Egyetemi doktori (PhD) értekezés tézisei

Kriptográfiai hash függvények és álvéletlenszám generátorok

Folláth János

Témavezető: Dr. Pethő Attila

Debreceni Egyetem
Természettudományi Doktori Tanács
Informatikai Tudományok Doktori Iskola
Debrecen, 2011.

Egyetemi doktori (PhD) értekezés tézisei

Kriptográfiai hash függvények és álvéletlenszám generátorok

Folláth János

Témavezető: Dr. Pethő Attila

Debreceni Egyetem
Természettudományi Doktori Tanács
Informatikai Tudományok Doktori Iskola
Debrecen, 2011.

Contents

1. Összefoglalás

Jelen dolgozat fő témája két kriptográfiai primitív (egy álvéletlenszám generátor és egy hash függvény), illetve azok egy lehetséges alkalmazási területe.

Az első fejezet egy rövid bevezetőt tartalmaz. Elhelyezi a kriptográfiát a modern technika eszközei között, hangsúlyozza annak fontosságát és bevezet a kriptográfia alapfogalmaiba. A bevezetőt követően elhelyezi a tanulmányozni kívánt primitíveket a kriptográfián belül és áttekintést ad a dolgozat egészéről és a benne foglalt eredményekről.

A második fejezet témája az álvéletlenszám generátorok és az álvéletlenség fogalma. Ez a fejezet áttekinti a klasszikus álvéletlenségi teszteket és az álvéletlenség egyes definícióit, majd ezekből kiindulva eljut a Sárközy és Mauduit által bevezetett álvéletlen mértékekig ([55]). A szóban forgó mértékek a normalitás a Jóleloszlás, illetve a korrelációs mértékek, amelyek közül (tekintettel arra, hogy a korrelációs mérték alapján felső korlát képezhető a Normalitás mértékre) a jóleloszlás és a korrelációs mértékek egyesítésével kapjuk a kombinált mértéket. Ezek az álvéletlen mértékek képezik a fő eszközt a dolgozat témájául szolgáló álvéletlen generátor tanulmányozásához:

Minden $k \in \mathbb{N}, M \in \mathbb{N}, X = (x_1, \ldots, x_k) \in \{-1, 1\}^k, a \in \mathbb{Z}, b \in \mathbb{N}, D = (d_q, \ldots, d_k) \in \mathbb{N}^k, d_1 < \ldots < d_k$ esetén legyen

$$T(E, M, X) = |\{n : 0 \leq n < M, (e_{n+1}, e_{n+2}, \ldots, e_{n+k}) = X\}|,$$

$$U(E, M, a, b) = \sum_{j=1}^{M} e_{a+jb}$$

és

$$V(E, M, D) = \sum_{n=0}^{M-1} e_{n+d_1} e_{n+d_2} \ldots e_{n+d_k}.$$

Definíció 1.1. *Egy $E_N = (e_1, \ldots, e_N) \in \{-1, 1\}^N$ sorozat k-ad rendű normalitásmértékén az*

$$N_k(E_N) = \max_{X \in \{-1,1\}^k} \max_{0 < M \leq N+1-k} |T(E_N, M, X) - M/2^k|$$

értéket értjük. A sorozat normalitás mértéke ennek alapján:

$$N(E_N) = \max_{k \le (\log N)/\log 2} N_k(E_N).$$

Definíció 1.2. *Egy $E_N = (e_1, \dots, e_N) \in \{-1, 1\}^N$ sorozat jóleloszlás mértékén a*

$$W(E_N) = \max_{a,b,t} |U(E_N, t, a, b)| = \max_{a,b,t} |\sum_{j=1}^{t} e_{a+jb}|,$$

ahol a maximumot minden olyan a, b, t értékekre vesszük, ahol $a \in \mathbb{Z},\ b, t \in \mathbb{N}$ és $1 \le a + b \le a + tb \le N$.

Definíció 1.3. *Egy $E_N = (e_1, \dots, e_N) \in \{-1, 1\}^N$ sorozat k-ad rendű korrelációs mértékén a*

$$C_k(E_N) = \max_{M,D} |V(E_N, M, D)| = \max_{M,D} \left| \sum_{n=0}^{M-1} e_{n+d_1} e_{n+d_2} \dots e_{n+d_k} \right|,$$

ahol a maximumot minden olyan $D = (d_1, \dots, d_k)$ és M felett vesszük ahol $M + d_k \le N$. A sorozat korrelációs mértéke ez alapján:

$$C(E_N) = \max_{k \le (\log N)/\log 2} C_k(E_N).$$

Definíció 1.4. *Egy $E_N = (e_1, \dots, e_N) \in \{-1, 1\}^N$ sorozat k-ad rendű (kombinált) álvéletlenségi mértékén a*

$$\begin{aligned} Q_k(E_N) &= \max_{a,b,t,D} \left| \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \dots e_{a+jb+d_k} \right| \qquad (1.1) \\ &= \max_{a,b,t,D} |Z(a, b, t, D)|, \end{aligned}$$

ahol

$$|Z(a, b, t, D)| = \left| \sum_{j=0}^{t} \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \dots e_{a+jb+d_k} \right| \qquad (1.2)$$

kifejezést az olyan $a, b, t, D = (d_1, d_2, \dots, d_k)$ -ra értjük amelyeknél minden $a + jb + d_l$ index $\{1, \dots, N\}$ -ba tartozik és a (1.1) maximumot a k dimenziós D -k felett értjük.

Ennek alapján a sorozat álvéletlenségi mértéke:

$$Q(E_N) = \max_{k \le (\log N)/\log 2} Q_k(E_N).$$

A harmadik fejezet témája maga a generátor. Cikkükben ([55]) Sárközi és Mauduit maguk is adtak példát jó álvéletlenségi mértékkel rendelkező generátorra, és később, részben más szerzők közreműködésével, több jó konstrukció is született ([39], [49] [36] [37] [56] [34]). A fejezetben ezek közös tervezési elve, a dupla csavar módszer és az egyik, az új konstrukcióhoz közel álló generátor kerül ismertetésre. Ezek után az új generátor konstrukciója következik, amely mindamellett, hogy jó álvéletlen mértékekkel rendelkezik, szemben az összes korábbi konstrukcióval kettő karakterisztikájú véges testeket vesz alapul:

Tétel 1.1. *Legyen $\mathbb{F}_q$ kettő karakterisztikájú véges test ($q = 2^k$) és legyen a multiplikatív rendje prím. Legyen χ additív nem fő karakter, α pedig $\mathbb{F}_q$ primitív eleme. Legyen a $f(x) \in \mathbb{F}_q[x]$ fokszáma $d \ge \log q$ páratlan és az együtthatói pedig csak akkor legyenek nullák, ha az adott tag kitevője páros. Ha*

$$E_{q-1} = \{\chi(f(\alpha^1)), \chi(f(\alpha^2)), \dots, \chi(f(\alpha^{q-1}))\} \in \{-1, +1\}^{q-1}, \tag{1.3}$$

akkor:

$$Q(E_N) \le 9dq^{1/2} \log q. \tag{1.4}$$

A kriptográfiában nem csupán álvéletlen sorozatokra, hanem nagy álvéletlen sorozat családokra van szükségünk. Fontos az is, hogy a sorozatok, ne csak külön, hanem együtt is jó tulajdonságokkal rendelkezzenek. Ilyen tulajdonság a család bonyolultság és a lavinahatás:

Definíció 1.5. *Legyen $N \in \mathbb{N}$, S pedig egy adott halmaz, minden $s \in S$ értékhez legyen hozzárendelve egy egyedi bináris sorozat:*

$$E_N = E_N(s) = (e_1, \dots, e_N) \in \{-1, 1\}^N.$$

Jelölje $F = F(S)$ az álvéletlen bináris sorozatoknak a családját:

$$F = F(S) = \{E_N(s) : s \in S\}. \tag{1.5}$$

Definíció 1.6. *Bináris sorozatok egy $F(S)$ családja rendelkezik a szigorú lavinahatás tulajdonsággal, ha*

$$m(F) = \min_{\substack{s,s' \in S \\ s \neq s'}} d(E_N(s), E_N(s')) \geq \left(\frac{1}{2} + o(1)\right) N.$$

Definíció 1.7. *Definiáljuk a j hosszú specifikációt egy $(i_1, \ldots, i_j)$ index halmaz és egy hozzá tartozó $(\varepsilon_{i_1}, \ldots, \varepsilon_{i_j}) \in \{+1, -1\}^j$ érték halmaz együtteseként. Azt mondjuk, hogy egy $\{e_1, \ldots, e_N\}$ bináris sorozat kielégíti a specifikációt, ha*

$$e_{i_1} = \varepsilon_1, \ldots, e_{i_j} = \varepsilon_j.$$

Definíció 1.8. *Az $E_N \in \{-1, +1\}^N$ bináris álvéletlen sorozatok egy F családjának $\Gamma(F)$ f-bonyolultsága a legnagyobb j egész, amelyre teljesül, hogy minden j hosszú specifikációhoz van legalább egy $E_N \in F$, amely kielégíti.*

A fejezet tárgyalja a generátor lineáris bonyolultságát is. Kiderül, hogy nem alkalmas kriptográfiai felhasználásra, ugyanis a lineáris bonyolultsága túl alacsony. Ezzel együtt fény derül egy szoros kapcsolatra a lineárisan visszacsatolt léptetőregiszterekkel. Ez a kapcsolat gyors hardveres implementációt tesz lehetővé, és a jó statisztikai tulajdonságokkal együtt kiválóan alkalmassá teszi a nem kriptográfiai alkalmazásokra. A fejezet utolsó három szakaszának eredményei saját eredmények és a [23] és [25] cikkekben kerültek publikálásra:

Definíció 1.9. *Ha egy $f(x) \in \mathbb{F}_q[x]$ polinom $f(x) = \sum_{i=0}^{d} a_i x^{2i+1}$ formájú, akkor fésűs polinomnak nevezzük.*

Tétel 1.2. *Legyen S a legfeljebb d fokú $f(x) \in \mathbb{F}_q$ fésűs polinomok halmaza. Definiáljuk az egyes $E_{q-1} = E_{q-1}(f) = \{e_1, \ldots, e_{q-1}\}$ sorozatokat (1.3) szerint, az $F = F(S)$ családot pedig (1.5) alapján. Ha $d = o(q^{1/2})$ teljesül, akkor az F sorozatcsalád rendelkezik a szigorú lavinahatás tulajdonsággal.*

Tétel 1.3. *Legyen S a legfeljebb d fokú $f(x) \in \mathbb{F}_q$ fésűs polinomok halmaza. Definiáljuk az egyes $E_{q-1} = E_{q-1}(f) = \{e_1, \ldots, e_{q-1}\}$ sorozatokat (1.3) szerint, az $F = F(S)$ családot pedig (1.5) alapján. Ha A egy $t \leq \lfloor \frac{d+1}{2} \rfloor$ tagból álló specifikáció és $G(A)$ a $F = F(S)$ család azon részhalmazát jelenti, amelyek az A specifikációt kielégítik, akkor*

$$|G(A)| = \frac{|F|}{2^t}$$

teljesül.

Folyomány 1.1. *Az F család f bonyolultsága legalább $\lfloor \frac{d+1}{2} \rfloor$.*

Definíció 1.10. *Legyen $f(x)$ továbbra is olyan, hogy megfelel a 1.1 Tétel feltételeinek. Legyen ekkor a bináris álvéletlen sorozat:*

$$e_n = \begin{cases} 1, & \text{ha } \chi(f(\alpha^n)) = -1, \\ 0, & \text{egyébként.} \end{cases} \tag{1.6}$$

Definíció 1.11. *Egy sorozat lineáris bonyolultságán a legrövidebb olyan lineárisan visszacsatolt léptetőregiszter bitekben kifejezett hosszát értjük, amely a sorozatot generálni tudja.*

Tétel 1.4. *A (1.10) definícióban megadott bináris sorozat lineáris bonyolultsága $\frac{k(d+1)}{2}$.*

A negyedik fejezetben egy új hash függvény konstrukcióról van szó. A fejezet a hash függvényekről szól általánosságban, tartalmazza a hash függvény definícióját és a kriptográfiai hash függvényekkel kapcsolatos elvárások megfogalmazását. Ezután a konstrukció Codefish néven implementált elődjét ismerteti ([10]). Ezen konstrukció (pontosabban annak az implementáláshoz felhasznált módosított speciális esete) kriptanalízise is itt kapott helyet.

Ezek után az új konstrukció és a vele kapcsolatos elméleti eredmények következnek. A konstrukció kiküszöböli elődje hibáit ([6]) és az operandusok méretében is előrelépést jelent. Elméleti megfontolások alapozzák meg a függvény előképellenállóságát és egy jó statisztikai tulajdonsága is bizonyítást nyer. A függvény lavinahatásával kapcsolatos vizsgálatok is itt szerepelnek: habár a függvény implementációban felhasznált változata bizonyíthatóan nem rendelkezik a szigorú lavinahatással, aszimptotikusan nagyon hasonlóan viselkedik hozzá:

Definíció 1.12 (UDHash)**.** *Legyen az $f(\underline{X}) \in \mathbb{F}_q[X_1, \ldots, X_m]$ polinom a következő formájú:*

$$f(\underline{X}) = b(X_1, \ldots, X_m) + a(X_1, \ldots, X_m),$$

ahol $a(\underline{X})$ és $b(\underline{X})$ homogén polinomok, amelyeknek a fokszámaira teljesül, hogy $k = \deg a(\underline{X}) < \deg b(\underline{X}) = n$ és $\deg_{X_i} b(\underline{X}) = n$ minden $1 \leq i \leq m$ esetén. Tegyük fel továbbá, hogy léteznek olyan $1 \leq j_1 < j_2 \leq n$ indexek, hogy a

$$b_o(X_{j_1}, X_{j_2}) = b(0, \ldots, X_{j_1}, 0, \ldots, 0, X_{j_2}, 0, \ldots, 0)$$

bináris formának nincs többszörös gyöke.

Tétel 1.5. *Legyen az* $f(\underline{X}) \in \mathbb{F}_q[X_1, \ldots, X_m]$ *polinom olyan, hogy megfelel a 1.12 Definíciónak. Jelölje* $N(f, \gamma, q)$ *az* $f(x_1, \ldots, x_m) = \gamma$ *egyenlet megoldásainak számát* $x_1, \ldots, x_m \in \mathbb{F}_q$ *esetén. Ekkor*

$$|N(f, \gamma, q) - q^{m-1}| \leq (n-1)(n-2)q^{m-3/2} + 5n^{13/3}q^{m-2}. \tag{1.7}$$

Továbbá, ha $q > 15n^{13/3}$*, akkor*

$$|N(f, \gamma, q) - q^{m-1}| \leq (n-1)(n-2)q^{m-3/2} + (5n^2 + n + 1)q^{m-2}. \tag{1.8}$$

Tétel 1.6. *Definiáljuk az* $f \in \mathbb{F}_{2^k}[x_1, \ldots, x_m]$ *polinomot, mint* $f(x_1, \ldots, x_m) = \sum_{i=1}^{m} \alpha_i x_i^n + \sum_{i=1}^{m} \beta_i x_i$*, ahol* $n = 2^l + 1$ *olyan, hogy* $(l, k) = 1$*. Ekkor*

$$(1 - q\varepsilon)^{m-1}(\frac{1}{q} - \varepsilon) \leq$$
$$P(f(x_1, \ldots, x_m) - f(x_1 + \delta_1, \ldots, x_m + \delta_m) = \gamma)$$
$$\leq (1 + q\varepsilon)^{m-1}(\frac{1}{q} + \varepsilon),$$

ahol $0 \leq \varepsilon \leq nq^{-\frac{3}{2}}$.

A hash függvény előkép ellenállóságára vonatkozó megállapítások Bérczes Attilával és Pethő Attilával közös eredményeink és a [7] cikkben kerültek publikálásra. A lavinahatásra és a hozzá kapcsolódó aszimptotikus állításra vonatkozó tétel saját eredmény és eddig még nem lett publikálva.

Az ötödik fejezetben az említett hash függvény implementációjáról és a DESignIn beléptetőrendszerről van szó. A hash függvényünk egy iteratív hash függvény és a korábbiakban csak a tömörítőfüggvény került ismertetésre. Tárgyalásra kerül a függvény paraméterválasztása és az alkalmazott iterációs eljárás. Ezek után kerülnek megfontolásra a konkrét implementációs kérdések, a véges test kiválasztása, továbbá a futási időre és a lavinahatásra vonatkozó tesztek. Végül, mint lehetséges alkalmazási terület, a DESignIn azonosító rendszer kerül ismertetésre. A DESignIn tervezési megfontolásai közös eredményeink Huszti Andreával és Pethő Attilával és a [26] cikkben kerültek publikálásra. A szóban forgó gyakorlati vizsgálatok eredményei eddig nem lettek publikálva és a B, illetve a D Appendixben találhatóak.

A legtöbb kriptográfiai primitív esetén a szempont az, hogy gyorsan számíthatóak legyenek. A hash függvények esetén azonban az is szempont lehet, hogy a

leggyorsabb implementáció is viszonylag lassú legyen. A számítási erőforrások manapság olcsók és skálázhatóak, ezért a gyors hash függvények esetén a feltöréssel próbálkozóknak is könnyebb dolga van. Thomas Roth az Amazon Elastic Compute Cloud szolgáltatásának segítségével tört fel erős kriptográfiai hash függvénnyel védett jelszavakat olcsó wifi készülékeken [1] 20 perc alatt, percenként 28 centes költséggel. Az UDHash ebből a szempontból is előnyös, hiszen a leggyorsabb implementációja is lassabb, mint a napjainkban gyakorlatban használt hash függvényeké.

A lavinahatásra vonatkozó eredmény feltételei sajnos túl szigorúak ahhoz, hogy a gyakorlati megvalósítás esetén ezeknek megfelelő paramétereket alkalmazzunk. Ezért a konstrukció lavinahatás tulajdonságára vonatkozóan gyakorlati vizsgálatok is folytak.

A lavinahatásra vonatkozó teszteredmények az B Függelékben kerülnek közlésre. Itt az egyes ábrák alatt a hash függvény paraméterezése a lineáris és a nemlineáris tagok együtthatóival, illetve a nemlineáris tag kitevőjével van megadva. A grafikon x tengelyén található számok 0-761 -ig az egyes bemeneti biteket jelölik, az y tengely számozása 0-243-ig a kimeneti bitekhez tartozik. Az z tengely pedig 0-1499-ig a bemeneti minták számát jelöli. Egy (x,y,z) pont az ábrán azt jelenti, hogy a bemenet x. bitjét megváltoztatva a kimenet y. bitje z darab minta esetében változott meg.

Látható, hogy a tesztek esetében a pontok a $z = 750$ sík környezetében találhatóak, azaz az empirikus valószínűség minden esetben a lavinahatás tulajdonságtól elvárt $\frac{1}{2}$ közelében van. Azaz, habár az UDHash a fent választott paraméterezés mellett, szigorúan vett értelemben bizonyíthatóan nem rendelkezik a lavinahatás tulajdonságával, a gyakorlatban egy, a lavinahatáshoz nagyon közeli viselkedést mutat.

A hash függvények és az álvéletlen-szám generátorok számos kriptográfiai protokollban fontos szerepet játszanak. A jelen dolgozatban ismertetett kriptográfiai primitívek lehetséges alkalmazási területének egy példája az UDSignIn azonosító rendszer.

Az UDSignIn egy univerzális webes alapú azonosítórendszernek lett tervezve. A feladata az egyszerű jelszavas bejelentkezés kiváltása, kényelmes megoldást kínál arra a problémára, hogy a biztonságos jelszavakat rendszerint nehéz megjegyezni, és hogy manapság egy átlagos felhasználó több tucat webes accounttal is rendelkezhet.

A jelszavas azonosítás esetén a biztonság érdekében a felhasználóknak minden egyes accounthoz más, erős, azaz nehezen megjegyezhető jelszót kellene észben tartania. Ez rendszerint ahhoz vezet, hogy gyenge jelszavakat használnak, vagy,

hogy több helyen is ugyanazt a jelszót használják, esetleg felírják valahová. A jelszavas azonosítás felváltása tanúsítványok segítségével való azonosításra nem csak a rendszer biztonságát növeli, de a felhasználóknak is kényelmesebb megoldást jelent.

Az UDSignIn ezt a problémát egy hardvertoken segítségével hidalja át. Az azonosításhoz aszimmetrikus kriptográfiát használ, a szerver azonosításában már meglévő, széles körben elterjedt és bevált technikára, konkrétan az SSL valamelyik változatára támaszkodik. Az UDSignIn technikai leírása, és a vele kapcsolatos elméleti, gyakorlati és tervezési megfontolások a [26] cikkben kerültek publikálásra.

2. Summary

The main topics of this dissertation are two cryptographic primitives (a pseudorandom generator and a hash function) and a possible application of them.

Chapter 1 contains a short introduction. It describes cryptography as a tool of modern technology, emphasises its importance and gives an introduction to the basic notions of cryptography. After the introduction it determines the places of the primitives to study and their relation to other areas of cryptography, and it gives an overview of the whole dissertation and the main results.

The themes of Chapter 2 are the pseudorandom generators and the concept of pseudorandomness. This chapter overviews the classic pseudorandomness tests and the distinct definitions of pseudorandomness. Then taking these as a starting point it reaches the pseudorandomness measures introduced by Mauduit and Sárközy ([55]). The measures in question are the normality, the well-distribution and the correlation measures. The combination of the correlation and the well-distribution measure leads to the combined measure (The normality measure is left out from the combined measure because with the help of the correlation measure one can give an upper bound for it). These pseudorandomness measures constitute the main tools to study the mentioned pseudorandom generator:

For every $k \in \mathbb{N}, M \in \mathbb{N}, X = (x_1, \ldots, x_k) \in \{-1, 1\}^k, a \in \mathbb{Z}, b \in \mathbb{N}, D = (d_q, \ldots, d_k) \in \mathbb{N}^k, d_1 < \ldots < d_k$ let

$$T(E, M, X) = |\{n : 0 \leq n < M, (e_{n+1}, e_{n+2}, \ldots, e_{n+k}) = X\}|,$$

$$U(E, M, a, b) = \sum_{j=1}^{M} e_{a+jb}$$

and

$$V(E, M, D) = \sum_{n=0}^{M-1} e_{n+d_1} e_{n+d_2} \ldots e_{n+d_k}.$$

Definition 2.1. *Let us define the k. order normality measure of the* $E_N = (e_1, \ldots, e_N) \in \{-1, 1\}^N$ *sequence as*

$$N_k(E_N) = \max_{X \in \{-1,1\}^k} \max_{0 < M \leq N+1-k} |T(E_N, M, X) - M/2^k|,$$

and the normality measure of the sequence as

$$N(E_N) = \max_{k \leq (\log N)/\log 2} N_k(E_N).$$

Definition 2.2. *Let us define the well-distribution measure of the* $E_N = (e_1, \ldots, e_N) \in \{-1, 1\}^N$ *sequence:*

$$W(E_N) = \max_{a,b,t} |U(E_N, t, a, b)| = \max_{a,b,t} |\sum_{j=1}^{t} e_{a+jb}|,$$

where the maximum is taken over all a, b, t *values, such that* $a \in \mathbb{Z},\ b, t \in \mathbb{N}$ *and* $1 \leq a + b \leq a + tb \leq N$.

Definition 2.3. *Let us define the k. order correlation measure of the* $E_N = (e_1, \ldots, e_N) \in \{-1, 1\}^N$ *sequence:*

$$C_k(E_N) = \max_{M,D} |V(E_N, M, D)| = \max_{M,D} \left| \sum_{n=0}^{M-1} e_{n+d_1} e_{n+d_2} \ldots e_{n+d_k} \right|,$$

where the maximum is taken over all $D = (d_1, \ldots, d_k)$ *and* M *such that* $M + d_k \leq N$. *The correlation measure of the sequence:*

$$C(E_N) = \max_{k \leq (\log N)/\log 2} C_k(E_N).$$

Definition 2.4. *Let us define the k. order (combined) pseudorandom measure of the* $E_N = (e_1, \ldots, e_N) \in \{-1, 1\}^N$ *sequence as follows:*

$$\begin{aligned} Q_k(E_N) &= \max_{a,b,t,D} \left| \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \ldots e_{a+jb+d_k} \right| \\ &= \max_{a,b,t,D} |Z(a, b, t, D)|, \end{aligned} \tag{2.1}$$

where

$$|Z(a,b,t,D)| = \left| \sum_{j=0}^{t} \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \dots e_{a+jb+d_k} \right| \tag{2.2}$$

and for all $a, b, t, D = (d_1, d_2, \dots, d_k)$*, such that* $a + jb + d_l \in \{1, \dots, N\}$ *and the* (2.1) *maximum is taken over all* k *dimensional* D*.*

The pseudorandom measure of the sequence is:

$$Q(E_N) = \max_{k \le (\log N)/\log 2} Q_k(E_N).$$

Chapter 3 is about the generator itself. In their paper ([55]) Sárközi and Mauduit gave an example of a pseudorandom generator having good pseudorandom measures. Later (partly with further coauthors) more good constructions were born ([39], [49] [36] [37] [56] [34]). In this chapter the common design principle of these generators: the double twist method and one of the previous generators will be described. Thereafter the construction of the new generator follows. This new generator has good pseudorandomness measures and, contrary to the previous constructions, operates over fields with even characteristics:

Theorem 2.1. *Let* $\mathbb{F}_q$ *be an even characteristic finite field* ($q = 2^k$) *with prime multiplicative order. Let* χ *be a non-principal additive character and* α *a primitive element of* $\mathbb{F}_q$*. Let* $f(x) \in \mathbb{F}_q[x]$ *have an odd degree of* $d \ge \log q$ *and let its coefficients be zeroes if and only if the corresponding exponent is even. If*

$$E_{q-1} = \{\chi(f(\alpha^1)), \chi(f(\alpha^2)), \dots, \chi(f(\alpha^{q-1}))\} \in \{-1, +1\}^{q-1}, \tag{2.3}$$

then:

$$Q(E_N) \le 9dq^{1/2} \log q. \tag{2.4}$$

In cryptography it is not sufficient to have pseudorandom sequences: we need large families of pseudorandom sequences. It is important to have sequences, which not only alone as a single sequence, but together as a family also have good properties. Such properties are the avalanche effect and the family complexity. Also these properties of the new construction will be proven:

Definition 2.5. *Let $N \in \mathbb{N}$, and S a given set. Let it be assigned a unique binary sequence to every $s \in S$:*

$$E_N = E_N(s) = (e_1, \ldots, e_N) \in \{-1, 1\}^N.$$

Let $F = F(S)$ denote the family of pseudorandom binary sequences:

$$F = F(S) = \{E_N(s) : s \in S\}. \tag{2.5}$$

Definition 2.6. *The $F(S)$ family of binary sequences posesses the strict avalanche property, if*

$$m(F) = \min_{\substack{s,s' \in S \\ s \neq s'}} d(E_N(s), E_N(s')) \geq \left(\frac{1}{2} + o(1)\right) N.$$

Definition 2.7. *Let us define the specification of length j as the pair of an $(i_1, \ldots, i_j)$ index set and an $(\varepsilon_{i_1}, \ldots, \varepsilon_{i_j}) \in \{+1, -1\}^j$ value set. An $\{e_1, \ldots, e_N\}$ binary sequence satisfies the specification, if*

$$e_{i_1} = \varepsilon_1, \ldots, e_{i_j} = \varepsilon_j.$$

Definition 2.8. *The $\Gamma(F)$ f-complexity of an F family of $E_N \in \{-1, +1\}^N$ pseudorandom binary sequenc is the biggest j integer, for which it holds, that for every specification of length j exists an $E_N \in F$ which satisfies it.*

The chapter discusses also the linear complexity of the generator. It turns out, that it is not suitable for cryptographic use, because its linear complexity is low. With this result a tight connection with the linear shift registers is also discovered. This connection makes possible a very fast hardware implementation, and together with the good statistical properties it makes the generator an excellent choice for non-cryptographic applications. The results of the three last sections are my results and are contained in the papers [23] and [25]:

Definition 2.9. *Let us define the notion of comb polinomials as the $f(x) \in \mathbb{F}_q[x]$ polynomials of the form $f(x) = \sum_{i=0}^{d} a_i x^{2i+1}$.*

Theorem 2.2. *Let S be the set of the $f(x) \in \mathbb{F}_q$ comb pomials with degree at most d. Let us define the distinct $E_{q-1} = E_{q-1}(f) = \{e_1, \ldots, e_{q-1}\}$ sequences as in (2.3), and the $F = F(S)$ sequence family as in (2.5). If $d = o(q^{1/2})$ holds, then the F family of pseudorandom binary sequences possesses the srict avalanche property.*

Theorem 2.3. *Let S be set of the $f(x) \in \mathbb{F}_q$ comb pomials with degree at most d. Let us define the distinct $E_{q-1} = E_{q-1}(f) = \{e_1, \ldots, e_{q-1}\}$ sequences as in (2.3), and the $F = F(S)$ sequence family as in (2.5). If A is a specification of length $t \leq \lfloor \frac{d+1}{2} \rfloor$ and $G(A)$ denotes the subset of the $F = F(S)$ family satisfying A, then*

$$|G(A)| = \frac{|F|}{2^t}$$

holds.

Corollary 2.1. *The f-complexity of F is at least $\lfloor \frac{d+1}{2} \rfloor$.*

Definition 2.10. *Let $f(x)$ be, such that it satisfies the conditions of Theorem 2.1. Let the pseudorandom binary sequence be:*

$$e_n = \begin{cases} 1, & \text{if } \chi(f(\alpha^n)) = -1, \\ 0, & \text{otherwise.} \end{cases} \tag{2.6}$$

Definition 2.11. *The linear complexity of a sequence is the bitlength of the shortest linear feedback shift register generating it.*

Theorem 2.4. *The linear comlexity of the sequence given in Definition 2.10 is $\frac{k(d+1)}{2}$.*

The main topic of Chapter 4 is a new hash function. The chapter starts with an introduction to hash functions in general, defines the notion of hash function and the requirements regarding the cryptographic hash functions. Thereafter the predecessor of the new construction, which was implemented under the name Codefish, will be described ([10]). The cryptanalysis of this construction (more precisely of its modified special case used by the implementation) is also part of this chapter.

Thereafter follows the new construction and the theoretical results about it. The construction fixes the flaws of its predecessor ([6]) and it means an advance regarding the operand size. Theoretical considerations constantiate its preimage resistance, and one of its good statistical properties also will be proven. The investigations regarding the functions avalanche effect also take place here: although the version of the function used in the implementation does not possess the strict avalanche criterion, assymptotically it behaves very similar:

Definition 2.12 (UDHash)**.** *Let the polynomial* $f(\underline{X}) \in \mathbb{F}_q[X_1, \ldots, X_m]$ *be the form of*

$$f(\underline{X}) = b(X_1, \ldots, X_m) + a(X_1, \ldots, X_m),$$

where $a(\underline{X})$ *and* $b(\underline{X})$ *are homogeneous polynomials with degrees such that* $k = \deg a(\underline{X}) < \deg b(\underline{X}) = n$ *and* $\deg_{X_i} b(\underline{X}) = n$ *holds for every* $1 \leq i \leq m$*. Suppose furthermore, that there are* $1 \leq j_1 < j_2 \leq n$ *indicies, such that*

$$b_o(X_{j_1}, X_{j_2}) = b(0, \ldots, X_{j_1}, 0, \ldots, 0, X_{j_2}, 0, \ldots, 0)$$

binary form does not have multiple roots.

Theorem 2.5. *Let the* $f(\underline{X}) \in \mathbb{F}_q[X_1, \ldots, X_m]$ *polynomial such that it satisfies Definition 2.12. Let* $N(f, \gamma, q)$ *denote the number of the solutions of the* $f(x_1, \ldots, x_m) = \gamma$ *equation, where* $x_1, \ldots, x_m \in \mathbb{F}_q$*. In this case the following inequality holds:*

$$|N(f, \gamma, q) - q^{m-1}| \leq (n-1)(n-2)q^{m-3/2} + 5n^{13/3}q^{m-2}. \tag{2.7}$$

Furthermore, if $q > 15n^{13/3}$*, then*

$$|N(f, \gamma, q) - q^{m-1}| \leq (n-1)(n-2)q^{m-3/2} + (5n^2 + n + 1)q^{m-2}. \tag{2.8}$$

Theorem 2.6. *Let us define the* $f \in \mathbb{F}_{2^k}[x_1, \ldots, x_m]$ *polynomial, as* $f(x_1, \ldots, x_m) = \sum_{i=1}^{m} \alpha_i x_i^n + \sum_{i=1}^{m} \beta_i x_i$*, where* $n = 2^l + 1$ *such that* $(l, k) = 1$*. In this case*

$$(1 - q\varepsilon)^{m-1}(\frac{1}{q} - \varepsilon) \leq$$
$$P(f(x_1, \ldots, x_m) - f(x_1 + \delta_1, \ldots, x_m + \delta_m) = \gamma)$$
$$\leq (1 + q\varepsilon)^{m-1}(\frac{1}{q} + \varepsilon),$$

holds, where $0 \leq \varepsilon \leq nq^{-\frac{3}{2}}$*.*

The establishment of the functions preimage resistance is a joint work with Attila Bérczes and Attila Pethő and is contained in the paper [7]. The results regarding the avalanche criterion and the theorem about the corresponding assymptotic behavior are my results and are yet unpublished.

Chapter 5 is about the implementation of the mentioned hash function and the DESignIn authentication system. Our hash function is an iterative hash function and previously only the compression function was described. The parameter selection and the iteration method will be described in this section. Thereafter the specific implementation issuses, the choice of the finite field and the test results regarding the performance and the avalanche effect will be considered. Lastly, as a possible application area, the DESignIn authentication system will be described. The design considerations of the DESignIn are joint work with Andrea Huszti and Attila Pethő and are contained in the paper [26]. The test results in question are yet unpublished and they take place in the Appendices B and D.

In the case of most cryptographic primitives it is important, that one be able to compute them fast. In the case of hash functions it can also be desirable, that the fastest implementation of the function be relatively slow. The computational resources nowadays are cheap and scalable. This means that an adversary has greater power against fast hash functions. Thomas Roth broke passwords on wifi devices protected by a strong cryptographic hash function [1]. He used the Elastic Compute Cloud service of Amazon. It took 20 minutes and costed 28 cents per minute. The UDHash is advantageous also from this point of view, because even its fastest implementation is slower than the nowadays widespread hash functions.

Unfortunately the conditions of the theorem regarding the avalanche effect are too strict to use parameters satisfying them in the practical implementation. Thus, there were practical investigations regarding the avalanche effect.

The test results regarding the avalanche effect are in the Appendix B. Here under the distinct figures the parametrisation is given with the coefficients of the linear and nonlinear members and the exponent of the nonlinear members. The numbers 0-761 on the x-axis of the diagram stand for the distinct input bits, the numbering 0-243 of the y-axis belongs to the output bits. The z-axis in turn 0-1499 denotes the amount of the input samples. An (x,y,z) point on the diagram means, that the change of the x. input bit changed the y. output bit in the case of z samples.

It is easy to see, that in the case of these tests the points are in the neighbourhood of the $z = 750$ plane, that is the empiric probability is near $\frac{1}{2}$, the value expected by the avalanche effect. Thus, although the UDHash with the above described parametrisation does not possess the strict avalanche property, in practice it shows a very similar behavior to the avalanche effect.

Hash functions and pseudorandom number generators play crucial role in

numerous cryptographic protocols. The UDSignIn authentication system is a possible application area for the cryptographic primitives described in this dissertation.

The UDSignIn was designed to be a universal web-based authentication system. Its task is to replace the simple password based login. It offers a comfortable solution for the problem, that the secure passwords are usually hard to memorize, and nowadays an avarage user has more dozens of account on the web.

In the case of password authentication in order to achieve secrecy the users should choose distinct strong (i.e. hard to remember) password for each of their accounts. This usually leads to the use of weak passwords or matching passwords for distinct accounts or possibly the users simply write the passwords down. The replacement of the password authentication with the help of certificates not only increases the security of the system, but also means a more comfortable solution for the users.

The UDSignIn solves this problem with the use of a hardware security token. It uses asymmetric cryptography for authentication. It also utilises the already existent and widespread SSL technology. The technical description of the UD-Hash and the corresponding theoretical, practical and design considerations are contained in the paper [26].

Irodalomjegyzék

[1] Acm tech news. http://technews.acm.org/archives.cfm?fo=2011-01-jan/jan-14-2011.html#501867. 1, 2

[2] G.B. Agnew – R.C. Mullin – I.M. Onyszchuk – S.A. Vanstone: An implementation for a fast public-key cryptosystem. In *J. Cryptology*, 3. évf. (1991), 63–79. p.

[3] G.B. Agnew – R.C. Mullin – S.A. Vanstone: An implementation of elliptic curve cryptosystems over $\mathbb{F}_{2^{155}}$. In *IEEE J. Selected Areas in Comm.*, 11. évf. (1993) 5. sz., 804–813. p.

[4] Rudolf Ahlswede – Levon Khachatrian – Christian Mauduit – András Sárközy: A complexity measure for families of binary sequences. In *Period. Math. Hungar.*, 46. évf. (2003. Június) 2. sz., 107–118. p.

[5] Ágnes Andics: On the linear complexity of binary sequences. In *Ann. Univ. Sci. Budapest. Eötvös Sect. Math.*, 48. évf. (2005), 173–180. p.

[6] Jean-Philippe Aumasson: Cryptanalysis of a hash function based on norm form equations. In *Cryptologia*, 33. évf. (2009. Január), 12–15. p. ISSN 0161-1194.
URL `http://portal.acm.org/citation.cfm?id=1506456.1506458`. 4 p. 1, 2

[7] A. Bérczes – J. Folláth – A. Pethő: On a family of preimage-resistant functions. In *Tatra Mountains Mathematical Publications*, 47. évf. (2010), 1–13. p. 1, 2

[8] A. Bérczes – I. Járási: An application of index forms in cryptography. In *Periodica Math. Hungar.*, 58. évf. (2008), 35–45. p.

[9] A. Bérczes – J. Ködmön: Methods for the calculation of values of a norm form. In *Publ. Math. Debrecen*, 63. évf. (2003), 751–768. p.

[10] A. Bérczes – J. Ködmön – A. Pethő: A one-way function based on norm form equations. In *Periodica Mathematica Hungarica*, 49. évf. (2004), 1–13. p. 1, 2

[11] E. R. Berlekamp: Factoring polynomials over large finite fields. In *Math. Comp.*, 24. évf. (1970), 713–715. p.

[12] Emile Borel: *Leçons sur la théorie des fonctions*. Gauthier-Villars, 1950. ISBN 2-87647-086-1.

[13] Nina Brandstätter – Arne Winterhof: Linear complexity profile of binary sequences with small correlation measure. In *Period. Math. Hungar.*, 52. évf. (2006. Június) 2. sz., 1–8. p.

[14] J. Buchmann – S. Paulus: A one-way function based on ideal arithmetic in number fields. In *Lect. Notes Comput. Sci.*, 1294. évf. (1997), 385–394. p.

[15] A. Cafure – G. Matera: Improved explicit estimates on the number of solutions of equations over a finite field. In *Finite Fields Appl.*, 12. évf. (2006), 155–185. p.

[16] Julien Cassaigne – Christian Mauduit – András Sárközy: On finite pseudorandom binary sequences VII: The measures of pseudorandomness. In *Acta Arith.*, 103. évf. (2002) 2. sz., 97–118. p.

[17] Çetin K.Koç – Tolga Acar: Montgomery multiplication in $GF(2^k)$. In *Designs, Codes and Cryptography*, 14. évf. (1998) 1. sz., 57–69. p.

[18] L. R. Chao – Y. C. Lin: Associative one-way function and its significances to cryptographics. In *In. J. Inf. Manage. Sci.*, 5. évf. (1994), 53–59. p.

[19] Robert Coulter – Marie Henderson: A note on the roots of trinomials over a finite field. In *Bull. Austral. Math. Soc.*, 69. évf. (2004), 429–432. p.

[20] Joan Daemen – Vincent Rijmen: The block cipher rijndael. In *Proceedings of the The International Conference on Smart Card Research and Applications* (konferenciaanyag). London, UK, 2000, Springer-Verlag, 277–284. p. ISBN 3-540-67923-5.
URL `http://portal.acm.org/citation.cfm?id=646692.759487`. 8 p.

[21] Don Davis – Ross Ihaka – Philip Fenstermacher: Cryptographic randomness from air turbulence in disk drives. In *Proceedings of the 14th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '94 konferenciasorozat. London, UK, 1994, Springer-Verlag, 114–120. p. ISBN 3-540-58333-5.
URL `http://portal.acm.org/citation.cfm?id=646759.705839`. 7 p.

[22] Whitfield Diffie – Martin Helman: New directions in cryptography. In *IEEE Transactions on Information Theory*, IT-22. évf. (1976), 644–654. p.

[23] János Folláth: Construction of pseudorandom binary sequences I. In *Period. Math. Hungar.*, 57. évf. 1. sz., 73–81. p. 1, 2

[24] János Folláth: Álvéletlen számok generálása és szerepük a kriptográfiában, 2005.

[25] János Folláth: Construction of pseudorandom binary sequences II. In *Periodica Mathematica Hungarica*, 60. évf. (2010) 2. sz. 1, 2

[26] János Folláth – Andrea Huszti – Attila Pethő: Asymmetric authentication system. In *Proceedings of ICAI'07 7th International Conference on Applied Informatics* (konferenciaanyag). 1, 2

[27] E. Fouvry – C. Mauduit: Méthodes de crible et fonctions sommes des chiffres. In *Acta Arith.*, 77. évf. (1996) 4. sz., 339–351. p.

[28] E. Fouvry – C. Mauduit: Sommes des chiffres et nombres presque premiers. In *Math. Ann.*, 305. évf. (1996) 3. sz., 571–599. p.

[29] Róbert Freud – Edit Gyarmati: *Számelmélet.* Nemzeti Tankönyvkiadó, 2000.

[30] John Friedlander – Henryk Iwaniec: Estimates for character sums. In *Proc. Amer. Math. Soc.*, 119. évf. (1993), 365–372. p.

[31] A. O. Gelfond: Sur les nombres qui ont des propriétés additives et multiplicatives données. In *Acta Arith.*, 13. évf. (1967/1968), 259–265. p.

[32] O. Goldreich – L. Levin – N. Nisan: On constructiong 1-1 one-way functions. In *Electronic colloquium on computational complexity*, TR-95-029. évf. (1995).

[33] Oded Goldreich: *Foundations of Cryptography*. 1. köt. Cambridge Univrsity Press, 2001.

[34] Louis Goubin – Christian Mauduit – András Sárközy: Construction of large families of pseudorandom binary sequences. In *Journal of Number Theory*, 106. évf. (2004) 1. sz., 56–69. p. 1, 2

[35] Great internet mersenne prime search (gimps). http://www.mersenne.org/.

[36] K. Gyarmati: On a family of pseudorandom binary sequences. In *Period. Math. Hungar.*, 49. évf. (2004), 45–63. p. 1, 2

[37] K. Gyarmati: *General Theory of Information Transfer and Combinatorics*. Lecture Notes in Comp. Sci. sorozat. On a fast version of a pseudorandom generator fejezet. Springer Verlag, Heidelberg, 2006, 326–342. p. 1, 2

[38] Katalin Gyarmati: Concatenation of pseudorandom binary sequences. In *Period. Math. Hungar.*, 58. évf. (2009) 1. sz., 99–120. p.

[39] Katalin Gyarmati – András Sárközy – Attila Pethő: On linear recursion and pseudorandomness. In *Acta Arith.*, 118. évf. (2005) 4. sz., 359–374. p. 1, 2

[40] M.A. Hasan – M.Z. Wang – V.K. Bhargava: A modified massey-omura parallel multiplier for a class of finite fields. In *IEEE Trans. Computers*, 42. évf. (1993) 10. sz., 1278–1280. p.

[41] L. A. Hemanspaandra – J. Rothe: Creating strong, total, commutative, associative one-way function in complexity theory. In *J. Comput. Syst. Sci.*, 58. évf. (1999), 648–659. p.

[42] Tamás Herendi: *Linear Recurring Sequences*. Phd értekezés (Debreceni Egyetem). 2002.

[43] Tamás Herendi: Uniform distribution of linear recurring sequences modulo prime powers. In *Finite Fields and Their Applications*, 10. évf. (2004. Január) 1. sz., 1–23. p.

[44] Jeffrey Hoffstein – Daniel Lieman: *Cryptography and Computational Number Theory*. Progress in Computer Science and Applied Logic sorozat, 20. köt. The Distribution of the Quadratic Symbol in Function Fields and a Faster Mathematical Stream Cipher fejezet. Birkhäuser Verlag, 2001, 59–68. p.

[45] Donald E. Knuth: *The Art of Computer Programming, Volume II: Seminumerical Algorithms, 2nd Edition*. Addison-Wesley, 1981. ISBN 0-201-03822-6.

[46] S. Lang – A. Weil: The number of points of varieties in finite fields. In *Amer. J. Math.*, 76. évf. (1954), 819–827. p.

[47] A.K. Lenstra – H.W. Lenstra Jr. – L. Lovász: Factoring polynomials with rational coefficients. In *Math. Ann.*, 261. évf. (1982), 515–534. p.

[48] Rudolf Lidl – Harald Niederreiter: *Finite Fields*. Encyclopedia of Mathematics sorozat, 20. köt. Cambridge University Press, 1997.

[49] H. Liu: A family of pseudorandom binary sequences constructed by the multiplicative inverse. In *Acta Arithmetica*, 130. évf. (2007) 2. sz., 167–180. p. 1, 2

[50] Florence Jessie Collinson MacWilliams – Neil James Alexander Sloane: *The Theory of Error-Correcting Codes*. North-Holland Mathematical Library sorozat, 16. köt. North-Holland Publishing Company, 1977.

[51] J.L. Massey – J.K. Omura: Computational method and apparatus for finite field arithmetic. US Patent No. 4,587,627„ 1986.

[52] C. Mauduit – J. Rivat – A. Sárközy: Construction of pseudorandom binary sequences using additive characters. In *Monatsh. Math.*, 141. évf. (2004), 197–208. p.

[53] C. Mauduit – A. Sárközy: On the arithmetic structure of sets characterized by sum of digits properties. In *J. Number Theory*, 61. évf. (1996) 1. sz., 25–38. p.

[54] C. Mauduit – A. Sárközy: On the arithmetic structure of the integers whose sum of digits is fixed. In *Acta Arith.*, 81. évf. (1997) 2. sz., 145–173. p.

[55] Christian MAUDUIT – András SÁRKÖZY: On finite pseudorandom binary sequences I: Measure of pseudorandomness, the Legendre symbol. In *Acta Arith.*, 82. évf. (1997) 4. sz., 365–377. p. 1, 1, 2, 2

[56] Christian MAUDUIT – András SÁRKÖZY: Construction of pseudorandom binary sequences by using the multiplicative inverse. In *Acta Math. Hungar.*, 108. évf. (2005) 3. sz., 239–252. p. 1, 2

[57] Alfred J. MENEZES – Paul C. van OORSCHOT – Scott A. VANSTONE: *Handbook of Applied Cryptography*. CRC Press, 2001.

[58] R. C. MERKLE: A fast software one-way hash function. In *J. Cryptology*, 3. évf. (1990), 43–48. p.

[59] Ivan NIVEN – H. S. ZUCKERMAN: On the definition of normal numbers. In *Pacific J. Math.*, 1. évf. (1951) 1. sz., 103–109. p.

[60] G. I. PERELMUTER: On certain character sums. In *Uspehi Mat. Nauk*, 18. évf. (1963) 2. sz., 145–149. p.

[61] Arash REYHANIMASOLEH – Anwar HASAN: Fast normal basis multiplication general purpose processors. In *IEEE Transactions on Computers*, 52. évf. (2003) 11. sz., 1379–1390. p.

[62] R. L. RIVEST – A. SHAMIR – L. ADLEMAN: A method for obtaining digital signatures and public-key cryptosystems. In *Commun. ACM*, 21. évf. (1978. Február), 120–126. p. ISSN 0001-0782.
URL `http://doi.acm.org/10.1145/359340.359342`. 7 p.

[63] András SÁRKÖZY: A finite pseudorandom binary sequence. In *Studia Sci. Math. Hungar.*, 38. évf. (2001), 377–384. p.

[64] Wolfgang SCHMIDT: A lower bound for the number of solutions of equations over finite fields. In *J. Number Theory*, 6. évf. (1974), 448–480. p.

[65] Wolfgang SCHMIDT: *Equations over Finite Fields. An Elementary Approach*. Lecture Notes in Mathematics sorozat, 536. köt. Springer-Verlag, 1976.

[66] Secure socket layer (ssl). http://wp.netscape.com/eng/ssl3/.

[67] I. Shparlinski: *Number theoretic methods in cryptography.* Progress in Computer Science and Applied Logic sorozat, 17. köt. Birkhäuser Verlag, Basel, 1999.

[68] Douglas R. Stinson: *Cryptography - Theory and Practice.* Discrete Mathematics and its Applications sorozat. Chapman & Hall/CRC, 2006.

[69] Q. Sun: A kind of trap-door one-way function over algebraic integers. In *J. Sichuan Univ., Nat. Sci. Ed.*, 2. évf. (1986), 22–27. p.

[70] B. Sunar – C.K. Koc: An efficient optimal normal basis type ii multiplier. In *IEEE Trans. Computers*, 50. évf. (2001) 1. sz., 83–88. p.

[71] Aimo Tietäväinen: *Algebra, some current trends.* Lecture Notes in Math. sorozat, 1352. köt. Incomplete sums and two applications of Deligne's result fejezet. Springer Verlag, New York, 1988, 190–205. p.

[72] Viktória Tóth: Collision and avalanche effect in families of pseudorandom binary sequences. In *Period. Math. Hungar.*, 55. évf. (2007. November) 2. sz., 185–196. p.

[73] Ivan Matveyevich Vinogradov: *Elements of Number Theory.* Dover Publications, 2003.

[74] Joachim von zur Gathen – Jürgen Gerhard: *Modern Computer Algebra.* Cambridge University Press, 1999.

A. Tesztkonfiguráció

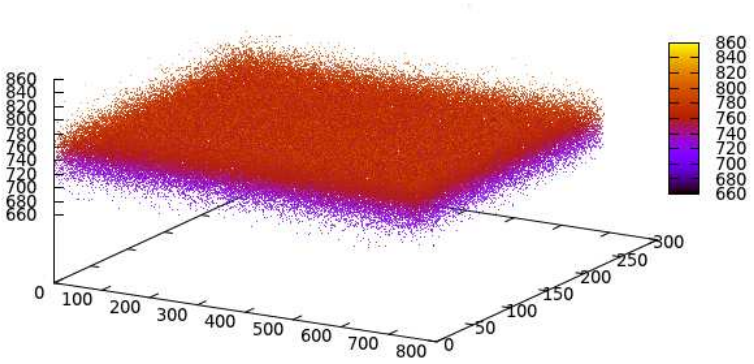
A.1. Hardver

```
vendor_id       : GenuineIntel
cpu family      : 6
model           : 23
model name      : Intel(R) Celeron(R) CPU        E3400  @ 2.60GHz
stepping        : 10
cpu MHz         : 2600.947
cache size      : 1024 KB
cpu cores       : 2
fpu             : yes
fpu_exception   : yes
cpuid level     : 13
wp              : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr
                  pge mca cmov pat pse36 clflush dts acpi mmx fxsr
                  sse sse2 ss ht tm pbe syscall nx lm constant_tsc
                  arch_perfmon pebs bts rep_good nopl aperfmperf
                  pni dtes64 monitor ds_cpl vmx est tm2 ssse3 cx16
                  xtpr pdcm xsave lahf_lm dts tpr_shadow vnmi
                  flexpriority
bogomips        : 5201.89
clflush size    : 64
cache_alignment : 64
address sizes   : 36 bits physical, 48 bits virtual
MemTotal        : 2021360 kB
```

A.2. Szoftver

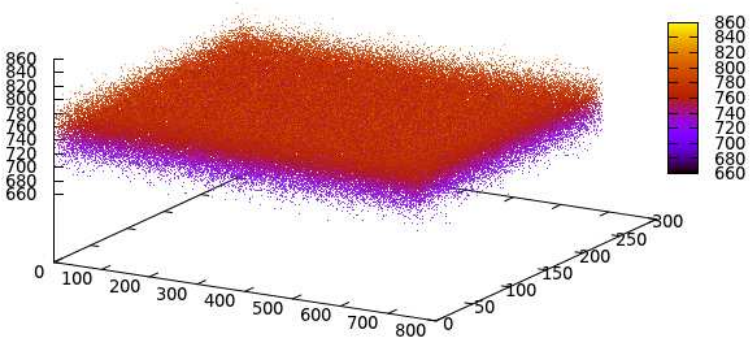
Szoftver	Verzió
Ubuntu	11.04
gcc	4.5.2
GNU MP	4.3.2
Crypto++	5.6.0

B. Lavinahatás tesztek



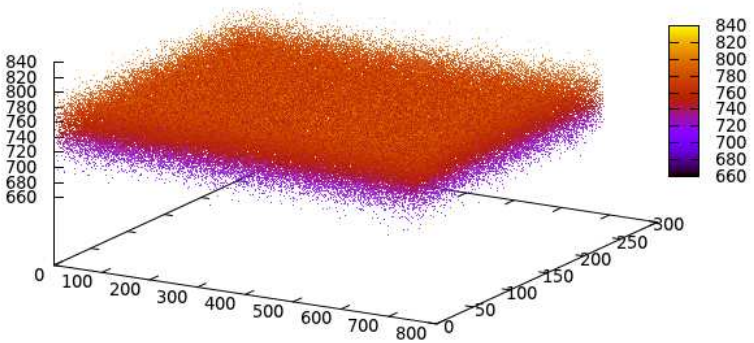
B.1. ábra. Alap teszteredmények

Kitevő: 286295073
Az összetett tag együtthatói:
3d1b58ba507ed7ab625558ec238e1f2974b0dc5119495cff327b23c6643c9869,
519b500d431bd7b76b68079a4e6afb667fdcc2331befd79f3352255a109cf92e,
3a95f874081386412ca886110836c40e189a769b54e49eb479838cb24353d0cd
A lineáris tag együtthatói:
1190cde766ef438d4db127f80216231b515f007c5bd062c241b71efb79e2a9e3,
6763845e75a2a8d4721da3172443a858436c6125628c895d7c83e458257130a3,
440badfc05072367614fd4a1419ac24122221a704516dde97c3dbd3d737b8ddc
Kitevő: 286295073
Az összetett tag együtthatói:
680c1b62443d8e597a1c574377d02f4866613afa24a7c25e0eed54217fcf7bf2,



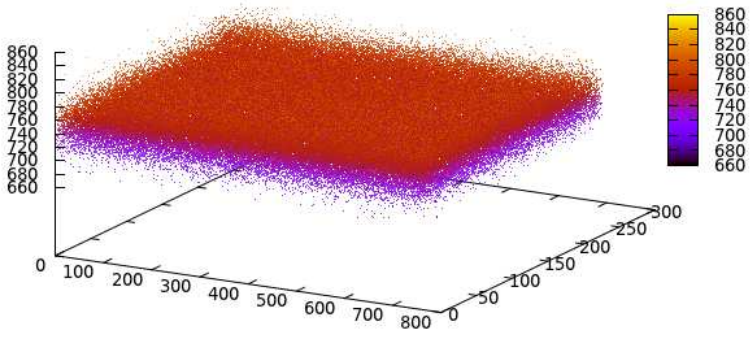
B.2. ábra. Teszteredmények más együtthatókkal

6d5e56326881ca2d1642e53a02208f331e81e2ee73333b123d5c5c2d37cd332f,
2df5b11c2fdc7fd51ad7b7c6115a9ce6651e5e3b53fe40b97e8820947c2e42da
A lineáris tag együtthatói:
57cffdde091852a979ef5e9e462d4a4336cc7f001ad4086200c828696a5674f1,
1c1463c6023ee43c7e674f6b4b72653c27954eaa4aaa3cd33c9179df629e2171,
6453d5b017a483cb6a9868e9700f352168ad2b6a337dbb410b69b04a461f650f



B.3. ábra. Teszteredmények kis kitevővel

Kitevő: 127
Az összetett tag együtthatói:
3d1b58ba507ed7ab625558ec238e1f2974b0dc5119495cff327b23c6643c9869,
519b500d431bd7b76b68079a4e6afb667fdcc2331befd79f3352255a109cf92e,
3a95f874081386412ca886110836c40e189a769b54e49eb479838cb24353d0cd
A lineáris tag együtthatói:
1190cde766ef438d4db127f80216231b515f007c5bd062c241b71efb79e2a9e3,
6763845e75a2a8d4721da3172443a858436c6125628c895d7c83e458257130a3,
440badfc05072367614fd4a1419ac24122221a704516dde97c3dbd3d737b8ddc



B.4. ábra. Teszteredmények alacsony súlyú kitevővel

Kitevő: 268435459 ($2^{28} + 2^1 + 2^0$)
Az összetett tag együtthatói:
3d1b58ba507ed7ab625558ec238e1f2974b0dc5119495cff327b23c6643c9869,
519b500d431bd7b76b68079a4e6afb667fdcc2331befd79f3352255a109cf92e,
3a95f874081386412ca886110836c40e189a769b54e49eb479838cb24353d0cd
A lineáris tag együtthatói:
1190cde766ef438d4db127f80216231b515f007c5bd062c241b71efb79e2a9e3,
6763845e75a2a8d4721da3172443a858436c6125628c895d7c83e458257130a3,
440badfc05072367614fd4a1419ac24122221a704516dde97c3dbd3d737b8ddc

C. Sebességtesztek UDHash függvényei

C.1. UDHash254

Kitevő:

12

Az összetett tag együtthatói:

3d1b58ba507ed7ab625558ec238e1f2974b0dc5119495cff327b23c6643c9869,
519b500d431bd7b76b68079a4e6afb667fdcc2331befd79f3352255a109cf92e,
3a95f874081386412ca886110836c40e189a769b54e49eb479838cb24353d0cd

A lineáris tag együtthatói:

1190cde766ef438d4db127f80216231b515f007c5bd062c241b71efb79e2a9e3,
6763845e75a2a8d4721da3172443a858436c6125628c895d7c83e458257130a3,
440badfc05072367614fd4a1419ac24122221a704516dde97c3dbd3d737b8ddc

C.2. UDHash509

Kitevő:

12

Az összetett tag együtthatói:

1190cde766ef438d4db127f80216231b515f007c5bd062c241b71efb79e2a9e33
d1b58ba507ed7ab625558ec238e1f2974b0dc5119495cff327b23c6643c9869,
440badfc05072367614fd4a1419ac24122221a704516dde97c3dbd3d737b8ddc3
a95f874081386412ca886110836c40e189a769b54e49eb479838cb24353d0cd,
15b5af5c741226bb235ba86147398c89393865751cf10fd823f9c13c649bb77c5
20eedd1374a3fe675c6c33a12e685fb3dc240fb1ba026fa684a481a579478fe

A lineáris tag együtthatói:

6763845e75a2a8d4721da3172443a858436c6125628c895d7c83e458257130a35
19b500d431bd7b76b68079a4e6afb667fdcc2331befd79f3352255a109cf92e,
38437fdb7644a45c4b588f54542289ec2cd89a3257e4ccaf2a487cb01d4ed43b3
855585c70a64e2a2d517796580bd78f2463b9ea5e884adc77465f017724c67e,
06b9476442c296bd5f5e7fd0098a3148100f8fca6590700b1f48eaa11381823a2
5a70bf71dbabf00310c50b35ff87e057e0c57b177ae35eb10233c993f6ab60f

C.3. UDHash256

Modulus:

628503907844138419186562739485275657779508862386893721474692236956
01627048263

Kitevő:

31378397166559283966765678011653532519 3

Az összetett tag együtthatói:

616309944986795191724102638347419151468155942153823823366260288647
93279450618,
592023207485630449627802331363236261768565619144303109483719501936
83290073201,
188959985259665703319191147102059767066184752960342748287576331774
77018717100

A lineáris tag együtthatói:

```
188013062533933815456187202687414331943249015883608319900568154091
73708257948,
492050709691232541497239841724811202778208114412962566757854714921
77716203125 9,
266899935942294966963389662896300056882392916297827041542384623711
321522020864
```

C.4. UDHash512

Modulus:

```
133478789543240246517116323734764591884281378818183507238665895291
552649334060796444394418488016862952802189317849302962159780992891
735352178255032226627228 1
```

Kitevő:

```
111014492188910947555385041036688199156943917908453052200992005575
727851660423
```

Az összetett tag együtthatói:

```
132676712675572896158444304737378609350249409211650836653473960506
423942152711717821090055542067039261190771708076263565960324816071
022659974703106215015 56,
103872745013076925645389271273070726734975631558612552837500952206
995956662303038885160563331097994241537529525195701833473734458710
652713374387269576291 58,
856926752093821826249200817054868331971866442448138071078954740205
864045948664742215074151408487318632640247217873934926478637674330
831735032505379799084 7
```

A lineáris tag együtthatói:

```
166023202398036249765559080093058335012423535990578413377113805080
951596890276819993045743652117163294204753520471263301114058996729
2643616109292525964756,
310017269523333243359762637274163049508884541180672327806590158988
```

```
085273256214451024050621432497214755406010180048968763682391327973
894819714050552155859 9,
123733747304399180791823208711197904759064144114306956412667681673
132280085439577466844902890978619144292692380712862285347513780623
36304877052322618828459
```

D. Sebességtesztek

Hash	Megabájt/másodperc
UDHash254 (páros karakterisztika)	0.019
UDHash509 (páros karakterisztika)	0.017
UDHash256 (páratlan karakterisztika)	1.06
UDHash512 (páratlan karakterisztika)	0.44
CRC32	441
Adler32	1191
MD5	420
SHA-1	223
SHA-256	160
SHA-512	197
Tiger	356
Whirpool	85
RIPEMD-160	171
RIPEMD-320	186
RIPEMD-128	256
RIPEMD-256	278

E. Publikációs jegyzék

E.1. Publikációk

1. J. Folláth, A. Huszti, A. Pethő, DeSignIn Asymmetric Authentication System, Proceedings of ICAI'07 7th International Conference on Applied Informatics, pp. 53-61.

2. J. Folláth, Construction of Pseudorandom Binary Sequences Using Additive Characters Over GF(2^k), Periodica Mathematica Hungarica Vol. 57 (1), 2008, pp. 73-81.

3. A. Bérczes, J. Folláth, A. Pethő, On a Family of Preimage-Resistant Functions, Tatra Mountains Mathematical Publications, 47, 1-13 (2010)

4. J. Folláth, Construction of Pseudorandom Binary Sequences Using Additive Characters Over GF(2^k) II., Periodica Mathematica Hungarica, Volume 60, Number 2, 2010, pp. 127-135

5. L. Aszalós, N. Bátfai, L. Csirmaz, J. Folláth, T. Herendi, T. Kovács, A. Pethő, P. Varga, Secure Utilisation of Local and Regional Data Assets through Mobile Environments, Proceedings of ICAI'10 8th International Conference on Applied Informatics, beküldve

6. J. Folláth, A. Huszti, A. Pethő, Informatikai biztonság és kriptográfia, Kempelen Farkas Digitális Tankönyvtár, megjelenés alatt

E.2. Szoftverek

- DESignIn bejelentkező rendszer
  http://www.inf.unideb.hu/designin/signature/login.php

- A 2. cikkben ismertetett álvéletlenszám generátor implementációja
  http://www.inf.unideb.hu/~follathj/downloads/gf2k-dev_1.0.tar.gz

- A 3. cikkben ismertetett hash függvény implementációja
  http://www.inf.unideb.hu/~follathj/downloads/udhash.tar.gz

F. Előadások

1. DeSignIn Asymmetric Authentication System, *NyírCrypt Central European Conference on Cryptography*, Nyíregyháza, Magyarország, 2006
2. DeSignIn Asymmetric Authentication System, *PhD hallgatók informatikai konferenciája*, Szeged, Magyarország, 2006.
3. Pseudorandom Sequence Construction over GF(2^k), *Egri diofantikus és kriptográfiai napok*, Eger, Magyarország, 2007.
4. Pseudorandom Sequence Construction over GF(2^k), *Conference on Uniform Distribution*, Marseilles, Franciaország, 2007.
5. Pseudorandom Sequence Construction over GF(2^k), *Cenral European Conference on Cryptography*, Graz, Ausztria, 2008.
6. Pseudorandom Sequence Construction over GF(2^k), *Soproni diofantikus és kriptográfiai napok*, Sopron, Magyarország, 2007.
7. On a family of collision-free functions, *Central European Conference on Cryptography*, Trebic, Csehország, 2009.
8. Pseudorandom Binary Sequences Over Fields of Characteristic 2, *Seminar on Number Theory*, Zágráb, Horvátország, 2009
9. Pseudorandom Binary Sequences Over Fields of Characteristic 2, *Debreceni diofantikus és kriptográfiai napok*, Debrecen, Magyarország, 2009.
10. Notes on a collision-resistant hash function, *8th International Conference on Applied Informatics*, Eger, Magyarország 2010.
11. Secure Utilization of Local and Regional Data Assets Through Mobile Environments *8th International Conference on Applied Informatics*, Eger, Magyarország 2010.
12. Notes on a Family of Preimage-Resistant Functions *10th Central European Conference on Cryptology*, Bedlewo, Lengyelország, 2010.

13. Notes on a Family of Preimage-Resistant Functions, *2nd International Conference on Uniform Distribution Theory*, Strobl, Ausztria, 2010.

14. Notes on a Family of Preimage-Resistant Functions, *Number Theory and its Applications*, Debrecen, Magyarország, 2010.

15. Kriptográfiai álvéletlenszám generátorok, hash függvények és alkalmazásaik, *13. Gyires Béla Informatikai Nap*, Debrecen, Magyarország, 2010.

16. Notes on a Family of Preimage-Resistant Functions, *11th Central European Conference on Cryptology*, Debrecen, Magyarország, 2011.