# Keno: Mit Sicherheit zufällig

***Sergio Montenegro, R. Rasche***
***FhG FIRST***
***Kekule Str 7***
***12489 Berlin***
***www.first.fhg.de/~sergio***

**Es war einmal ...**

Alte chinesische Schriftrollen legen nahe, dass Cheung Leung das Glücksspiel, das heute unter dem Namen Keno auf der ganzen Welt bekannt ist, etwa 200 Jahre vor Christus eingeführt hat. Damals befand sich Cheungs Stadt bereits mehrere Jahre im Krieg. Obwohl sich die Stadt in arger Bedrängnis befand, waren ihre Bürger immer weniger bereit, einen Beitrag in die Kriegskasse zu zahlen. Der findige Cheung nun, dem die Leidenschaft seiner Landsleute für alles Neue und das Glücksspiel durchaus nicht unbekannt war, erfand kurzum ein einfach zu verstehendes neues Lotteriespiel, um an das dringend benötigte Geld zu gelangen.

Das Spiel erwies sich als unmittelbarer Erfolg. In kürzester Zeit befand sich in der Kriegskasse reichlich Geld. Die Stadt wurde gerettet. Bald darauf verbreitete sich Keno über ganz China. Während es anfangs galt, chinesische Schriftzeichen zu erraten, sind es heute bei Lotto-Hessen Zahlen, die erraten werden müssen. Aus 70 Zahlen (1 bis 70) werden 20 gezogen. Der Spieler kann zwei bis zehn Zahlen tippen. Der Gewinn richtet sich nach dem Einsatz, der Anzahl der getippten Zahlen und der Anzahl der richtig erratenen Zahlen.

Während die Gewinnchancen über die Jahrhunderte die gleichen geblieben sind, hat sich die Methode der Ziehung doch ziemlich geändert. Heute werden bei Lotto-Hessen die Keno-Zahlen täglich mit einer zuverlässigen und sicheren elektronischen Lottofee aus dem Hause FhG FIRST (Fraunhofer Institut für Rechnerarchitektur und Softwaretechnik FIRST in Berlin) generiert. Abbildung 1 zeigt das Ziehungssystem mit einem Keno-Generator und zwei Visualisierer mit Monitor.

***Abbildung 1: Keno-Raum (Fotomontage)***

**Das Keno-Ziehungssystem der FhG FIRST**

Die neueste und vielleicht modernste Ziehungsvariante können die Zuschauer des Hessischen Rundfunks seit dem 2. Februar dieses Jahres täglich außer sonntags live mitverfolgen. Das in der Zentrale von ***Lotto Hessen*** installierte und von Forschern des Fraunhofer Instituts FIRST in Berlin entwickelte Ziehungssystem arbeitet voll elektronisch und weitestgehend autonom. Es besitzt - um den hohen Ansprüchen sowohl an Zuverlässigkeit, Nicht-Manipulierbarkeit aber auch in notariell/juristischer Hinsicht gerecht zu werden - einige Besonderheiten.

Das Ziehungssystem besteht aus den Aktoren

- Ziehungsbeamter (Mensch)
- Keno-Generator
- Visualisierungsrechner

Der ***Ziehungsbeamte*** steuert und protokolliert die Ziehung. Über einen Schalter gibt er dem Keno-Generator das Start-Signal zur Bestimmung der Gewinnzahlen und das Freigabe-Signal zur Ausgabe der Zahlen.

Der ***Keno-Generator*** besteht aus Gründen der Fehlertoleranz aus zwei

unabhängigen, baugleichen Rechnern, die über eine I2C-Schnittstelle internen Zustand und Daten synchronisieren können. Die Software wurde auf das FhG-FIRST-eigene Betriebssystem BOSS implementiert. BOSS wurde besonders für hohe Verlässlichkeit und Fehlertoleranzunterstützung entworfen. Jeder Rechner besitzt folgende Schnittstellen:

- ein Display, auf dem er die ermittelten Zahlen im 2-Sekunden-Takt ausgeben kann,
- einen Infrarot-Sender, um im 2-Sekunden-Takt Daten zum Visualisierungsrechner übermitteln zu können,
- einen Schalter, dessen Betätigung in einer ersten Phase die Ziehung und in einer späteren Phase die Übermittlung der Zahlen zum Visualisierungsrechner starten kann,
- zwei weitere Schalter um eventuell die Dauer einer Ziehung (mindestens 40 Sekunden) vorgeben zu können.

Weitere Schnittstellen besitzt der Keno-Generator nicht.

Der ***Visualisierungsrechner*** ist ein unter Windows XP laufender handelsüblicher Mini-PC, der mit zwei unabhängigen Infrarot-Kanälen und einer nach Fernseh-Standards modifizierten 3D-Grafikkarte ausgestattet ist. Er empfängt die Zahlen aus dem Keno-Generator und generiert eine 3D Animation für den Fernsehsender und für die Zuschauer.

**Keno-Generator: Interna**

Hard- und Software des Keno-Generators sind bewusst einfach gehalten, insbesondere, um die Verifikation und Prüfung durch den TÜV möglich zu machen. Hinter einem Keno-Generator verbergen sich zwei über einen I2C-Bus gekoppelte, identische Keno-Rechner. (siehe Abbildung 2). Diese Architektur gewährleistet ein hohes Maß an Ausfallsicherheit und Fehlertoleranz. Jeweils ein aus diskreten Transistoren aufgebauter Rauschgenerator, der aus dem Lawinen-Rauschen eines Transistors mittels Verstärker und Digitalisierer einen zufälligen Bitstrom erzeugt, komplettiert das Ensemble. Um die Stromversorgung der Hardware bemüht sich ein Solarmodul, das mit Studio-Lampen beleuchtet wird. Dadurch entfällt jegliche Kabel-Verbindung zur Aussenwelt, um das System möglichst isoliert zu betreiben. Dies macht die Nicht-Manipulierbarkeit für das Publikum sichtbar.

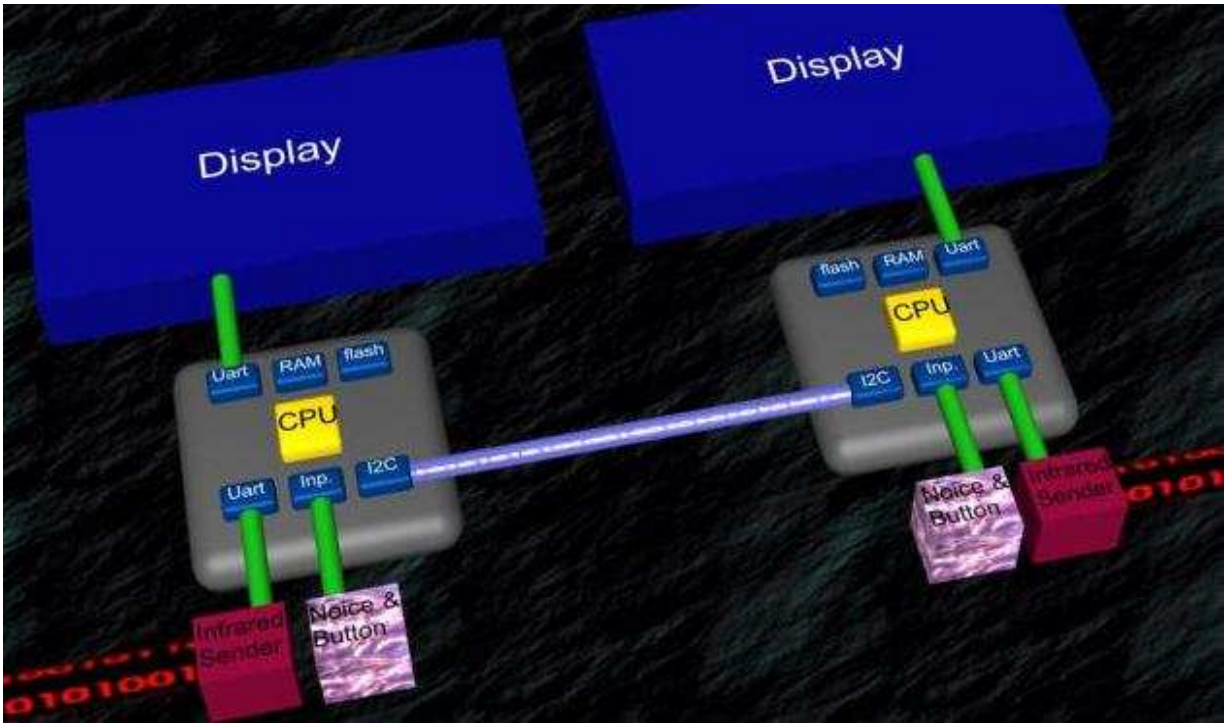


***Abbildung 2: Hardware des Kenogenerators***

**Erzeugung der Keno-Zahlen**

Der Hardware-Rauschgenerator liefert pro Lesezyklus ein Bit (0 oder 1). Diese Bits werden geshiftet, um ***random bytes*** zu formen. 100 dieser Bytes (800 Bits) dienen zu Initialisierung (***seed***) des Software-Random-Generators tt800 (http://www.math.keio.ac.jp/matumoto/mt19937.c, siehe Abbildung 3).

tt800.c

```
/* A C-program for TT800 : July 8th 1996 Version */
/* by M. Matsumoto, email: matumoto@math.keio.ac.jp */
/* genrand() generate one pseudorandom number with double precision */
/* which is uniformly distributed on [0,1]-interval */
/* for each call.  One may choose any initial 25 seeds */
/* except all zeros. */

/* See: ACM Transactions on Modelling and Computer Simulation, */
/* Vol. 4, No. 3, 1994, pages 254-266. */

#include <stdio.h>
#define N 25
#define M 7

static unsigned long x[N]={ /* initial 25 seeds, change as you wish */
        0x95f24dab, 0x0b685215, 0xe76ccae7, 0xaf3ec239, 0x715fad23,
        0x24a590ad, 0x69e4b5ef, 0xbf456141, 0x96bc1b7b, 0xa7bdf825,
        0xc1de75b7, 0x8858a9c9, 0x2da87693, 0xb657f9dd, 0xffdc8a9f,
        0x8121da71, 0x8b823ecb, 0x885d05f5, 0x4e20cd47, 0x5a9ad5d9,
        0x512c0c03, 0xea857ccd, 0x4cc1d30f, 0x8891a8a1, 0xa6b7aadb
};

long genrand() {
    unsigned long y;
    static int k = 0;
    static unsigned long mag01[2]={
        0x0, 0x8ebfd028 /* this is magic vector 'a', don't change */
    };
    if (k==N) { /* generate N words at one time */
      int kk;
      for (kk=0;kk<N-M;kk++) {
        x[kk] = x[kk+M] ^ (x[kk] >> 1) ^ mag01[x[kk] % 2];
      }
      for (; kk<N;kk++) {
        x[kk] = x[kk+(M-N)] ^ (x[kk] >> 1) ^ mag01[x[kk] % 2];
      }
      k=0;
    }
    y = x[k];
    y ^= (y << 7) & 0x2b5b2500; /* s and b, magic vectors */
    y ^= (y << 15) & 0xdb8b0000; /* t and c, magic vectors */
    y &= 0xffffffff; /* you may delete this line if word size = 32 */
/*
   the following line was added by Makoto Matsumoto in the 1996 version
   to improve lower bit's corellation.
   Delete this line to o use the code published in 1994.
*/
    y ^= (y >> 16); /* added to the 1994 version */
    k++;
    return y;
}
```

*Abbildung 3: Pseudo-Random-Generator tt800*

Jede Zufallszahl für Keno und Plus 5 wird aus einer Zahl aus dem tt800 und einem Byte aus dem Hardware-Rauschgenerator durch ein logisches XOR gebildet. Dies macht aus jede Ziehung ein Unikat. Reproduzierbarkeit ist nicht möglich. Nach dem Einschalten erzeugt der Keno-Generator auf diese Weise einen kontinuierlichen Strom von etwa 1000 Pseudo-Zufallszahlen pro Sekunde. Bei einer Ziehung entnimmt der Keno-Generator diesem Zahlenstrom nach und nach die 20 Glückszahlen (nur die unteren 7 Bit einer Zahl werden berücksichtigt), wobei er nur diejenigen auswählt, die im Bereich von 1 bis 70 liegen und nicht bereits in der Ziehung vorgekommen sind. Anschließend startet der Plus- 5-Generator. Er nimmt die unteren 17 Bits einer 32-Bit-Zahl und selektiert die Zahlen im Bereich 0 bis 9999 (Siehe Abbildung 4).

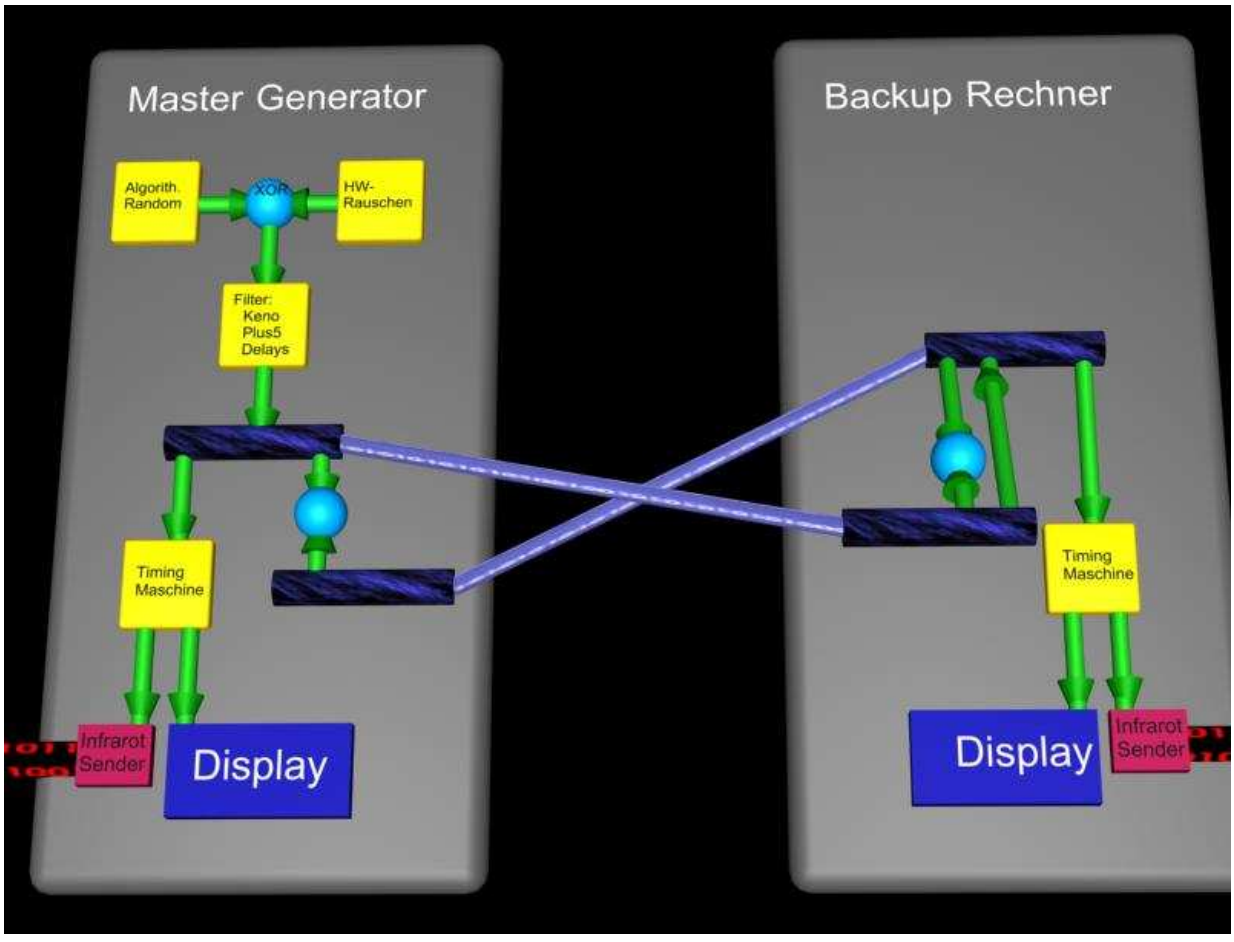


***Abbildung 4: Generierung der Zeihung***

***Unvorhersehbarkeit***. Da der vom Hardware-Rauschgenerator gelieferte ***seed*** für den tt800 so unbekannnt ist wie die Zeit zwischen dem Einschalten des Generators und dem Start der Ziehung - ausgelöst durch das Betätigen der Start-Taste durch den Ziehungsbeamten (pro Sekunde werden ständig ca. 1000 Zahlen generiert), können die vom Keno-Generator ermittelten Gewinnzahlen als unvorhersehbar

gelten.

***Verteilung.*** Statistische Analysen haben gezeigt, dass der tt800 die Keno-Zahlen mit einer Gleichverteilung in einem Korridor kleiner als +/- 0,1% (ideal wäre 0%, absolute Gleichverteilung) generiert.

***Periode.*** Um alle Kombinationen von Keno-Zahlen - 20 Zahlen aus 70 - erzeugen zu können, wird ein Generator mit einer Periode von 70!/((70-20)!*20!) benötigt. Mit $2^{800}$ ist die Periode des tt800 also mehr als ausreichend. Durch den XOR mit dem Hardware-Random-Generator erhält man eine unendliche Periode, damit hat jede Zahlenkombination (fast) dieselbe Chance.

***Nicht-Manipulierbarkeit.*** Um eine Manipulation des Keno-Generators von außen ausschließen zu können, sind lediglich drei Schalter als Bedienelemente vorhanden. Auf zu- und abgehende Kabel wurde grundsätzlich verzichtet. Die Stromversorgung erfolgt autonom über vorhandene Solarzellen. Die Datenübertragung zum Visualisierungsrechner erfolgt - bewusst unidirektional - per Infrarot. Ist eine Ziehung vom Ziehungsbeamten erst einmal gestartet worden, kann sie nicht mehr unterbrochen werden. Der Keno-Generator ist in ein Plexiglas-Prisma eingeschweißt und kann nicht mehr berührt/verändert werden.

***Validierung.*** Es wurden rigorose Tests der Hardware und ***code review*** von der ***TÜV Secure iT-GmbH*** des TÜV Rheinland Berlin Brandenburg durchgeführt, um Manipulationen an der Software oder Hardware ausschließen zu können, und etwa 24 Millionen Test-Ziehungen bescheinigen dem Keno-System höchste Zuverlässigkeit und eine nahezu perfekte Gleichverteilung der ermittelten Glückszahlen. Zusätzlich wurde eine formale Verifikation des Ziehungsablaufs unter Verwendung des Model-Checkers SMC durchgeführt.

**Visualisierung**

In C++ wurde auf einem üblichen Windows XP Rechner eine 3D-Visualisierung (Programmierschnittstelle DX9) für den Ziehungsvorgang implementiert. Einzige Besonderheit dieses Systems ist eine Matrox-Grafikkarte mit modifiziertem Ausgang für 50Hz PAL, die direkt sendefähige Bilder für Live-TV liefert. Die über zwei voneinander unabhängigen Infrarot-Kanäle eingehenden Daten - die über eine Prüfsumme gesicherten Glückszahlen - steuern die 3D-Animations (Siehe Abbildung 5).

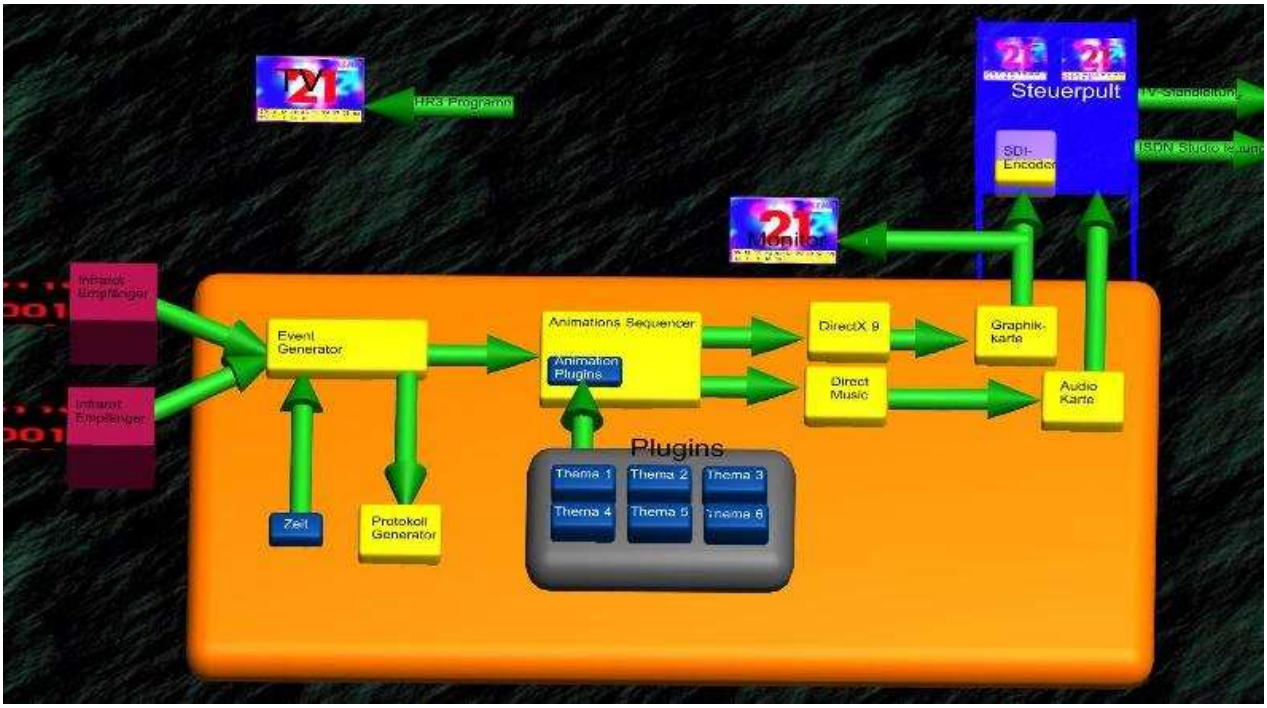


***Abbildung 5: Visualisierungsprozess***

Der Verfasser wünscht allen Keno-Fans viel Glück.