Soft Input Dekripcija i njena iterativna primena

Nataša Živić, Christoph Ruland, *Senior Member, IEEE*

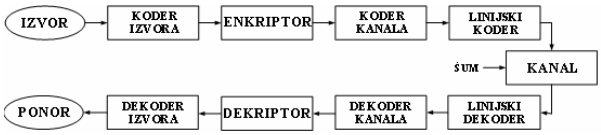
***Sadržaj* — U ovom radu je opisano na koji način komunikacioni sistemi koji koriste kriptografiju (enkripciju i dekripciju) mogu da poboljšaju svoje performanse, odnosno smanje BER kao posledicu prenosa preko šumovitog kanala. Poznato je da je dekriptor veoma osetljiv na ulazne greške, tj. da je dovoljan samo jedan pogrešan bit na ulazu u dekriptor da bi na izlazu u proseku čak 50 % bita bilo pogrešno. Iz tog razloga je neophodno ispraviti sve greške na ulazu u dekriptor. Korišćenjem SISO konvolucionog dekodera ili turbo dekodera u kombinaciji sa dekriptorom postižu se željeni rezultati, što je opisano kao metod Soft Input Dekripcije u ovom radu. Kada se Soft Input Dekripcija primenjuje na iterativan način, poboljšava se dekodovanje i time dodatno umanjuje BER poslate informacije.**

***Ključne reči* — kanalsko kodovanje, kriptografija, digitalni potpisi, konovlucioni turbo kodovi, SISO dekoder**

I. UVOD

DANAŠNJI komunikacioni sistemi koriste sve više enkripciju i dekripciju, kako bi obezbedili bilo šifrovanje informacija, bilo autentikaciju pošiljaoca informacija preko digitalnih potpisa. Bankovne i ostale novčane transakcije preko Interneta ne mogu se zamisliti bez korišćenja kriptografskih mehanizama zaštite. Pored toga, decentralizacija energetskog tržišta (struja, gas, voda itd.) zahteva uvodjenje kriptografije radi zašite mernih podataka u interesu provajdera energenata, kao i potrošača.

Uprošćena šema komunikacionog sistema (Sl. 1) prikazuje dodatne elemente – enkriptor na predajnoj i dekriptor na prijemnoj strani sistema.



Sl. 1 – Uprošćena šema komunikacionog sistema sa enkriptorom i dekriptorom

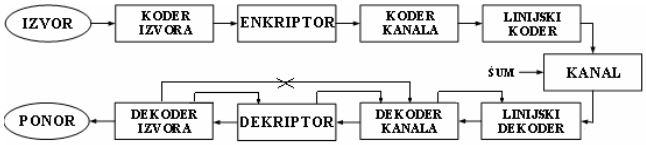
Uvodjenjem povratnih sprega izmedju elemenata na prijemnom delu poboljšavaju se performanse sistema, pošto povratne informacije omogućavaju finije podešavanje i korekciju dekodovanih informacija [1] (Sl. 2).

N. Živić, University of Siegen, Hoelderlinstrasse 3, Germany (tel:+492717403322, fax:+492717402536, email: natasa.zivic@uni-siegen.de)

C. Ruland, University of Siegen, Germany (tel:+492717402522, fax:+492717402536, email: christoph.ruland@uni-siegen.de)

Povratna sprega izmedju dekodera izvora i dekodera kanala, koja omogućava ''udruženo dekodovanje izvora i kanala'' (joint source-channel decoding) [2] ne može da se koristi usled prisustva dekriptora, odnosno mora da se ''podeli'' na dve povratne sprege: od dekodera izvora ka dekriptoru, i od dekriptora ka dekoderu kanala.

Ovaj rad se bavi kooperacijom dekriptora i dekodera kanala. U poglavljima 2 i 3 opisan je metod i dati rezultati simulacija Soft Input Dekripcije: na koji način dekriptor koristi izlazne informacije kanalskog dekodera za ispravljanje pogrešno dekodovanih bita. U poglavljima 4 i 5 opisano je, uz rezultate simulacija, kako povratna sprega od dekriptora ka dekoderu kanala poboljšava dekodovanje u iteracijama.



Sl. 2 – Uprošćena šema komunikacionog sistema sa povratnim spregama

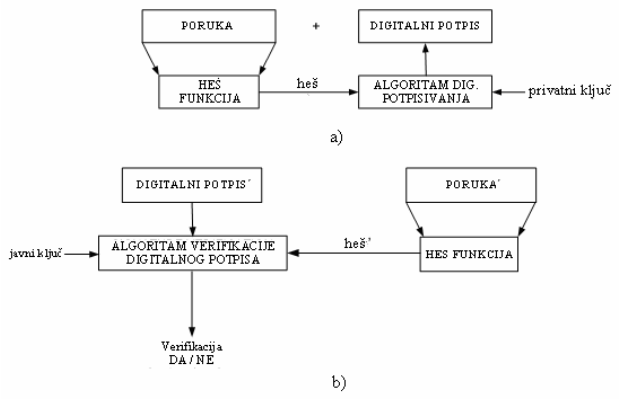
U ovom radu funkcija enkriptora i dekriptora biće ograničena na primenu asimetričnih tehnika kriptografije, odnosno na generisanje i verifikaciju digitalnog potpisa, respektivno, radi objašnjenja metode Soft Input Dekripcije. Pored asimetričnih, Soft Input Dekripcija nalazi primenu i kod simetričnih tehnika (MAC – Message Authentication Code [3] i H-MAC – Hashed - Message Authentication Code [4]).

Postoje dva tipa digitalnih potpisa: digitalni potpisi sa apendiksom (digital signatures with appendix [5]) i digitalni potpisi sa regeneracijom poruke (digital signatures giving message recovery [6]).

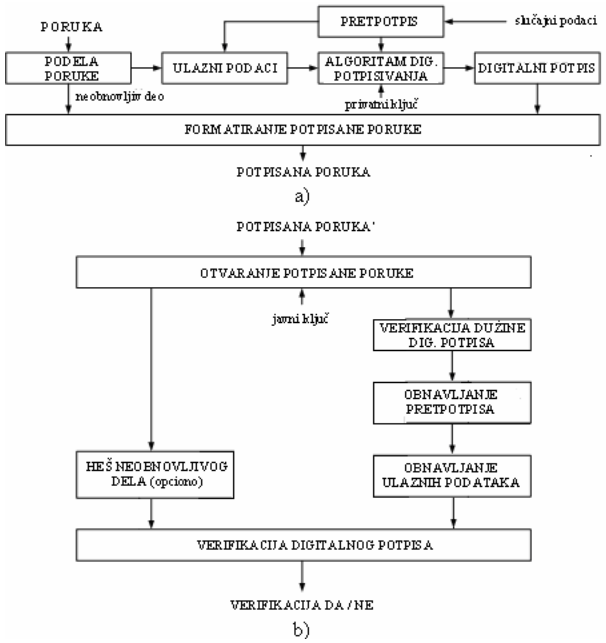
Kod digitalnih potpisa sa apendiksom (Sl. 3) poruka koju treba signirati (potpisati) može biti proizvoljne dužine. Enkriptor generiše digitalni potpis koristeći heš (hash – kratak oblik poruke definisane dužine, dobijen pomoću heš funkcije) i privatni ključ. Preko kanala se prenosi poruka sa njoj ''prikačenim'' digitalnim potpisom, odnosno apendiksom. Dekriptor verifikuje digitalni potpis uporedjivanjem heš vrednosti dobijene iz primljene poruke i heš vrednosti dobijene iz primljenog digitalnog potpisa pomoću javnog ključa. Ukoliko su ove dve vrednosti jednake, verifikacija digitalnog potpisa je uspešna. U slučaju različitih heš vrednosti (bilo da je greška u prenešenoj poruci, bilo u primljenom digitalnom potpisu), verifikacija je neuspešna.

Digitalni potpisi sa regeneracijom poruke (Sl. 4) se primenjuju na ''kratke'' poruke, što znači da je dužina poruke i redundanse koja se dodaje poruci pre

signiranja manja od dužine korišćenog privatnog ključa. Ukoliko je poruka duža od dozvoljene, deli se na obnovljiv deo (koji je uključen u digitalni potpis) i neobnovljiv deo (koji se prenosi sa digitalnim potpisom).



Sl. 3 – Digitalni potpisi sa apendiksom
a) generacija b) verifikacija



Sl. 4 – Digitalni potpisi sa regeracijom poruke
a) generacija b) verifikacija

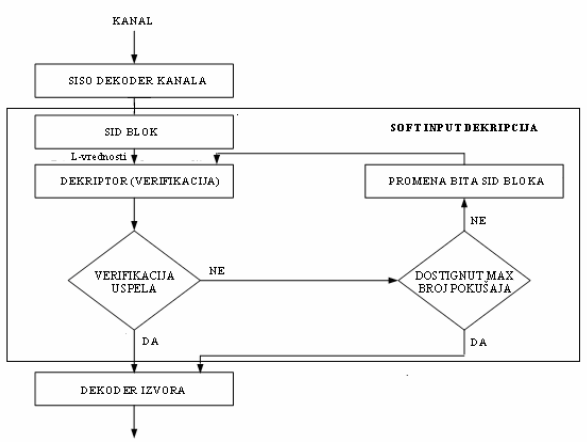
II. METOD SOFT INPUT DEKRIPCIJE

Soft Input Dekripcija je metod dekriptovanja informacije, koja je prethodno dekodovana SISO (Soft Input / Soft Output) konvolucionim dekoderom, uz korišćenje tzv. L-vrednosti ili ''soft output'' vrednosti dekodera. SISO dekoder na ulazu i izlazu ima realne ili ''soft'' vrednosti umesto vrednosti bita (''0'' ili ''1''), što je slučaj sa dekoderima koji imaju ''hard'' izlaz. Niže L-vrednosti su pokazatelj veće verovatnoće da je bit pogrešno dekodovan (kada je L-vrednost 0, bit je sa verovatnoćom jednakom 1/2 tačno dekodovan, odnosno podjednaka je verovatnoća da je poslati bit ''0'' i ''1''), i obrnuto: više L-vrednosti podrazumevaju veću verovatnoću ispravnog dekodovanja (ako je |L|-vrednost ∞, verovatnoća je jednaka 1). ''Soft'' dekodovanje omogućava bolje rezultate od ''hard'' dekodovanja, pošto se izlazne realne vrednosti koriste kao dodatna informacija u dekodovanju. Najčešće korišćeni SISO algoritmi su SOVA (Soft Output Viterbi Algorithm) [7] i MAP (Maximum Likelihood Algorithm) [8]. U simulacijama u ovom radu korišćen je MAP algoritam, koji je pokazao bolje performanse pri Soft Input Dekripciji u poredjenju sa SOVA algoritmom.

U ovom radu informacija koja se obradjuje metodom Soft input Dekripcije je digitalni potpis. Kako informacija može da obuhvata i drugo, kao npr. podatke sa MAC/H-MAC-om (u slučaju simetričnih tehnika kriptografije), koji nisu predmet ovog rada, za informaciju u Soft Input Dekripciji (SID) koristi se naziv SID blok. Dakle, ovde se pod SID blokom (Sl. 4) podrazuva digitalni potpis (Sl.3 i Sl. 4). Kada se koriste digitalni potpisi sa apendiksom, podrazumeva se da je informacija ispravna na mestu primaoca, odnosno posmatra se prenos SID bloka – samog digitalnog potpisa. Kod digitalnih potpisa sa regeneracijom poruke SID blok je digitalni potpis, u kome je informacija koja se potpisuje već integrisana, prema Sl. 4.

Algoritam Soft Input Dekripcije [9] prikazan je na Sl. 5 i zasniva se na sledećem: algoritam je uspešno završen ako je rezultat verifikacije pozitivan. Ukoliko je negativan, algoritam analizira |L|-vrednosti na ulazu u dekriptor i invertuje bite (operacijom XOR "1") koji imaju najmanje |L|-vrednosti (''0'' -> ''1'', ''1'' -> ''0''). Nakon toga dekriptor vrši sledeću verifikaciju i proverava rezultat. Ukoliko je rezultat opet negativan, algoritam invertuje sledeću kombinaciju bita sa najmanjim |L|-vrednostima itd. Soft Input Dekripcija se završava kada je rezultat verifikacije pozitivan ili kada se dostigne maksimalni, unapred definisani broj pokušaja.

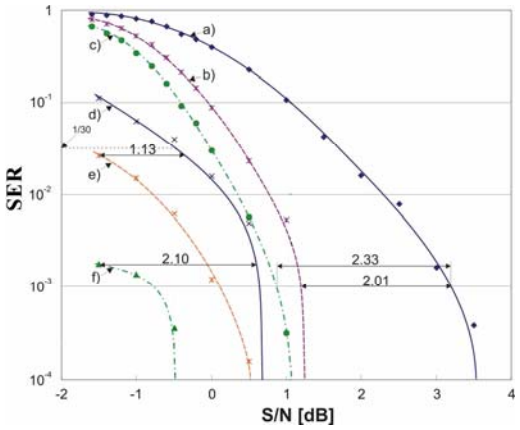
Redosled invertovanja bita sa najnižim |L|-vrednostima definisan je rastućim binarnim brojačem: najpre se invertuje samo bit sa najnižom |L|-vrednošću (što odgovara binarnoj kombinaciji 00.....001, gde ''1'' pokazuje poziciju bita koji se invertuje), zatim samo bit sa sledećom najnižom |L|-vrednošću (što odgovara binarnoj kombinaciji 00.....010), nakon toga se invertuju oba bita sa najnižim |L|-vrednostima (binarna kombinacija 00.....011); sledeća kombinacija obuhvata samo bit sa trećom po redu najnižom |L|-vrednošću (binarna kombinacija 00.....100), itd. do poslednje kombinacije: invertovanje svih bita sa unapred definisanim brojem najnižih |L|-vrednosti (binarna kombinacija svih jedinica). U ovom radu maksimalan broj invertovanih bita je ograničen na 8, odnosno 16. Drugim rečima, maksimalan broj pokušaja odnosno kombinacija algoritma Soft Input Dekripcije je 2^8 odnosno 2^{16}, respektivno.



Sl. 5 – Algoritam Soft Input Dekripcije

III.REZULTATI SIMULACIJA SOFT INPUT DEKRIPCIJE

U simulacijama je SID blok dužine 320 bita, što odgovara digitalnim potpisima na bazi eliptičnih krivih (ECC – Elliptic Curve Cryptography [10] na polju GF (p), pri čemu je p darametar dužine 160 bita. Simuliran je AWGN kanal.



Sl. 6 Kodni dobitak pri dekriptovanju SID bloka dužine 320 bita primenom

a) konvolucionog kodovanja bez SID
b) konv. kodovanja sa SID sa 8 najnižih L-vrednosti
c) konv. kodovanja sa SID sa 16 najnižih L-vrednosti
d) turbo kodovanja bez SID
e) turbo kodovanja sa SID sa 8 najnižih L-vrednosti
f) turbo kodovanja sa SID sa 16 najnižih L-vrednosti

U simulacijama je korišćen konvolucioni koder/SISO konvolucioni dekoder (sa kodnim količnikom r = 1/2 i m = 2), kao i turbo koder/dekoder (sa kodnim količnikom r = 1/3 sastvaljen od 2 paralelna rekurzivna sistematična konvoluciona kodera sa r = 1/2 i blok interlivera dubine 17). Broj interacija turbo dekodera je 3.

Konvolucioni i turbo dekoder koriste MAP algoritam dekodovanja. U simulacijama je korišćen C/C++ programski jezik. Za svaku tačku krivih na Sl. 6 koja prikazuje rezultate simulacija, uradjeno je 50.000 testova.

Rezultati simulacija izraženi su u SER (Signature Error Rate) u dB, pošto je u pitanju ispravljanje digitalnih potpisa, a ne pojedinačnih bita kao u slučaju BER [11]: svi biti digitalnog potpisa moraju biti tačni, da bi digitalni potpis bio tačan i primenjiv. SER je difinisan kao:

$$SER = \frac{broj\ pogrešnih\ dig.\ potpisa}{ukupan\ broj\ primljenih\ dig.\ potpisa} \quad (1)$$

IV. ITERATIVNI POSTUPAK SOFT INPUT DEKRIPCIJE

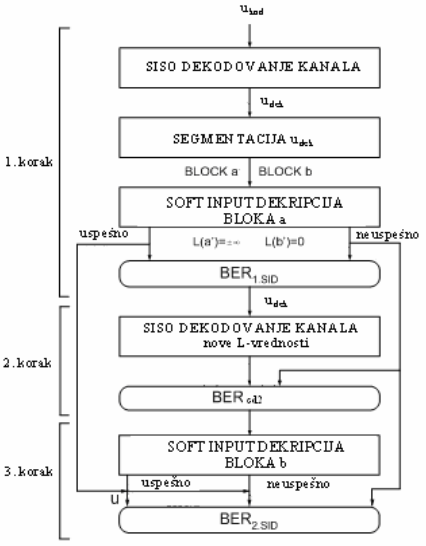
Interesantno je ispitati na koji na način SID blok (u ovom slučaju digitalni potpis) koji je već ispravljen metodom Soft Input Dekripcije, može dalje da se upotrebi za korigovanje bita sledećeg SID bloka.

Posmatrajmo informaciju u_{dek} po izlasku iz SISO dekodera, koja sadrži 2 SID bloka, *a* i *b*, pri čemu je dužina bloka *b* veća ili jednaka dužini bloka *a*. Ukoliko su biti bloka *a* i *b* ''ukršteni'':

$$u_{dek} = \begin{cases} a_1 b_1 a_2 b_2 \ldots a_m\ b_n, & m = n \\ a_1 b_1 \ldots b_{\frac{n}{m}}\ a_2 \ldots a_m\ \ b_{n-\frac{n}{m}+1} \ldots b_n & m < n \end{cases} \quad (2)$$

moguće je ostvariti bolje rezultate dekodovanje (niži BER) primenom Soft Input Dekripcije u iteracijama. Iterativni postupak Soft Input Dekripcije se sastoji iz 3 koraka (Sl. 7):

1. Soft Input Dekripcija SID bloka *a*
2. Dekodovanje SID bloka *b* korišćenjem novih L-vrednosti SID bloka *b* koji je ispravljen Soft Input Dekripcijom u koraku 1, i
3. Soft Input Dekripcija SID bloka *b*.



Sl. 7 Algoritam Soft Input Dekripcije u iteracijama

Dakle, posle dekodovanja informacije u_{kod} u u_{dek}, se samo na bite bloka *a* primeni metod Soft Input Dekripcije. Ukoliko je metod uspešan, odnosno SID blok *a* ispravljen, pre ponovnog dekodovanja u_{kod} u u_{dek} se L-vrednosti bloka *a* promene, odnosno postave na $\pm\infty$, zavisno od toga da li je odgovarajući bit bloka *a*

jednak 1 ili 0. Naime, pošto su nakon uspešne Soft Input Dekripcije biti bloka *a* tačni, njihove L-vrednosti treba da odgovaraju verovatnoći da su biti tačni: verovatnoća je jednaka 1.

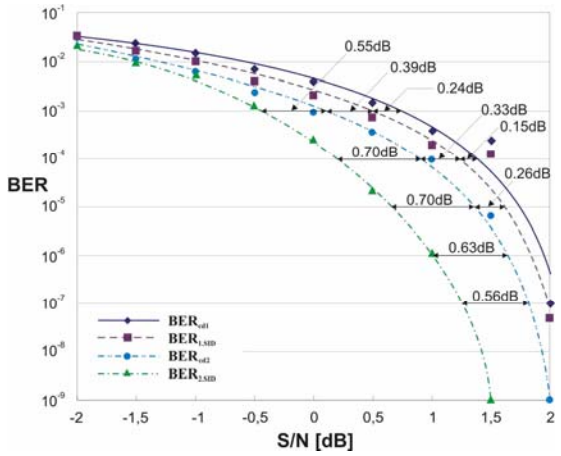
Nakon toga se vrši sledeće (drugo po redu) dekodovanje informacije u_{kod}, ali ovaj put sa novim L-vrednostima bloka *a*. Rezultati pokazuju da je BER bloka b nakon dekodovanja ovakve ''ukrštene'' forme blokova *a* i *b*, niža nego u slučaju kada bi se samo blok *b* dekodovao bez ''pomoći'' ispravljenoh L-vrednosti bloka *a*.

U trećem koraku se na blok *b* dodatno primenjuje Soft Input Dekripcija, kako bi se BER dodatno umanjio.

Iz prethodnog je jasno zašto je dužina bloka *b* veća ili jednaka dužini bloka *a*: kako je blok *b* pre Soft Input Dekripcije već poboljšano kodiran pomoću ispravljenih L-vrednosti bloka *a*, ovaj kodni dobitak se može iskoristiti za primenu dužeg bloka *b*.

V. REZULTATI SIMULACIJA SOFT INPUT DEKRIPCIJE U ITERACIJAMA

Algoritam Soft Input Dekripcije u iteracijama je simuliran koristeći iste elemente sistema kao u simulacijama u poglavlju III. Jedina razlika je u tome što simulacije sa turbo kodovanjem ovde nisu izvršene, pošto se redukcija BER i prednost korišćenja Soft Input Dekripcije u iteracijama jasno vidi iz simulacija konvolucionog koda. Analogni reziltati bi se dobili i simuliranjem turbo koda. Dužina SID bloka *a* i bloka *b* je po 320 bita.



Sl. 8 Algoritam Soft Input Dekripcije u iteracijama – BER nakon svakog koraka algoritma

Rezultati simulacija na Sl. 8 prikazuju BER posle svakog koraka algoritma prikazanog na Sl. 7: BER_{cd1} (nakon prvog dekodovanja), $BER_{1.SID}$ (nakon 1. koraka), BER_{cd2} (nakon 2. koraka) i $BER_{2.SID}$ (nakon 3.koraka).

VI. ZAKLJUČAK

U ovom radu opisani su metodi Soft Input Dekripcije i Soft Input Dekripcije u iteracijama na primerima digitalnih potpisa dužine 320 bita. Rezultati simulacija pokazuju značajni kodni dobitak oba metoda u odnosu na slučaj kada se metodi ne koriste. Osetljivost digitalnih potpisa i ostalih kriptografskih mehanizama zahteva 100% tačnost kriptoinformacija, za šta je Soft Input Dekripcija dobro rešenje, posebno u sredinama sa niskim odnosnom signal šum.

Soft Input Dekripcija u iteracijama se može proširiti na primenu više od jedne iteracije. U tom slučaju bi se više od dva SID bloka iterativno dekodovala, postižući veće kodno pojačanje svakom sledećom iteracijom (turbo efekat).

LITERATURA

[1] S. A Barbulescu: *What a wonderful turbo world*, ISBN 0-9580520-0-X, Adelaide (2002)

[2] J. Hagenauer, N. Dütsch, J. Barros, A. Schaefer: Incremental and Decremental Redundancy in Turbo Source-Channel Coding, *1st Int. Symposium on Control, Communications and Signal Processing*, Hammamet, Tunisia, pp. 595-598, March 2004

[3] ISO/IEC 9797-1: Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, 1999

[4] ISO/IEC 9797-2: Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a hash-function, 2000

[5] ISO/IEC 14888-1: Information technology – Security techniques – Digital signatures with appendix – Part 1: General, 1998

[6] ISO/IEC 9796: Information technology – Security techniques – Digital signatures giving message recovery, 1997

[7] J. Hagenauer, P. Höher: A Viterbi algorithm with soft-decision outputs and its applications, *Proc. IEEE GLOBECOM `89*, Dallas, Texas, USA, vol. 3, pp. 1680-1686, November 1989

[8] L. Bahl, J. Jelinek, J. Raviv, F. Raviv: Optimal decoding of linear codes for minimizing symbol error rate, *IEEE Transactions on Information Theory*, IT-20, pp. 284-287, March 1974.

[9] N. Živić, C. Ruland: Softinput Decryption, *4th Turbocode Conference, 6th Source and Channel Code Conference*, VDE/IEEE, Munich, April 3 – 7, 2006

[10] ISO/IEC 15946-4: Information technology – Security techniques – Cryptographic Techniques based on Elliptic Curves – Part 4: Digital signatures giving message recovery, 2004

[11] D. B. Drajić: *Uvod u statističku teoriju informacija*, Akademska misao, Beograd, 2003

***Abstract* — In this paper it is described in which way communication systems which use cryptography (encryption and decryption) can improve their performances, i.e. reduce BER as a result of a tranfer over a noisy channel. It is well known that decryptor is very sensitive to input errors, i.e. only one wrong bit at input of a decryptor is enough for even 50 % of wrong bits at the output if a decryptor. For that reason it is necessary to correct all of errors at the input of a decryptor. The whished results are got by using SISO convolutional decoder and turbo decoder in combination with decryptor, which is described as Soft Input Decryption method in this work. If Soft input Decryption is iteratively applied, decoding improves and BER additionaly reduces.**

SOFT INPUT DECRYPTION AND ITS ITERATIVE APPLICATION

Nataša Živić i Christoph Ruland