Andreas Pfitzmann

Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo Hong Kong

Autor

Andreas Pfitzmann
Universität Karlsruhe
Institut für Rechnerentwurf und Fehlertoleranz
Postfach 6980, D-7500 Karlsruhe 1

CR Subject Classifications (1987): C.2, D.4.6, E.3, H.4.3, K.4.1

ISBN 3-540-52327-8 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-52327-8 Springer-Verlag New York Berlin Heidelberg

CIP-Titelaufnahme der Deutschen Bibliothek.
Pfitzmann, Andreas:
Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz / Andreas Pfitzmann. - Berlin; Heidelberg; New York; London; Paris; Tokyo; Hong Kong: Springer, 1990
(Informatik-Fachberichte; 234)
ISBN 3-540-52327-8 (Berlin ...) brosch.
ISBN 0-387-52327-8 (New York ...) brosch.
NE: GT

Druck- und Bindearbeiten: Weihert-Druck GmbH, Darmstadt
2145/3140 - 543210 - Gedruckt auf säurefreiem Papier

Wie bereits in [Pfi1_85 Seite 92] begründet, ist es sinnvoll, m und nicht $m \bullet (\ddot{u}+1)$ als Kostenfunktion des MIX-Netzes anzunehmen und entsprechend MIX-Netze mit gleichem m zu vergleichen: m bestimmt die Verzögerungszeit, den Umschlüsselungs- und Übertragungsaufwand. Die die Produktions-Kosten der MIXe charakterisierende Zahl $m \bullet (\ddot{u}+1)$ ist für den Vergleich nicht wesentlich, da gemäß Abschnitt 3.2.2.4 jede Informationseinheit nur von wenigen MIXen gemixt werden kann und diese wenigen MIXe einen so geringen Teil aller MIXe darstellen dürften, daß in jedem Fall auch $m \bullet (\ddot{u}+1)$ MIXe vorhanden sind.

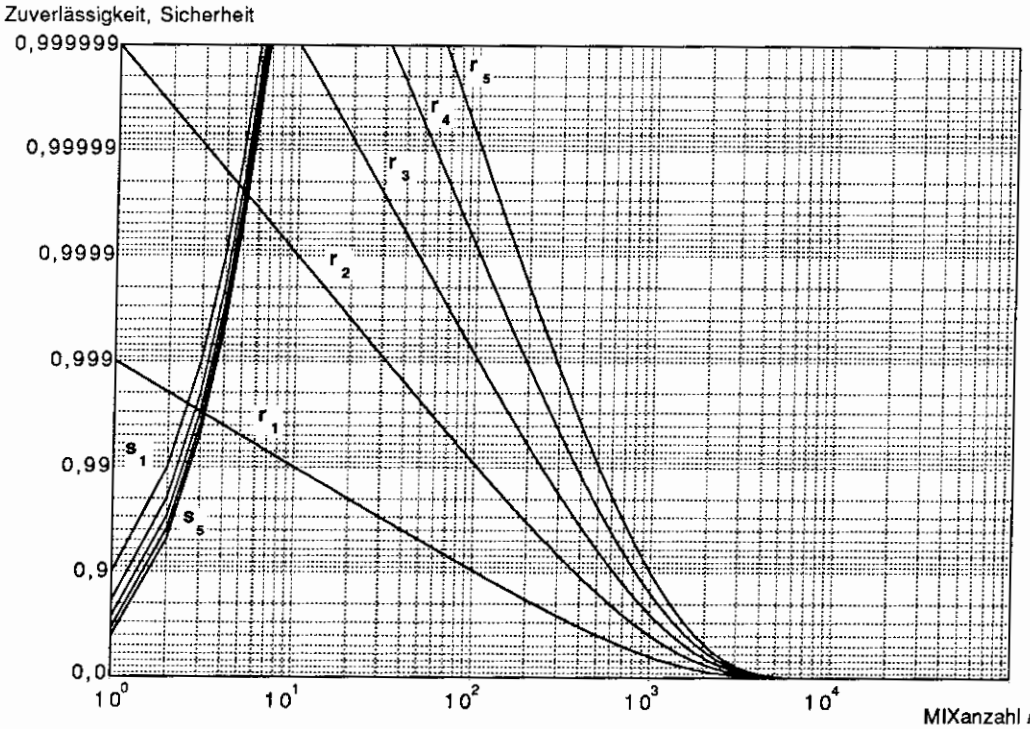

Bild 61: Werte für „Verschiedene MIX-Folgen" und die Parameterkombination $r = 0{,}999$ und $s = 0{,}9$

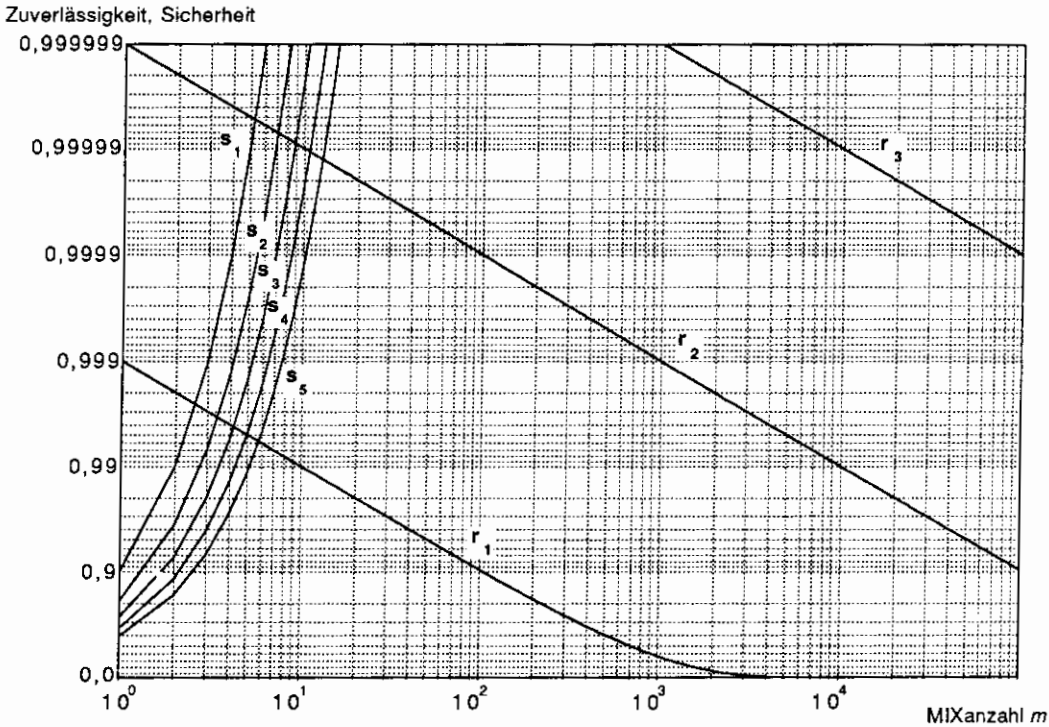

Bild 62: Werte für „MIXe mit Reserve-MIXen" und die Parameterkombination $r = 0{,}999$ und $s = 0{,}9$

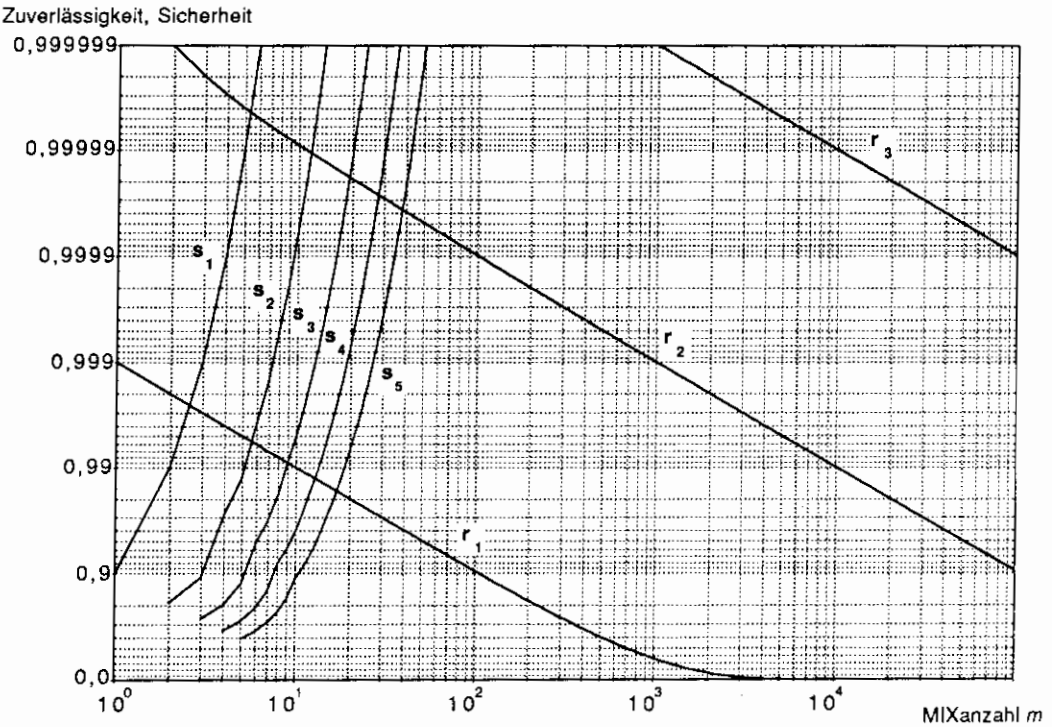

Bild 63: Werte für „Auslassen von MIXen" und die Parameterkombination $r = 0{,}999$ und $s = 0{,}9$

Der Gebrauch dieser Bilder sei an einem Beispiel beschrieben. Gesucht sei für jedes Fehlertoleranzverfahren und jede Parameterkombination das minimale m, so daß $\mathbf{r}_{\ddot{u}+1}(m) \geq 0{,}99999$ und $\mathbf{s}_{\ddot{u}+1}(m) \geq 0{,}99999$. Für die Parameterkombination $r = 0{,}999$ und $s = 0{,}9$ kann aus Bild 61 für „Verschiedene MIX-Folgen" der Wert $m = 6$ (bei $\ddot{u} = 3$), aus Bild 62 für „MIXe mit Reserve-MIXen" der Wert $m = 7$ (bei $\ddot{u} = 2$) und aus Bild 63 für „Auslassen von MIXen" der Wert $m = 12$ (bei $\ddot{u} = 2$) abgelesen werden. Entsprechend kann für die Paramertkombination $r = 0{,}99$ und $s = 0{,}9$ aus Bild 64 für „Verschiedene MIX-Folgen" der Wert $m = 6$ (bei $\ddot{u} = 4$), aus Bild 65 für „MIXe mit Reserve-MIXen" der Wert $m = 9$ (bei $\ddot{u} = 3$) und aus Bild 66 für „Auslassen von MIXen" der Wert $m = 30$ (bei $\ddot{u} = 4$) abgelesen werden. Aus den Bildern 67, 68 und 69 können die entsprechenden Werte nicht abgelesen werden, da bei „Verschiedenen MIX-Folgen" hierfür die „Kurven" für größere Werte von $\ddot{u}$ nötig wären und bei „MIXe mit Reserve-MIXen" und „Auslassen von MIXen" hierfür ein größerer Bereich von m und $\ddot{u}$ nötig wäre. Aus Gründen der graphischen Lesbarkeit und eines einheitlichen Maßstabes in allen 9 Bildern wurde darauf bewußt verzichtet.

Eine naive Interpretation dieser quantitativen Bewertungsergebnisse könnte nun lauten, daß „Verschiedene MIX-Folgen" das beste Fehlertoleranzverfahren sind, da es bei vorgegebenen Parametern immer die kleinsten Werte von m ermöglicht und keinerlei Koordinations-Problem existiert. Deshalb sei noch einmal daran erinnert, daß Ende-zu-Ende-Fehlerbehebung statistische Angriffe über Sende- und Empfangsraten und -zeitpunkte ermöglicht, die Sicherheit von „Verschiedene MIX-Folgen" von dem einfachen Bewertungsmodell also deutlich überschätzt wird.

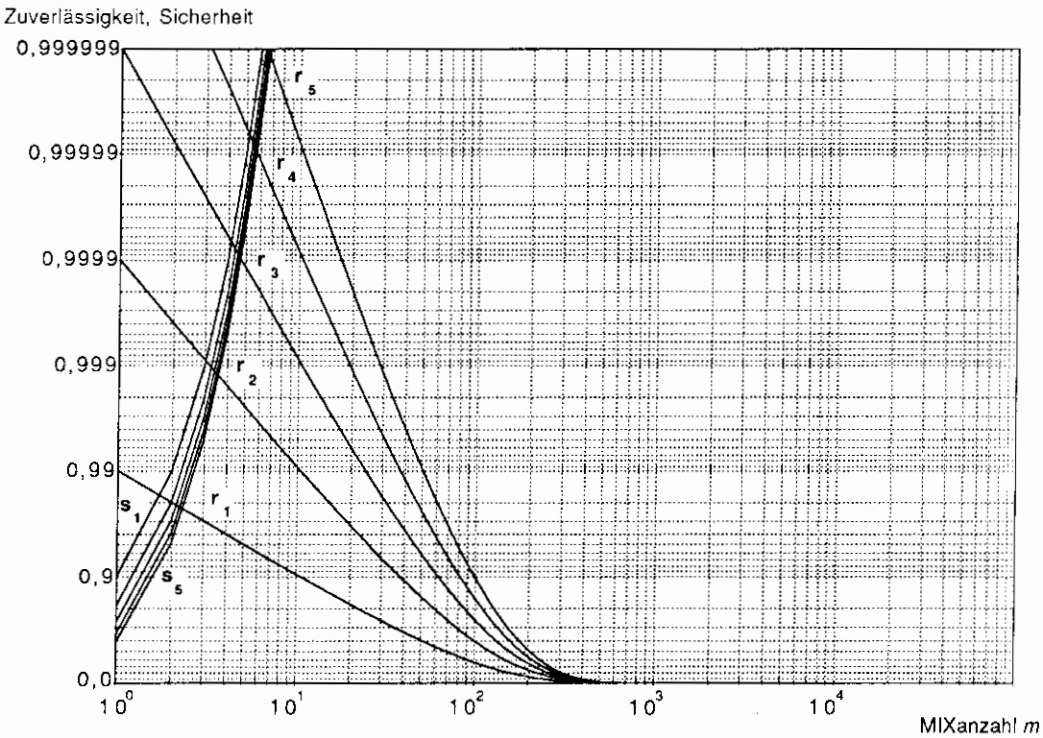

Bild 64: Werte für „Verschiedene MIX-Folgen" und die Parameterkombination $r = 0{,}99$ und $s = 0{,}9$

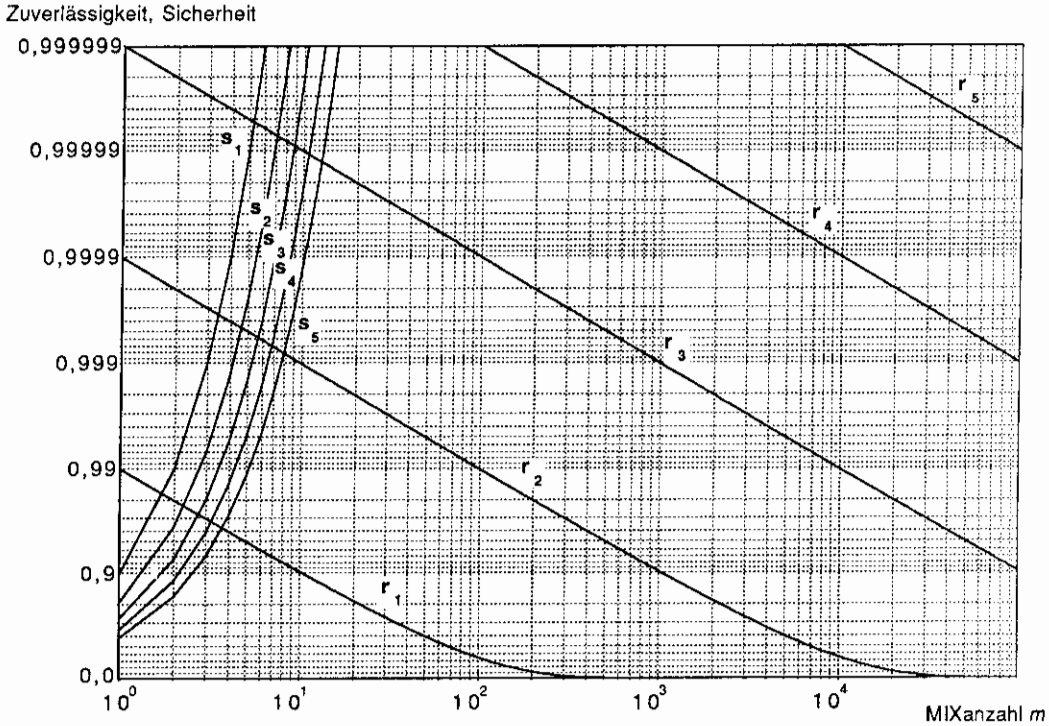

Bild 65: Werte für „MIXe mit Reserve-MIXen" und die Parameterkombination $r = 0{,}99$ und $s = 0{,}9$

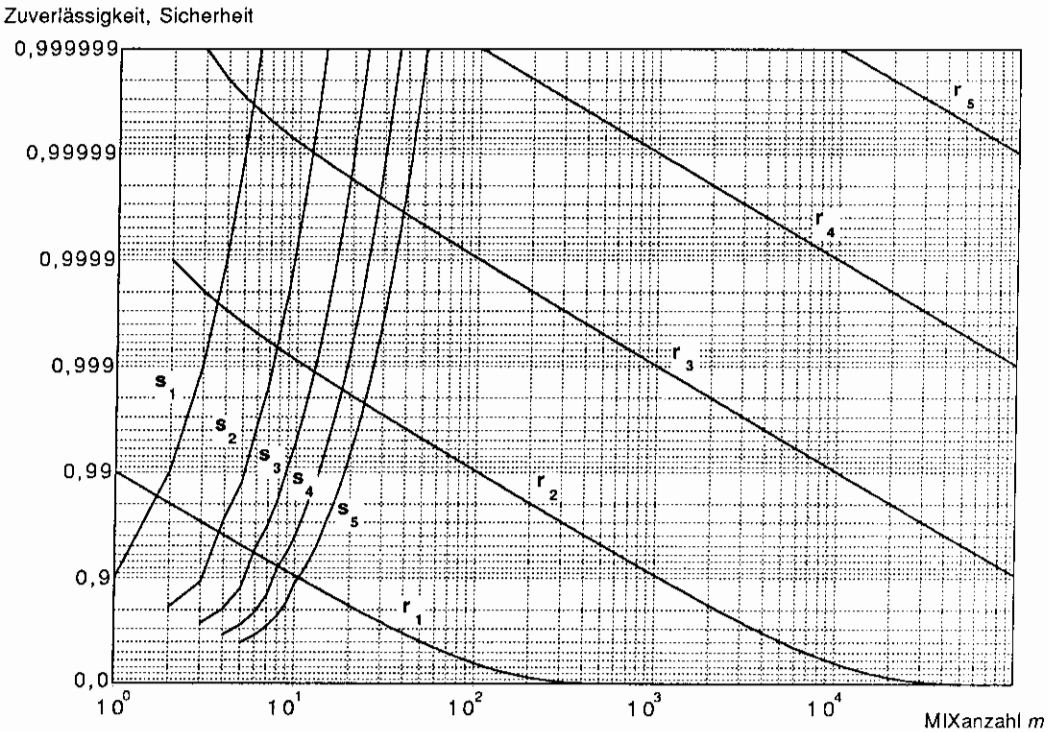

Bild 66: Werte für „Auslassen von MIXen" und die Parameterkombination $r = 0{,}99$ und $s = 0{,}9$

Die Bewertungsergebnisse für „MIXe mit Reserve-MIXen" und „Auslassen von MIXen" sind vergleichbarer und ähnlicher. Ersteres schneidet für kleine Werte von m deutlich, für große Werte von m nur sehr geringfügig besser ab. Dies liegt daran, daß aus den geschilderten Gründen bei „Auslassen von MIXen" die Sicherheit der ersten $\ddot{u}$ MIXe mit 0 angesetzt wird. Dies wirkt sich bei kleinem m deutlich, bei großem m so gut wie nicht aus. Da aber auch hier der genaue Aufwand und die genaue Nutzleistung (Verzögerungszeit, Durchsatz) vom unterliegenden Kommunikationsnetz, dem zu bedienenden Verkehr und den verwendeten Koordinations-Protokollen abhängt, kann letztlich nur eine quantitative Bewertung, die all diese Parameter berücksichtigt (und hoffentlich unter praktischen Randbedingungen einige fixieren kann) definitiv entscheiden.

Entsprechendes gilt, wenn auch schwach koordinierte MIXe bei „Auslassen von MIXen" in den Vergleich einbezogen werden. Dies kann mittels obiger Formeln für „Auslassen von MIXen" geschehen, indem unter Verwendung der Ergebnisse von Abschnitt 5.3.2.4 für die Berechnung von $\mathbf{r}$ und $\mathbf{s}$ nicht gleiche, sondern verschiedene Werte für $\ddot{u}$ verwendet werden. Die Werte können aus den Bildern 63, 66 und 69 direkt abgelesen werden, indem für die Situation, daß jeder MIX die nächsten $\ddot{u}$ MIXe auslassen kann, die „Kurven" $\mathbf{r}_{\ddot{u}+1}$ und $\mathbf{s}_{2\ddot{u}+1}$ zum Ablesen verwendet werden.

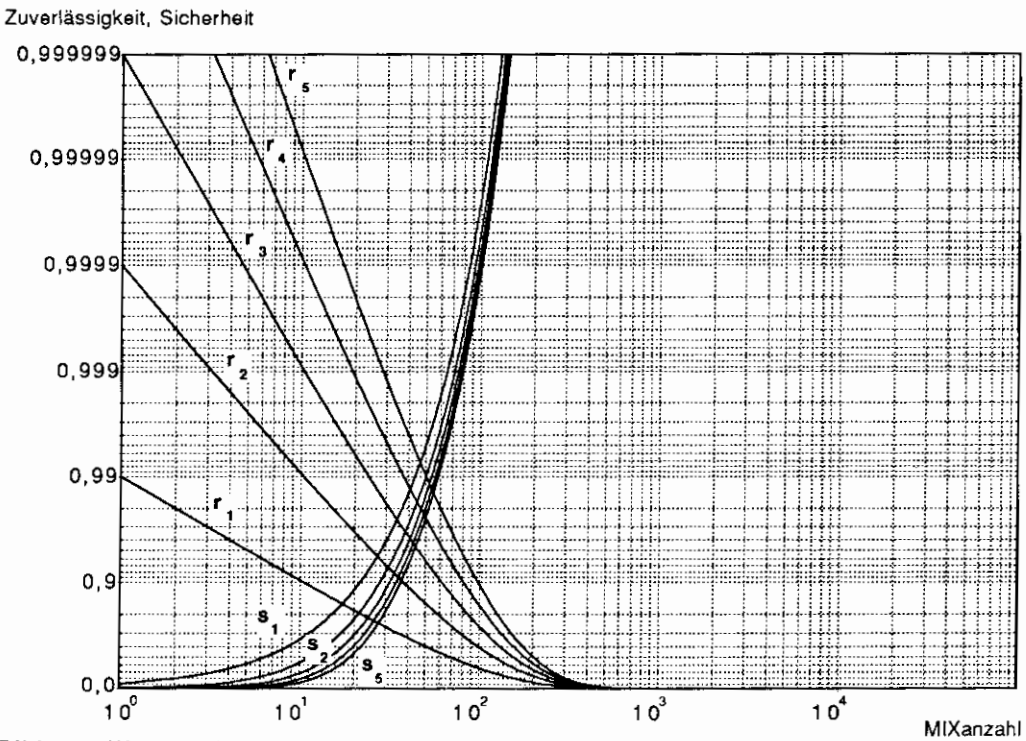

Bild 67: Werte für „Verschiedene MIX-Folgen" und die Parameterkombination $r = 0{,}99$ und $s = 0{,}1$

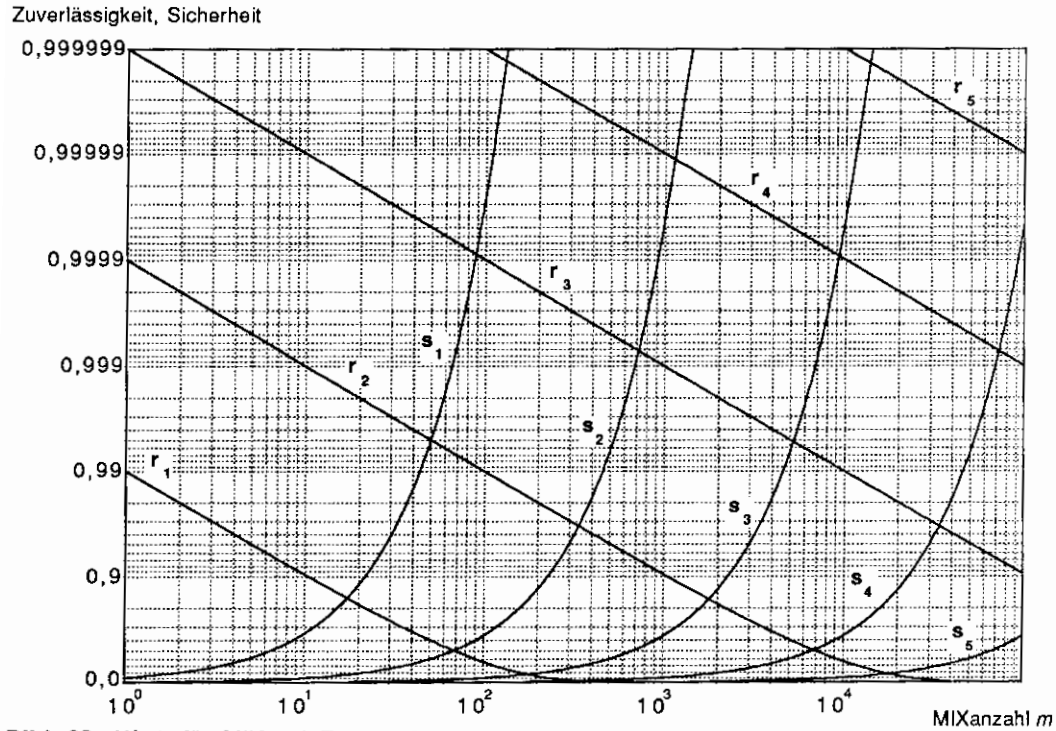

Bild 68: Werte für „MIXe mit Reserve-MIXen" und die Parameterkombination $r = 0{,}99$ und $s = 0{,}1$

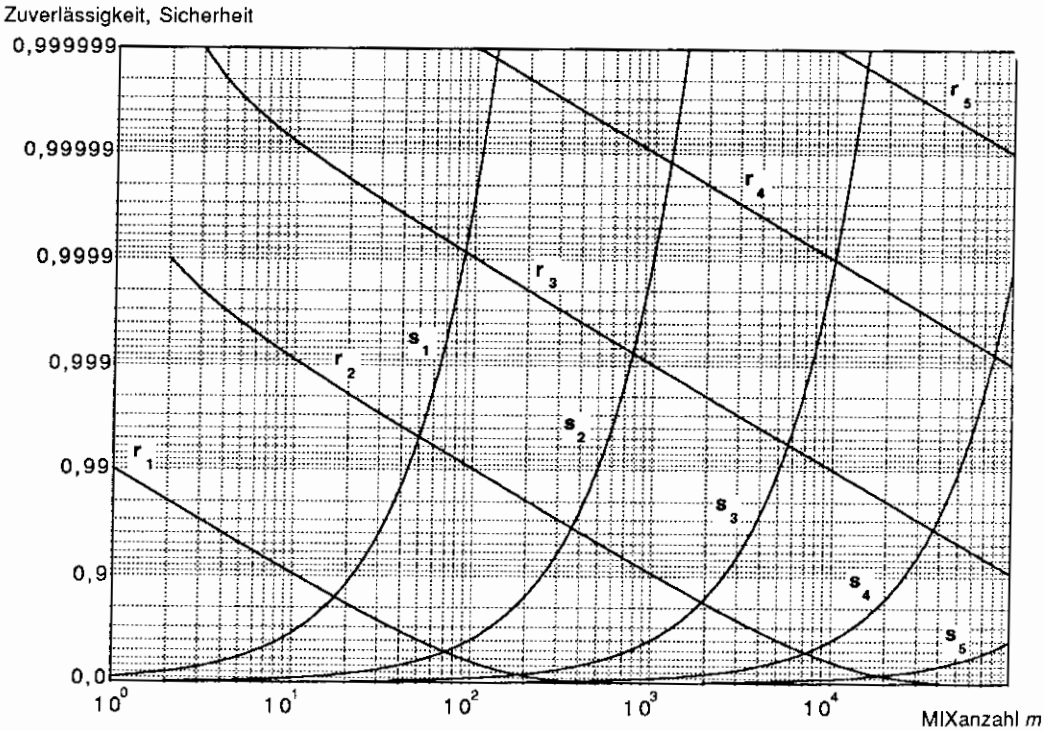

Bild 69: Werte für „Auslassen von MIXen" und die Parameterkombination $r = 0{,}99$ und $s = 0{,}1$