Kako sakriti sliku?

Franka Miriam Brueckler, *CoolMath*, 2. *veljače* 2011.

Sheme praga (*treshold schemes*)

Definicija

(t, n)**-shema praga** je metoda podjele tajne na n učesnika tako da bilo kojih t od njih mogu odrediti tajnu, ali bilo kojih $t-1$ (ili manje) njih ne mogu dobiti nikakvu informaciju o tajni na osnovu dijelova koje posjeduju.

Pojam su 1979. uveli (nezavisno jedan od drugog) američki kriptograf i profesor matematike **George Blakley** i hebrejski kriptograf **Adi Shamir**. Shamir je poznat i kao jedan od suotkrivača RSA-algoritma za šifriranje, koji je danas standard za elektronske transakcije.

Primjerice:

- $(2, 3)$-shema praga dijeli tajnu na tri učesnika tako da nijedan od njih sam ne može iz svog dijela shvatiti o čemu je riječ.

Primjerice:

- $(2, 3)$-shema praga dijeli tajnu na tri učesnika tako da nijedan od njih sam ne može iz svog dijela shvatiti o čemu je riječ.
- $(3, 10)$-shema praga dijeli tajnu na deset učesnika tako da nijedan od njih sam niti u paru s nekim drugim ne može iz svojih dijelova rekonstruirati tajnu.

Primjerice:

- $(2,3)$-shema praga dijeli tajnu na tri učesnika tako da nijedan od njih sam ne može iz svog dijela shvatiti o čemu je riječ.
- $(3,10)$-shema praga dijeli tajnu na deset učesnika tako da nijedan od njih sam niti u paru s nekim drugim ne može iz svojih dijelova rekonstruirati tajnu.

Naravno, mora postojati i osoba koja želi tajnu raspodijeliti na neke učesnike. Ta se osoba u literaturi zove *dealer D*. On će dakle svakom učesniku (na siguran način) dati dio informacije o tajni, konstruiran tako da se potpuna informacija o tajni podijeli na n dijelova, takvih da bilo kojih t njih omogućuje rekonstrukciju tajne, a nikoji manji broj ne. Sigurnost sheme ne smije ovisiti o nekoj računskoj pretpostavci, tj. — bar u teoriji — čak ni uz beskonačno jaka računala nikojih $t-1$ ili manje učesnika ne bi smjeli moći rekonstruirati tajnu.

(n, n)-sheme praga

Pretpostavimo da je tajna niz b binarnih znamenki (bitova). *Dealer* ju želi raspodijeliti na n dijelova tako da samo svi skupa omogućuju saznavanje cijelog niza.

[1] $0 \oplus 1 = 1 \oplus 0 = 1$, $0 \oplus 0 = 1 \oplus 1 = 1$.

(n, n)-sheme praga

Pretpostavimo da je tajna niz b binarnih znamenki (bitova). *Dealer* ju želi raspodijeliti na n dijelova tako da samo svi skupa omogućuju saznavanje cijelog niza. To može učiniti tako da generira $n-1$ slučajan binarni broj iste duljine kao što je b. Prvih $n-1$ učesnika će dobiti po jedan od tih slučajnih binarnih brojeva, a zadnji će dobiti broj koji je nim-zbroj[1] od b i svih tih brojeva.

[1] $0 \oplus 1 = 1 \oplus 0 = 1$, $0 \oplus 0 = 1 \oplus 1 = 1$.

(n, n)-sheme praga

Pretpostavimo da je tajna niz b binarnih znamenki (bitova). *Dealer* ju želi raspodijeliti na n dijelova tako da samo svi skupa omogućuju saznavanje cijelog niza. To može učiniti tako da generira $n-1$ slučajan binarni broj iste duljine kao što je b. Prvih $n-1$ učesnika će dobiti po jedan od tih slučajnih binarnih brojeva, a zadnji će dobiti broj koji je nim-zbroj[1] od b i svih tih brojeva.Tajni niz b se može jednostavno rekonstruirati tako da se nim-zbroje svi brojevi koje su dobili učesnici.

[1] $0 \oplus 1 = 1 \oplus 0 = 1$, $0 \oplus 0 = 1 \oplus 1 = 1$.

Primjer.

Neka je $b = 01010111$ *i želimo ga raspodijeliti na* $n = 3$ *učesnika. Prvi će dobiti slučajni broj* b_1 *duljine* 8*, recimo* 01111000*, drugi isto tako* $b_2 = 11011001$*, a treći dobije* $b_3 = b \oplus b_1 \oplus b_2 = 11110110$*.*

Primjer.

Neka je $b = 01010111$ *i želimo ga raspodijeliti na* $n = 3$ *učesnika. Prvi će dobiti slučajni broj* b_1 *duljine* 8, *recimo* 01111000, *drugi isto tako* $b_2 = 11011001$, *a treći dobije* $b_3 = b \oplus b_1 \oplus b_2 = 11110110$.
Rekonstrukcija:
$b_1 \oplus b_2 \oplus b_3 = 01111000 \oplus 11011001 \oplus 11110110 = 01010111 = b$.

Primjer.

Neka je $b = 01010111$ *i želimo ga raspodijeliti na* $n = 3$ *učesnika. Prvi će dobiti slučajni broj* b_1 *duljine* 8*, recimo* 01111000*, drugi isto tako* $b_2 = 11011001$*, a treći dobije* $b_3 = b \oplus b_1 \oplus b_2 = 11110110$*.*
Rekonstrukcija:
$b_1 \oplus b_2 \oplus b_3 = 01111000 \oplus 11011001 \oplus 11110110 = 01010111 = b$*.*

Zadatak

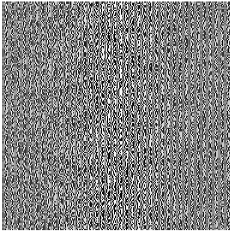
Možete li smisliti (n, n)-shemu praga za slučaj da je tajna općenit broj, bez da ga se prevodi u binarni?

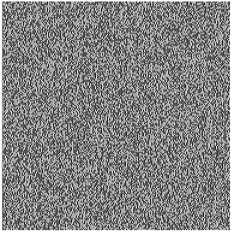
Vizualna kriptografija

Kriptografija se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati.
Kriptoanaliza ili dekriptiranje se bavi proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja ključa. Kriptologija obuhvaća kriptografiju i kriptoanalizu.[a]

Vizualna kriptografija

Kriptografija se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati. **Kriptoanaliza** ili dekriptiranje se bavi proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja ključa. Kriptologija obuhvaća kriptografiju i kriptoanalizu.[a] **Vizualnu kriptografiju** uveli su Adi Shamir i Moni Naor (izraelski informatičar) 1994. Radi se o metodi kojom se tajna slika (koja naravno može sadržavati i tekst) šifrira tako da se dešifriranje ne provodi, kao uobičajeno, računske, nego putem ljudskog vida.

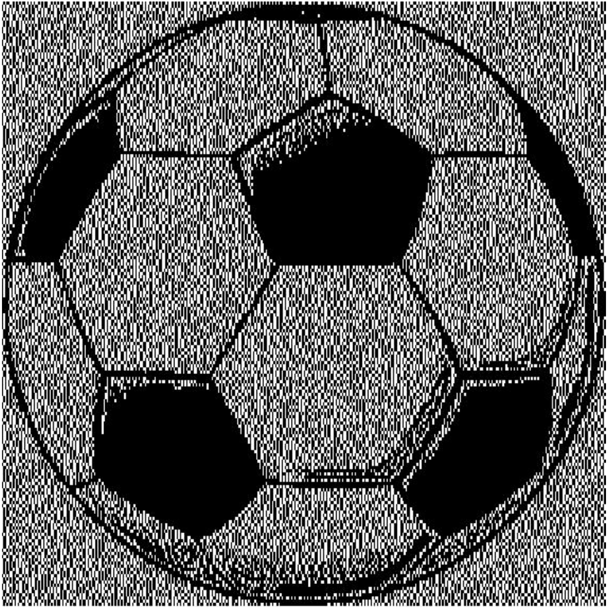




---

[a] A. Dujella, Kriptografija, `http://web.math.hr/~duje/kript/osnovni.html`.

Kako sakriti sliku?



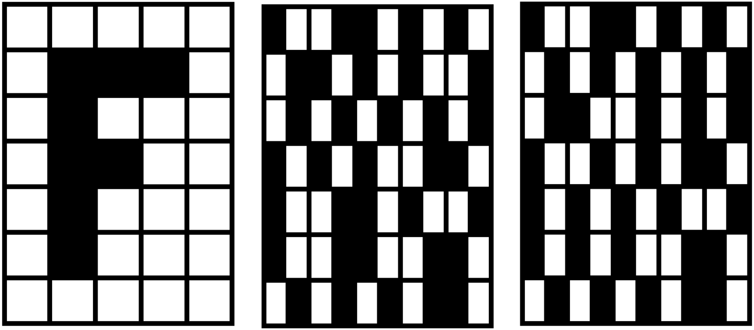
Konstrukcija vizualne $(2,2)$-sheme praga

Pretpostavimo da je tajna crno-bijela rasterska slika. Podijelite se u trojke. Trebat će vam i po jedan novčić. Jedan član je *dealer*; on neka nacrta „tajnu” rastersku sliku na papiru s kvadratićima.

Konstrukcija vizualne $(2,2)$-sheme praga

Pretpostavimo da je tajna crno-bijela rasterska slika. Podijelite se u trojke. Trebat će vam i po jedan novčić. Jedan član je *dealer*; on neka nacrta „tajnu" rastersku sliku na papiru s kvadratićima. Temeljem te slike ostalo dvoje će konstruirati dvije folije koje tek kad se preklope otkrivaju stvarnu sliku.
Obzirom da je slika crno-bijela, na folijama će biti raster s crnim i prozirnim „pikselima". Vaše folije već sadrže prikladan prazan raster. Podebljano su zaokruena po dva polja koja odgovaraju ukupno po jednom pikselu originalne slike.

Kako sakriti sliku?

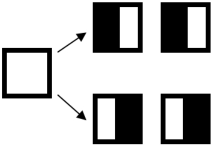


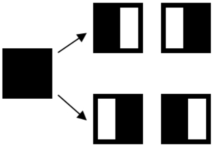
Šifriranje bijelog piksela

Bacite novčić. Ako padne pismo, na obje folije zacrnite lijevu polovinu kvadratića, a ako padne glava desnu.

Šifriranje crnog piksela

Bacite novčić. Ako padne pismo, prvi od vas zacrnjuje lijevu, a drugi desnu polovinu kvadratića na svojoj foliji. Ako padne glava, obrnuto.





Sigurnost? Problemi?

Zamisli da gledaš određeni piksel u svojoj foliji. On je pola crn, a pola bijel (proziran). Obje moguće varijante (koji je lijevi, koji je desni) su jednako vjerojatne, neovisno o tome je li originalni piksel u tajnoj slici crni ili bijeli. Dakle, tvoja folija ti ne daje nikakav „hint” o tome kakva je originalna slika.

Sigurnost? Problemi?

Zamisli da gledaš određeni piksel u svojoj foliji. On je pola crn, a pola bijel (proziran). Obje moguće varijante (koji je lijevi, koji je desni) su jednako vjerojatne, neovisno o tome je li originalni piksel u tajnoj slici crni ili bijeli. Dakle, tvoja folija ti ne daje nikakav „hint” o tome kakva je originalna slika.
Zbog toga što pri preklapanju originalni bijeli pikseli budu pola crni („sivi”), imamo 50%-tni gubitak kontrasta, što može otežati dešifriranje. Uz to, folije je teško pravilno poravnati i lako se miču, a pri printanju se i malo rastegnu. Općenito, metoda najbolje funkcionira sa slikama s relativno malo relativno velikih piksela.

Malo o vizualnim $(2, n)$-shemama praga

Svakom originalnom pikselu na folijama odgovara neki broj m podpiksela; taj se broj zove ekspanzijom piksela (za opisanu $(2, 2)$-shemu je $m = 2$).
Da lakše opišemo metodu, crne podpiksele ćemo označiti s 1, a bijele (prozirne) s 0. Tada svakom originalnom pikselu na svakoj foliji odgovara m-znamenkasti binarni broj koji kaže kako trebaju biti obojani podpikseli na toj foliji.

Krećemo od dviju matrica M_0 i M_1 s po n redaka i m stupaca. Matricu M_0 koristimo za šifriranje bijelog, a M_1 za šifriranje crnog originalnog piksela. Obje te matrice sastoje se od nula i jedinica.

Primjer.

$(2,4)$-*shema praga s ekspanzijom* $m = 6$

$$M_0 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}, \quad M_1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Na slučajan način odaberemo jednu od mogućih $m!$ permutacija skupa $\{1, 2, \ldots, m\}$.

Na slučajan način odaberemo jednu od mogućih $m!$ permutacija skupa $\{1, 2, \ldots, m\}$.U odgovarajućoj matrici u skladu s tom permutacijom promijenimo poredak stupaca. Pojedini retci tako dobivene matrice koriste se za kodiranje piksela na pojedinim folijama.

Primjer.

(2, 3)*-shema praga s ekspanzijom* $m = 3$

$$M_0 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad M_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Imamo $3! = 6$ *mogućih permutacija stupaca. Ako ih poistovjetimo s rezultatima bacanja kockice* ⚀ = (123), ⚁ = (132), ⚂ = (213), ⚃ = (231), ⚄ = (312), ⚅ = (321), *onda bacanjem kocke odaberemo koju ćemo permutaciju koristiti.*

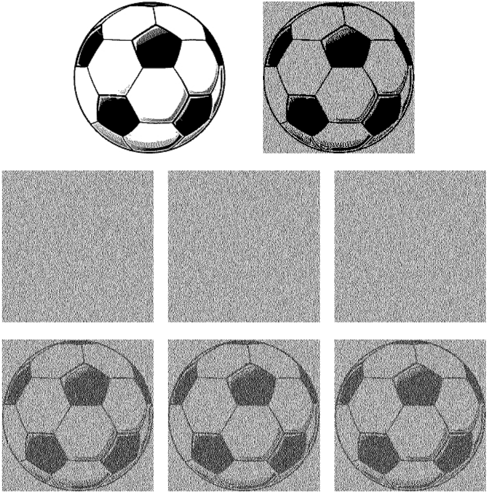
Nastavak primjera

Recimo da želimo šifrirati neki crni piksel. Gledamo matricu M_1. Bacimo kocku, recimo da je ispalo ⚂. Znači, gledamo permutaciju (213), dakle stupce od M_1 preuredimo tako da zamijenimo prvi i drugi:

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Retci odgovaraju pojedinim folijama. Dakle, na prvoj će foliji srednja trećina piksela biti crna, na drugoj lijeva, a na trećoj desna.

Kako sakriti sliku?



Naravno, matrice M_0 i M_1 ne smiju biti bilo kakve, nego takve da zadovoljavaju sigurnosni uvjet i garantiraju vidljivost slike pri preklapanju dviju folija nastalih prethodno opisanim postupkom.

Naravno, matrice M_0 i M_1 ne smiju biti bilo kakve, nego takve da zadovoljavaju sigurnosni uvjet i garantiraju vidljivost slike pri preklapanju dviju folija nastalih prethodno opisanim postupkom. Kao prvo, odabere se broj w koliko brojeva u svakom od redaka matrica M_0 i M_1 će biti iznosa 1

Naravno, matrice M_0 i M_1 ne smiju biti bilo kakve, nego takve da zadovoljavaju sigurnosni uvjet i garantiraju vidljivost slike pri preklapanju dviju folija nastalih prethodno opisanim postupkom. Kao prvo, odabere se broj w koliko brojeva u svakom od redaka matrica M_0 i M_1 će biti iznosa 1(w/m bit će udio „crnine" za originalno bijele piksele pri preklapanju dviju folija). Svih prvih w stupaca od M_0 sadržavat će samo jedinice, a ostatak nule.

Naravno, matrice M_0 i M_1 ne smiju biti bilo kakve, nego takve da zadovoljavaju sigurnosni uvjet i garantiraju vidljivost slike pri preklapanju dviju folija nastalih prethodno opisanim postupkom.
Kao prvo, odabere se broj w koliko brojeva u svakom od redaka matrica M_0 i M_1 će biti iznosa $1(w/m$ bit će udio „crnine" za originalno bijele piksele pri preklapanju dviju folija). Svih prvih w stupaca od M_0 sadržavat će samo jedinice, a ostatak nule.
Zašto je bitno da svi retci u M_0 budu jednaki?

Naravno, matrice M_0 i M_1 ne smiju biti bilo kakve, nego takve da zadovoljavaju sigurnosni uvjet i garantiraju vidljivost slike pri preklapanju dviju folija nastalih prethodno opisanim postupkom.
Kao prvo, odabere se broj w koliko brojeva u svakom od redaka matrica M_0 i M_1 će biti iznosa 1 (w/m bit će udio „crnine" za originalno bijele piksele pri preklapanju dviju folija). Svih prvih w stupaca od M_0 sadržavat će samo jedinice, a ostatak nule.
Zašto je bitno da svi retci u M_0 budu jednaki?
A zašto da brojevi jedinica u retcima od M_0 i M_1 budu jednaki?

Naravno, matrice M_0 i M_1 ne smiju biti bilo kakve, nego takve da zadovoljavaju sigurnosni uvjet i garantiraju vidljivost slike pri preklapanju dviju folija nastalih prethodno opisanim postupkom.
Kao prvo, odabere se broj w koliko brojeva u svakom od redaka matrica M_0 i M_1 će biti iznosa 1(w/m bit će udio „crnine" za originalno bijele piksele pri preklapanju dviju folija). Svih prvih w stupaca od M_0 sadržavat će samo jedinice, a ostatak nule.
Zašto je bitno da svi retci u M_0 budu jednaki?
A zašto da brojevi jedinica u retcima od M_0 i M_1 budu jednaki?
Kakva je matrica M_0 u originalnoj $(2, 2)$-shemi?

Nadalje, odaberemo broj γ između 0 i 1 koji će opisivati relativni kontrast u slici koja nastaje preklapanjem

Nadalje, odaberemo broj γ između 0 i 1 koji će opisivati relativni kontrast u slici koja nastaje preklapanjem(svaki crni piksel bit će pri preklapanju bar u udjelu $\frac{w}{m} + \gamma$ crn, dok je bijeli to točno u udjelu $\frac{w}{m}$). Retci matrice M_1 moraju biti takvi da koja god dva od njih nim-zbrojimo ($\oplus$), dobit ćemo „redak" s bar $w + \gamma m$ jedinica. Recimo, u originalnoj $(2,2)$-shemi imali smo $m = 2$, $w = 1$ i $\gamma = 1/2$, Nadalje, odaberemo broj γ između 0 i 1 koji će opisivati relativni kontrast u slici koja nastaje preklapanjem(svaki crni piksel bit će pri preklapanju bar u udjelu $\frac{w}{m} + \gamma$ crn, dok je bijeli to točno u udjelu $\frac{w}{m}$). Retci matrice M_1 moraju biti takvi da koja god dva od njih nim-zbrojimo ($\oplus$), dobit ćemo „redak" s bar $w + \gamma m$ jedinica. Recimo, u originalnoj $(2, 2)$-shemi imali smo $m = 2$, $w = 1$ i $\gamma = 1/2$,u primjeru s $(2, 4)$-shemom $m = 6$, $w = 3$ i $\gamma = 1/3$,

Nadalje, odaberemo broj γ između 0 i 1 koji će opisivati relativni kontrast u slici koja nastaje preklapanjem(svaki crni piksel bit će pri preklapanju bar u udjelu $\frac{w}{m} + \gamma$ crn, dok je bijeli to točno u udjelu $\frac{w}{m}$). Retci matrice M_1 moraju biti takvi da koja god dva od njih nim-zbrojimo ($\oplus$), dobit ćemo „redak" s bar $w + \gamma m$ jedinica. Recimo, u originalnoj $(2, 2)$-shemi imali smo $m = 2$, $w = 1$ i $\gamma = 1/2$,u primjeru s $(2, 4)$-shemom $m = 6$, $w = 3$ i $\gamma = 1/3$, a u primjeru s $(2, 3)$-shemom je $m = 3$, $w = 1$ i $\gamma = 1/3$.
Nije teško uvjeriti se da za isti kontrast pri većem broju sudionika n treba i veća ekspanzija m. Može se dokazati i koliko iznosi najjači mogući kontrast u proizvoljnoj $(2, n)$-shemi opisanog tipa:

$$\gamma_{\max} = \frac{\lfloor \frac{n}{2} \rfloor \cdot \lceil \frac{n}{2} \rceil}{n(n-1)}$$

Nadalje, odaberemo broj γ između 0 i 1 koji će opisivati relativni kontrast u slici koja nastaje preklapanjem(svaki crni piksel bit će pri preklapanju bar u udjelu $\frac{w}{m} + \gamma$ crn, dok je bijeli to točno u udjelu $\frac{w}{m}$). Retci matrice M_1 moraju biti takvi da koja god dva od njih nim-zbrojimo ($\oplus$), dobit ćemo „redak" s bar $w + \gamma m$ jedinica. Recimo, u originalnoj $(2, 2)$-shemi imali smo $m = 2$, $w = 1$ i $\gamma = 1/2$,u primjeru s $(2, 4)$-shemom $m = 6$, $w = 3$ i $\gamma = 1/3$, a u primjeru s $(2, 3)$-shemom je $m = 3$, $w = 1$ i $\gamma = 1/3$.
Nije teško uvjeriti se da za isti kontrast pri većem broju sudionika n treba i veća ekspanzija m. Može se dokazati i koliko iznosi najjači mogući kontrast u proizvoljnoj $(2, n)$-shemi opisanog tipa:
$\gamma_{\max} = \dfrac{\lfloor \frac{n}{2} \rfloor \cdot \lceil \frac{n}{2} \rceil}{n(n-1)}$(što je $1/2$ za $n = 2$, $1/3$ za $n = 3$ i 4, $3/10$ za $n = 5$ i 6, $2/7$ za $n = 7$ i 8, $5/18$ za $n = 9$ i 10). Limes tih brojeva je $1/4$.

Nadalje, odaberemo broj γ između 0 i 1 koji će opisivati relativni kontrast u slici koja nastaje preklapanjem(svaki crni piksel bit će pri preklapanju bar u udjelu $\frac{w}{m} + \gamma$ crn, dok je bijeli to točno u udjelu $\frac{w}{m}$). Retci matrice M_1 moraju biti takvi da koja god dva od njih nim-zbrojimo ($\oplus$), dobit ćemo „redak" s bar $w + \gamma m$ jedinica. Recimo, u originalnoj $(2, 2)$-shemi imali smo $m = 2$, $w = 1$ i $\gamma = 1/2$,u primjeru s $(2, 4)$-shemom $m = 6$, $w = 3$ i $\gamma = 1/3$, a u primjeru s $(2, 3)$-shemom je $m = 3$, $w = 1$ i $\gamma = 1/3$.
Nije teško uvjeriti se da za isti kontrast pri većem broju sudionika n treba i veća ekspanzija m. Može se dokazati i koliko iznosi najjači mogući kontrast u proizvoljnoj $(2, n)$-shemi opisanog tipa:
$\gamma_{\max} = \dfrac{\lfloor \frac{n}{2} \rfloor \cdot \lceil \frac{n}{2} \rceil}{n(n-1)}$(što je $1/2$ za $n = 2$, $1/3$ za $n = 3$ i 4, $3/10$ za $n = 5$ i 6, $2/7$ za $n = 7$ i 8, $5/18$ za $n = 9$ i 10). Limes tih brojeva je $1/4$. Dokazano je i da ma koliko veliki n imali, moguće je osigurati taj kontrast od bar 25%.

Glavni izvor ove prezentacije je članak Douga Stinsona

www.cs.jhu.edu/~fabian/courses/CS600.624/stinson.pdf.