographischen Schlüssel abhängige Fehlererkennungscode ist schwer kontrollierbar, aber die Verteilung und der Mittelwert der Fehlerwahrscheinlichkeit über alle Random Codes sind analytisch berechenbar.

Damit ergibt sich eine Art "Umkehrung" der üblichen Informationstheorie: Beim Beweis des Kanalcodierungstheorems wird der Mittelwert über alle Random Codes durch eine Schranke majorisiert und der übliche Schluß per *Random Coding Argument* ist dann, daß es mindestens einen Code gibt, der so gut ist wie der Mittelwert. Bei der Fragestellung hier interessiert jedoch, wie stark die Codeeigenschaften vom Mittelwert abweichen können, wie schlecht beispielsweise die MAC-Fehlererkennung beim ungünstigsten Schlüssel ist.

2 Prinzip des Message Authentication Code

Mit dem in **Bild 1** dargestellten Prinzip des Message Authentication Code wird die Integrität und Authentizität einer Nachricht gewährleistet. Aus dem binären Informationswort $\boldsymbol{X}$ der Länge k wird im *Authentikator* $A_{\boldsymbol{Z}}$ ein binäres kryptographisches Prüfwort $\boldsymbol{MAC} = A_{\boldsymbol{Z}}(\boldsymbol{X})$ der Länge $n-k$ berechnet. Übertragen wird das Codewort $\boldsymbol{Y} = (\boldsymbol{X}, A_{\boldsymbol{Z}}(\boldsymbol{X})) = (\boldsymbol{X}, \boldsymbol{MAC})$ mit der Länge n.

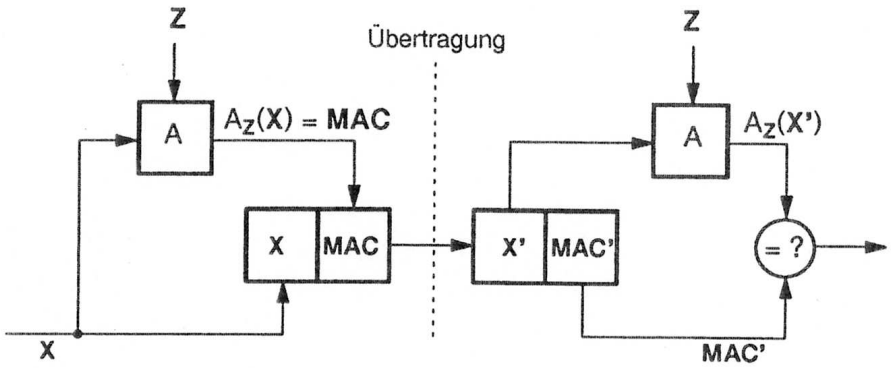

Bild 1: Message Authentication Code (MAC)

Bei der Übertragung wird $\boldsymbol{Y} = (\boldsymbol{X}, \boldsymbol{MAC})$ verfälscht zu $\boldsymbol{Y}' = (\boldsymbol{X}', \boldsymbol{MAC}')$. Im Empfänger ist ebenfalls der Authentikator realisiert. Nur wenn $A_{\boldsymbol{Z}}(\boldsymbol{X}') = \boldsymbol{MAC}'$ festgestellt wird, akzeptiert der Empfänger die Nachricht – anderenfalls wird die Nachricht als ungültig eingestuft und nicht akzeptiert. Der in Sender und Empfänger identische Authentikator ist eine vom Schlüssel $\boldsymbol{Z}$ abhängige deterministische und komplizierte nichtlineare Funktion, die üblicherweise durch den *Cipher Block Chaining Mode* (CBC) eines *Blockverschlüsslers* $E_{\boldsymbol{Z}}$ gebildet wird [1, 10]. Bei einer aus 3 Klartext-Blöcken bestehenden Nachricht $\boldsymbol{X} = (\boldsymbol{X}_1, \boldsymbol{X}_2, \boldsymbol{X}_3)$ gilt beispielsweise:

$$\boldsymbol{MAC} = A_{\boldsymbol{Z}}(\boldsymbol{X}) = E_{\boldsymbol{Z}}(\boldsymbol{X}_3 + E_{\boldsymbol{Z}}(\boldsymbol{X}_2 + E_{\boldsymbol{Z}}(\boldsymbol{X}_1))). \tag{1}$$

Zur Blockverschlüsselung $E_{\boldsymbol{Z}}$ können beispielsweise die Standards DES (Data Encryption Standard [10]) oder IDEA (International Data Encryption Algorithm [11]) verwendet werden, die jeweils $n-k = 64$-Bit Blöcke in 64-Bit Blöcke umsetzen. Für praktisch vernünftige Blockverschlüssler $E_{\boldsymbol{Z}}$ sollte das von Shannon formulierte *Diffusions-Prinzip* [10] erfüllt sein, nach dem die Änderung eines Bits im Eingangsblock bzw. die Änderung eines Bits im Schlüssel die Änderung von rund 50% der Bits im Ausgangsblock bewirkt (Avalanche-Effekt). Dieses für den DES per Simulation [12] bzw. für den IDEA analytisch [11] nachgewiesene Prinzip überträgt sich unmittelbar auf den MAC, d.h.: Die Änderung eines Bits im Informationswort $\boldsymbol{X}$ bzw. die Änderung eines Bits im Schlüssel $\boldsymbol{Z}$ führt zur Änderung von rund 50% der Bits im Prüfwort $\boldsymbol{MAC}$.

Der aktive Angreifer kann den Übertragungsweg auftrennen und selbst Nachrichten einspielen, wobei er keine Kenntnis des Schlüssels hat. Beim *Impersonation Attack* [10] wird mit P_I die Wahrscheinlichkeit bezeichnet, daß der Angreifer den Empfänger zur Akzeptanz eines Codewortes bringen kann. Wenn die Schlüssellänge $\geq n-k$ ist, kann $P_I = 2^{-(n-k)}$ gezeigt werden [2, 3].

In der codierungstheoretischen Interpretation erweist sich der MAC offensichtlich als ein systematischer, nichtlinearer binärer (n, k)-Code, der mit dem Schlüssel $\boldsymbol{Z}$ parametrisiert ist. Die Codemenge ist durch $\Gamma_{\boldsymbol{Z}} = \{(\boldsymbol{X}, \boldsymbol{MAC}) \mid A_{\boldsymbol{Z}}(\boldsymbol{X}) = \boldsymbol{MAC}\}$ gegeben und die ebenfalls von $\boldsymbol{Z}$ abhängige Minimaldistanz wird mit $d_{\min}$ bezeichnet. Die Übertragung wird modelliert als $(\boldsymbol{X}', \boldsymbol{MAC}') = (\boldsymbol{X}, \boldsymbol{MAC}) + (\boldsymbol{e}_1, \boldsymbol{e}_2)$ mit einem entsprechend partitionierten Fehlermuster $\boldsymbol{e} = (\boldsymbol{e}_1, \boldsymbol{e}_2)$ und dann gilt:

$$(\boldsymbol{X}', \boldsymbol{MAC}') \in \Gamma_{\boldsymbol{Z}} \quad \Longleftrightarrow \quad \underbrace{A_{\boldsymbol{Z}}(\boldsymbol{X} + \boldsymbol{e}_1)}_{A_{\boldsymbol{Z}}(\boldsymbol{X}')} = \underbrace{A_{\boldsymbol{Z}}(\boldsymbol{X}) + \boldsymbol{e}_2}_{\boldsymbol{MAC}'}. \tag{2}$$

Die Erkennung eines Fehlermusters ist also nicht nur vom Fehlermuster selbst abhängig, sondern auch vom gesendeten Informationswort $\boldsymbol{X}$. Unabhängig von $\boldsymbol{X}$ werden allerdings alle Fehlermuster mit einem Hamminggewicht $w_H(\boldsymbol{e}) < d_{\min}$ erkannt. Der MAC kann natürlich nicht als Fehlerkorrekturcode verwendet werden, da aus kryptographischen Gründen jede einfach auswertbare algebraische Struktur fehlen muß.

Bei zufälliger Wahl von $\boldsymbol{Z}$ sind die Codemenge, die Minimaldistanz und alle weiteren Codeparameter als zufällige Größen anzusehen. Aufgrund des Diffusionsprinzips kann für das Prüfwort eine binomiale Verteilung unterstellt werden. Ferner kann das Prüfwort als unabhängig vom Informationswort angenommen werden, obwohl für einen fest gewählten Code das Prüfwort natürlich eine Funktion des Informationswortes ist. Nachfolgend wird die Unabhängigkeit nur für die Gewichte der Wörter verwendet.

3 Fehlererkennung bei Random Codes

Für einen beliebigen binären (n, k)-Code Γ mit der Coderate $R = k/n$ wird die *Gewichtsverteilung* mit A_d und die *Distanzverteilung* mit $\tilde{A}_d$ bezeichnet:

$$\begin{aligned} A_d &= \text{(Anzahl der Codewörter vom Hamminggewicht } d\text{)} \\ \tilde{A}_d &= 2^{-k} \cdot \text{(Anzahl der Codewörterpaare mit der Hammingdistanz } d\text{)}. \end{aligned}$$

Klar ist $\sum_{d=0}^{n} A_d = \sum_{d=0}^{n} \tilde{A}_d = 2^k$; $A_d = \tilde{A}_d = 0$ für $1 \le d \le d_{\min}$; $\tilde{A}_0 \ge 1$; $\tilde{A}_0 = 1$ genau dann, wenn alle Codewörter verschieden sind; $A_d = \tilde{A}_d$ und $A_0 = 1$ für lineare Codes. Mit $B_d(\boldsymbol{a})$ wird die Gewichtsverteilung von $\Gamma - \boldsymbol{a} = \{\boldsymbol{b} - \boldsymbol{a} | \boldsymbol{b} \in \Gamma\}$ bezeichnet. Bei einem *Distanz-invarianten* Code [4] ist $B_d(\boldsymbol{a})$ von $\boldsymbol{a} \in \Gamma$ unabhängig. In jedem Fall gilt jedoch

$$\tilde{A}_d \;=\; 2^{-k} \cdot \sum_{\boldsymbol{a} \in \Gamma} B_d(\boldsymbol{a}). \tag{3}$$

Vorausgesetzt wird jetzt der *binäre symmetrische Kanal* (BSC) mit der Bitfehlerwahrscheinlichkeit ϵ. Für die Wahrscheinlichkeit P_{ue} eines unerkannten Fehlers gilt [4]

$$P_{ue}(\epsilon) \;=\; \sum_{d=1}^{n} \tilde{A}_d \epsilon^d (1-\epsilon)^{n-d}. \tag{4}$$

Unabhängig von den Codeeigenschaften gilt

$$P_{ue}(0.5) \;=\; \frac{2^k - \tilde{A}_0}{2^n} \;\approx\; 2^{-(n-k)}. \tag{5}$$

Dies ist jedoch nur eine *trügerische* obere Grenze [6], da es sogenannte *improper Codes* [8] gibt, für die

$$P_{wc} \;:=\; \max_{\epsilon} P_{ue}(\epsilon) \;>\; P_{ue}(0.5) \tag{6}$$

gilt, d.h. $P_{ue}(\epsilon)$ wird nicht bei $\epsilon = 0.5$ maximal. In [8, 9] und einer ganzen Reihe weitere Arbeiten wurden einzelne Codeklassen auf diese Eigenschaft hin untersucht. Zu den improper Codes zählen auch zyklische Codes und sogar einige BCH-Codes. Beispielsweise ergibt sich ein sehr schlechter linearer $(2k, k)$-Code, wenn alle Prüfstellen Null sind: Dann gilt nämlich $A_d = \binom{k}{d}$ und $P_{ue}(\epsilon) = (1-\epsilon)^k(1-(1-\epsilon)^k)$ und daraus folgt $P_{ue}(0.5) = 2^{-k} \approx 0$ sowie $P_{ue}(\epsilon) = 1/4$ für $\epsilon = 1 - 2^{-1/k} \approx 0$.

In **Tabelle 1** werden 4 Klassen von Random Codes betrachtet, für die jeweils die Erwartungswerte der Gewichts- und Distanzverteilung angegeben sind. Bei RC1 wird die Generatormatrix in der systematischen Form $\boldsymbol{G} = (\boldsymbol{E}, \boldsymbol{P})$ mit einer k-dim. Einheitsmatrix $\boldsymbol{E}$ und einer $(k, n-k)$-dim. Binärmatrix $\boldsymbol{P}$ angenommen. Alle $2^{k(n-k)}$ möglichen Matrizen $\boldsymbol{P}$ werden mit gleicher Wahrscheinlichkeit gewählt. Bei RC2 werden alle $n2^k$ Bits in den 2^k Codewörtern statistisch unabhängig voneinander gewählt. Dabei können gleiche Codewörter auftreten, die bei RC3 durch Neuwahl eliminiert werden. Das MAC-Verfahren entspricht schließlich RC4, bei dem nur die $(n-k)2^k$ Prüfbits in den 2^k Codewörtern zufällig gewählt werden.

Beweise zu Tabelle 1: Das Ergebnis für RC1 findet sich in [4, 6]. Die Gewichtsverteilungen bei RC2 und RC3 sind offensichtlich binomial. Die Codewörter werden jetzt als $\boldsymbol{a}_i = (\boldsymbol{u}_i, \boldsymbol{p}_i)$ mit $i = 1, 2, 3, \ldots, 2^k$ durchnumeriert. Für RC4 ergibt sich die Verteilung von $w_H(\boldsymbol{a}_i) = w_H(\boldsymbol{u}_i) + w_H(\boldsymbol{p}_i)$ wegen der Unabhängigkeit aus der Faltung zweier Binomialverteilungen und ist somit wieder binomial. Für die Berechnung der Distanzverteilungen wird

$$\Gamma - \boldsymbol{a}_1 \;=\; \{\boldsymbol{0}\} \cup \{\boldsymbol{a}_2 - \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{2^k} - \boldsymbol{a}_1\} \tag{7}$$

vermerkt. Generell gilt (sei $\delta_d = 0$ für $d \neq 0$ und $\delta_0 = 1$):

$$E(B_d(\boldsymbol{a}_1)) \;=\; \sum_{i=1}^{2^k} P(w_H(\boldsymbol{a}_i - \boldsymbol{a}_1) = d) \;=\; \delta_d + (2^k - 1)P(w_H(\boldsymbol{a}_i - \boldsymbol{a}_1) = d). \tag{8}$$

Die rechte Gleichheit in (8) gilt sofern $P(w_H(\boldsymbol{a}_i - \boldsymbol{a}_1) = d)$ unabhängig von $\boldsymbol{a}_i$ für $i \geq 2$ ist. Bei Unabhängigkeit von $\boldsymbol{a}_1$ gilt weiter $E(B_d(\boldsymbol{a}_1)) = E(\tilde{A}_d)$. Sei nun $i \geq 2$. Bei RC2 ist $\boldsymbol{a}_i - \boldsymbol{a}_1$ exakt binomialverteilt und somit gilt $P(w_H(\boldsymbol{a}_i - \boldsymbol{a}_1) = d) = 2^{-n}\binom{n}{d}$ für $d = 0, \ldots, n$ und mit (7) folgt dann $E(\tilde{A}_d)$ wie in Tabelle 1. Es seien $\boldsymbol{b}, \boldsymbol{b}'$ zufällige und statistisch unabhängige Wörter gemäß RC2. Bei RC3 gilt dann für $d = 0, \ldots, n$

$$\begin{aligned} 2^{-n}\binom{n}{d} &= P(w_H(\boldsymbol{b} - \boldsymbol{b}') = d) \\ &= P(w_H(\boldsymbol{b} - \boldsymbol{b}') = d \mid \boldsymbol{b} \neq \boldsymbol{b}') \cdot P(\boldsymbol{b} \neq \boldsymbol{b}') + \\ &\quad P(w_H(\boldsymbol{b} - \boldsymbol{b}') = d \mid \boldsymbol{b} = \boldsymbol{b}') \cdot P(\boldsymbol{b} = \boldsymbol{b}') \\ &= P(w_H(\boldsymbol{a}_i - \boldsymbol{a}_1) = d) \cdot (1 - 2^{-n}) + \delta_d \cdot 2^{-n} \end{aligned}$$

und daraus folgt $P(w_H(\boldsymbol{a}_i - \boldsymbol{a}_1) = d) = \frac{1}{2^n - 1}\left(\binom{n}{d} - \delta_d\right)$ und damit $E(\tilde{A}_d)$ wie in Tabelle 1. Bei RC4 kann die Distanzverteilung nicht direkt über die Faltung wie bei der Gewichtsverteilung berechnet werden, weil $\boldsymbol{u}_i - \boldsymbol{u}_1$ und $\boldsymbol{p}_i - \boldsymbol{p}_1$ nur für $i \geq 2$ statistisch unabhängig

Klasse	$E(A_d)$	$E(\tilde{A}_d)$	$E(P_{ue}(\epsilon))$
RC1	$\begin{cases} 1 & d=0 \\ 2^{-(n-k)}\left(\binom{n}{d}-\binom{n-k}{d}\right) & d\geq 1 \end{cases}$		$2^{-(n-k)}(1-(1-\epsilon)^k)$
RC2	$2^{-(n-k)}\binom{n}{d}$	$\begin{cases} \frac{2^k-1}{2^n}+1 & d=0 \\ \frac{2^k-1}{2^n}\binom{n}{d} & d\geq 1 \end{cases}$	$\frac{2^k-1}{2^n}(1-(1-\epsilon)^n)$
RC3	$2^{-(n-k)}\binom{n}{d}$	$\begin{cases} 1 & d=0 \\ \frac{2^k-1}{2^n-1}\binom{n}{d} & d\geq 1 \end{cases}$	$\frac{2^k-1}{2^n-1}(1-(1-\epsilon)^n)$
RC4	$2^{-(n-k)}\binom{n}{d}$	$\begin{cases} 1 & d=0 \\ 2^{-(n-k)}\left(\binom{n}{d}-\binom{n-k}{d}\right) & d\geq 1 \end{cases}$	$2^{-(n-k)}(1-(1-\epsilon)^k)$
RC1: Linearer Random Code			
RC2: Allgemeiner Random Code (Beweis des Kanalcodierungstheorems)			
RC3: Random Code ohne gleiche Codewörter			
RC4: Systematischer Random Code (Message Authentication Code)			

Tabelle 1: Erwartungswerte von A_d, $\tilde{A}_d$, P_{ue} bei verschiedenen Klassen von Random Codes

sind. Sei weiterhin $i \geq 2$. Wie bei RC3 mit k statt n folgt für $d = 0, \ldots, k$:

$$P(w_H(\boldsymbol{u}_i - \boldsymbol{u}_1) = d) \;=\; \frac{1}{2^k-1}\left(\binom{k}{d} - \delta_d\right).$$

Dagegen sind die $\boldsymbol{p}$-Differenzen eventuell $\boldsymbol{0}$ auch für $i \geq 2$ und für $d = 0, \ldots, n-k$ gilt:

$$P(w_H(\boldsymbol{p}_i - \boldsymbol{p}_1) = d) \;=\; 2^{-(n-k)}\binom{n-k}{d}.$$

Durch Faltung ergibt sich daraus für $d = 0, \ldots, n$

$$P(w_H(\boldsymbol{a}_i - \boldsymbol{a}_1) = d) \;=\; \frac{2^{-(n-k)}}{2^k-1}\left(\binom{n}{d} - \binom{n-k}{d}\right)$$

und hieraus folgt das angegebene Ergebnis für $E(\tilde{A}_d)$. Die restlichen Ergebnisse aus Tabelle 1 folgen aus $E(P_{ue}(\epsilon)) = \sum_{d=1}^{n} E(\tilde{A}_d)\epsilon^d(1-\epsilon)^{n-d}$. □

Das MAC-Verfahren entspricht also nicht exakt, aber näherungsweise sowohl dem linearen Random Code wie dem Random Code mit oder ohne gleiche Codewörter. Aus Tabelle 1 folgt

$$\max_{\epsilon} E(P_{ue}(\epsilon)) \;\approx\; 2^{-(n-k)} \;=\; P_I. \tag{9}$$

Wenn dagegen die Wahl des Random Codes und die Bitfehlerwahrscheinlichkeit als verkoppelt angesehen werden, so gilt nach [6]

$$E(\max_{\epsilon} P_{ue}(\epsilon)) \;=\; E(P_{wc}) \;\leq\; n \cdot 2^{-(n-k)}. \tag{10}$$

Unlängst wurde dies verschärft zu [7]

$$E(P_{wc}) \;\le\; \sqrt{\frac{n\pi}{2}} \cdot 2^{-(n-k)} \cdot \exp\left(\frac{1}{12n}\right). \tag{11}$$

Klar ist natürlich $\max_\epsilon E(P_{ue}(\epsilon)) \le E(P_{wc})$. Nach (9) gilt im Mittel über alle Codes die trügerische Grenze für jedes ϵ, aber für einzelne Codes kann P_{ue} auch wesentlich größer ausfallen. Mindestens bei der Hälfte aller Codes bzw. aller Schlüssel wird P_{wc} oberhalb der trügerischen Grenze liegen. In diesem Fall gilt dann auch $P_{wc} > P_I$ – die Ursache liegt darin, daß P_I als Mittelung über alle zufällig gewählten Schlüssel definiert ist.

Für $f(\epsilon) = \epsilon^d(1-\epsilon)^{n-d}$ wird $\max_\epsilon f(\epsilon) = f(d/n) = 2^{-nH_2(d/n)}$ vermerkt, wobei $H_2(\lambda) = -\lambda\log_2(\lambda) - (1-\lambda)\log_2(1-\lambda)$ die *binäre Entropiefunktion* bezeichnet. Eine untere Grenze ergibt sich wie folgt:

$$\begin{aligned} P_{wc} &= \max_\epsilon \sum_{d=1}^{n} \tilde{A}_d \epsilon^d (1-\epsilon)^{n-d} \;\ge\; \max_d \left(\tilde{A}_d \cdot 2^{-nH_2(d/n)}\right) \\ &\ge 2^{-nH_2(d_{\min}/n)} \quad \text{bei linearen Codes.} \end{aligned} \tag{12}$$

Wenn also $d_{\min}$ für einzelne lineare Codes besonders klein ausfällt, wird P_{wc} besonders groß. Zur Vereinfachung wird jetzt mit der binomialen Gewichtsverteilung gerechnet. Unmittelbar klar ist $P(P_{wc} \ge 2^{-nH_2(d/n)}) \;\ge\; P(A_d \ge 1)$ und daraus folgt:

$$E(P_{wc}) \;\ge\; \max_d \left(2^{-nH_2(d/n)} \cdot P(A_d \ge 1)\right). \tag{13}$$

Bei unabhängiger Wahl der Codewörter sind die A_d binomialverteilt mit

$$P(A_d = s) \;=\; \binom{2^k}{s} p_d^s (1-p_d)^{2^k - s}, \tag{14}$$

wobei $p_d = P(w_H(\boldsymbol{a}) = d) = 2^{-k}E(A_d)$ ist. Somit folgt (sei z.B. $\eta = 10^{-5}$):

$$P(A_d \ge 1) \;=\; 1 - (1-p_d)^{2^k} \;\approx\; \left\{ \begin{array}{ll} E(A_d) & E(A_d) < \eta \\ 1 - \exp(-E(A_d)) & E(A_d) > \eta \end{array} \right\}. \tag{15}$$

Für Werte d mit $E(A_d) \ll 1$ gilt also $P(A_d \ge 1) \approx E(A_d)$.

4 Asymptotisches Verhalten für $n \to \infty$

Die mittlere Minimaldistanz beim linearen Random Code liegt auf der *asymptotischen Gilbert-Varshamov-Grenze* [5], d.h.

$$H_2\left(\frac{E(d_{\min})}{n}\right) \;=\; 1 - \frac{k}{n} \;=\; 1 - R. \tag{16}$$

Die gleiche mittlere Minimaldistanz folgt aus $1 = E(A_d) = 2^{-(n-k)}\binom{n}{d}$, denn durch Logarithmieren ergibt sich mit $\frac{1}{n}\log_2\binom{n}{d} \to H_2(d/n)$ für $n \to \infty$ [5]:

$$0 \;=\; \log_2 1 \;=\; n\left(-1 + R + \frac{1}{n}\log_2\binom{n}{d}\right) \;\approx\; n\left(-1 + R + H_2\left(\frac{d}{n}\right)\right).$$

Darüberhinaus gilt die trügerische Grenze genau dann, wenn der Code besser als die asypmtotische Gilbert-Varshamov-Grenze ist, d.h.

$$P_{wc} < 2^{-(n-k)} \quad \Longleftrightarrow \quad H_2\left(\frac{d_{\min}}{n}\right) \geq 1 - R. \tag{17}$$

Mit (16) folgt aus (12) wieder $E(P_{wc}) \geq 2^{-(n-k)}$, denn $-2^{-nH_2(d/n)}$ ist konvex in d, so daß die Ungleichung von Jensen anwendbar ist.

5 Numerische Ergebnisse

Für $n-k = 64$ werden Codes der Raten 0.9, 0.75, 0.2 betrachtet. Die Blocklängen betragen also 640, 256, 80. In den **Tabellen 2,3,4** sind jeweils die Logarithmen (zur Basis 10) von $E(A_d)$, $P(A_d \geq 1)$ und $2^{-nH_2(d/n)}$ für den interessanten d-Bereich angegeben. Beim Übergang zum linearen Random Code ergeben sich nur marginale Änderungen.

d	$E(A_d)$	$P(A_d \geq 1)$	$2^{-nH_2(d/n)}$
4	−9.4	−9.4	−10.6
5	−7.3	−7.3	−12.7
6	−5.3	−5.3	−14.8
7	−3.3	−3.3	−16.8
8	−1.4	−1.4	−18.7
9	+0.4	−0.0	−20.6
10	+2.2	+0.0	−22.4

Tabelle 2: (640, 576)−Code

d	$E(A_d)$	$P(A_d \geq 1)$	$2^{-nH_2(d/n)}$
4	−11.0	−11.0	−9.0
5	−9.3	−9.3	−10.7
6	−7.7	−7.7	−12.4
7	−6.1	−6.1	−14.0
8	−4.7	−4.7	−15.5
9	−3.2	−3.2	−16.9
10	−1.8	−1.8	−18.3
11	−0.5	−0.5	−19.8
12	+0.8	+0.0	−21.0
13	+2.1	+0.0	−22.3

Tabelle 3: (256, 192)−Code

d	$E(A_d)$	$P(A_d \geq 1)$	$2^{-nH_2(d/n)}$
8	−8.8	−8.8	−11.3
10	−7.0	−7.0	−13.1
12	−5.5	−5.5	−14.7
14	−4.1	−4.1	−16.1
16	−2.8	−2.8	−17.4
18	−1.7	−1.7	−18.5
20	−0.7	−0.8	−19.5
21	−0.3	−0.4	−20.0
22	+0.1	−0.1	−20.4
23	+0.6	−0.0	−20.8

Tabelle 4: (80, 16)−Code

Der asymptotische Erwartungswert der Minimaldistanz gemäß (17) beträgt 8.3, 10.7, 19.5. Tatsächlich findet der Wechsel von $E(A_d) < 1$ auf $E(A_d) > 1$ bei $d = d_{\min} = 8..9, 11..12, 21..22$ statt, was durch die horizontalen Linien gekennzeichnet wird. Gemäß (15) gilt $E(A_d) \approx P(A_d \geq 1)$ für $d < d_{\min}$ und $P(A_d \geq 1) \approx 1$ für $d \geq d_{\min}$. Für $d \approx d_{\min}$ gilt $2^{-nH_2(d/n)} \approx 2^{-(n-k)} = 10^{-19.3}$.

Betrachte den $(256, 192)$-Code: Im Mittel ist bei jedem $10^{3.2}$-ten Schlüssel $P_{wc} > 10^{-16.9}$ und bei jedem $10^{6.1}$-ten Schlüssel sogar $P_{wc} > 10^{-14.0}$. Es gibt also sehr schlechte Codes, die aber nur selten auftreten. Im Mittel gilt $E(P_{wc}) = 10^{-19.3}$. Da die Anzahl der Schlüssel aber zwischen 2^{56} bis 2^{128} liegt, können sehr schlechte Codes tatsächlich ausgewählt werden, bei denen P_{wc} um viele Zehnerpotenzen schlechter als $E(P_{wc})$ ausfällt.

6 Zusammenfassung

Im Mittel über alle Random Codes bzw. alle Schlüssel für den Message Authentication Code gilt für die Wahrscheinlichkeit eines unerkannten Fehlermusters bei ungünstigster BSC-Bitfehlerwahrscheinlichkeit immer $E(P_{ue}) = 2^{-(n-k)} = P_I$. Bei einzelnen Schlüsseln bzw. einzelnen Codes fällt P_{wc} allerdings wesentlich größer aus und überschreitet dann auch die Grenzen (10) und (11).

Es bleibt noch die Frage zu untersuchen, wie stark sich die Ergebnisse verändern, wenn das Diffusions-Prinzip für den verwendeten Blockverschlüssler nicht ideal erfüllt ist. Ein entsprechender Test muß sich immer auf eine vergleichsweise kleine Stichprobe beschränken. Deshalb ist der Zusammenhang zwischen P_{wc} und dem Stichprobenumfang noch genauer zu analysieren.

Literatur

[1] Friedrichs,B.: Sicherungsverfahren für die Datenübertragung über „Bedrohte Kanäle“ bei sicherheitsrelevanten Diensten. ANT Nachrichtentechnische Berichte Heft 10, S. 47-63, August 1993.

[2] Friedrichs,B.: Verfahren zur Kanalcodierung und Authentizität für sicherheitsrelevante Mobilkommunikation. 8. Aachener Kolloquium Signaltheorie, März 1994, S. 89-92.

[3] Friedrichs,B.: Authentische und zuverlässige Mobilkommunikation für sicherheitsrelevante Anwendungen. Teil I: Sicherheitsanforderungen und grundlegende Verfahren. Teil II: Systemarchitektur und Einbettung in GSM. Eingereicht bei Frequenz.

[4] MacWilliams,F.J.; Sloane,N.J.A.: The Theory of Error-Correcting Codes. Amsterdam: North-Holland 1977.

[5] Peterson,W.W.; Welden,E.J.: Error-Correcting Codes. Cambridge (MA): MIT Press 1972.

[6] Massey,J.L.: Coding Techniques for Digital Data Networks. Proc. Int. Conf. Inform. Theory and Systems, NTG Fachberichte Band 65, S. 307-315, Sept. 1978.

[7] Kløve,T.: On Massey's Bound on the Worst-Case Probability of Undetected Error. Proc. IEEE Int. Symp. Inform. Theory, S. 242, Juni 1994.

[8] Leung-Yan-Cheong,S.K., Barnes,E.R.; Friedman,D.U.: On some Properties of the Undetected Error Probability of Linear Codes. IEEE-IT, Vol. 25, S. 110-112, 1979.

[9] Wolf,J.K.; Michelson,A.M.; Levesque,A.H.: On the Probability of Undetected Error for Linear Block Codes. IEEE-COM, Vol. 30, S. 317-324, 1982.

[10] Simmons,G.J.(Ed.): Contemporary Cryptology. New York: IEEE Press 1992.

[11] Lai,X.: On the Design and Security of Block Ciphers. ETH Series in Information Processing Vol.1. Konstanz: Hartung-Gorre 1992.

[12] Heider,F.-P.; Kraus,D.; Welschenbach,M.: Mathematische Methoden der Kryptoanalyse. Braunschweig: Vieweg 1985.