7. Kriptografija prilagođena uređajima s ograničenim mogućnostima

Lightweight Cryptography

Kriptografija prilagođena ugrađenim sustavima i Internetu stvari

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
- 7.2.2023. NIST je odabrao algoritam ASCON

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 i *tag*

Funkcija za izračunavanje sažetka poruke, *hash*

- opcionalna
- 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

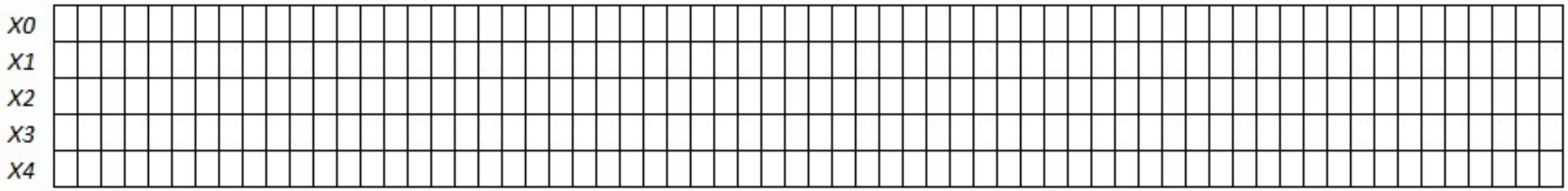
ACE	**ASCON**	Bleep64	CiliPadi	CLAE	CLX	COMET	DryGASCON
Elephant	ESTATE	FlexAEAD	ForkAE	Fountain	GAGE and InGAGE	**GIFT-COFB**	Gimli
Grain-128AEAD	HERN & HERON	HYENA	**ISAP**	KNOT	LAEM	Lilliput-AE	Limdolen
LOTUS-AEAD and LOCUS-AEAD	mixFeed	ORANGE	Oribatida	**PHOTON-Beetle**	Pyjamask	Qameleon	Quartet
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** **Joan Daemen** **...**	Yarara and Covet

ASCON

- pobjednik u natječaju CAESAR i 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*)

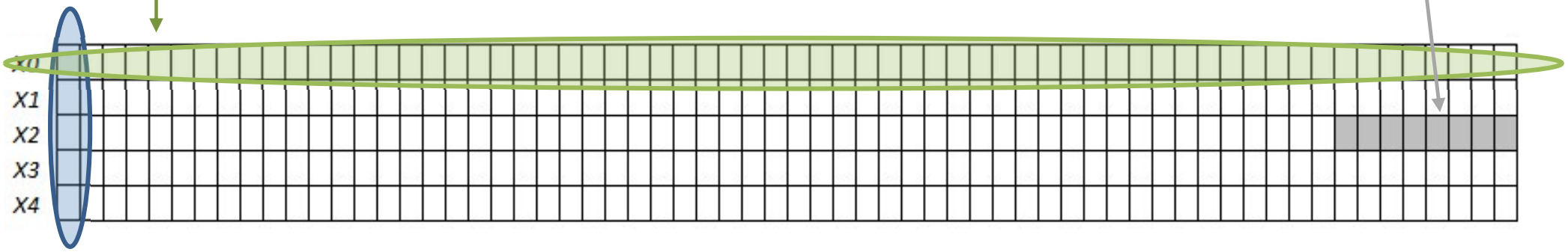
ASCON – struktura podataka

- *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:



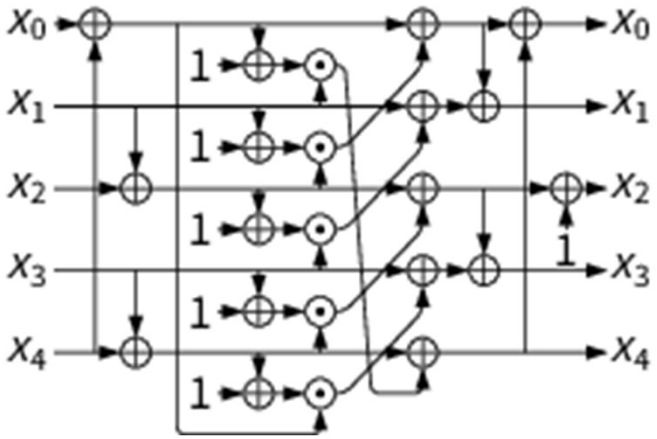
ASCON – permutacija *p*

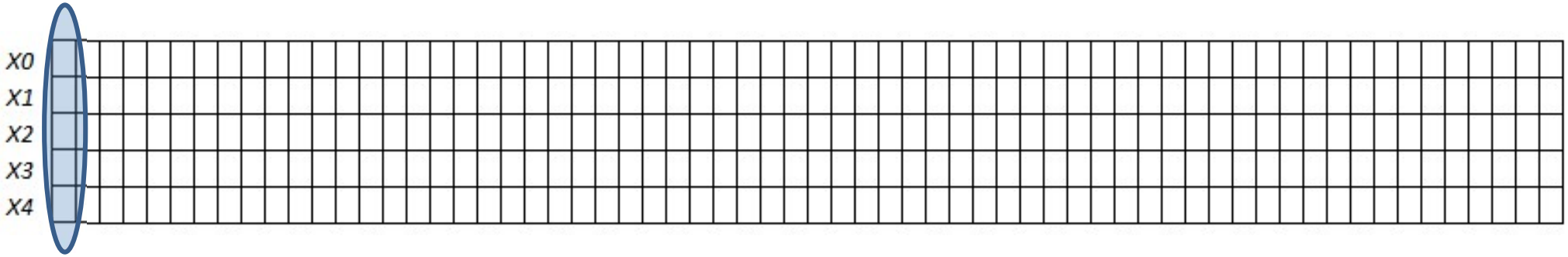
- zbrajanja s konstantom *Cr* (jedan bajt) i to samo nad *X2*
- supstitucije (*nonlinear substitution layer*)
  - S-BOX
  - djeluje nad svim stupcima stanja što se može paralelizirati
- linearne difuzije (*lineat diffusion layer*)
  - djeluje nad retcima stanja što se također može paralelizirati



ASCON – permutacija p - supstitucija

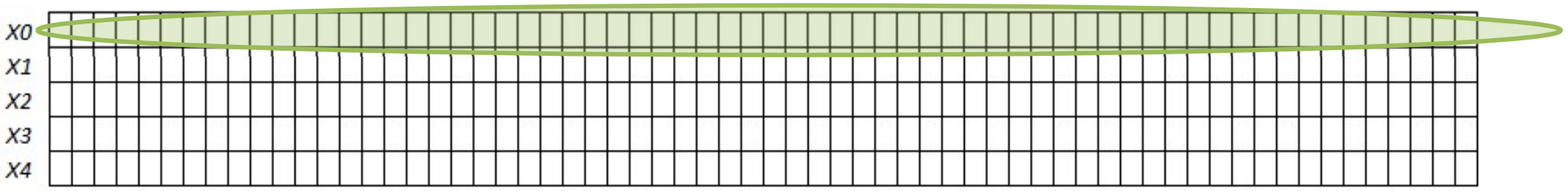
- djeluje nad svih 64 stupaca stanja
- umjesto supstitucijske tablice, može se prikazati slikom:
  - slika je preuzeta sa službenih stranica algoritma https://ascon.iaik.tugraz.at/specification.html





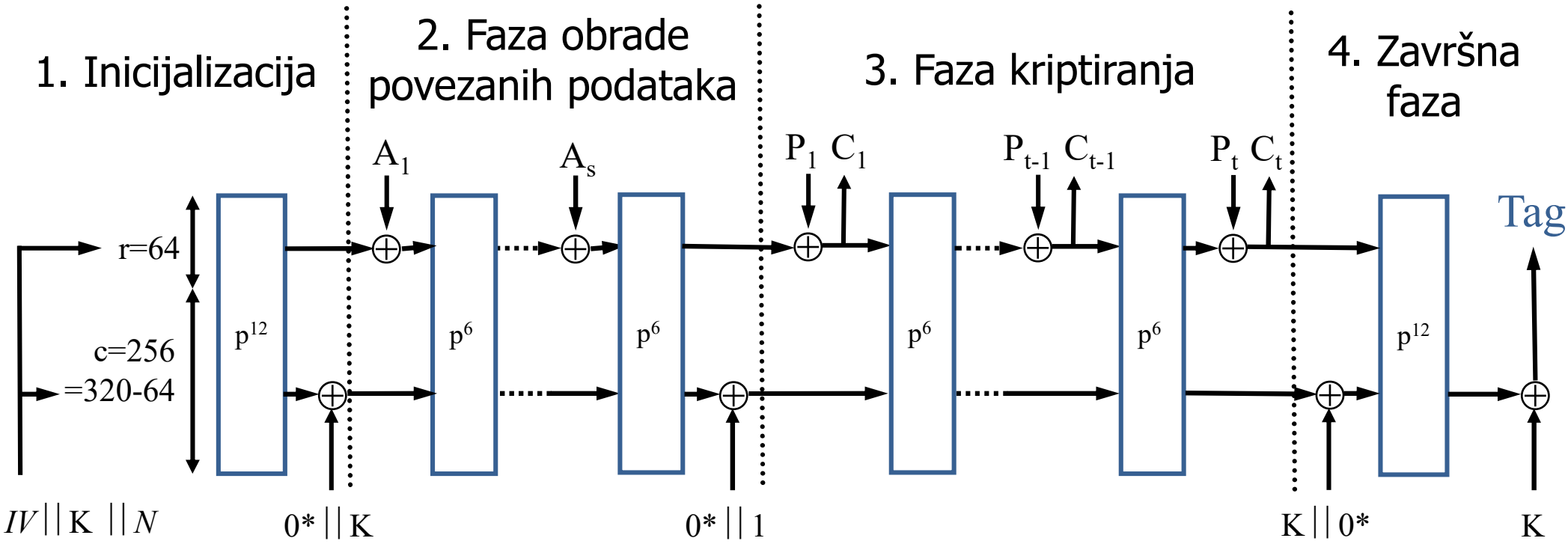
ASCON – permutacija *p* - difuzija

- 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

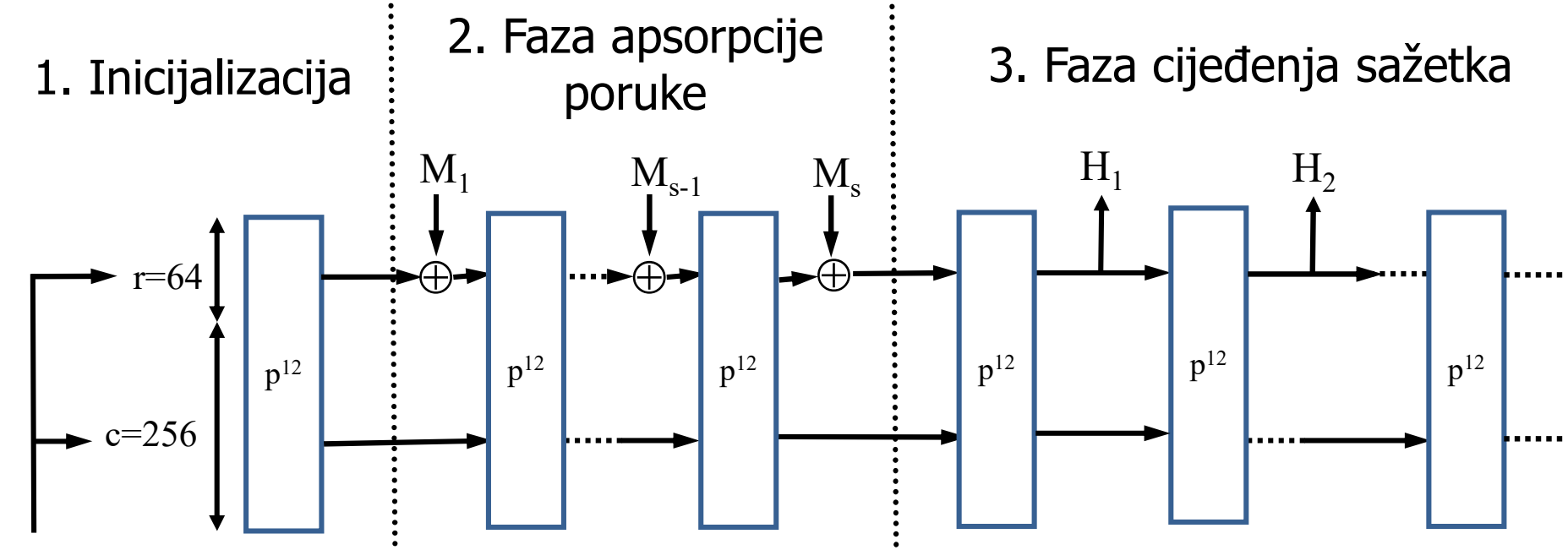
- odvija se u 4 faze
- permutacije se obavljaju ili u 12 ili u 6 rundi
- permutacije kod algoritma ASCON-128a se obavljaju ili u 12 ili u 8 rundi



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

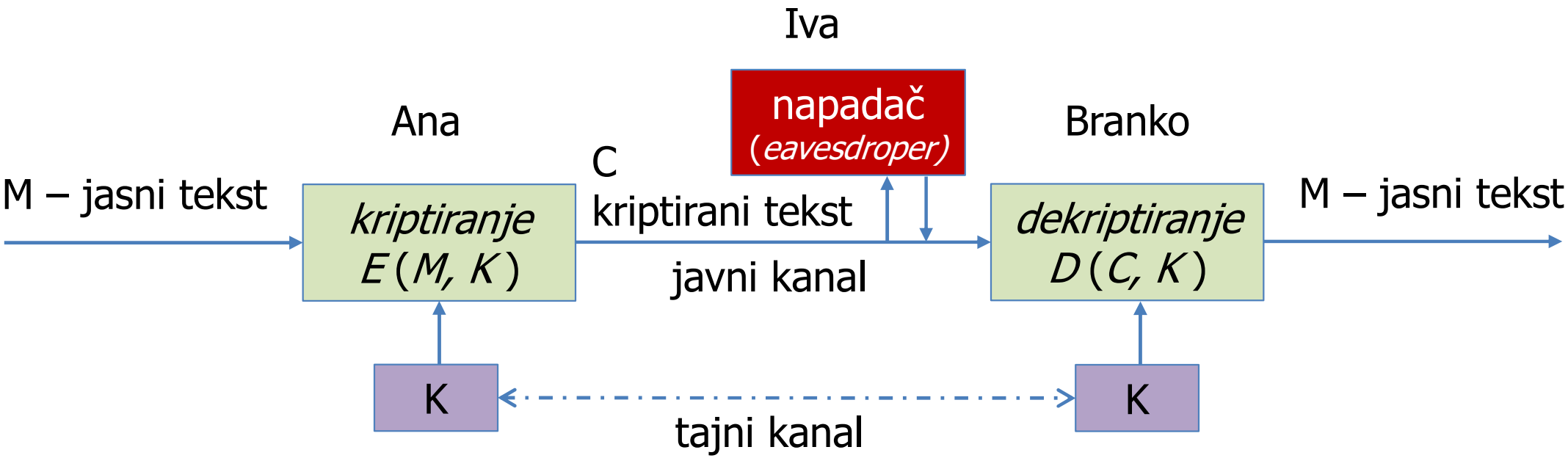


8. Kvantna i postkvantna kriptografija

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

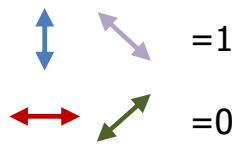


4 moguće polarizacije fotona:

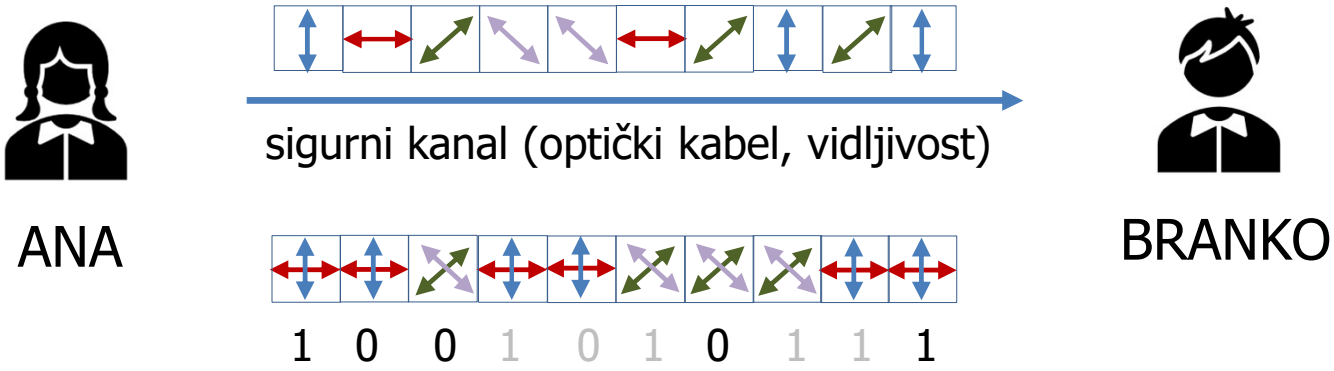
- baza ⊕ : foton je ili vertikalno (90°) ili horizontalno (0°) polariziran
- baza ⊗ : foton je dijagonalno polariziran (45° ili 135°)

Protokol BB84

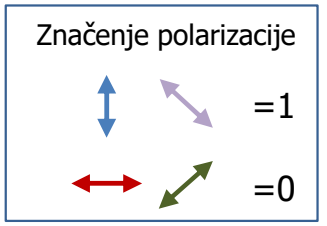
Značenje polarizacije



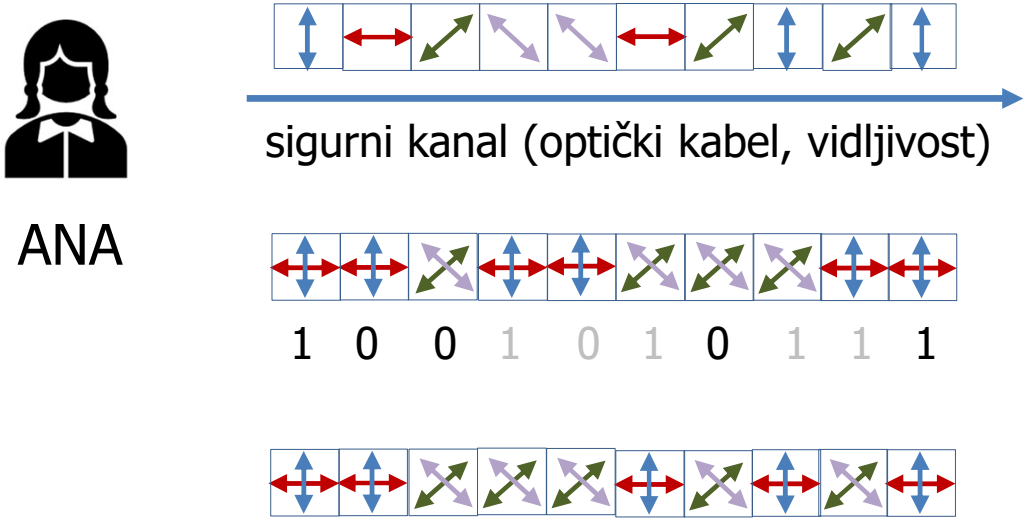
1 Ana nasumično bira slučajni niz bitova i polarizacija i šalje Branku



Protokol BB84

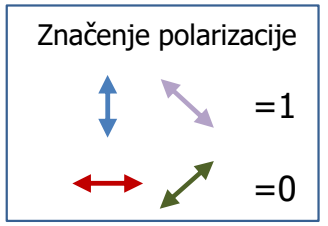


1 Ana nasumično bira slučajni niz bitova i polarizacija i šalje Branku

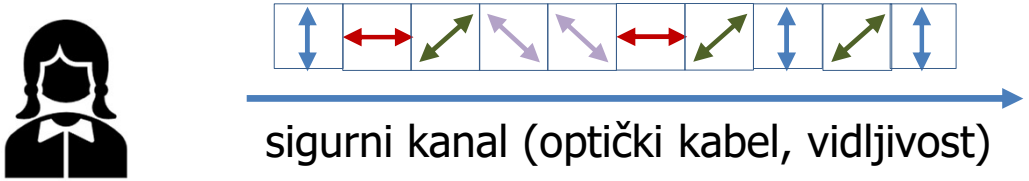


2 Branko primajući fotone nasumično bira polarizaciju i kada pogriješi dobit će kao rezultat s jednakom vjerojatnošću 0 ili 1

Protokol BB84

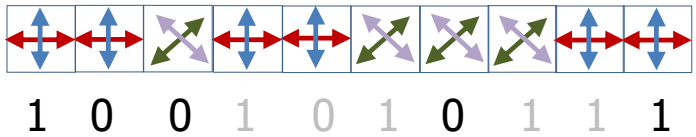


1 Ana nasumično bira slučajni niz bitova i polarizacija i šalje Branku

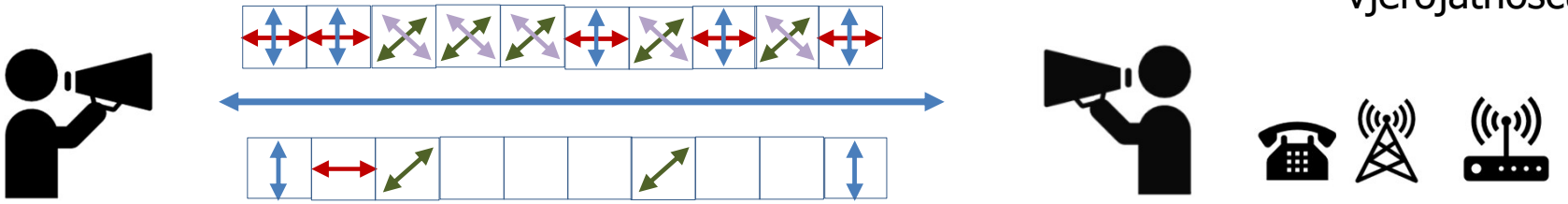


ANA

BRANKO



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

Problemi s QKD

- obavezna ili optička vidljivost (koja je nepouzdana) ili optički kabel (bez prekida)
- zahtjeva specijalno sklopovlje
- mala brzina, ograničena skalabilnost
- teško integrirati s postojećim kriptografskim sklopovljem
- visoka cijena
- još uvijek u eksperimentalnoj fazi

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

Tijek natječaja

21.12.2017. NIST objavljuje 69 kandidata koji zadovoljavaju uvjete natječaja

30.1.2019. objavljeno 26 kandidata za drugi krug natječaja

- 17 algoritama za kriptografsku zaštitu javnim ključem i za razmjenu ključeva (*Public-key Encryption and Key-establishment Algorithms*)
- 9 algoritama za digitalni potpis (*Digital Signature Algorithms*)

22.7.2020. objavljeno 15 algoritama za 3. krug

- 4 finalista i 5 zamjenskih kandidata algoritama za kriptografsku zaštitu javnim ključem i za razmjenu ključeva
- 3 finalista i 3 zamjenska kandidata algoritama za digitalni potpis

5.7.2022. objavljeno 4 algoritma koji se šalju u standardizacijski postupak

- 1 algoritam za kriptografsku zaštitu javnim ključem i za razmjenu ključeva i 3 algoritma za digitalni potpis (6.9.2022. raspisuje se natječaj za dodatne alg. DSA), a 4 algoritma za uspostavu ključeva (*Key-establishment Algorithm*) idu u 4. krug

11.3.2025. proglašen pobjednik natječaja za algoritam za uspostavu ključeva

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 kriptografsku zaštitu javnim ključem i za razmjenu ključeva
(4 finalista i 5 zamjenskih kandidata)
Public-key Encryption and Key-establishment Algorithms

BIKE	**Classic McEliece** Bernstein, ...	**CRYSTALS-KYBER** Peter Schwabe, ...	**FrodoKEM**	**HQC**	LAC	**LEDAcrypt**	NewHope
NTRU ... Peter Schwabe	**NTRU Prime** Bernstein, Tanja Lange, ...	NTS-KEM	ROLO	Round5	RQC	**SABER**	**SIKE**
Three Bears							

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

CRYSTALS-DILITHIUM ... Peter Schwabe	**FALCON**	**GeMSS**	LUOV	MQDSS	**Picnic**	qTESLA	**Rainbow**
SPHINCS+ Bernstein, T. Lange, P. Schwabe, ...							

5.7.2022. objavljeno 4 algoritma koji se šalju u standardizacijski postupak i ...

Jedan algoritam algoritma za kriptografsku zaštitu javnim ključem (*Public-key Encryption*) i

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

CRYSTALS-Kyber is Lattice-based; NP problem: Learning with Errors

tri algoritma za digitalni potpis (*Digital Signature Algorithms*)

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

CRYSTALS-Dilithium and **Falcon** are Lattice-based; NP problem: Short Integer Solution
SPHINCS+ is Hash-based - relies on collision resistance and pre-image resistance of cryptographic hash functions

... i 4 algoritma za razmjenu, odnosno uspostavu ključeva (*Key-establishment Algorithm*) idu u 4. krug natječaja

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

2023. autori W. Castryck i T. Decru u radu "An efficient key recovery attack on sidh," su pokazali uspješan napad na SIKEp434 u svega 10 min na samo jednoj jezgri

11.3.2025. proglašen pobjednik 4. krug natječaja za algoritam uspostave tajnog ključa (*Key-establishment Algorithm*)

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

CRYSTALS-KYBER – 5.7.2022. odabran algoritam za kriptografsku zaštitu javnim ključem

HQC – 11.3.2025. odabran algoritam uspostave tajnog ključa

6.9.2022. NIST raspisuje natječaj za dodatne algoritme za digitalni potpis uz 3 PQ-DSA algoritma koji su poslani na standardizaciju

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

rok za dostavu algoritama bio je 1.6.2023.

40 prispjelih kandidata je razvrstan u 7 kategorija:

- Code-based Signatures
  (Based on decoding random linear codes, considered infeasible for both classical and quantum computers.)
- Isogeny Signatures (Difficulty in computing isogenies between elliptic curves, even for quantum computers.)
- Lattice-based Signatures (Hardness of finding short vectors in lattices; enables security against quantum attacks.)
- MPC-in-the-Head Signatures
- Multivariate Polynomials (Hard to solve systems of multivariate quadratic equations over finite fields.)
- Symmetric-based Signatures
- Ostali

https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures

17.6.2023. objavljeno 40 kandidata za PQ DSA za 1. krug natječaja

https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures

CROSS	Enhanced pqsigRM	FuLeeca	LESS	MEDS	Wave	SQIsign	EagleSign
EHTv3 and EHTv4	HAETAE	HAWK	HuFu	Raccoon	SQUIRRELS	Biscuit	MIRA
MiRitH	MQOM	PERK	RYDE	SDitH	3WISE	DME-Sign	HPPC
MAYO	PROV	QR-UOV	SNOVA	TUOV	UOV	VOX	AIMer
Ascon-Sign	FAEST	SPHINCS-alpha	ALTEQ	eMLE-Sig 2.0	KAZ-SIGN	Preon	Xifrat1-Sign.I

Code-based Signatures (6)

Isogeny Signatures (1)

Lattice-based Signatures (7)

MPC-in-the-Head Signatures (7)

Multivariate Signatures (10)

Symmetric-based Signatures (4)

Ostali (5)

29.8.2024. objavljeno 12 kandidata za PQ DSA za 2. krug natječaja

https://csrc.nist.gov/Projects/pqc-dig-sig/round-2-additional-signatures

CROSS	Enhanced pqsigRM	FuLeeca	LESS	MEDS	Wave	SQIsign	EagleSign
EHTv3 and EHTv4	HAETAE	HAWK	HuFu	Raccoon	SQUIRRELS	Biscuit	MIRA
MiRitH	MQOM	PERK	RYDE	SDitH	3WISE	DME-Sign	HPPC
MAYO	PROV	QR-UOV	SNOVA	TUOV	UOV	VOX	AIMer
Ascon-Sign	FAEST	SPHINCS-alpha	ALTEQ	eMLE-Sig 2.0	KAZ-SIGN	Preon	Xifrat1-Sign.I

Code-based Signatures (2)

Isogeny Signatures (1)

Lattice-based Signatures (1)

MPC-in-the-Head Signatures (5)

Multivariate Signatures (4)

Symmetric-based Signatures (1)

Ostali (0)

Napadi na PQC

- 2023. autori W. Castryck i T. Decru u radu "An efficient key recovery attack on sidh," su pokazali uspješan napad na SIKEp434 u svega 10 min na samo jednoj jezgri

- 10. mj 2025. danski znanstvenici postigli znatan pomak u kriptoanalizi PQ kriptosustava zasnovanih na rešetkama*

* Lynn Engelberts, Yanlin Chen, Amin Shiraz Gilani, Maya-Iggy van Hoof, Stacey Jeffery, Ronald de Wolf; An Improved Quantum Algorithm for 3-Tuple Lattice Sieving, dostupno na https://arxiv.org/pdf/2510.08473

Problemi s implementacijom algoritama PQC

Računalno su zahtjevni

- veliki ključevi
- CPU zahtjevni

  = > teško ostvarivi sigurnosni sklopovski moduli (engl. *Hardware Security Module, HSM*) odgovarajućih performansi