Sigurnost računalnih sustava

Computer Systems Security

Kriptografske tehničke sigurnosne mjere

Marin Golub

Sadržaj

- Uvod: Jesu li i koliko su kriptoalgoritmi sigurni?
- Napadi na simetrične i asimetrične kriptosustave
- Asimetrični kriptosustavi
  - Kriptosustavi zasnovani na eliptičkim krivuljama
- Funkcije za izračunavanje sažetka poruke
  - Napadi na funkcije za izračunavanje sažetka poruke
  - Elektronički vs. digitalni potpis
  - SHA-2 i SHA-3
- Kvantna kriptografija
- Natječaji za nove kriptografske algoritme koji su u tijeku
  - Kriptografija prilagođena ugrađenim računalima (*Lightweight Cryptography*)
  - Asimetrična kriptografija nakon kvantnih računala (*Post-Quantum Cryptography*)

Osnovni pojmovi

Kriptologija = kriptografija + kriptoanaliza

Kriptografija

- znanstvena disciplina (ili umjetnost?) sastavljanja poruka sa ciljem skrivanja sadržaja poruka

Kriptoanaliza

- znanstvena disciplina koja se bavi analizom skrivenih aspekata sustava i koristi se kako bi se ispitala (ili narušila) sigurnost kriptografskog sustava

Jesu li i koliko su kriptoalgoritmi sigurni?

- postoje specijalizirana računala za napad grubom silom na DES kriptosustav: COPACOBANA (*A Cost-Optimized PArallel COde Breaker*)
- 12.12.2009. faktoriziran RSA-768
- na kvantnom računalu je riješen problem faktoriziranja velikih brojeva i problem diskretnog logaritma
- 17.8.2004. - kineski i francuski znanstvenici su objavili članak pod naslovom: "*Kolizija za hash funkcije: MD4, MD5, Haval-128 i RIPEMD*"
- 13.2.2005. - kineski znanstvenici: "*Collision Search Attacks on SHA-1*"
- napadi koji koriste sporedna svojstva uređaja (*Side-Channel Attacks*, SCA)

Kriptoanaliza

- izvedenica iz grčkih riječi
  - *kryptós* – skriven i
  - *analýein* – rastavljati
- analiza informacijskog sustava u svrhu pronalaska skrivenih aspekata sustava
- obuhvaća primjerice
  - diferencijalnu kriptoanalizu
  - linearnu kriptoanalizu
  - analizu propusta u implementaciji
- uspješnost kriptoanalize ocjenjuje se uspoređivanjem s napadom grubom silom odnosno ispitivanjem svih mogućih ključeva

Vrste napada na kriptosustave
prema onome što je napadaču poznato

- napad s odabranim čistim tekstom (*chosen-plaintext attack*)
  - napadač posjeduje neograničene količine parova (M,C)
  - primjer s pametnim karticama
- napad s odabranim kriptiranim tekstom (*chosen-ciphertext attack*)
  - napadač posjeduje po svojoj volji odabrani C i pripadni M (također neograničene količine parova)
- napad s poznatim čistim tekstom (*known-plaintext attack*)
  - napadač posjeduje neke parove (M,C)
  - za napad mu treba određena količina parova
- napad s poznatim kriptiranim tekstom (*only-ciphertext attack*)
  - napadač posjeduje samo C a pokušava saznati K i M
  - napadaču je ovaj napad najteže uspješno provesti

- cilj je doznati tajni ključ

Napad na AES-128 *grubom silom*

- duljina ključa = 128 bita
- broj različitih ključeva:

  340282366920938463463374607431768211456
- pretpostavke:
  - zadano: (M,C), K=? ili
    (M1, C1) i (M2, C2), tj. znam M1 XOR M2 i C1 XOR C2, K=?
  - 1 milijardu računala
  - 1 milijardu ključeva po sekundi po računalu
- pretraga grubom silom će trajati oko $3.4*10^{20}$ sekundi

  = 10 tisuća milijardi godina

Implementacijski napadi

- napadi koji koriste propuste u programskoj i sklopovskoj implementaciji kriptografskih algoritma
  - napadi koji koriste sporedna svojstva kriptografskih uređaja (*engl. Side Channel Attacks*, SCA)
  - napadi umetanjem grešaka (*engl. Fault Injection, FI*)
  - mikrosondiranja

Simetrični kriptosustavi

Bitna svojstva simetričnih kriptosustava

- Difuzija
  - svaki bit jasnog teksta i svaki bit ključa mora utjecati na mnogo bitova kriptiranog teksta
  - promjena samo jednog bita jasnog teksta mora uzrokovati promjenu (statistički) polovicu bitova kriptiranog teksta
  - ostvaruje se primjerice permutacijom i u više koraka algoritma

- Konfuzija
  - kriptirani tekst treba ovisiti o jasnom tekstu i ključu tako da je kriptoanaliza suviše složena
  - svaki bit kriptiranog teksta treba ovisiti o više bitova ključa ali da se pritom prikrije veza između njih
  - ostvaruje se primjerice supstitucijom, tj. supstitucijskim tablicama

Algoritam kriptiranja bloka je *siguran*

- ako je teško na temelju kriptiranog teksta pronaći
  - jasni tekst i/ili
  - ključ
- ... čak i ako napadač:
  - ima na raspolaganju mnogo parova (M,C) gdje je $C = E(M,K)$
  - može kriptirati i dekriptirati, tj. izračunati:
    - $C=E(M,K)$ za proizvoljni M
    - $M=D(C,K)$ za proizvoljni C

Ponavljanje: DES

- 1977. razvijen u IBM-u
- najpoznatiji simetrični algoritam i još uvijek se koristi unatoč njegovoj nesigurnosti
- mala veličina ključa je najveći nedostatak koji se otklanja višestrukim kriptiranjem
  - triple DES (3DES) s ključem veličine 112 ili 168 bita
- kriptira se blok veličine 64 bita u 16 koraka uz pomoć 8 S-tablica
- simulacija

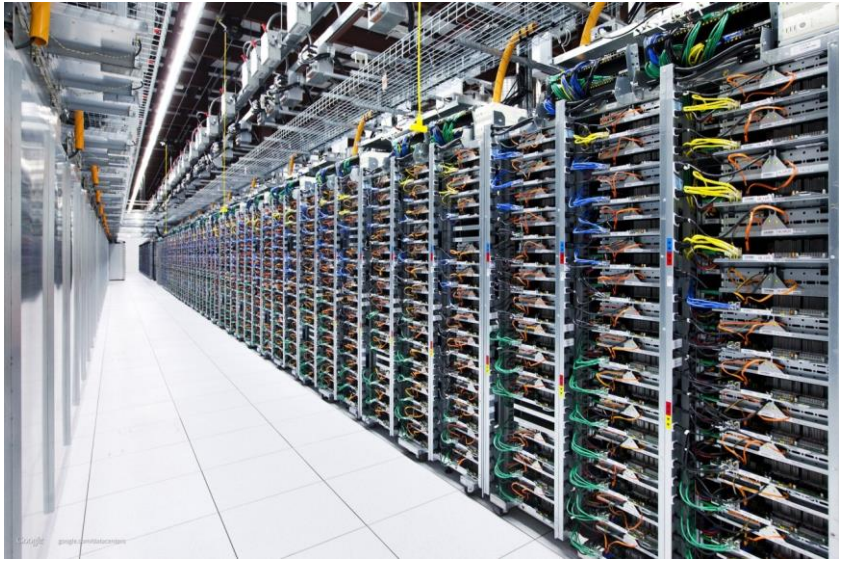
Ponavljanje: AES

- NIST (*National Institute of Standards and Technology*)
  - raspisao natječaj za napredni kriptosustav 12.9.1997.
  - proglašen pobjednik algoritam *Rijndael* 2.8.2000.
  - ostali finalisti: Serpent, Twofish, RC6 i MARS
- 3DES je proglašen kao privremeni standard
- veličina ključa od 128, 192 i 256 bita
- kriptira se blok veličine 128 bita u 10, 12 ili 14 (ovisno o veličini ključa) koraka uz pomoć
  - jedne S-tablice
  - 4 funkcije: *zamijeni znakove, posmakni redove, pomiješaj stupce* i XOR
  - zadnji korak bez funkcije *pomiješaj stupce* jer ne doprinosi sigurnosti
- stanje: matrica 4x4 bajta
- dekriptiranje: sve funkcije imaju svoj inverz

Osnovni algoritam kriptoanalize

Napad grubom silom

- napadač pokušava dekriptirati kriptirani tekst sa svim mogućim ključevima
- neka je poznat *M*, *C=E(M,K)*
- algoritam radi sljedeće:
  - za svaki mogući ključ *Ki*
  - ako je *C == E(M,Ki)* onda ispiši *Ki*
- takav se algoritam naziva algoritmom grube sile



Pretraživanje cijelog prostora rješenja
napad *grubom silom*

- najjednostavnija i najsporija vrsta napada
- nije moguće spriječiti ovaj napad
- uspješnost svih napada na kriptosustave mjeri se usporedbom s pretraživanjem cijelog prostora
- Napad koji ima veću složenost od složenosti pretraživanja cijelog prostora smatra se neuspješnim!
- Pretpostavka: napadač ili već ima na raspolaganju čisti tekst ili pretpostavlja da čisti tekst ima neku standardnu strukturu koju je moguće prepoznati.
  - Inače, u slučaju dekriptiranja poruke bez prepoznatljive strukture, napadač nema nikakve šanse da pretraživanjem cijelog prostora sazna koji je pravi ključ.

Napad na kriptosustav AES grubom silom

- duljina ključa = 128 bita
- broj različitih ključeva = 340282366920938463463374607431768211456
- pretpostavke:
  - 1 milijardu računala
  - 1 milijardu ključeva po sekundi po računalu
- gotovi smo za oko $3.4*10^{20}$ sekundi
- 10 tisuća milijardi godina

Napadi na DES

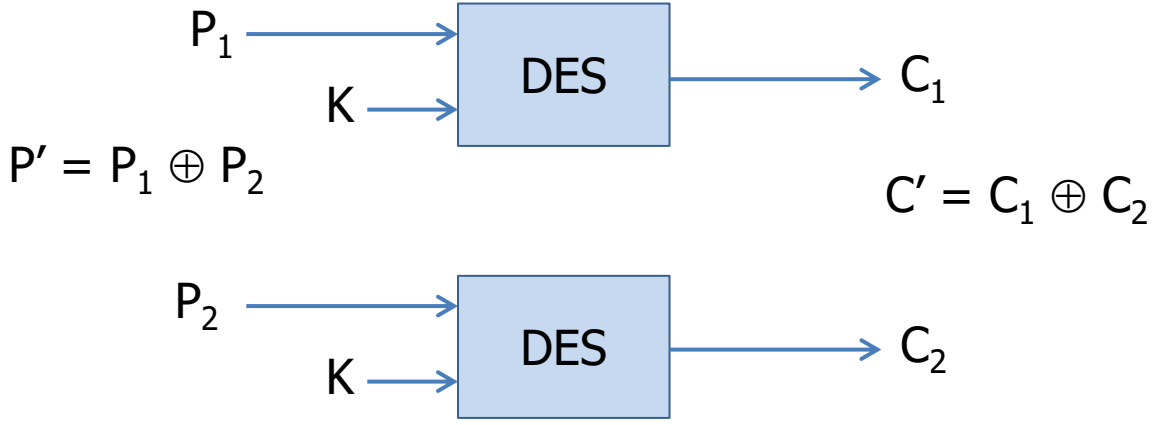
- bilo kakvim linearnim promjenama u postupku generiranja ključeva i u funkciji F, DES ne postaje otporniji na napade
- promjena u nelinearnom dijelu algoritma (S tablice) utječe na ranjivost algoritma
- DES bitno oslabljuje:
  - promjena redosljeda S tablica
  - slučajno odabrane S tablice
  - umjesto XOR neka složenija funkcija
- pristup: analiza pojednostavljenog kriptosustava (s manje iteracija ili rundi, za primjerice DES sa samo tri runde)

Kriptoanaliza

- diferencijalna kriptoanaliza
- linerna kriptoanaliza
- implementacijski napadi
  - napadi koji ne iskorištavaju slabosti algoritma (jer ih obično algoritam ni nema) već iskorištavaju sigurnosne propuste u programskim ili sklopovskim ostvarenjima
- uspješnost kriptoanalize ocjenjuje se uspoređivanjem s napadom grubom silom odnosno ispitivanjem svih mogućih ključeva

Diferencijalna kriptoanaliza
kriptosustava DES

- Eli Biham, Adi Shamir, knjiga pod naslovom "*Differential analysis of DES-like cryptosystems*", 1990.
- tehnika kojom se analizira učinak razlike između dva čista teksta na razliku između dva rezultirajuća kriptirana teksta
- razlike služe za određivanje vjerojatnosti mogućih ključeva



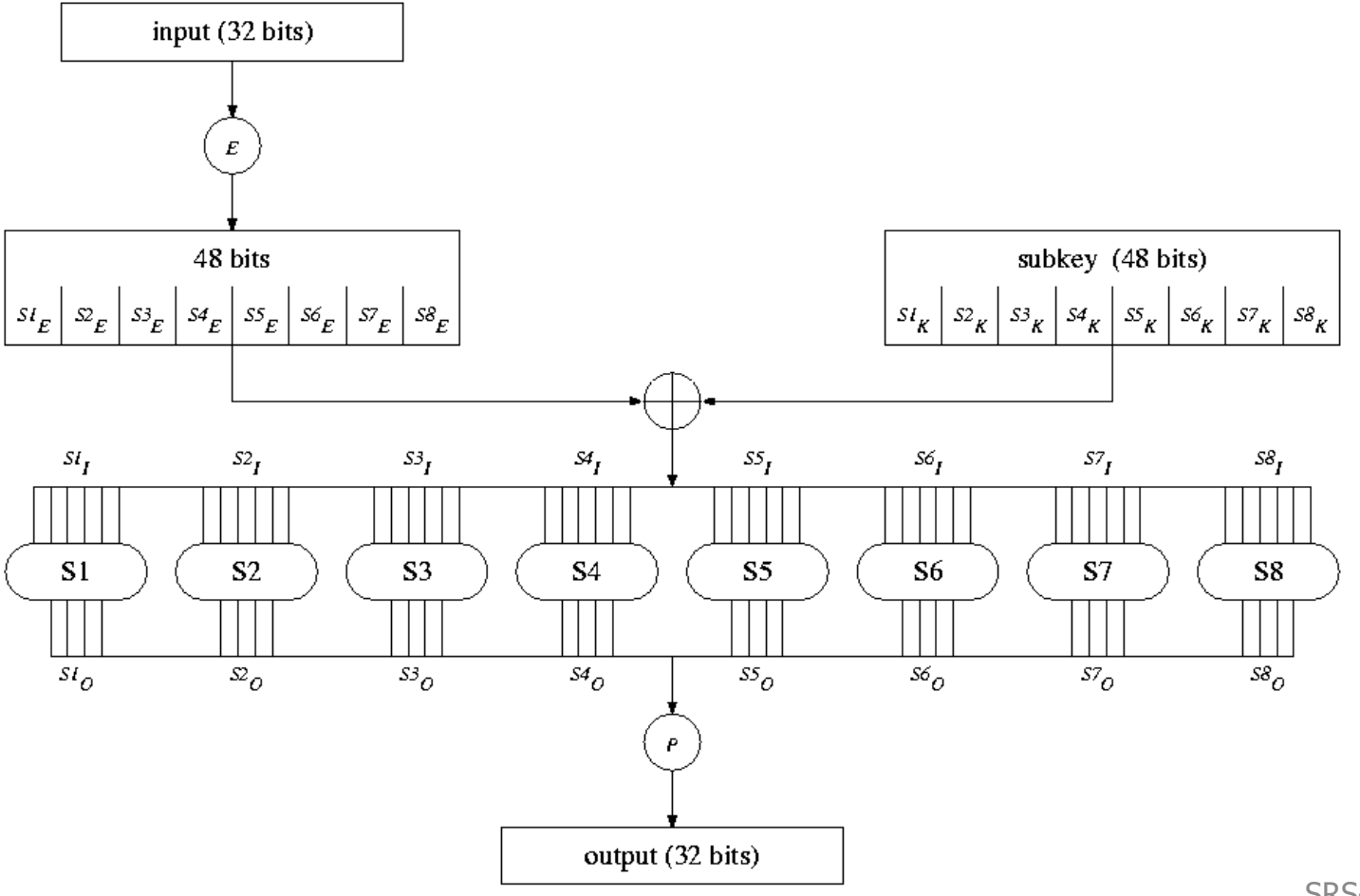
S-tablice ili S-kutije (*engl. S-boxes*)

- nisu linearne
  - poznavanje razlike ulaznog para ne garantira poznavanje razlike izlaza iz S-tablica
- za bilo koju ulaznu razliku kod S-tablica postoji ograničen broj mogućih izlazhih razlika
  - primjerice ima i onih koje se sigurno neće pojaviti
- ulaz u neku od 8 S-tablica je veličine 6 bita, a izlaz 4 bita
  - postoji 26 = 64 mogućih ulaznih razlika i
  - 24 = 16 izlaznih razlika
- supstitucijska tablica S1: (ako je ulaz u S1 tablicu 001101, izlaz je 13

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

- sve te mogućnosti mogu se pobrojati i zapisati u tablicu

DES: funkcija *F*



Broj mogućih izlaznih razlika za pojedinu ulaznu razliku tablice S1 (dio tablice)

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	6	0	2	4	4	0	10	12	4	10	6	2	4
2_x	0	0	0	8	0	4	4	4	0	6	8	6	12	6	4	2
3_x	14	4	2	2	10	6	4	2	6	4	4	0	2	2	2	0
4_x	0	0	0	6	0	10	10	6	0	4	6	4	2	8	6	2
5_x	4	8	6	2	2	4	4	2	0	4	4	0	12	2	4	6
6_x	0	4	2	4	8	2	6	2	8	4	4	2	4	2	0	12
7_x	2	4	10	4	0	4	8	4	2	4	8	2	2	2	4	4
8_x	0	0	0	12	0	8	8	4	0	6	2	8	8	2	2	4
9_x	10	2	4	0	2	4	6	0	2	2	8	0	10	0	2	12
A_x	0	8	6	2	2	8	6	0	6	4	6	0	4	0	2	10
B_x	2	4	0	10	2	2	4	0	2	6	2	6	6	4	2	12
C_x	0	0	0	8	0	6	6	0	0	6	6	4	6	6	14	2
D_x	6	6	4	8	4	8	2	6	0	6	4	6	0	2	0	2
E_x	0	4	8	8	6	6	4	0	6	6	4	0	0	4	0	8
F_x	2	0	2	4	4	6	4	2	4	8	2	2	2	6	8	8
									⋮							
30_x	0	4	6	0	12	6	2	2	8	2	4	4	6	2	2	4
31_x	4	8	2	10	2	2	2	2	6	0	0	2	2	4	10	8
32_x	4	2	6	4	4	2	2	4	6	6	4	8	2	2	8	0
33_x	4	4	6	2	10	8	4	2	4	0	2	2	4	6	2	4
34_x	0	8	16	6	2	0	0	12	6	0	0	0	0	8	0	6
35_x	2	2	4	0	8	0	0	0	14	4	6	8	0	2	14	0
36_x	2	6	2	2	8	0	2	2	4	2	6	8	6	4	10	0
37_x	2	2	12	4	2	4	4	10	4	4	2	6	0	2	2	4
38_x	0	6	2	2	2	0	2	2	4	6	4	4	4	6	10	10
39_x	6	2	2	4	12	6	4	8	4	0	2	4	2	4	4	0
$3A_x$	6	4	6	4	6	8	0	6	2	2	6	2	2	6	4	0
$3B_x$	2	6	4	0	0	2	4	6	4	6	8	6	4	4	6	2
$3C_x$	0	10	4	0	12	0	4	2	6	0	4	12	4	4	2	0
$3D_x$	0	8	6	2	2	6	0	8	4	4	0	4	0	12	4	4
$3E_x$	4	8	2	2	2	4	4	14	4	2	0	2	0	8	4	4
$3F_x$	4	8	4	2	4	0	2	4	4	2	4	8	8	6	2	2

Dio tablice koja prikazuje broj mogućih izlaznih razlika za pojedinu ulaznu razliku tablice S1

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	6	0	2	4	4	0	10	12	4	10	6	2	4
2_x	0	0	0	8	0	4	4	4	0	6	8	6	12	6	4	2
3_x	14	4	2	2	10	6	4	2	6	4	4	0	2	2	2	0
4_x	0	0	0	6	0	10	10	6	0	4	6	4	2	8	6	2
5_x	4	8	6	2	2	4	4	2	0	4	4	0	12	2	4	6
6_x	0	4	2	4	8	2	6	2	8	4	4	2	4	2	0	12
7_x	2	4	10	4	0	4	8	4	2	4	8	2	2	2	4	4
8_x	0	0	0	12	0	8	8	4	0	6	2	8	8	2	2	4
9_x	10	2	4	0	2	4	6	0	2	2	8	0	10	0	2	12
A_x	0	8	6	2	2	8	6	0	6	4	6	0	4	0	2	10
B_x	2	4	0	10	2	2	4	0	2	6	2	6	6	4	2	12
C_x	0	0	0	8	0	6	6	0	0	6	6	4	6	6	14	2
D_x	6	6	4	8	4	8	2	6	0	6	4	6	0	2	0	2
E_x	0	4	8	8	6	6	4	0	6	6	4	0	0	4	0	8
F_x	2	0	2	4	4	6	4	2	4	8	2	2	2	6	8	8
⋮																
30_x	0	4	6	0	12	6	2	2	8	2	4	4	6	2	2	4
31_x	4	8	2	10	2	2	2	2	6	0	0	2	2	4	10	8
32_x	4	2	6	4	4	2	2	4	6	6	4	8	2	2	8	0
33_x	4	4	6	2	10	8	4	2	4	0	2	2	4	6	2	4
34_x	0	8	16	6	2	0	0	12	6	0	0	0	0	8	0	6
35_x	2	2	4	0	8	0	0	0	14	4	6	8	0	2	14	0
36_x	2	6	2	2	8	0	2	2	4	2	6	8	6	4	10	0
37_x	2	2	12	4	2	4	4	10	4	4	2	6	0	2	2	4
38_x	0	6	2	2	2	0	2	2	4	6	4	4	4	6	10	10
39_x	6	2	2	4	12	6	4	8	4	0	2	4	2	4	4	0
$3A_x$	6	4	6	4	6	8	0	6	2	2	6	2	2	6	4	0
$3B_x$	2	6	4	0	0	2	4	6	4	6	8	6	4	4	6	2
$3C_x$	0	10	4	0	12	0	4	2	6	0	4	12	4	4	2	0
$3D_x$	0	8	6	2	2	6	0	8	4	4	0	4	0	12	4	4
$3E_x$	4	8	2	2	2	4	4	14	4	2	0	2	0	8	4	4
$3F_x$	4	8	4	2	4	0	2	4	4	2	4	8	8	6	2	2

Ako su ulazi jednaki, onda i na izlazu nema razlike.

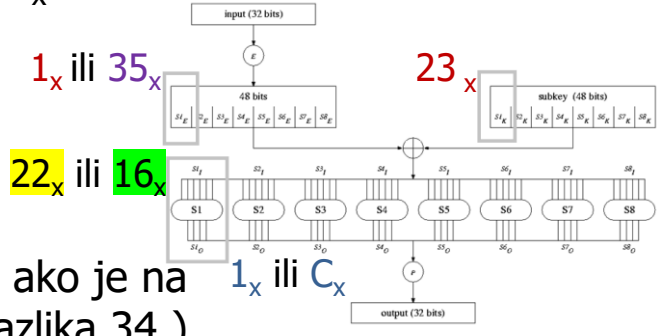
Na 6 od ukupno 64 načina se na izlazu dobije razlika 3x

Svi brojevi u tablici su parni jer je operacija XOR komutativna

U svakom retku suma brojeva je 64 jer se svaki 6-bitni ulaz može dobiti na 64 načina kao rezultat operacije XOR, npr.
1x = 000001 =
000000 ⊕ 000001 =
000001 ⊕ 000000 =
000010 ⊕ 000011 =
000011 ⊕ 000010 =
000100 ⊕ 000101 =
000101 ⊕ 000100 =
itd.
i sada treba samo izbrojati sve razlike na izlazu, npr.
S1(000000) = 1100
S1(000001) = 0000
a
1100 ⊕ 0000 = 1100
pa se u retku 1x i stupcu Dx=1100 dodaje jedna jedinica
ili
S1(000010) = 0100
S1(000011) = 1111
a
0100 ⊕ 1111 = 1011
pa se u stupcu Bx=1100 dodaje jedna jedinica, i tako 64 puta

Izlazna razlika Mogući ulazi za ulaznu razliku 34_x

1_x 03_x, $0F_x$, $1E_x$, $1F_x$, $2A_x$, $2B_x$, 37_x, $3B_x$
2_x 04_x, 05_x, $0E_x$, 11_x, 12_x, 14_x, $1A_x$, $1B_x$, 20_x, 25_x, 26_x, $2E_x$, $2F_x$, 30_x, 31_x, $3A_x$
3_x 01_x, 02_x, 15_x, 21_x, 35_x, 36_x
4_x 13_x, 27_x
7_x 00_x, 08_x, $0D_x$, 17_x, 18_x, $1D_x$, 23_x, 29_x, $2C_x$, 34_x, 39_x, $3C_x$
8_x 09_x, $0C_x$, 19_x, $2D_x$, 38_x, $3D_x$
D_x 06_x, 10_x, 16_x, $1C_x$, 22_x, 24_x, 28_x, 32_x
F_x 07_x, $0A_x$, $0B_x$, 33_x, $3E_x$, $3F_x$



1_x ili 35_x
23_x
22_x ili 16_x
1_x ili C_x

Ulaz u S-tablicu
(parovi za koje ⊕ daje 34_x)

$06_x \oplus 32_x = 34_x$
$10_x \oplus 24_x = 34_x$
$16_x \oplus 22_x = 34_x$
$1C_x \oplus 28_x = 34_x$

Mogući ključevi za izlaznu razliku D_x ako je na ulazu S1E = 1_x i S1E'=35_x (ulazna razlika 34_x)

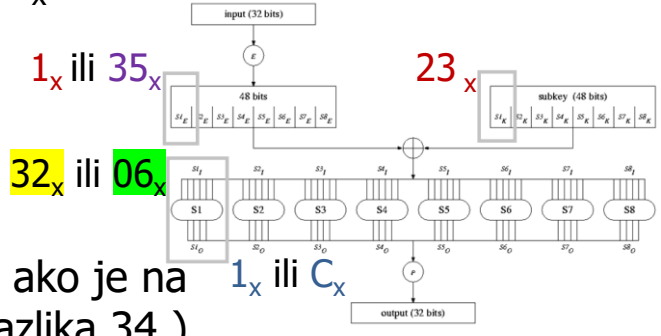
07_x, 33_x
11_x, 25_x
17_x, 23_x
$1D_x$, 29_x

primjer:
$1_x \oplus 23_x = 22_x$ u S1 izlaz je 1_x
$35_x \oplus 23_x = 16_x$ u S1, izlaz je C_x

izlazna razlika je $1_x \oplus C_x = D_x$

Izlazna razlika Mogući ulazi za ulaznu razliku 34_x

1_x 03_x, $0F_x$, $1E_x$, $1F_x$, $2A_x$, $2B_x$, 37_x, $3B_x$
2_x 04_x, 05_x, $0E_x$, 11_x, 12_x, 14_x, $1A_x$, $1B_x$, 20_x, 25_x, 26_x, $2E_x$, $2F_x$, 30_x, 31_x, $3A_x$
3_x 01_x, 02_x, 15_x, 21_x, 35_x, 36_x
4_x 13_x, 27_x
7_x 00_x, 08_x, $0D_x$, 17_x, 18_x, $1D_x$, 23_x, 29_x, $2C_x$, 34_x, 39_x, $3C_x$
8_x 09_x, $0C_x$, 19_x, $2D_x$, 38_x, $3D_x$
D_x 06_x, 10_x, 16_x, $1C_x$, 22_x, 24_x, 28_x, 32_x
F_x 07_x, $0A_x$, $0B_x$, 33_x, $3E_x$, $3F_x$



1_x ili 35_x
23_x
32_x ili 06_x
1_x ili C_x

Ulaz u S-tablicu
(parovi za koje ⊕ daje 34_x)

$06_x \oplus 32_x = 34_x$
$10_x \oplus 24_x = 34_x$
$16_x \oplus 22_x = 34_x$
$1C_x \oplus 28_x = 34_x$

Mogući ključevi za izlaznu razliku D_x ako je na ulazu S1E = 1_x i S1E'=35_x (ulazna razlika 34_x)

07_x, 33_x
11_x, 25_x
17_x, 23_x
$1D_x$, 29_x

ili drugi primjer:
$1_x \oplus 07_x = 06_x$ u S1 izlaz je 1_x
$35_x \oplus 07_x = 32_x$ u S1, izlaz je C_x

izlazna razlika je $1_x \oplus C_x = D_x$

Učinkovitost napada diferencijalnom kriptoanalizom

Broj rundi	4	6	8	9	10	11	12	13	14	15	16
Složenost	2^4	2^8	2^{16}	2^{26}	2^{35}	2^{36}	2^{43}	2^{44}	2^{51}	2^{52}	**2^{58}**

- Eli Biham, Adi Shamir, *Differential cryptoanalysis of the full 16-round DES*, 1991. - opisan je napad diferencijalnom analizom izvediv na potpuni DES koji je brži od pretraživanja pola prostora rješenja
- Joan Daemen, *Cipher and hash function design strategies based on linear and differential cryptoanalysis*, 1994. - opisana je metoda *Wide Trail Strategy* koja pruža zaštitu i od diferencijalne i od linearne analize

Linearna kriptoanaliza

- cilj je pronaći linearnu aproksimaciju danog algoritma

  $P[i_1, i_2, \ldots, i_a] \oplus C[j_1, j_2, \ldots, j_b] = K[k_1, k_2, \ldots, k_c]$

- primjer: neka s vjerojatnošću p=100% vrijedi:

  $P[1, 4, 13] \oplus C[1, 2, 3, 4, 6, 9, 11] = K[5, 6, 8]$

  - paritet 5., 6. i 8. bita ključa jednoznačno je određen paritetom pojednih bitova čistog i kriptiranog teksta
  - duljina ključa efektivno smanjila za 1 bit

- aproksimacija nikada nema vjerojatnost ni blizu 100%, obično je ta vjerojatnost vrlo blizu 50%
  - taj nedostatak nadoknađuje se uzimanjem veće količine parova čisti/kriptirani tekst
- obično postoji više lineanih aproksimacija za neki algoritam

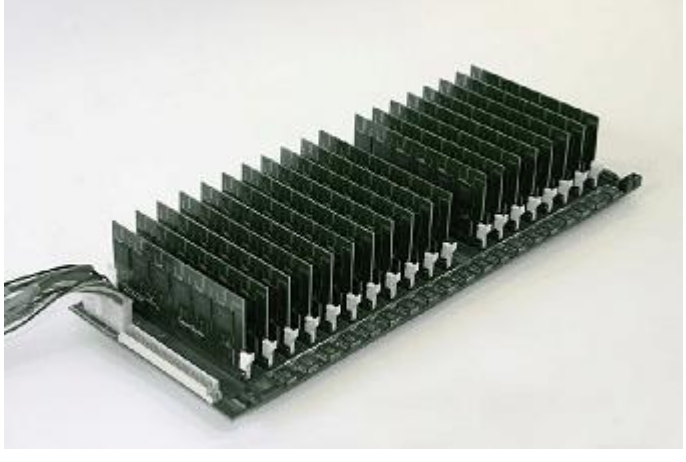
- DES Challenge I: 1997.

broj bitova ključa	vrijeme pronalaženja ključa
40	78 sekundi
48	5 sati
56	89 dana
64	41 godina
72	10.696 godina
80	2.738.199 godina
88	700.978.948 godina
96	179.450.610.898 godina
112	11.760.475.235.863.837 godina
128	770.734.505.057.572.442.069 godina

- DES Challenge II: 1998.
  - DES Cracker, 56 sati
- DES Challenge III: 1999.
  - distributed.net
  - 22h i 15min nakon pretrage 22,2% prostora rješenja

COPACOBANA

- *A Cost-Optimized Parallel Code Breaker*
- razvila su ga sveučilište Ruhr iz Bochuma i Christian-Albrechts iz Kiela 2006. g.
- FPGA arhitektura, programibilan sustav
- može se iskoristiti i u druge svrhe
- 400 000 000 enkripcija u sekundi
- pretraga traje prosječno manje od 9 dana
- cijena ≈ 9 kEUR (2006.g.)



Asimetrični kriptosustavi

Kriptosustavi zasnovani na eliptičkim krivuljama

Kriptosustavi zasnovani na eliptičkim krivuljama (*ECC*)

- sigurnost asimetričnih algoritama oslanja se na teško rješive probleme
  - rastav broja na proste faktore
  - problem diskretnog logaritma
- predstavili su je 1985. Victor Miller i Neal Koblitz

asimetrični kriptosustavi

- EC ElGamalov kriptosustav
- ECES (Elliptic Curve Encription System)
- Menzes-Vanstoneov kriptosustav
- Demytkov kriptosustav (1993., analogan RSA)
- KMOV kriptosustav (1991.)
- Kuwokado-Koyama kriptosustav

protokoli za razmjenu ključeva

- ECDH (Elliptic Curve Diffie-Hellman)
- EC Nyberg-Rueppelov protokol za razmjenu ključeva

digitalni potpis

- ECDSA (Elliptic Curve Digital Signature Algorithm)
- EdDSA (Edwards-curve Digital Signature Algorithm)
- ECSS (Elliptic Curve Signature Sheme)
- EC Nyberg-Rueppelova shema digitalnog potpisa
- OFF shema digitalnog potpisa

Opći oblik eliptičke krivulje
(*Weierstrassova forma*)

$$y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$$

$a_1, a_2, a_3, a_4, a_6 \in K$ (K je algebarski zatvoreno polje)

- eliptička krivulja se može definirati nad proizvoljnim poljem K:
  - polje racionalnih brojeva Q
  - polje realnih brojeva R
  - polje kompleksnih brojeva C
  - konačno polje Fq
- eliptička krivulja ili nesingularna kubna krivulja (engl. *nonsingular cubic curve*) je skup svih rješenja glatke Weierstrasseove jednadžbe
- rješenje je točka na eliptičkoj krivulji

Definicija eliptičke krivulje

Eliptička krivulja E nad poljem K je skup svih točaka $(x, y) \in K \times K$ koje zadovoljavaju jednadžbu:

$$y^2 = x^3 + ax + b,$$

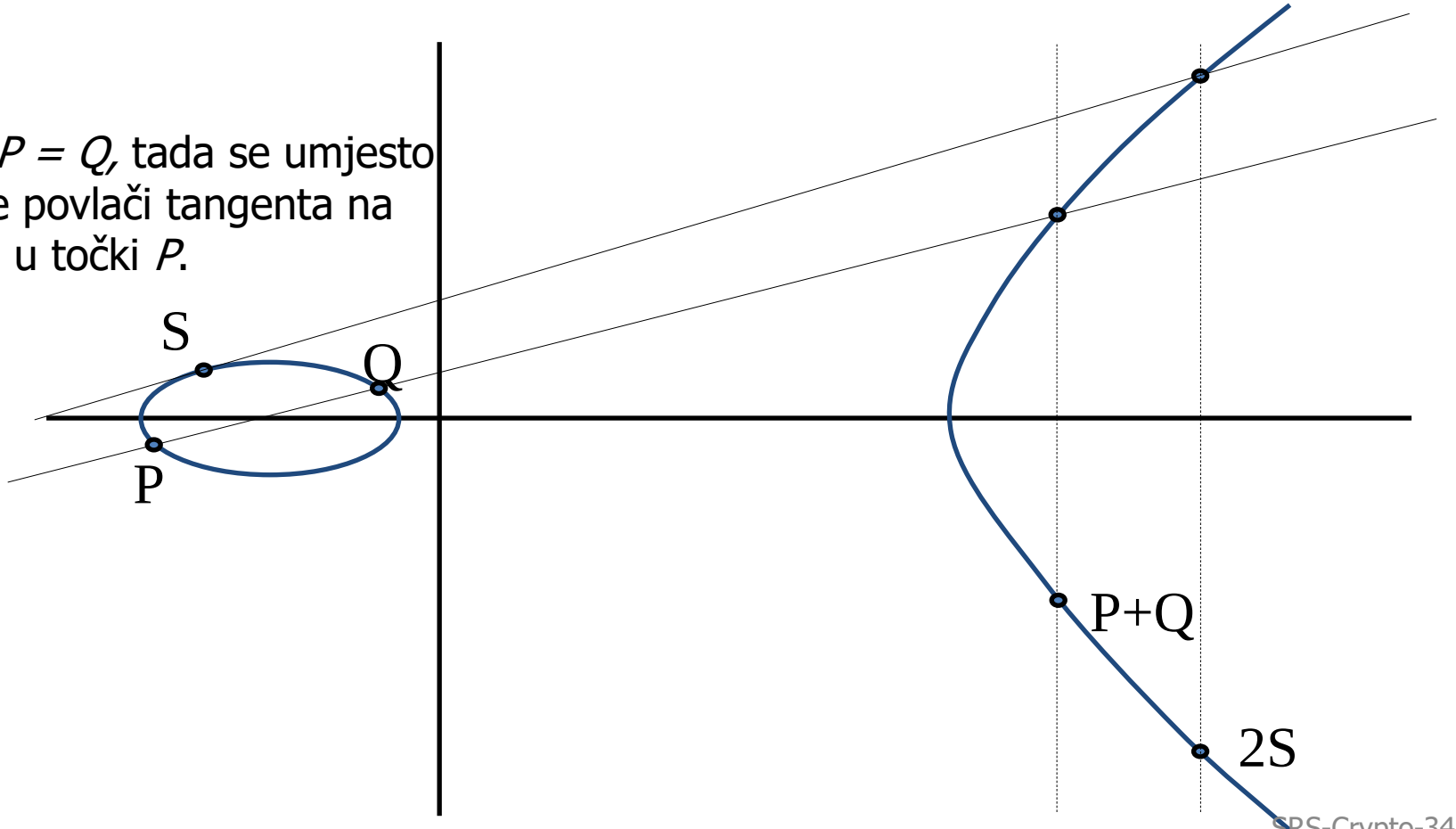
zajedno s još jednim elementom kojeg označavamo s O i zove se "točka u beskonačnosti".

K je konačno polje F_q karakteristike p

- gdje je $q = p$ prost broj *ili* $q = p^m$ za neki prirodan broj m.
- q – broj elemenata polja

Zbrajanje i množenje

Ako je *P = Q,* tada se umjesto sekante povlači tangenta na krivulju u točki *P*.



Problem diskretnog logaritma za eliptičke krivulje

Neka je dana eliptička krivulja E i točka $P \in E$ reda n.

Zadana je točka $Q \in E$:

$$Q = m * P, \qquad m \in \{2, 3, ..., n-2\}, \quad m = ?$$

Kada su E i P ispravno odabrani, rješavanje ECDLP-a smatra se nemogućim:

- za m = 0,1 i n -1 točka Q iznosi O, P i -P
- jedan od uvjeta je da je n (red točke P), toliko velik da je teško provjeriti sve mogućnosti od m

Kriptosustav EC Diffie-Hellman, ECDH

G
- generator
- javno poznata točka

ANA
- odabere k_a
- izračuna $P = k_a * G$

BRANKO
- odabere k_b
- izračuna $R = k_b * G$

šalje *P* →

← šalje *R*

- izračuna $P_1 = k_a * R$

- izračuna $P_2 = k_b * P$

Točka $P_1 = P_2 = k_a k_b G$ koristi se kao zajednički tajni ključ.

Kriptosustav EC ElGamal

Vrijednosti $E(F_q)$, G, n su javne: G (generator) je točka reda n na $E(F_q)$

$S_A = d_A$
$P_A = d_A * G$

ANA

$S_B = d_B$
$P_B = d_B * G$

BRANKO

Točka $P = dG$ je javni ključ, a je d privatni ključ ($P \in E(F_q)$, a d je slučajni broj).

Kriptiranje poruke $M \in E(F_q)$:

1. Ana generira slučajni broj $k \in \{2,3,...,n-2\}$ i izračuna $R = kG$.
2. Ana potraži Brankov javni ključ P_B i izračuna $S = M + kP_B$
3. Šalje (R, S) Branku

Dekriptiranje (R, S): originalna poruka je $M = S - d_B R$.

Dokaz: $S - d_B R = S - d_B kG = S - k d_B G = S - kP_B = M + kP_B - kP_B = M$

Asimetrični algoritmi zaključna razmatranja

- 12.12.2009. faktoriziran RSA-768
  - za što je prema autorima bilo potrebno 2000 godina na računalu
  - 2.2GHz-Opteron-CPU s 2GB RAM-a
  - priprema je trajala oko pola godine na 80 takvih računala, a
  - rastav je trajao još dvije godine na nekoliko stotina takvih računala
- procjenjuje se da je faktoriziranje RSA-1024 oko 1000 puta teže i da će se to dogoditi do 2020. godine. [T. Kleinjung, at all, Factorization of a 768-bit RSA modulus, dostupno na http://eprint.iacr.org/2010/006.pdf]
- Najbolji algoritam za rastav na proste faktore: *General Number Field Sieve,* GNFS
- 2009. je na grozdu od 200 igračkih konzola *PlayStation 3* razbijen 112-bitni kriptosustav zasnovan na eliptičkim krivuljama, ECC
  - postupak je trajao tri i pol mjeseca (što je usporedivo sa 640-bitnim RSA)

Koliko veliki ključ nam treba?

- Kritposustav koristi ključ od *N* –bita.
  - Značenje: Ključ se doslovno sastoji od *N* –bitova.
- Kritposustav pruža *n* -bita sigurnosti.
  - Trenutno najbolji poznati napad na kritposustav treba red veličine 2^n koraka da otkrije ključ (napad grubom silom je 2^N).
- *n* = efektivna duljina ključa
- AES128 – 128 bita stvarno, 126.1 efektivno
- RSA1024 => *N* =1024 bita stvarno, *n* =80 efektivno
- ekvivalenti po razini sigurnosti, odnosno po efektivnoj duljini ključa:
  - RSA1024 ≡ ECC163
  - RSA2048 ≡ ECC222
  - RSA4096 ≡ ECC409

Zašto takva veličina ključa?

- Želimo nivo sigurnosti izražen usporedbom sa AES-om: *Želim 128 bitova sigurnosti*
- Uzmimo najbolji poznati algoritam za razbijanje RSA (Faktorizacija broja *n* s pomoću postupka *General Number Field Sieve)* i analiziram njegovu složenost.
- Odaberemo veličinu ključa tako da najbolji napad za RSA treba slične resurse i vrijeme kao najbolji napad na 128 bitni AES.

Usporedba trajanja izvođenja kriptografskih funkcija

• AES128/CTR	1.0
• AES192/CTR	1.2
• AES256/CTR	1.4
• DES/CTR	4.3
• SHA-1	0.9
• SHA256	1.3
• RSA1024 kriptiranje	11 100
• RSA1024 dekriptiranje	213 000

izvor: www.cryptopp.com

Funkcije za izračunavanje sažetka poruke

Funkcije sažimanja ili *hash* funkcije

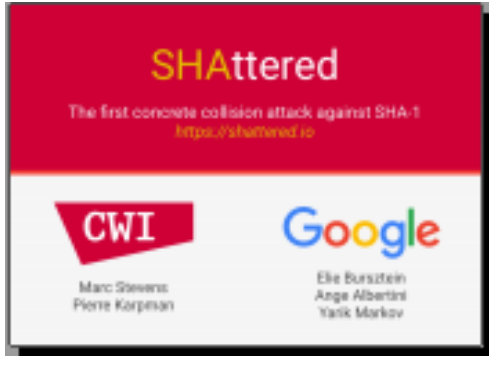
Važna svojstva funkcija za izračunavanje sažetka poruke

- Otpornost na izračunavanje originala
  ili prva domenska otpornost (*preimage resistance*)
  - $H=h(M) \Rightarrow \quad M=h^{-1}(H)$ ne postoji
- Otpornost na izračunavanje poruke koja daje isti sažetak
  ili druga domenska otpornost (*2-nd preimage resistance*)
  - za poznati M i $H=h(M)$ je nemoguće pronaći M' koji daje isti H
- Otpornost na kolizije (*collision resistance*)
  - nemoguće je pronaći bilo koje dvije poruke *M1* i *M2* za koje se dobiva isti sažetak $h(M1)=h(M2)$
- Difuzija
  - svaka, pa i najmanja promjena ulaznog podatka rezultira velikom i naizgled slučajnom promjenom na izlazu

Napadi na funkciju sažimanja SHA

- 1993. – objavljen SHA-0
- 1995. – NSA je predložila SHA-1 kao zamjenu za SHA-0
- 1998. – objavljen uspješan napad na SHA-0, ali ne i na SHA-1
- 2001. – NSA predlaže SHA-2
- 2005. – uspješan napad na SHA-1: pronađena kolizija
- 2007. – NIST raspisuje natječaj za SHA-3 i preporuča SHA-2
- 2012. – proglašen pobjednik natječaja SHA-3: Keccak
- 2017. – uspješan napad na SHA-1:
  - dva različita PDF dokumenta daju isti sažetak (Marc Sevens ispred svih u suradnji s tvrtkom Google)
  - https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html

- za pronalazak kolizije potrebno je:
  - MD5 → 1 pametni telefon i 30 s
  - SHA-1 → grubom silom i 12 000 000 GPU godina
  - SHA-1 → algoritam Shattered i 110 GPU godina



SHA-2

- osmislila NSA
- NIST publicirao 2001 u vrijeme natječaja za SHA-3
- skup funkcija:
  - SHA-224 = SHA2-224
  - SHA-256
  - SHA-384
  - SHA-512

Algoritam	Sažetak	Stanje	Blok	Poruka	Arhitektura	Broj rundi	Funkcije
SHA-1	**160**	**160**	**512**	**$2^{64} - 1$**	**32**	**80**	**+, and, or, xor, rot**
SHA-256/224	**256/224**	**256**	**512**	**$2^{64} - 1$**	**32**	**64**	**+, and, or, xor, shift, rot**
SHA-512/384	**512/384**	**512**	**1024**	**$2^{128} - 1$**	**64**	**80**	**+, and, or, xor, shift, rot**

SHA-3

- 2.11.2007. – NIST raspisuje natječaj za SHA-3
- informacije o natječaju su dostupne na http://csrc.nist.gov/groups/ST/hash/sha-3/index.html
- konačni izbor 2.10.2012. godine
- do 31.10.2008. zabilježeno je 64 prijava:

Abacus	ARIRANG	AURORA	BLAKE	Blender	BMW	BOOLE	Cheetah
CHI	CRUNCH	CubeHash	DCH	Dynamic SHA	Dynamic SHA2	ECHO	ECOH
ENDO-R	EnRUPT	ESSENCE	FSB	Fugue	Groestl	Hamsi	HASH 2x
JH	Keccak	Khichidi-1	LANE	Lesamnta	Luffa	LUX	Maraca
MCSSHA-3	MD6	MeshHash	NaSHA	NKS 2D	Ponic	SANDstorm	Sarmal
Sgail	Shabal	SHAMATA	SHAvite-3	SIMD	Skein	Spectral Hash	StreamHash
SwiFFTX	Tangle	TIB3	Twister	Vortex	Wamm	Waterfall	ZK-Crypt
?	?	?	?	?	?	?	?

SHA-3

- 24.6.2009. objavljena je lista od 14 kandidata za drugi krug:
  - BLAKE
  - BMW - Blue Midnight Wish
  - CubeHash (Bernstein)
  - ECHO (France Telecom)
  - Fugue (IBM)
  - Groestl (Knudsen)
  - Hamsi
  - JH
  - Keccak (Daemen)
  - Luffa
  - Shabal
  - SHAvite-3
  - SIMD
  - Skein (Schneier)

	ARIRANG		BLAKE		BMW		Cheetah
CHI	CRUNCH	CubeHash			Dynamic SHA2	ECHO	
		ESSENCE	FSB	Fugue	Groestl	Hamsi	
JH	Keccak		LANE	Lesamnta	Luffa		
	MD6					SANDstorm	
	Shabal		SHAvite-3	SIMD	Skein		
SwiFFTX							

SHA-3

- 9.12.2010. objavljen je popis 5 finalista
- 2.10.2012. proglašen pobjednik

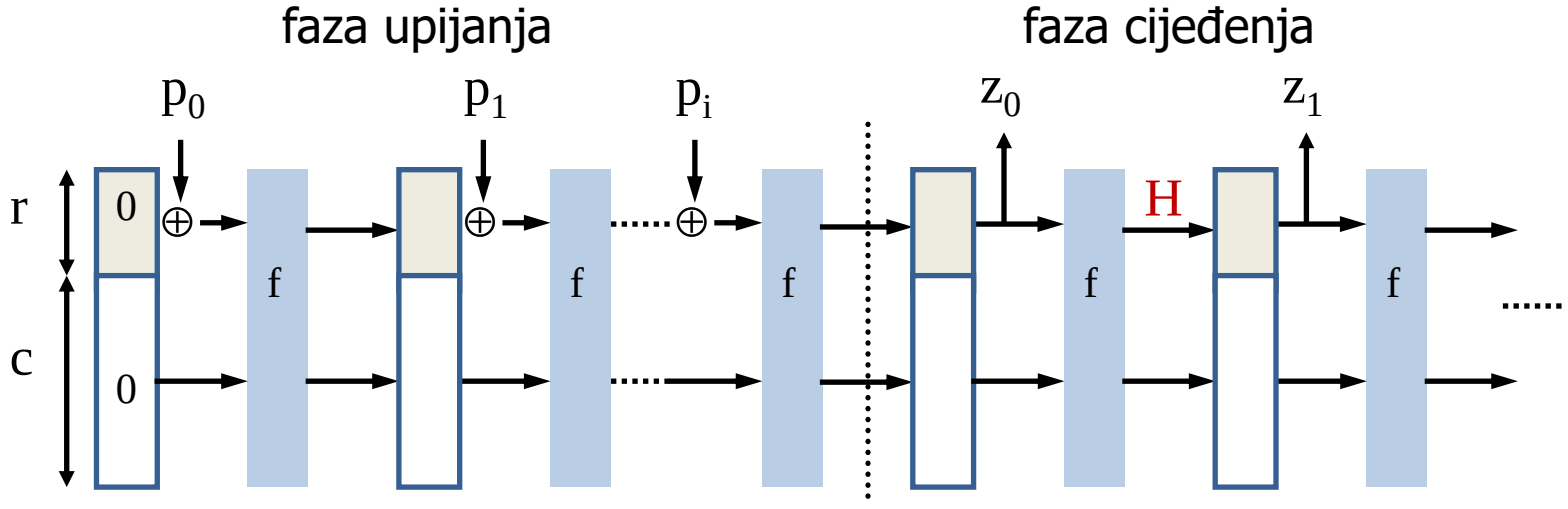
- BLAKE
- Groestl (Knudsen)
- JH
- Keccak (Daemen)
- Skein (Schneier)

			BLAKE		BMW		
		CubeHash				ECHO	
				Fugue	Groestl	Hamsi	
JH	Keccak				Luffa		
	Shabal		SHAvite-3	SIMD	Skein		

SHA-3

- autori su Guido Bertoni, Joan Daemen (autor AES-a), Michaël Peeters, and Gilles Van Assche
- značajno brži od ostalih finalista
- sažeci su jednake duljine kao i kod SHA-2:
  - SHA3-224
  - SHA3-256
  - SHA3-384
  - SHA3-512
- nadopunjavanje zadnjeg bloka teksta (*padding*) je izmijenjeno i obavlja se prema shemi M ||10*1
  - SHA-2: M II 10* II 64-bita za duljinu poruke u bitovima
  - izvorni prijedlog autora algoritma Keccak: M II 10*1000000

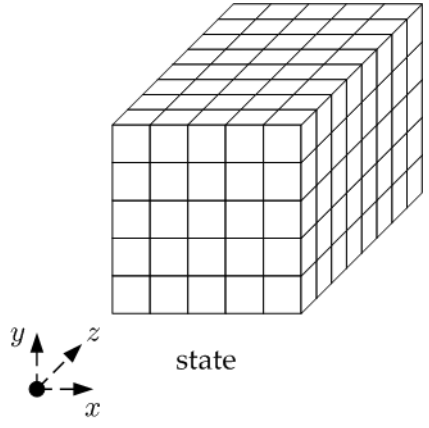
Spužvasta konstrukcija algoritma SHA-3

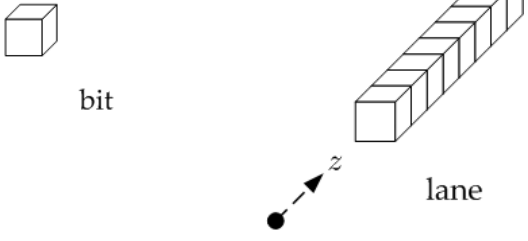


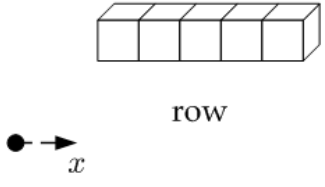
- 25w = c + r = 1600 (za 64 bitne riječi)
- SHA-3: c = 2 x veličina sažetka
  - SHA3-224: c = 448, r = 1152
  - SHA3-256: c = 512, r = 1088
  - SHA3-384: c = 768, r = 832
  - SHA3-512: c = 1024, r = 576

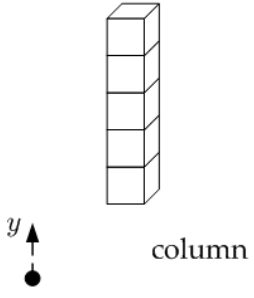
SHA-3: stanje, bit, traka, redak i stupac

- $X = Y = 5$
- duljina trake $Z = w \in \{1, 2, 4, 8, 16, 32, 64\}$
- w je duljina CPU riječi
- Keccak-$f[b]$ gdje je b broj bitova stanja $b = 25w$
  b $\in \{25, 50, 100, 200, 400, 800, 1600\}$
- slike su preuzete sa http://keccak.noekeon.org/

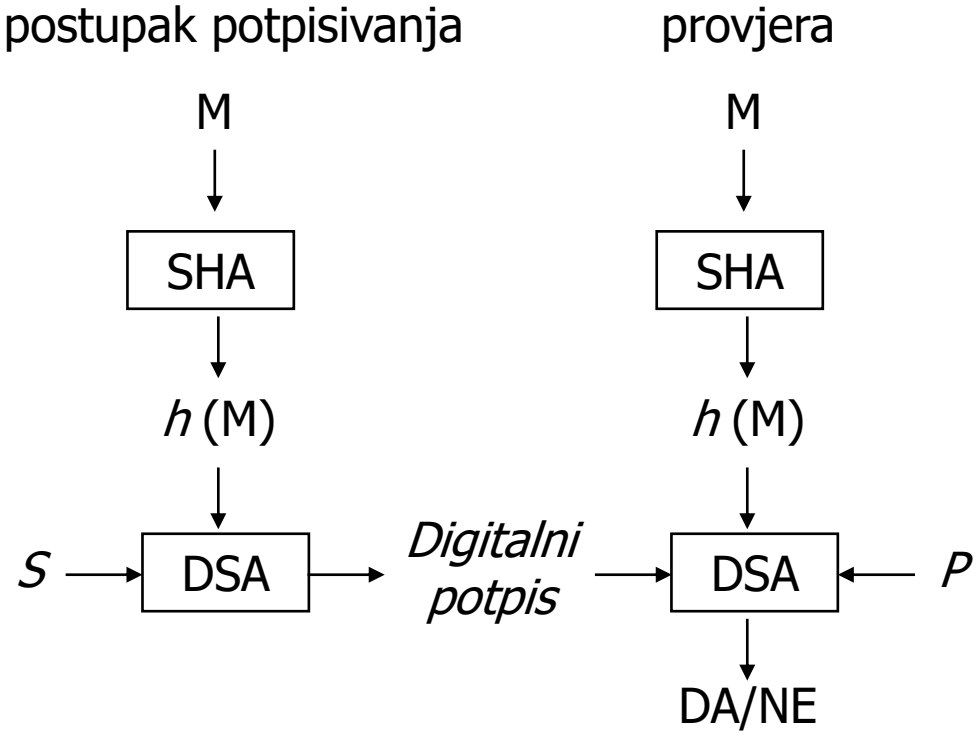








Digitalno potpisivanje dokumenata



- NIST je preporučio 1991. g. algoritam za digitalno potpisivanje elektroničkih dokumenata (*Digital Signature Algorithm* – DSA) da postane sastavni dio norme (*Digital Signature Standard* - DSS)

DSA: generiranje ključeva

- je zapravo *ElGamalov* digitalni potpis
  - L – broj bitova ključa
  - q – prim broj jednake duljine kao i H
  - p – L-bitni prim broj takav da je (p -1) višekratnik od q
  - $g = h^{(p-1)/q} \bmod p$ ($g > 1$), gdje je $h \in (1, p-1)$
  - izabrati $x \in (0, q)$ i izračunati
  - $y = g^x \bmod p$
- privatni ključ je $S = x$, a javni $P = (p, q, g, y)$

DSA: postupak potpisivanja i provjere potpisa

Postupak potpisivanja

- za svaku poruku m generira se slučajni broj $k \in (0, q)$
- $r = (g^k \bmod p) \bmod q$, $r \neq 0$
- $k^{-1} \in (0, q)$ takav da vrijedi $(k^{-1}\ k) \bmod q = 1$
- $s = (k^{-1}(H(m) + xr)) \bmod q$
- digitalni potpis = (r, s)

Provjera potpisa

- $w = s^{-1} \bmod q$
- $v = ((g^{(H(m)*w) \bmod q} * y^{(r*w) \bmod q}) \bmod p) \bmod q$
- potpis je ispravan ako je $v = r$

Pregled napada na funkcije sažimanja

- 1998. Dobbertin pronalazi kolizije za MD4 unutar 1 sekunde na PC računalu
- iste godine F. Chabaud i A. Joux izveli prvi uspješan napad na SHA-0 (prostor pretraživanja je smanjen s 2^{80} na 2^{61})
- 17.8.2004. objavljen rad kineskih i francuskih znanstvenika u kojem su opisane kolizije za MD4, MD5, Haval-128 i RIPEMD
- za SHA-0 je pretraživanja je smanjen s 2^{61} na 2^{51}
  - superračunalo s 256 Itanium procesora pronalazi za 13 dana koliziju
  - par dana nakon ove vijesti kineski znanstvenici objavljuju uspješan napad sa složenošću 2^{40}
  - veljača 2005. godine: prostor pretraživanja je smanjen na 2^{39}
- 13.2.2005. kineski znanstvenici: "*Collision Search Attacks on SHA-1* "
  - prostor pretraživanja 2^{69}
- u kolovozu 2005. prostor pretraživanja za SHA-1 je smanjen na 2^{63}

M1.txt

```
00000000 d1 31 dd 02 c5 e6 ee c4 69 3d 9a 06 98 af f9 5c
00000010 2f ca b5 87 12 46 7e ab 40 04 58 3e b8 fb 7f 89
00000020 55 ad 34 06 09 f4 b3 02 83 e4 88 83 25 71 41 5a
00000030 08 51 25 e8 f7 cd c9 9f d9 1d bd f2 80 37 3c 5b
00000040 96 0b 1d d1 dc 41 7b 9c e4 d8 97 f4 5a 65 55 d5
00000050 35 73 9a c7 f0 eb fd 0c 30 29 f1 66 d1 09 b1 8f
00000060 75 27 7f 79 30 d5 5c eb 22 e8 ad ba 79 cc 15 5c
00000070 ed 74 cb dd 5f c5 d3 6d b1 9b 0a d8 35 cc a7 e3
```

M2.txt

```
00000000 d1 31 dd 02 c5 e6 ee c4 69 3d 9a 06 98 af f9 5c
00000010 2f ca b5 07 12 46 7e ab 40 04 58 3e b8 fb 7f 89
00000020 55 ad 34 06 09 f4 b3 02 83 e4 88 83 25 f1 41 5a
00000030 08 51 25 e8 f7 cd c9 9f d9 1d bd 72 80 37 3c 5b
00000040 96 0b 1d d1 dc 41 7b 9c e4 d8 97 f4 5a 65 55 d5
00000050 35 73 9a 47 f0 eb fd 0c 30 29 f1 66 d1 09 b1 8f
00000060 75 27 7f 79 30 d5 5c eb 22 e8 ad ba 79 4c 15 5c
00000070 ed 74 cb dd 5f c5 d3 6d b1 9b 0a 58 35 cc a7 e3
```

MD5 Sum(M1.txt) = **a4c0d35c95a63a805915367dcfe6b751**

MD5 Sum(M2.txt) = **a4c0d35c95a63a805915367dcfe6b751**

M1.txt

```
00000000 d1 31 dd 02 c5 e6 ee c4 69 3d 9a 06 98 af f9 5c
00000010 2f ca b5 87 12 46 7e ab 40 04 58 3e b8 fb 7f 89
00000020 55 ad 34 06 09 f4 b3 02 83 e4 88 83 25 71 41 5a
00000030 08 51 25 e8 f7 cd c9 9f d9 1d bd f2 80 37 3c 5b
00000040 96 0b 1d d1 dc 41 7b 9c e4 d8 97 f4 5a 65 55 d5
00000050 35 73 9a c7 f0 eb fd 0c 30 29 f1 66 d1 09 b1 8f
00000060 75 27 7f 79 30 d5 5c eb 22 e8 ad ba 79 cc 15 5c
00000070 ed 74 cb dd 5f c5 d3 6d b1 9b 0a d8 35 cc a7 e3
```

M2.txt

```
00000000 d1 31 dd 02 c5 e6 ee c4 69 3d 9a 06 98 af f9 5c
00000010 2f ca b5 07 12 46 7e ab 40 04 58 3e b8 fb 7f 89
00000020 55 ad 34 06 09 f4 b3 02 83 e4 88 83 25 f1 41 5a
00000030 08 51 25 e8 f7 cd c9 9f d9 1d bd 72 80 37 3c 5b
00000040 96 0b 1d d1 dc 41 7b 9c e4 d8 97 f4 5a 65 55 d5
00000050 35 73 9a 47 f0 eb fd 0c 30 29 f1 66 d1 09 b1 8f
00000060 75 27 7f 79 30 d5 5c eb 22 e8 ad ba 79 4c 15 5c
00000070 ed 74 cb dd 5f c5 d3 6d b1 9b 0a 58 35 cc a7 e3
```

MD5 Sum(M1.txt) = **a4c0d35c95a63a805915367dcfe6b751**

MD5 Sum(M2.txt) = **a4c0d35c95a63a805915367dcfe6b751**

Digitalni certifikat

FER-ov digitalni certifikat od 2008 do 2018

```
Certificate:
   Data:
       Version: 3 (0x2)
       Serial Number: 75 (0x4b)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: C=US, ST=WA, L=Seattle, O=Thawte Consulting cc,
               OU=Certification Services Division,
               CN=Thawte Server CA/emailAddress=certs@thawte.com
       Validity
           Not Before: May 13 23:33:08 2008 GMT
           Not After : Dec 31 23:59:59 2020 GMT
       Subject: C=HR, ST=Grad Zagreb, L=Zagreb, O=FER, OU=CIP,
                CN=webmail.fer.hr/emailAddress=korisnik@webmail.fer.hr
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (1024 bit)
               Modulus:
                    00:cd:66:28:fb:b8:b3:b7:e0:72:77:48:2d:08:04:
                    e1:6d:1c:c5:4f:57:73:0c:e6:db:3b:8e:cd:c6:25:
                    61:7f:60:c9:da:a3:9f:1d:fa:d8:ef:00:7b:f9:54:
                    65:ab:7e:9e:9b:6d:ff:d4:12:ad:f8:ac:87:6e:83:
                    ec:65:5f:b4:2d:eb:b8:dc:1c:d7:32:b7:46:a5:e3:
                    a1:6c:0b:4c:1b:0c:89:0a:fb:0e:3a:c0:0f:af:b2:
                    62:1d:2f:60:e4:b1:27:b4:7c:59:00:2c:19:e9:f3:
                    a3:88:fe:01:d6:56:be:26:c7:f8:42:b1:79:39:98:
                    a1:b4:4a:84:dd:20:ca:e7:a9:db:6d:a6:73:88:e7:
                    81:8b:3e:81:3d:00:e5:5d:7f:3d:9b:cd:ba:9b:28:
                    88:88:7f:d7:69:2c:66:eb:8f:79:b8:ec:bc:bb:76:
                    67:b1:00:2a:70:bd:f1:21:66:6f:ba:74:81:82:30:
                    02:c0:a8:57:f8:9f:76:02:df:7f:49:44:4a:32:93:
                    48:a4:25:73:47:10:21:20:fe:b6:d2:09:1a:60:4f:
                    a5:d9:df:ea:55:49:43:c6:ce:96:0b:7d:a7:22:c1:
                    3e:5b:28:2e:2c:04:7a:b2:93:89:db:d8:2b:59:86:
                    a3:0a:c1:6f:f9:56:b2:a5:71:4c:4b:74:f3:b8:a1:
                    b4:65
               Exponent: 65537 (0x10001)
       X509v3 extensions:
           X509v3 Basic Constraints: critical
               CA:TRUE
   Signature Algorithm: md5WithRSAEncryption
       07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:
       a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:
       e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
       b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:
       70:47
```

Digitalni certifikat

Pristup web stranicama FER-a:
The connection to this site is encrypted and authenticated using TLS 1.2, ECDHE_RSA with P-256, and AES_128_GCM.

```
Certificate:
    Data: Version: 3 (0x2)
        Serial Number: 0a:2f:ab:75:d4:a1:ee:f5:ea:df:74:15:aa:fd:47:c4
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=NL, ST=Noord-Holland, L=Amsterdam, O=TERENA, CN=TERENA SSL CA 3
    Validity  Not Before: May 13 00:00:00 2018 GMT
              Not After : May 20 12:00:00 2020 GMT
    Subject: C=HR, L=Zagreb, O=Sveu\xC4\x8Dili\xC5\xA1te u Zagrebu, OU=CIP,
      CN=*.fer.unizg.hr
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c6:bb:ca:00:b5:40:96:b3:6b:2e:94:7e:43:77:
                    39:06:d2:4f:11:c0:c4:17:e5:eb:d6:10:a5:2c:fa:
                    4c:f1:50:35:59:59:2b:fa:b5:22:26:3f:0a:ff:f2:
                    f9:c4:d7:e2:67:5d:bf:b5:c1:cc:6b:77:31:e9:de:
                    95:b0:76:53:47:f7:1f:fe:c4:5b:c1:a7:fd:c4:fc:
                    61:d3:ea:b5:28:48:e5:d5:96:a0:11:ed:0b:00:a2:
                    42:c9:fa:94:26:89:f5:37:db:0a:9a:f8:95:e8:a6:
                    35:8a:68:33:90:c2:22:10:ad:65:3a:95:5f:64:1f:
                    6f:43:88:b2:1c:f8:29:9e:51:6b:e4:2d:8c:3e:39:
                    90:f7:31:8e:32:f8:0f:cf:3e:b4:7a:c6:f3:27:17:
                    a3:4e:3c:7c:27:07:3d:68:fc:5e:9c:87:86:74:ea:
                    22:32:d5:aa:93:e4:d4:78:23:d2:88:0f:e3:8f:05:
                    8c:54:b8:95:29:eb:c2:0a:fc:26:20:ca:52:ff:ce:
                    75:6b:29:82:d6:67:06:0b:49:53:37:0d:7e:cf:1c:
                    7e:88:90:8d:7a:e7:99:fc:9f:d7:5c:e2:1f:73:19:
                    cc:27:ba:31:6f:82:40:b0:cb:8a:d2:95:f4:6e:72:
                    78:b6:02:f5:f4:0b:b6:60:32:fb:3f:34:66:f2:a4:
                    12:c5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:67:FD:88:20:14:27:98:C7:09:D2:25:19:BB:E9:51:11:63:75:50:62
                  URI:http://crl3.digicert.com/TERENASSLCA3.crl
...
    Signature Algorithm: sha256WithRSAEncryption
         a3:aa:9b:c3:04:c3:5c:64:32:9c:8f:08:31:89:15:8a:52:19:
         fb:02:e9:dd:ab:59:3e:9e:d8:b8:52:b2:8d:df:5a:29:dc:2b:
         c0:01:7d:96:87:5c:a7:01:7e:26:c9:3b:be:01:d3:9c:71:62:
         e3:e5:a2:ce:5d:ee:59:b5:ed:20:d8:80:27:ac:af:f5:6a:73:
         79:35:d2:c5
```

Napad tablicama s unaprijed izračunatim sažecima

- *engl. rainbow table*
- za najčešće korištene zaporke se unaprijed izračunaju sažeci
- zapisi u datoteci sa zaštićenim lozinkama se uspoređuju s unaprijed izračunatim sažecima
- 20 najčešće korištenih zaporki 2018. g.

123456	12345	qwerty	welcome	123123
password	111111	iloveyou	666666	monkey
123456789	1234567	princess	abc123	654321
12345678	sunshine	admin	football	!@#$%^&*

Zaključak o funkcijama sažimanja

- kolizije su bezopasne sve dok izgledaju kao slučajan niz
- međutim, gubi se povjerenje u certifikate
  - protokoli koji koriste sažetak slučajnog simetričnog ključa nisu više sigurni
- problem nevidljivih podataka u Word dokumentu ili slučajnih nizova u slikama
- rješenje:
  - koristiti obične tekstualne datoteke ili potpisati sažetu datoteku (kao što PGP koristi *zip*)
  - koristiti novi algoritam sažimanja SHA-3

Preporuke prema europskom programu potpore klasifikacije kvalitete elektroničkog potpisa

Algoritam	niža razina sigurnosti	viša razina sigurnosti
RSA, n=	1024	2432
ECDSA	160	224
HASH	SHA-224	SHA-256

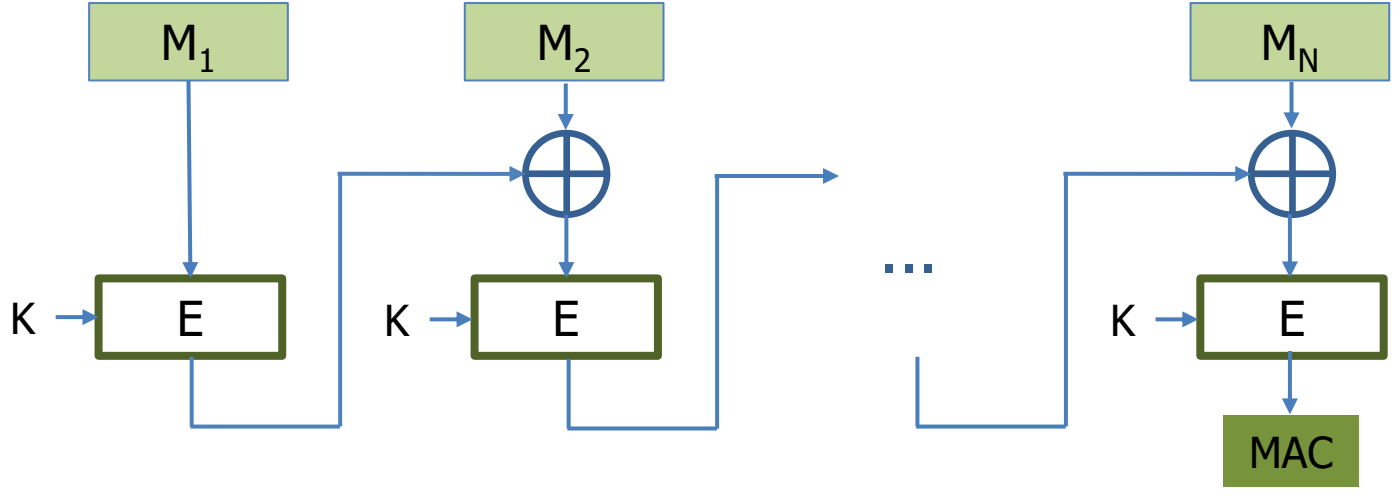
- Ostali parametri RSA:
  - $p \cong q$
  - d>>
  - e>65536

Autentifikacijsko kriptiranje

- postupak kriptiranja koji uključuje i autentifikaciju (*Authenticated Encryption,* AE) i osim tajnosti osigurava
  - integritet, odnosno izvornost (autentičnost)
  - autentifikaciju pošiljatelja
- kombinacija kriptografskih algoritama:
  kriptiranje + MAC (*Message Authentication Code*)
  - *Encrypt-then-MAC (EtM)*
  - *Encrypt-and-MAC (E&M)*
  - *MAC-then-Encrypt (MtE)*
- dodatak poruci MAC za razliku od digitalnog potpisa ne koristi asimetričnu kriptografiju, već samo simetričnu kriptografiju
  - ulaz u algoritam je uz poruku tajni ključ
  - Kako je osigurana autentičnost?
    - Poruku je poslao onaj tko ima tajni ključ.

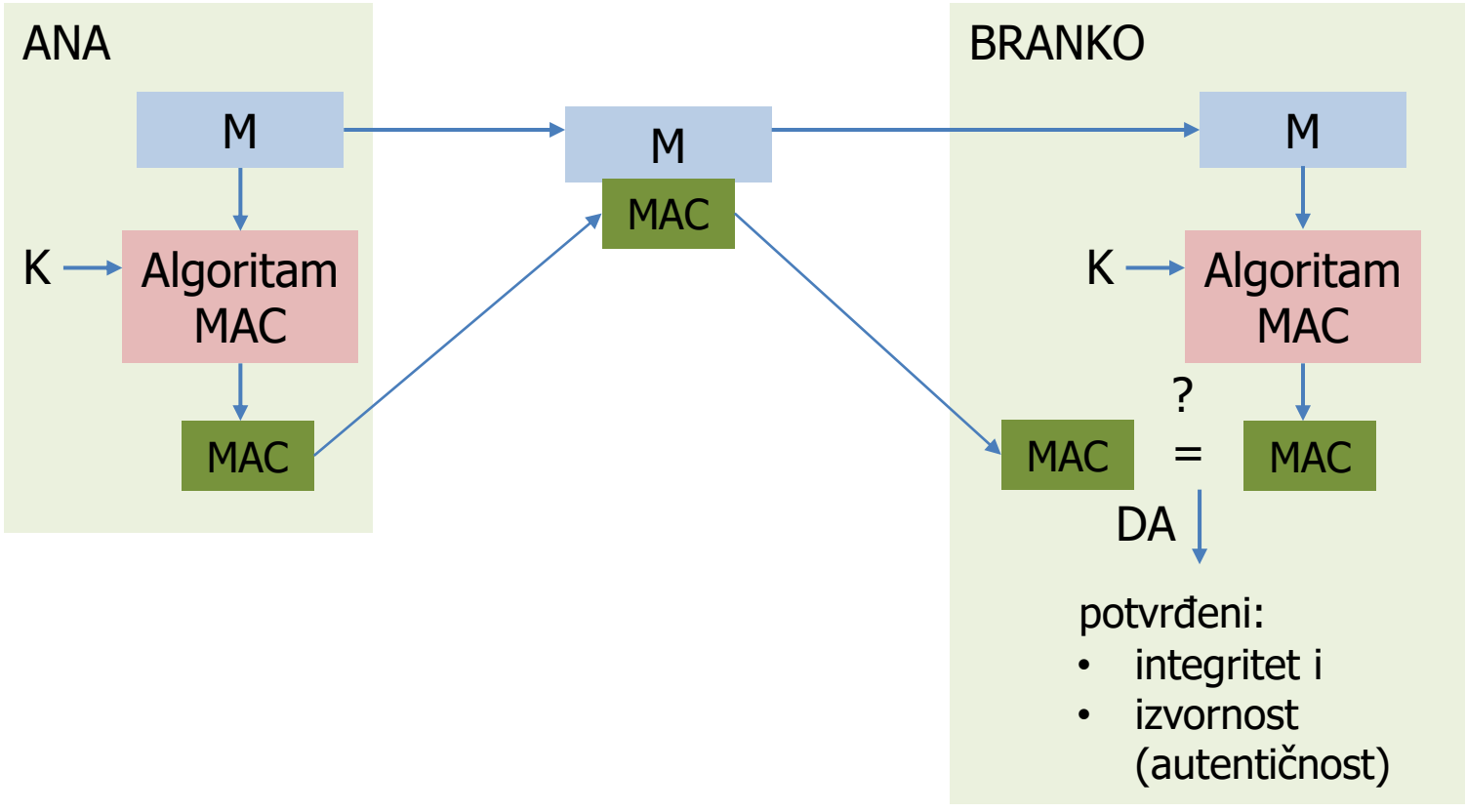
Algoritam MAC

- *Message Authentication Code*
- u CBC načinu rada naziva se CBC-MAC



- varijante:
  - One-key ili OMAC, PMAC, HMAC ...

Primjer kako se može koristiti dodatak poruci MAC



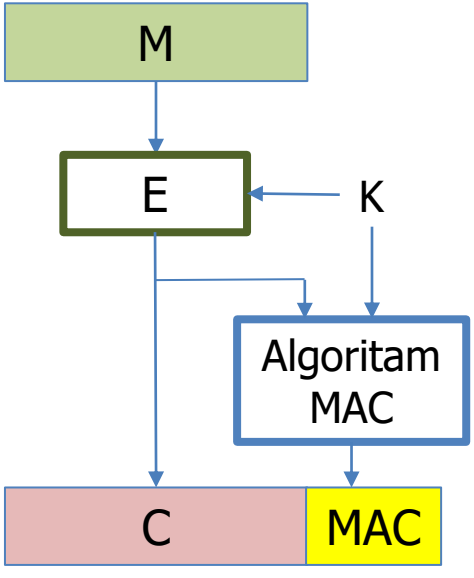
Algoritam HMAC

- *keyed-Hash Message Authentication Code*
  - HMAC_MD5
  - HMAC_SHA1
  - HMAC_SHA256
  - HMAC_SHA3

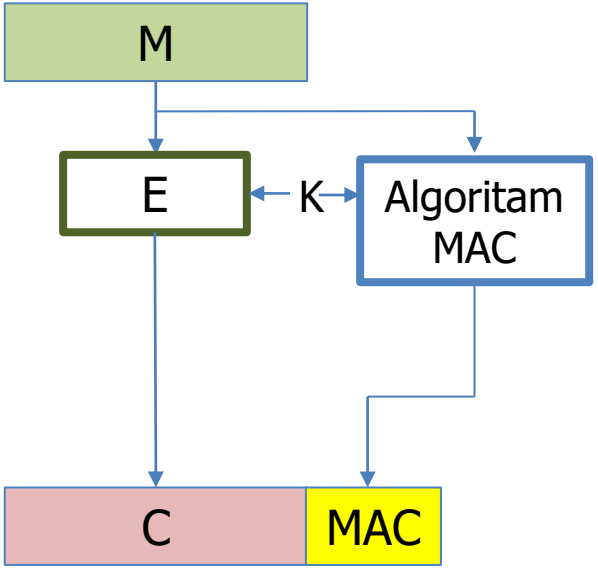
- $HMAC(K,M) = H\{(K' \oplus opad) || H[(K' \oplus ipad) || M]\}$
  - K' = H(K) ako je K veći od veličine bloka, inače K' = K
  - konstanta *opad (outer padding*) = 0x5c5c5c...5c5c
  - konstanta *ipad* (*inner padding*) = 0x363636...3636
  - *opad* i *ipad* su veličine jednog bloka

Kako uz integritet i autentičnost osigurati i tajnost?

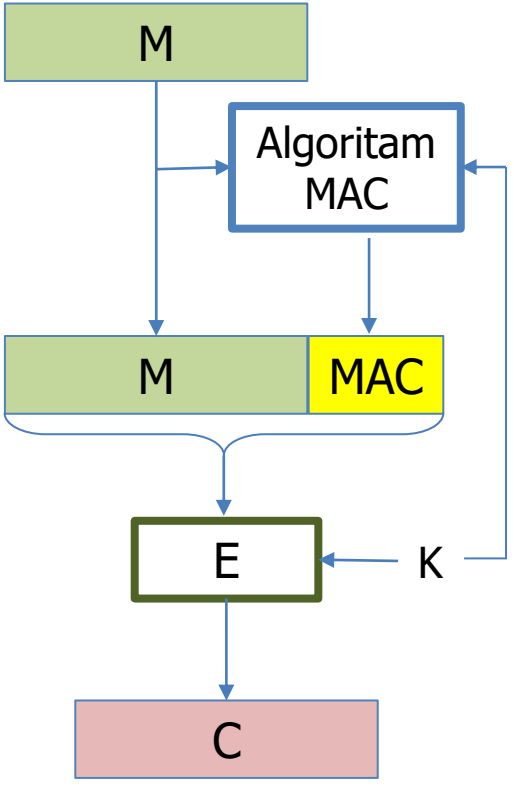
EtM



E&M

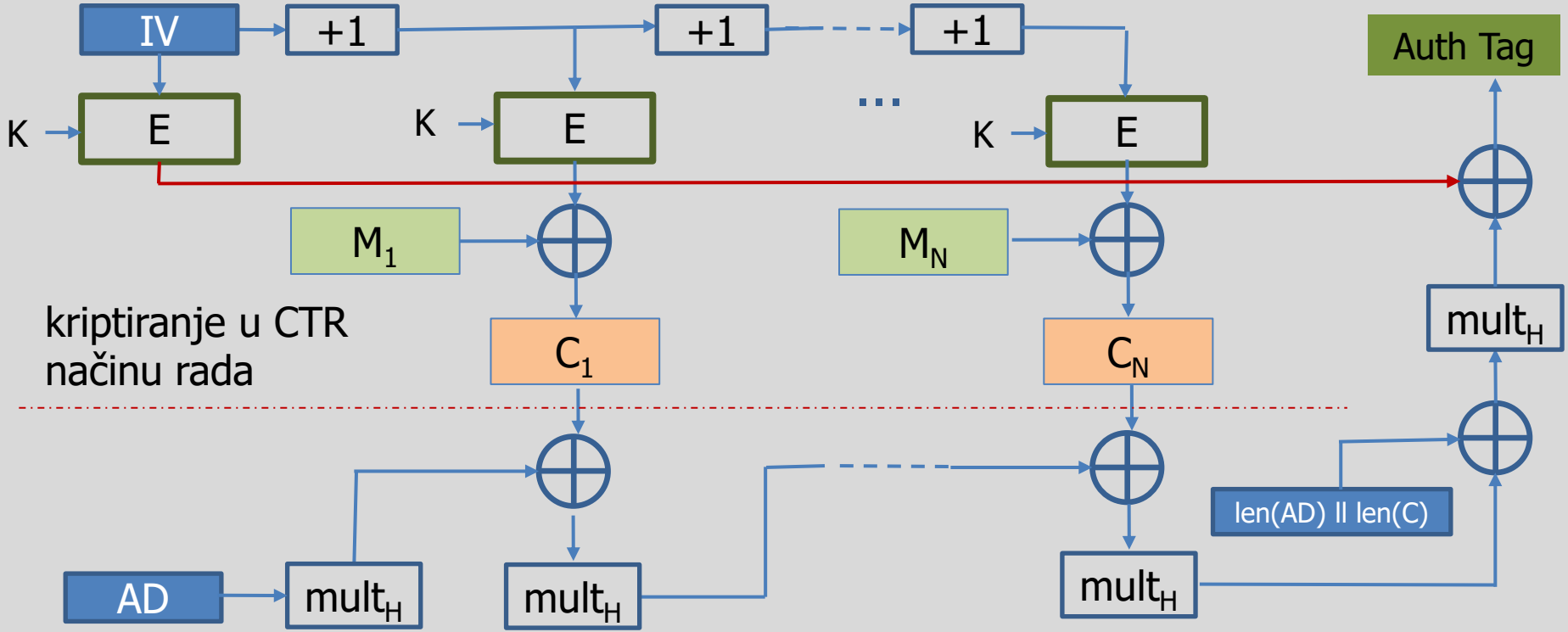


MtE



GCM - *Galois/Counter Mode*

- način autentifikacijskog kriptiranja koji je primjenjiv samo za simetrične blok algoritme s veličninom bloka 128 bita
- varijanta *Galois Message Authentication Code, GMAC* – samo za autentifikaciju



Zaključne napomene o autentifikacijskom kriptiranju

- nedostatak klasičnih autentifikacijskih kriptografskih shema poput *EtM, E&M i MtE* je upravo u primjeni više algoritama
- natječaj CAESAR (*Competition for Authenticated Encryption: Security, Applicability, and Robustness*) završio 20.3.2019. objavljeno 3 pobjednika u 3 kategorije i 5 rezervna algoritma
  - Ascon, ACORN, AEGIS (Bart Prenel, ...), OCB, Deoxys, COLM, AES-COPA, ELmD
  - 15 algoritama u trećem krugu natječaja, a ispali su:
    - AES-OTR, AEZ, CLOC and SILC, JAMBU, Katje (Daemen, ...), Keyak (Daemen, ...), MORUS, NORX, Tiaoxin
- u tijeku je i NIST-ov natječaj za novi algoritam prilagođen okruženju s ograničenim računalnim resursima (*lightweigt cryptography*)
  - algoritam treba osim simetričnog uključivati i autentifikacijsko kriptiranje (*Authenticated Encryption with Associated Data*, AEAD)

Pobjednici na natječaju CAESAR

Pobjednic su birani u tri kategorije:

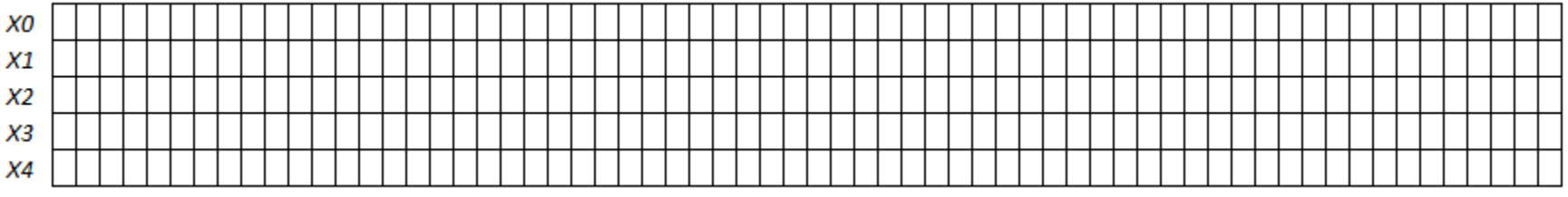
1. Algoritmi koji su najmanje zahtjevni na računalne resurse (*Lightweight applications - resource constrained environments*)
   - prvi izbor: Ascon (web)
   - drugi izbor: ACORN
2. Algoritmi visokih performansi (*High-performance applications*)
   - prvi izbor: AEGIS-128
   - drugi izbor: OCB
3. Višerazinska sigurnost (*Defense in depth*)
   - prvi izbor: Deoxys-II
   - drugi izbor: COLM ili AES-COPA ili ELmD

ASCON

- pobjednik u natječaju CAESAR i sudjeluje u NIST-ovom natječaju za kriptografiju prilagođenu uređajima s ograničenim mogućnostima (*lightweight crypto*)
- uz autentifikacijsko kriptiranje (ASCON-128 i ASCON-128a) omogućuje i izračunavanje sažetka poruke (ASCON-HASH i ASCON-XOF)
- jasni tekst *M* i pridruženi podaci *AD* (*Associated Data*) se dijele na blokove od po
  - r=64 bita = ASCON-128 (broj rundi *b* =6) ili
  - r=128 bitova = ASCON-128a (broj rundi *b* =8)
- ključ *K* je veličine 128 bita kao i *nonce N* i *tag T*
- kriptiranje ili sažimanje obavlja se iterativnom uporabom samo jedne „lagane" (*lightweight*) funkcije permutacije *p* koja se sastoji od
  - zbrajanja s konstantom
  - supstitucije (*nonlinear substitution layer*)
  - linearne difuzije (*lineat diffusion layer*)

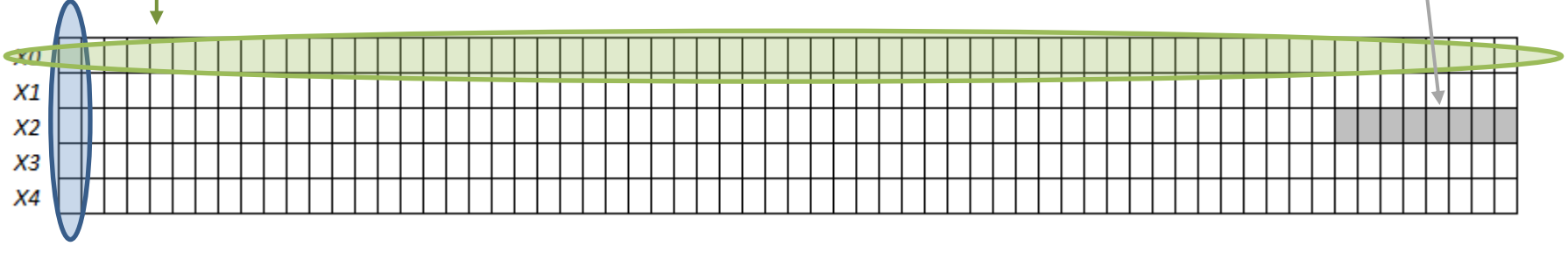
ASCON – struktura podataka

- *lagana* permutacija *p* obavlja se nad *stanjem*
- ulaz u permutaciju i izlaz iz permutacije je stanje (*state*), tj. struktura podataka koja prelazi iz stanja u stanje
- sastoji se od pet 64-bitnih riječi: x_0, x_1, x_2, x_3 i x_4
- ukupne veličine 320 bitova:



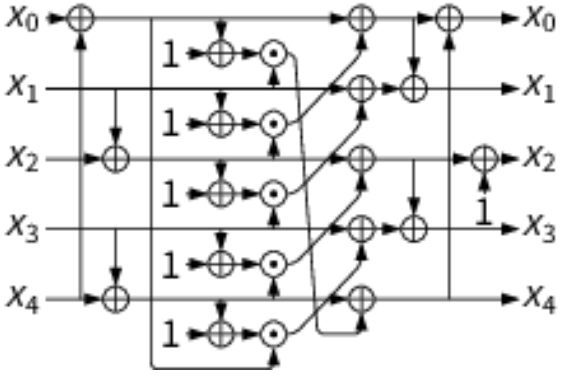
ASCON – permutacija *p*

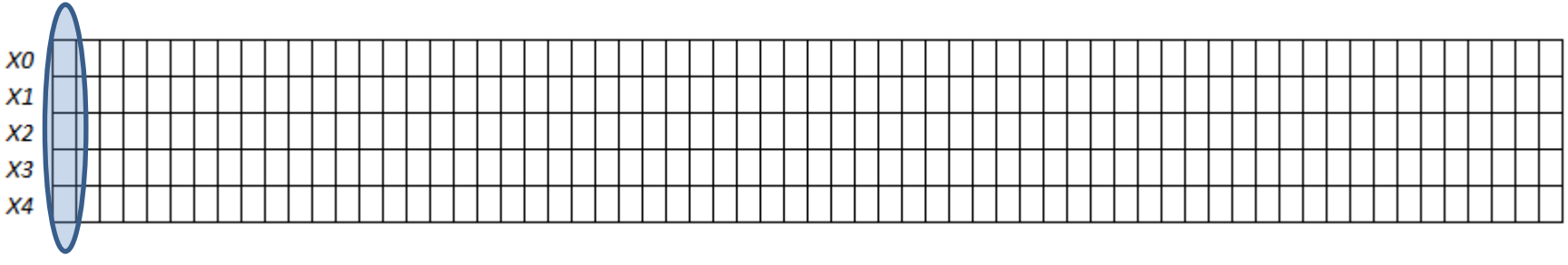
- zbrajanja s konstantom *Cr* (jedan bajt) i to samo nad *X2*
- supstitucije (*nonlinear substitution layer*)
  - S-BOX
  - djeluje nad svim stupcima stanja što se može paralelizirati
- linearne difuzije (*lineat diffusion layer*)
  - djeluje nad retcima stanja što se također može paralelizirati



ASCON – permutacija *p* - supstitucija

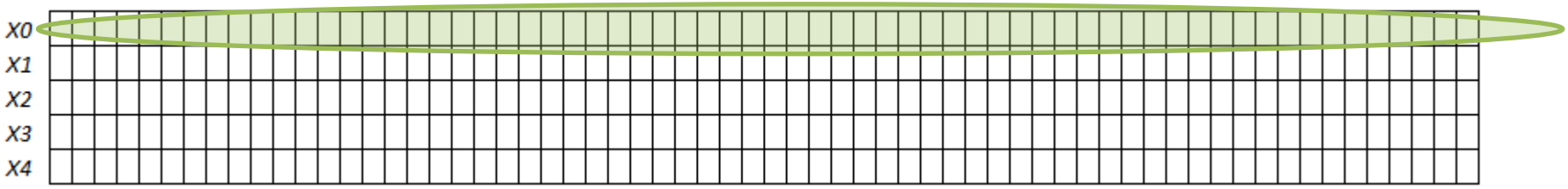
- djeluje nad svih 64 stupaca stanja
- umjesto supstitucijske tablice, može se prikazati slikom:
  - slika je preuzeta sa službenih stranica algoritma https://ascon.iaik.tugraz.at/specification.html





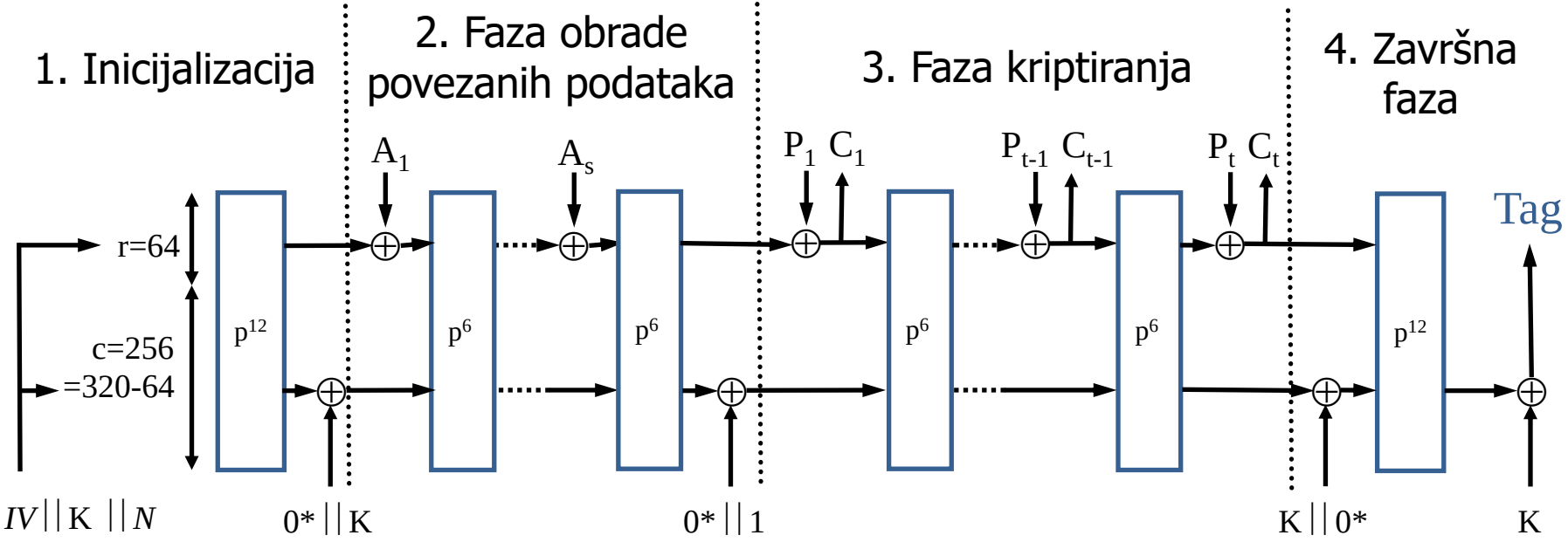
ASCON – permutacija *p* - difuzija

- djeluje nad svih 5 redaka stanja
- koristi se rotacija, oznaka <<<
- zbrajaju se tri varijante svakog retka:
  - X0 = X0 ⊕ (X0 <<< 19) ⊕ (X0 <<< 28)
  - X1 = X1 ⊕ (X1 <<< 61) ⊕ (X1 <<< 39)
  - X2 = X2 ⊕ (X2 <<< 1) ⊕ (X2 <<< 6)
  - X3 = X3 ⊕ (X3 <<< 10) ⊕ (X3 <<< 17)
  - X4 = X4 ⊕ (X4 <<< 7) ⊕ (X4 <<< 41)



Dvostruka spužvasta konstrukcija algoritma ASCON-128

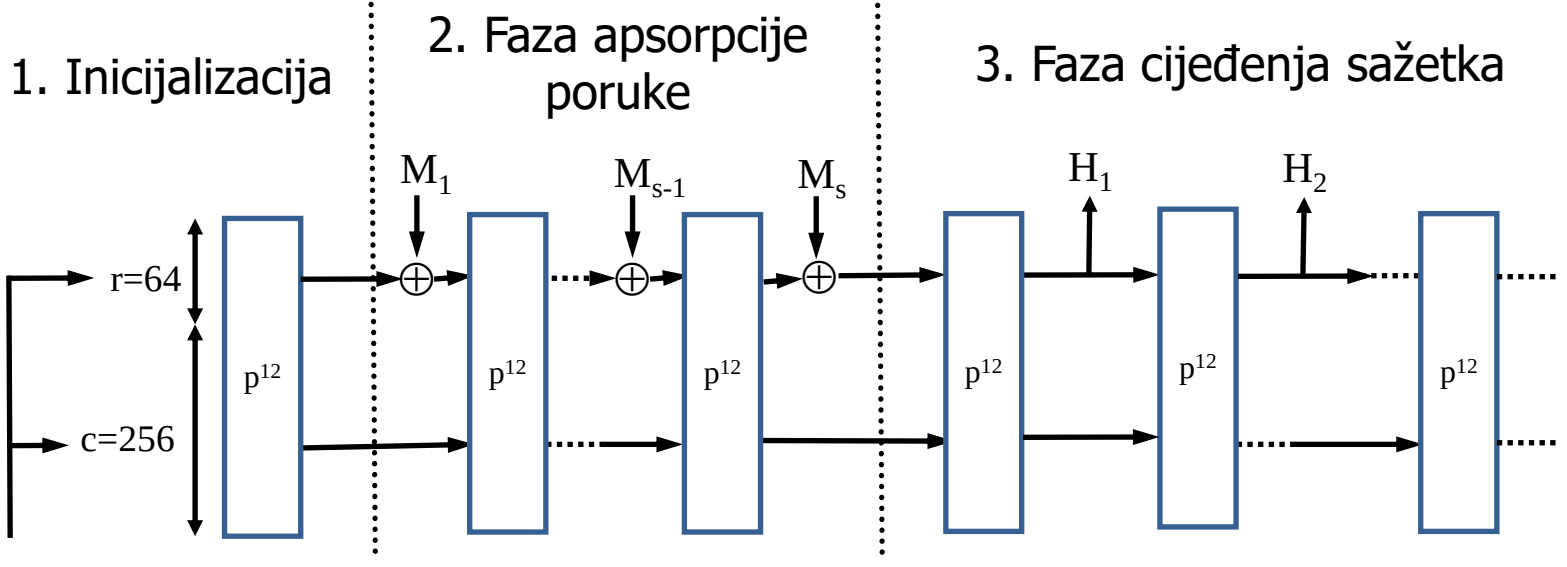
- odvija se u 4 faze
- permutacije se obavljaju ili u 12 ili u 6 rundi
- permutacije kod algoritma ASCON-128a se obavljaju ili u 12 ili u 8 rundi



IV je unaprijed određen i iznosi 80400c0600000000

Izračunavanje sažetka uz pomoć algoritma ASCON-HASH

- odvija se u 3 faze
- veličina sažetka najmanje 256 bita
- ima više varijanti, a u ovoj osnovnoj se sve permutacije obavljaju u 12 rundi
- varijanta algoritma ASCON-XOF je jednaka ASCON-HASH, ali sažetak može biti proizvoljne duljine



Kriptografija prilagođena okruženju s ograničenim računalnim resursima

Lightweight Cryptography

Natječaj

- https://csrc.nist.gov/Projects/Lightweight-Cryptography/
- za ograničene računalne resurse, primjerice
  - ugrađene sustave
  - Internet stvari
- Na NIST-ovoj radionici 20.6.2015. "Lightweight Cryptography Workshop 2015" iskazuje se potreba za novim oblikom kriptografije koja djeluje u okruženju s ograničenim računalnim resursima.
- NIST raspisuje natječaj 27.8.2018.
- 25.2.2019. je pristiglo 57 kandidata od kojih 56 zadovoljava uvjete natječaja
- 29.3.2021. objavljeno 10 finalista

Uvjeti natječaja 1/3

- algoritam ili skup algoritama koji osim
  - simetrične i
  - autentifikacijske kriptografije (*Authenticated Encryption with Associated Data*, AEAD)

  mogu opcionalno imati funkcionalnost
  - izračunavanja sažetka (*hash*)
- zahtjevi za spremnikom (RAM i ROM) trebaju biti što je moguće manji
- moraju se moći izvoditi i u sljedećim sklopovskim okruženjima
  - FPGA
  - ASIC
  - 8, 16 i 32-bitnim mikrokontrolerima

Uvjeti natječaja 2/3

- veličina ključa 128 bita ili više
- složenost napada grubom silom ne smije biti manja od 2^{112}
- ako algoritam podržava veći ključ od 128 bita tada mora
  - imati mogućnost veličine ključa od 256 bita i
  - složenost napada grubom silom mora biti najmanje 2^{224}
- najmanja veličina parametara:
  - nonce treba biti veličine najmanje 96 bita
  - *tag* najmanje 64 bita
- najveća duljina poruke ne smije biti manja od $2^{50}-1$

Uvjeti natječaja 3/3

Simetrični i autentifikacijski algoritam, AEAD

- ulaz u AEAD se sastoji od 4 dijela
  - jasni tekst varijabilne duljine
  - pridruženi podaci (*associated data*) varijabilne duljine
  - *nonce*
  - ključ
- izlaz je kriptirani tekst

Funkcija za izračunavanje sažetka poruke, *hash*

- opcionalan
- izlaz mora biti minimalno 256 bita
- napad grubom silom mora biti najmanje složenosti 2^{112}

18.4.2019. objavljeno
56 kandidata za prvi krug natječaja

ACE	**ASCON**	**Bleep64**	**CiliPadi**	**CLAE**	**CLX**	**COMET**	**DryGASCON**
Elephant	**ESTATE**	**FlexAEAD**	**ForkAE**	**Fountain**	**GAGE and InGAGE**	**GIFT-COFB**	**Gimli**
Grain-128AEAD	**HERN & HERON**	**HYENA**	**ISAP**	**KNOT**	**LAEM**	**Lilliput-AE**	**Limdolen**
LOTUS-AEAD and LOCUS-AEAD	**mixFeed**	**ORANGE**	**Oribatida**	**PHOTON-Beetle**	**Pyjamask**	**Qameleon**	**Quartet**
REMUS	**Romulus**	**SAEAES**	**Saturnin**	**Shamash & Shamashash**	**SIMPLE**	**SIV-Rijndael256**	**SIV-TEM-PHOTON**
SKINNY-AEAD /SKINNY-HASH	**SNEIK**	**SPARKLE**	**SPIX**	**SpoC**	**Spook**	**Subterranean 2.0**	**SUNDAE-GIFT**
Sycon	**TGIF (Thank Goodness It's Friday)**	**TinyJambu**	**Triad**	**TRIFLE**	**WAGE**	**Xoodyak**	**Yarará and Coral**

30.8.2019. objavljeno
32 kandidata za drugi krug natječaja
od čega 12 kandidata imaju mogućnost izračunavanja sažetka

ACE	**ASCON**	Bleep64	CiliPadi	CLAE	CLX	**COMET**	**DryGASCON**
Elephant	**ESTATE**	FlexAEAD	**ForkAE**	Fountain	GAGE and InGAGE	**GIFT-COFB**	**Gimli**
Grain-128AEAD	HERN & HERON	**HYENA**	**ISAP**	**KNOT**	LAEM	Lilliput-AE	Limdolen
LOTUS-AEAD and LOCUS-AEAD	**mixFeed**	**ORANGE**	**Oribatida**	**PHOTON-Beetle**	**Pyjamask**	Qameleon	Quartet
REMUS	**Romulus**	**SAEAES**	**Saturnin**	Shamash & Shamashash	SIMPLE	SIV-Rijndael256	SIV-TEM-PHOTON
SKINNY-AEAD /SKINNY-HASH	SNEIK	**SPARKLE**	**SPIX**	**SpoC**	**Spook**	**Subterranean 2.0**	**SUNDAE-GIFT**
Sycon	TGIF (Thank Goodness It's Friday)	**TinyJambu**	Triad	TRIFLE	**WAGE**	**Xoodyak**	Yarará and Coral

29.3.2021. objavljeno 10 finalista

od čega 4 kandidata imaju mogućnost izračunavanja sažetka

ACE	**ASCON**	Bleep64	CiliPadi	CLAE	CLX	COMET	DryGASCON
Elephant	ESTATE	FlexAEAD	ForkAE	Fountain	GAGE and InGAGE	**GIFT-COFB**	Gimli
Grain-128AEAD	HERN & HERON	HYENA	**ISAP**	KNOT	LAEM	Lilliput-AE	Lindobler
LOTUS-AEAD and LOCUS-AEAD	mixFeed	ORANGE	Oribatida	**PHOTON-Beetle**	Pyjamask	Qameleon	Quartet
REMUS	**Romulus**	SAEAES	Saturnin	Shamash & Shamashash	SIMPLE	SIV-Rijndael256	SIV-TEM-PHOTON
SKINNY-AEAD /SKINNY-HASH	SNEIK	**SPARKLE**	SPIX	SpoC	Spook	Subterranean 2.0	SUNDAE-GIFT
Sycon	TGIF (Thank Goodness It's Friday)	**TinyJambu**	Triad	TRIFLE	WAGE	**Xoodyak** **Joan Daemen** **...**	Yarará and Corá

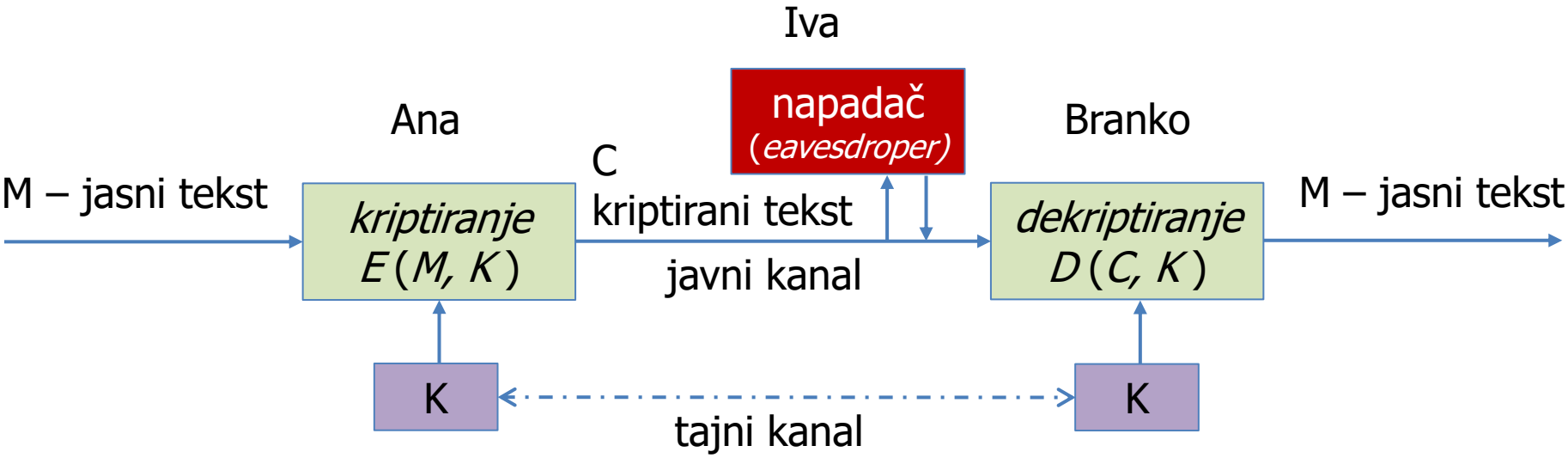
Elektronički potpis

- 17. siječnja 2002. donešen je Zakon o elektroničkom potpisu
- Elektronički potpis je skup podataka u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koji služe za identifikaciju potpisnika i vjerodostojnosti potpisanoga elektroničkog dokumenta.
- Napredan elektronički potpis je elektronički potpis koji pouzdano jamči identitet potpisnika i koji udovoljava sljedećim zahtjevima:
  1. elektronički potpis je povezan isključivo s potpisnikom,
  2. nedvojbeno identificira potpisnika,
  3. nastaje korištenjem sredstava kojima potpisnik može samostalno upravljati i koja su isključivo pod nadzorom potpisnika,
  4. sadržava izravnu povezanost s podacima na koje se odnosi i to na način koji nedvojbeno omogućava uvid u bilo koju izmjenu izvornih podataka.

Kvantna kriptografija

- danas se računalna sigurnost zasniva na nedokazanoj činjenici da ne postoji djelotvoran algoritam za faktorizaciju velikih brojeva te za izračun diskretnog logaritma
- Shor, 1994.: kvantni algoritam (može se ostvariti na kvantnom računalu) za brzu faktorizaciju brojeva
- moguće rješenje: protokol QKD
- prvi takav protokol: BB84
  - predložili su ga Charles H.Bennett (IBM) i Gilles Brassard
  - koristi dva kanala: javni i kvantni (optički kabel)

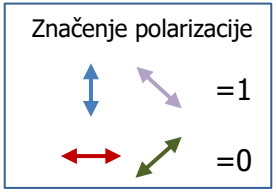
Protokol BB84



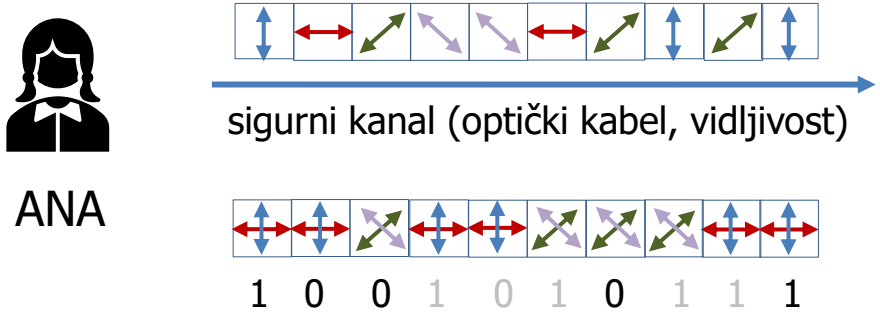
4 moguće polarizacije fotona:

- baza $\oplus$: foton je ili vertikalno (90°) ili horizontalno (0°) polariziran
- baza $\otimes$: foton je dijagonalno polariziran (45° ili 135°)

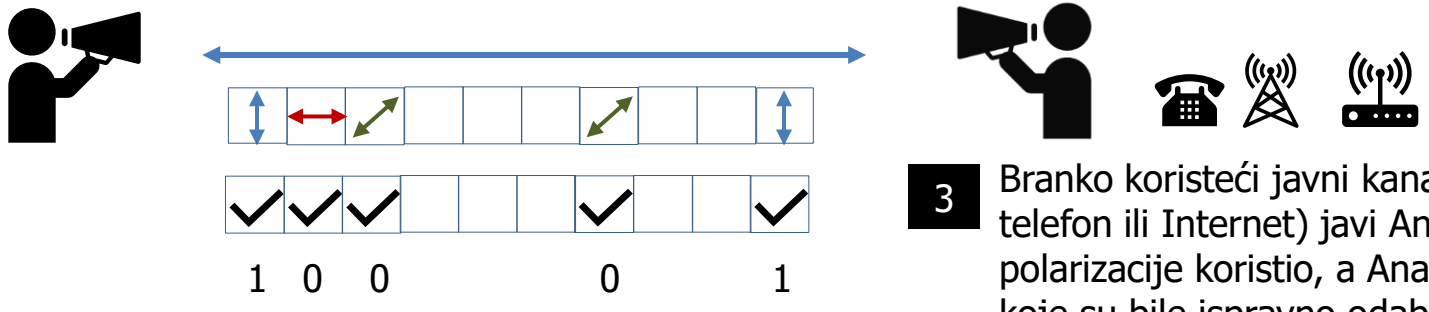
Protokol BB84



1 Ana nasumično bira slučajni niz bitova i polarizacija i šalje Branku



2 Branko primajući fotone nasumično bira polarizaciju i kada pogriješi dobit će kao rezultat s jednakom vjerojatnošću 0 ili 1



3 Branko koristeći javni kanal (primjerice telefon ili Internet) javi Ani koje je polarizacije koristio, a Ana mu odgovara koje su bile ispravno odabrane

4 Kada god su Ana i Branko odavrali jednake baze, ti bitovi su zajednički i čine tajni ključ

Prednosti i nedostaci protokola BB84

- sigurnost protokola temelji se na
  - nemogućnosti kloniranja fotona
  - Heisenbergovom principu neodređenosti
- puls polariziranog svjetla s *jednim* fotonom
- mora se ugraditi kod za ispravku pogrešaka koje se javljaju tijekom prijenosa
- duži kabel ili veća udaljenost – veća vjerojatnost pogreške
  - 2004. g.: - max. dužina kabla 60 km
    - max. udaljenost oko 2 km
    - brzina prijenosa ~ 1 kb/s
      (a treba 1 Mb/s)
  - 2015.g.: 10 kb/s na udaljenosti od 50 km

- Prvi komercijalni produkt 2002. g

Main features

- First commercial quantum key distribution system
- Key distribution distance: up to 60 km
- Key distribution rate: up to 1000 bits/s
- Compact and reliable

- 2004. g., prva sigurna transakcija između banaka koju je ostvarila grupa prof. Antona Zeilingera na Bečkom sveučilištu primijenivši protokol QKD

Post-quantum kriptografija javnog ključa

ili

Asimetrična kriptografija otporna na napade kvantnim računalom

Public-Key Post-Quantum Cryptography

Natječaj

- https://csrc.nist.gov/Projects/post-quantum-cryptography
- Na NIST-ovoj radionici 2.4.2015. "Workshop on Cybersecurity in a Post-Quantum World" iskazuje se potreba za novim kriptografskim algoritmima koji su otporni na napade kvantnim računalom.
- Motiv:
  - posljednjih se godina mnogo istražuje u području kvantnih računala
  - ako se ikad izgradi kvantno računalo s velikim brojem q-bitova klasična asimetrična kriptografija će biti kompromitirana (RSA, DSA i ECC)
- NIST raspisuje natječaj 20.12.2016. rok je 30.11.2017.
- predloženi algoritmi moraju zadovoljavati određene uvjete
- 21.12.2017. NIST objavljuje 69 kandidata koji zadovoljavaju uvjete natječaja
- 22.7.2020. objavljeno 15 algoritama za 3. krug

Uvjeti natječaja 1/2

- sigurnost predloženog algoritma se ne smije temeljiti na:
  - nemogućnosti faktorizacije velikih brojeva
  - nemogućnosti izračunavanja inverza diskretnog logaritma
- moguće funkcionalnosti predloženog algoritma su:
  - asimterična kriptografija (*publickey encryption*) i/ili
  - razmjena ključeva (*key exchange, KEM*) i/ili
    - kao i asimetrična kriptografija, služi za razmjenu simetričnog ključa najmanje duljine 256 bita
  - digitalni potpis (*digital signature*)
    - najveća duljina poruke koja se potpisuje je 2^{63} bitova

Uvjeti natječaja 2/2

- pretpostavlja se da napadač nema više od 2^{64} parova (M,C) i napada s odabranim čistim ili kriptiranim tekstom
- u analizi složenosti napada na predloženi algoritam, sigurnost algoritma će se uspoređivati s napadima na
  - AES128, AES192, AES256
  - SHA256, SHA384, SHA512 odnosno
  - SHA3-256, SHA3-384, SHA3-512

21.12.2017. objavljeno
69 kandidata za prvi krug natječaja

BIG QUAKE12	BIKE	CFPKM	Classic McEliece	Compact LWE	CRYSTALS-DILITHIUM	CRYSTALS-KYBER	DAGS
Ding Key Exchange	DME	DRS	DualModeMS	Edon-K	EMBLEM and R.EMBLEM	FALCON	FrodoKEM
GeMSS	Giophantus	Gravity-SPHINCS	Guess Again	Gui	HILA5	HiMQ-3	HK17
HQC	KCL	KINDI	LAC	LAKE	LEDAkem	LEDApkc	Lepton
LIMA	Lizard	LOCKER	LOTUS	LUOV	McNie	Mersenne-756839	MQDSS
NewHope	NTRUEncrypt	pqNTRUSign	NTRU-HRSS-KEM	NTRU Prime	NTS-KEM	Odd Manhattan	Ouroboros-R
Picnic	Post-quantum RSA-Encryption	Post-quantum RSA-Signature	pqsigRM	QC-MDPC KEM	qTESLA	RaCoSS	Rainbow
Ramstake	RankSign	RLCE-KEM	Round2	RQC	RVB	SABER	SIKE
SPHINCS+	SRTPI	Three Bears	Titanium	WalnutDSA			

Prije drugog kruga autori 5 algoritama su povukli svoje prijave, ostaje 64 kandidata

BIG QUAKE12	BIKE	CFPKM	Classic McEliece	Compact LWE	CRYSTALS-DILITHIUM	CRYSTALS-KYBER	DAGS
Ding Key Exchange	DME	DRS	DualModeMS	Edon-K	EMBLEM and R.EMBLEM	FALCON	FrodoKEM
GeMSS	Giophantus	Gravity-SPHINCS	Guess Again	Gui	HILA5	HiMQ-3	HK17
HQC	KCL	KINDI	LAC	LAKE	LEDAkem	LEDApkc	Lepton
LIMA	Lizard	LOCKER	LOTUS	LUOV	McNie	Mersenne-756839	MQDSS
NewHope	NTRUEncrypt	pqNTRUSign	NTRU-HRSS-KEM	NTRU Prime	NTS-KEM	Odd Manhattan	Ouroboros-R
Picnic	Post-quantum RSA-Encryption	Post-quantum RSA-Signature	pqsigRM	QC-MDPC KEM	qTESLA	RaCoSS	Rainbow
Ramstake	RankSign	RLCE-KEM	Round2	RQC	RVB	SABER	SIKE
SPHINCS+	SRTPI	Three Bears	Titanium	WalnutDSA			

U prvom krugu otpala 33 algoritma

BIG QUAKE12	BIKE	CFPKM	Classic McEliece	Compact LWE	CRYSTALS-DILITHIUM	CRYSTALS-KYBER	DAGS
Ding Key Exchange	DME	DRS	DualModeMS	Edon-K	EMBLEM and R.EMBLEM	FALCON	FrodoKEM
GeMSS	Giophantus	Gravity-SPHINCS	Guess Again	Gui	HILA5	HiMQ-3	HK17
HQC	KCL	KINDI	LAC	LAKE	LEDAkem	LEDApkc	Lepton
LIMA	Lizard	LOCKER	LOTUS	LUOV	McNie	Mersenne-756839	MQDSS
NewHope	NTRUEncrypt	pqNTRUSign	NTRU-HRSS-KEM	NTRU Prime	NTS-KEM	Odd Manhattan	Ouroboros-R
Picnic	Post-quantum RSA-Encryption	Post-quantum RSA-Signature	pqsigRM	QC-MDPC KEM	qTESLA	RaCoSS	Rainbow
Ramstake	RankSign	RLCE-KEM	Round2	RQC	RVB	SABER	SIKE
SPHINCS+	SRTPI	Three Bears	Titanium	WalnutDSA			

... a neki su se udružili

- LEDAcrypt = LEDAkem + LEDApkc
- NTRU = NTRUEncrypt + NTRU-HRSS-KEM
- ROLLO = LAKE + LOCKER + Ouroboros-R
- Round5 = HILA5 + Round2

BIG QUAKE12	BIKE	CFPKM	Classic McEliece	Compact LWE	CRYSTALS-DILITHIUM	CRYSTALS-KYBER	DAGS
Ding Key Exchange	DME	DRS	DualModeMS	Edon-K	EMBLEM and R.EMBLEM	FALCON	FrodoKEM
GeMSS	Giophantus	Gravity-SPHINCS	Guess Again	Gui	HILA5	HiMQ-3	HK17
HQC	KCL	KINDI	LAC	LAKE	LEDAkem	LEDApkc	Lepton
LIMA	Lizard	LOCKER	LOTUS	LUOV	McNie	Mersenne-756839	MQDSS
NewHope	NTRUEncrypt	pqNTRUSign	NTRU-HRSS-KEM	NTRU Prime	NTS-KEM	Odd Manhattan	Ouroboros-R
Picnic	Post-quantum RSA-Encryption	Post-quantum RSA-Signature	pqsigRM	QC-MDPC KEM	qTESLA	RaCoSS	Rainbow
Ramstake	RankSign	RLCE-KEM	Round2	RQC	RVB	SABER	SIKE
SPHINCS+	SRTPI	Three Bears	Titanium	WalnutDSA			

30.1.2019. objavljeno
26 kandidata za drugi krug natječaja

BIG QUAKE12	**BIKE**	CFPKM	**Classic McEliece**	Compact LWE	**CRYSTALS-DILITHIUM**	**CRYSTALS-KYBER**	DAGS
Ding Key Exchange	DME	DRS	DualModeMS	Edon-K	EMBLEM and R.EMBLEM	**FALCON**	**FrodoKEM**
GeMSS	Giophantus	Gravity-SPHINCS	Guess Again	Gui	**HILA5**	HiMQ-3	HK17
HQC	KCL	KINDI	**LAC**	**LAKE**	**LEDAkem**	**LEDApkc**	Lepton
LIMA	Lizard	**LOCKER**	LOTUS	**LUOV**	McNie	Mersenne-756839	**MQDSS**
NewHope	**NTRUEncrypt**	pqNTRUSign	**NTRU-HRSS-KEM**	**NTRU Prime**	**NTS-KEM**	Odd Manhattan	**Ouroboros-R**
Picnic	Post-quantum RSA-Encryption	Post-quantum RSA-Signature	pqsigRM	QC-MDPC KEM	**qTESLA**	RaCoSS	**Rainbow**
Ramstake	RankSign	RLCE-KEM	**Round2**	**RQC**	RVB	**SABER**	**SIKE**
SPHINCS+	SRTPI	**Three Bears**	Titanium	WalnutDSA			

26 algoritama za 2. krug je podijeljeno u dvije skupine

Algoritmi za razmjenu ključeva (17)
Public-key Encryption and Key-establishment Algorithms

BIKE	**Classic McEliece**	**CRYSTALS-KYBER**	**FrodoKEM**	**HQC**	**LAC**	**LEDAcrypt**	**NewHope**
NTRU	**NTRU Prime**	**NTS-KEM**	**ROLO**	**Round5**	**RQC**	**SABER**	**SIKE**
Three Bears							

Algoritmi za digitalni potpis (9)
Digital Signature Algorithms

CRYSTALS-DILITHIUM	**FALCON**	**GeMSS**	**LUOV**	**MQDSS**	**Picnic**	**qTESLA**	**Rainbow**
SPHINCS+							

22.7.2020. objavljeno 15 algoritama za 3. krug

Algoritmi za razmjenu ključeva (4 finalista i 5 zamjenskih kandidata)
Public-key Encryption and Key-establishment Algorithms

BIKE	**Classic McEliece**	**CRYSTALS-KYBER**	**FrodoKEM**	**HQC**	LAC	**LEDAcrypt**	NewHope
NTRU	**NTRU Prime**	NTS-KEM	ROLO	Round5	RQC	**SABER**	**SIKE**
Three Bears							

Algoritmi za digitalni potpis (3 finalista i 3 zamjenska kandidata)
Digital Signature Algorithms

CRYSTALS-DILITHIUM	**FALCON**	**GeMSS**	LUOV	MQDSS	**Picnic**	qTESLA	**Rainbow**
SPHINCS+							

Zaključak

- Simetrični algoritmi: AES
  - uskoro će biti normirani algoritmi prilagođeni ugrađenim računalima i Internetu stvari, tj. algoritmi koji su manje zahtjevni na računalne resurse
- Asimetrični algoritmi:
  - za sada RSA-2048 i ECC
  - „post-kvantni” algoritmi
- Funkcije za izračunavanje sažetka poruke: SHA-3