Miodrag J. MIHALJEVIĆ*

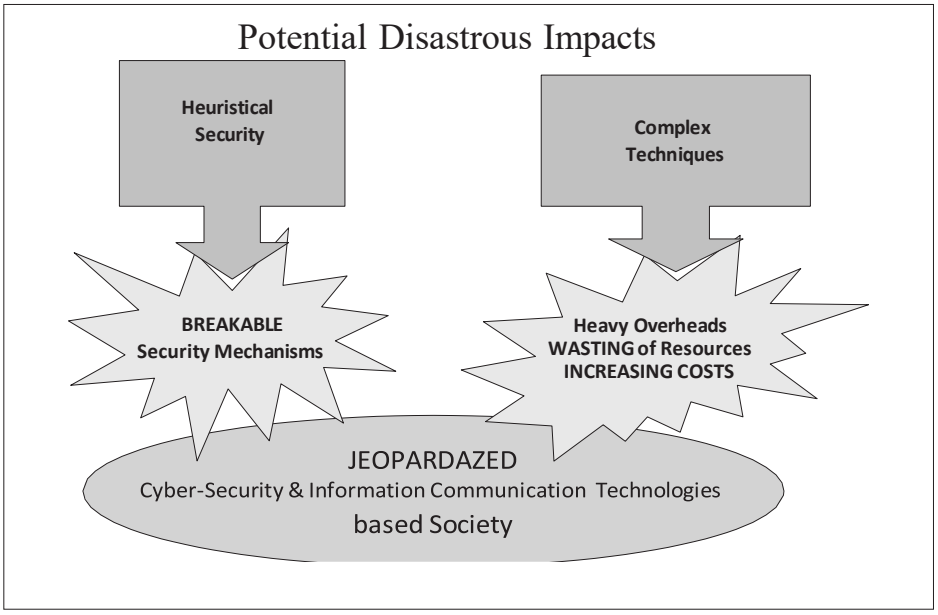
ILUSTRATIVNI NAPRECI U TEHNIKAMA KRIPTOLOGIJE I BLOKČEJN TEHNOLOGIJE

Sažetak: Cilj ovog rada je da ilustrativno ukaže na neke otvorene probleme i neke napredne tehnike u domenu informacione bezbednosti i blokčejn tehnologije. Kao ilustrativni problemi i povezana napredna rešenja razmatraju se domeni za zaštitu tajnosti i za redukciju energetske potrošnje u javnim blokčejn sistemima. Prikazuje se pristup za ojačavanje kriptografske sigurnosti postupaka šifrovanja niske složenosti i primena trgovine između potrebnih energetskih i memorijskih resursa u klasi blokčejn konsenzus protokola zasnovanih na tzv. dokazu o radu.

1. UVOD

Informaciono-komunikacione tehnologije (IKT) i digitalni (sajber) prostor su neraskidivo isprepletani sa našim fizičkim trodimenzionalnim prostorom. IKT i sajber prostor se stalno proširuju i pružaju nam nove pogodnosti. Blokčejn tehnologija i informaciona bezbednost su izuzetno bitne komponente i za IKT-e i u digitalnom prostoru da sve njihove pogodnosti ne bi postale i ulazna vrata za zlonamerne aktivnosti sa potencijalno katastrofalnim posledicama. Osnova za informacionu bezbednost je kriptologija, naučna disciplina formirana sredinom dvadesetog veka, a blokčejn tehnologija je desetak godina stara tehnologija zasnovana na nekim rezultatima kriptologije. Kriptologija daje osnove za zaštitu tajnosti i kontrolu integriteta, autentičnosti i neporecivosti. Kriptologija se razvila nad vekovima starim problemima šifrovanja i „razbijanja šifara". Interes za blokčejn tehnologiju počinje sa njenom prvom velikom primenom — bitkoin kriptovalutom. Cilj ovog rada je da ukaže na neke otvorene probleme i neke

* Dr Miodrag Mihaljević, naučni savjetnik, dopisni član Srpske akademije nauka i umetnosti (SANU), zamjenik direktora Matematičkog instituta SANU



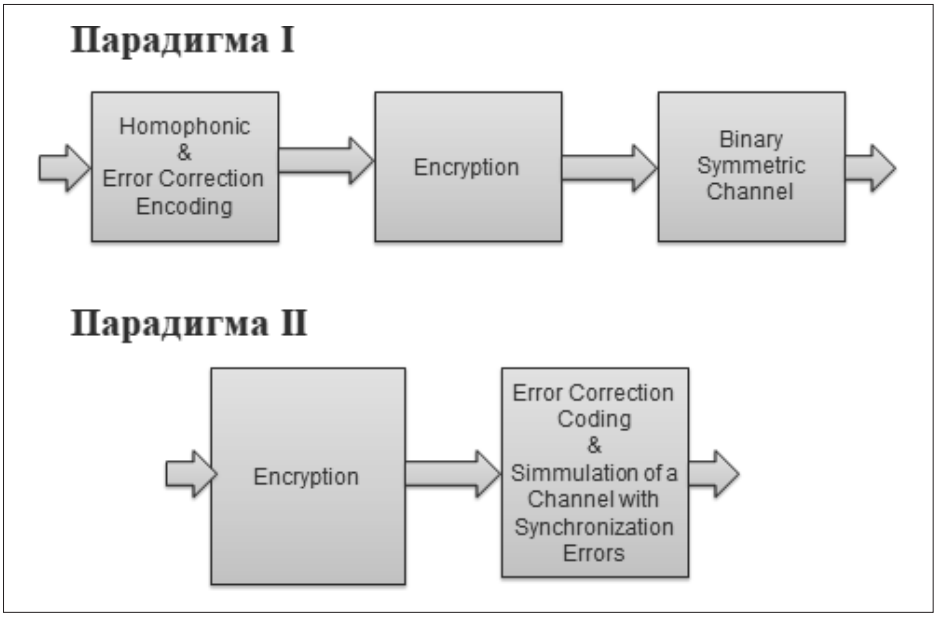
Slika 1. Ilustracija implikacija primene tehnika koje su samo heuristički sigurne i/ili koje imaju visoku implementacionu složenost

napredne tehnike u domenu informacione bezbednosti i blokčejn tehnologije. Kao na osnovni otvoreni problem ukazuje se na potrebu da tehnike koje podržavaju informacionu bezbednost i blokčejn istovremeno treba da obezbede željenu visoku sigurnost, ali i malo dodatno opterećenje funkcionalnosti sistema. Slika 1 ilustruje posledice neadekvatne sigurnosti i/ili složenosti tehnika koje se koriste u sajber prostoru.

Kao ilustrativni problemi i povezana napredna rešenja razmatraju se domeni za zaštitu tajnosti i za redukciju energetske potrošnje u javnim blokčejn sistemima. Prikazuje se pristup za ojačavanje kriptografske sigurnosti postupaka šifrovanja (enkripcije) niske složenosti i primena trgovine između potrebnih energetskih i memorijskih resursa u klasi blokčejn konsenzus protokola, zasnovanih na tzv. dokazu o radu.

2. INFORMACIONA BEZBEDNOST — OJAČANA KRIPTOGRAFSKA SIGURNOST ENKRIPCIJE PRIMENOM KODOVA ZA ISPRAVLJANJE GREŠAKA

Kao napredne tehnike enkripcije koje imaju visok potencijal primenljivosti i u blokčejn sistemima, u okviru ovog odeljka ukazuje se na pristup zasnovan na korišćenju kodova za ispravljanje grešaka za ojačavanje kriptografske



Slika 2. Dve paradigme za ojačavanje kriptografske sigurnosti date tehnike enkripcije primenom rezultata iz oblasti kodova

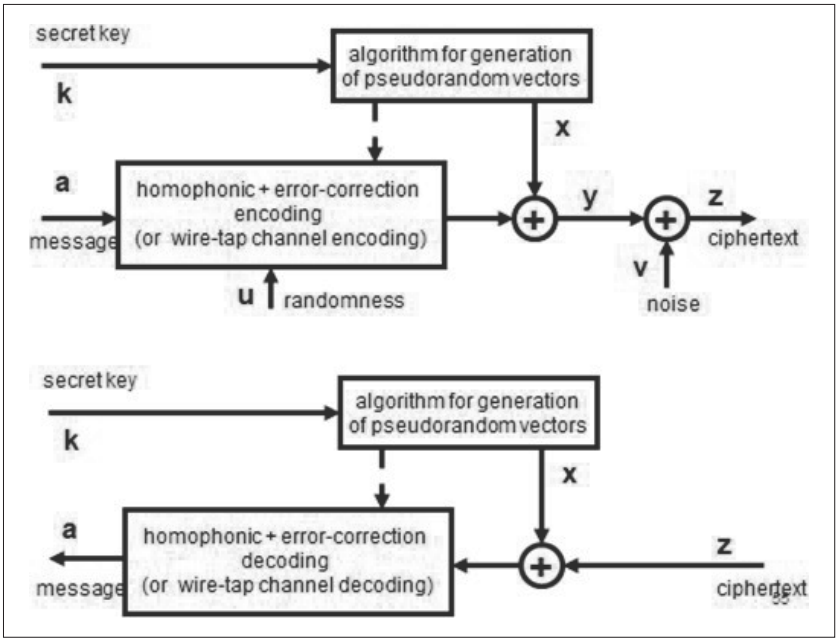
sigurnosti algoritama šifrovanja niske implementacione složenosti. Dva oblika ovog pristupa prikazana na Slici 2 su razmatrana u [1]–[5]. Paradigma I razmatrana u [1]–[3] zasniva se na primeni homofonskih i kodova za ispravljanje grešaka u binarnim simetričnim komunikacionim kanalima. Ovako kodovan ulazni vektor je predmet enkripcije, a dobijeni šifrat predmet degradacije aditivnim šumom, koji simulira binarni simetrični kanal u kome se svaki ulazni bit komplementira sa unapred zadatom verovatnoćom. Paradigma II razmatrana u [4] i [5] se zasniva na specijalnoj degradaciji inicijalno dobijenog šifrata, primenom simulatora komunikacionog kanala sa sinhronizacionim greškama u kome može da nastupi brisanje ili umetanje bita u inicijalno formirani šifrat.

Partikularni oblici Paradigmi I i II prikazani su na slikama 3 i 4.

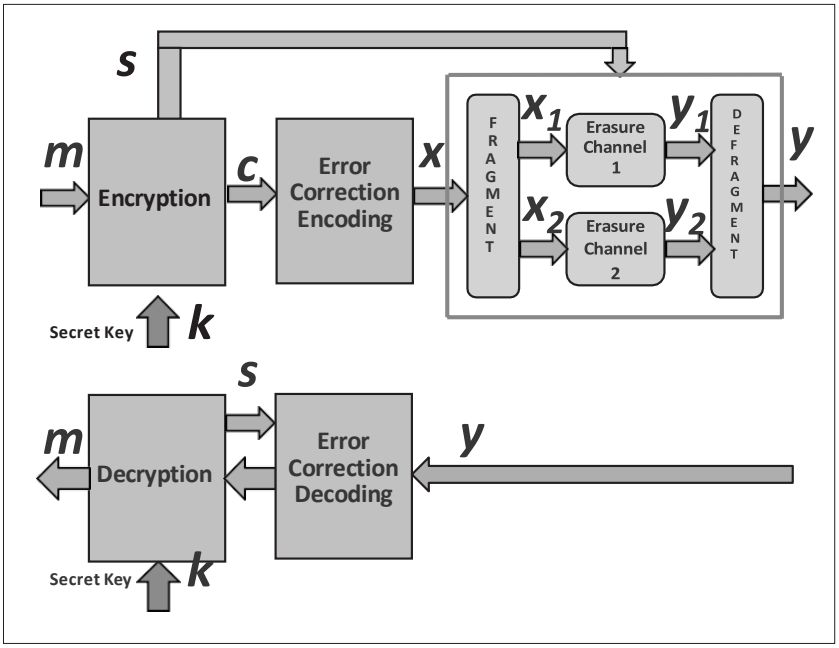
Na Slici 3 je data partikularna forma kriptografski ojačane sekvencijalne enkripcije saglasno Paradigmi I, koja je predložena i analizirana u [1]–[3].

Slika 4 prikazuje partikularnu formu kriptografski ojačane blok enkripcije saglasno Paradigmi II, koja je predložena i analizirana u [4] i [5].

Za detaljna tumačenja i razmatranja ovih predloga sugeriše izvorno upoznavanje na osnovu [1]–[4].



Slika 3. Partikularna forma kriptografski ojačane sekvencijalne enkripcije saglasno Paradigmi I prikazana i analizirana u [1]–[3]



Slika 4. Partikularna forma kriptografski ojačane blok enkripcije saglasno Paradigmi II prikazana i analizirana u [4]–[5]

3. BLOKČEJN TEHNOLOGIJA — KONSENZUS PROTOKOL SA SUŠTINSKI REDUKOVANOM POTROŠNJOM ENERGIJE

Blokčejn je distribuirani način dodavanja i čuvanja velikih količina podataka iz raznih domena tako da se dodaju samo verifikovani podaci, i jednom dodati podaci više ne mogu da budu menjani.

Suštinska svojstva su:

— da se verifikacija podataka koji se dodaju vrši bez postojanja tzv „treće strane od apsolutnog poverenja";

— da se nepromenjivost prethodno dodatih podataka ostvaruje primenom tehnika kriptologije.

Ukazuje se da su dve suštinske komponente svakog blokčejn sistema digitalna knjiga — blokčejn i konsenzsus protokol. Takođe, bitno svojstvo većine blokčejn sistema je da omogućavaju postojanje pametnih ugovora. U nastavku se sumiraju osnovna svojstva navedene tri komponente.

Digitalna knjiga — lanac blokova. Osnovna komponenta blokčejn tehnologije je distribuirana baza podataka, koja može da se modeluje kao digitalna knjiga (Ledger), u koju mogu da se dodaju strane, i svaka dodata strana je neraskidivo vezana sa svim prethodno dodatim stranama, koje ne mogu da se menjaju. Alternativno, ova knjiga se može posmatrati kao niz ulančanih blokova, odakle i naziv blokčejn.

Konsenzus protokol. Kao kompenzacija sa nepostojanje treće strane od arbitražnog poverenja, blokčejn tehnologija koristi konsenzus protokol za verifkovano ažuriranje digitalne knjige. Blokčejn konsenzus protokol je osnova za distribuirano ažuriranje.

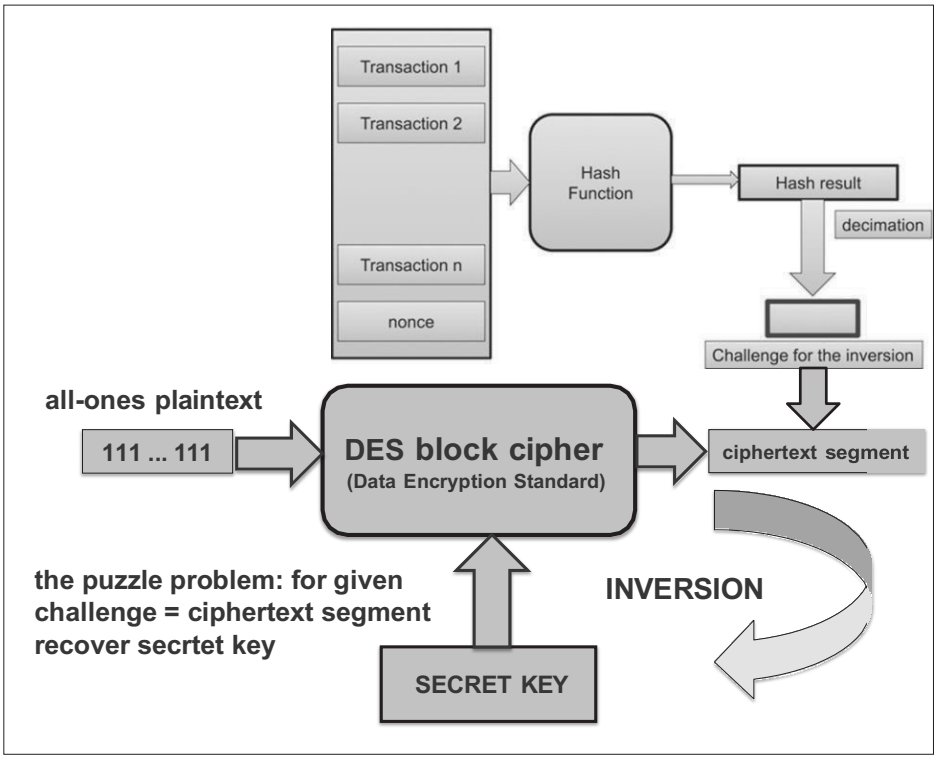
Pametni ugovori (Smart contracts) su programi kojima se vrši automatsko ugovaranje (mašina — mašina, bez direktnog ljudskog učešća) na osnovu specificiranih preferenci ugovornih strana. Pametni ugovori omogućuju postojanje veoma kratkotrajnih ugovornih obaveza i uspostavljanje ogromnog broja ugovora, a blokčejn paradigma obezbeđuje njihovu „overu" bez angažovanja treće strane od poverenja (notara).

Bitna klasa blokčejn konsenzus protokola je zasnovana na nekom kriptografskom problemu koji se naziva kriptografska slagalica.

Slika 5 pokazuje primer problema slagalice za konsenzus protokol predložen u [6]–[7]. Kao problem koji entiteti-verifikatori (rudai) rešavaju tokom izvršenja blokčejn konsenzus protokola postavljeno je sledeće:

— nepoznatim tajnim ključem primenom poznatog algoritma enkripcije generisati šifrat koji odgovara otvorenom tekstu koji se sastoji od vektora jedinica;

— na osnovu dobijenog šifrata (kao izazova) rekonstruisati tajni ključ kojim je šifrat generisan.



Slika 5. Konsenzus slagalica predložena i razmatrana u [6]–[7]

4. ZAKLJUČAK

Dat je jedan kompaktan rezime nekih naprednih pristupa od interesa za informacionu bezbednost i blokčejn tehnologiju objavljenih u [1]–[5] i [6]–[7], respektivno. Cilj je bio da se potencijalno zainteresovanim čitaocima da objedinjeni rezime izabranih tehnika: (a) za ojačavanje kriptografske sigurnosti primenom kodova za ispravljanje grešaka; (b) blokčejn konsenzus protokola koji omogućavaju redukciju energetskih resursa, koji se koriste u procesu verifikacije blokčejn transakcija.

LITERATURA

[1] F. Oggier and M. J. Mihaljevic, „An Information-Theoretic Security Evaluation of a Class of Randomized Encryption Schemes“, *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 2, Feb. 2014, pp. 158–168.
[2] M. J. Mihaljevic and F. Oggier, „Security Evaluation and Design Elements for a Class of Randomized Encryptions“, *IET Information Security*, vol. 13, no. 1, Jan. 2019, pp. 36–47.
[3] V. Mikhalev, M. J. Mihaljevic, O. Kara and F. Armknecht, „Selected Design and Analysis Techniques of Contemporary Symmetric Encryption“, in Security of Ubiquitous Computing Systems, Eds. G. Avoine and J. Hernandez-Castro, Springer, 2021, pp. 49–62.
[4] M. J. Mihaljevic, „A Security Enhanced Encryption Scheme and Evaluation of Its Cryptographic Security“, *Entropy*, vol. 21(7), July 2019 (11 pages).
[5] M. J. Mihaljevic, L. Wang and S. Xu, „An Approach for Security Enhancement of Certain Encryption Schemes Employing Error Correction Coding and Simulated Synchronization Errors“, *Entropy*, vol. 24(3), 406; March 2022 (10 pages).
[6] M. J. Mihaljevic, „A Blockchain Consensus Protocol Based on Dedicated Time-Memory— Data Trade-Off“, *IEEE Access*, vol. 8, Aug. 2020, pp. 141258–141268.
[7] M. J. Mihaljevic, L. Wang, S. Xu and M. Todorovic, „An Approach for Blockchain Pool Mining Employing the Consensus Protocol Robust against Block Withholding and Selfish Mining Attacks“, *Symmetry*, vol. 14 (8), 1711, Aug. 2022 (28 pages).

Miodrag J. MIHALJEVIĆ

ILLUSTRATIVE ADVANCES IN CRYPTOLOGY AND BLOCKCHAIN TECHNOLOGY TECHNIQUES

Abstract

The aim of this paper is to provide an illustrative address on some open problems and some advanced techniques in the fields of information security and blocking technology. The domains of secrecy protection and reduction of energy consumption in permissionless blockchain systems are considered. The following is pointed out: (a) An approach to strengthening the cryptographic security of lightweight encryption employing error-correction coding, and (b) An approach that employs trade-off between necessary energy and memory resources in the Proof-of-Work (PoW) based blockchain consensus protocols.