Dve decenija razvoja kriptologije u Matematičkom institutu SANU

Miodrag Mihaljević

70 godina MI-SANU
Dan Odeljenja za računarstvo
Beograd, 27 maj 2016

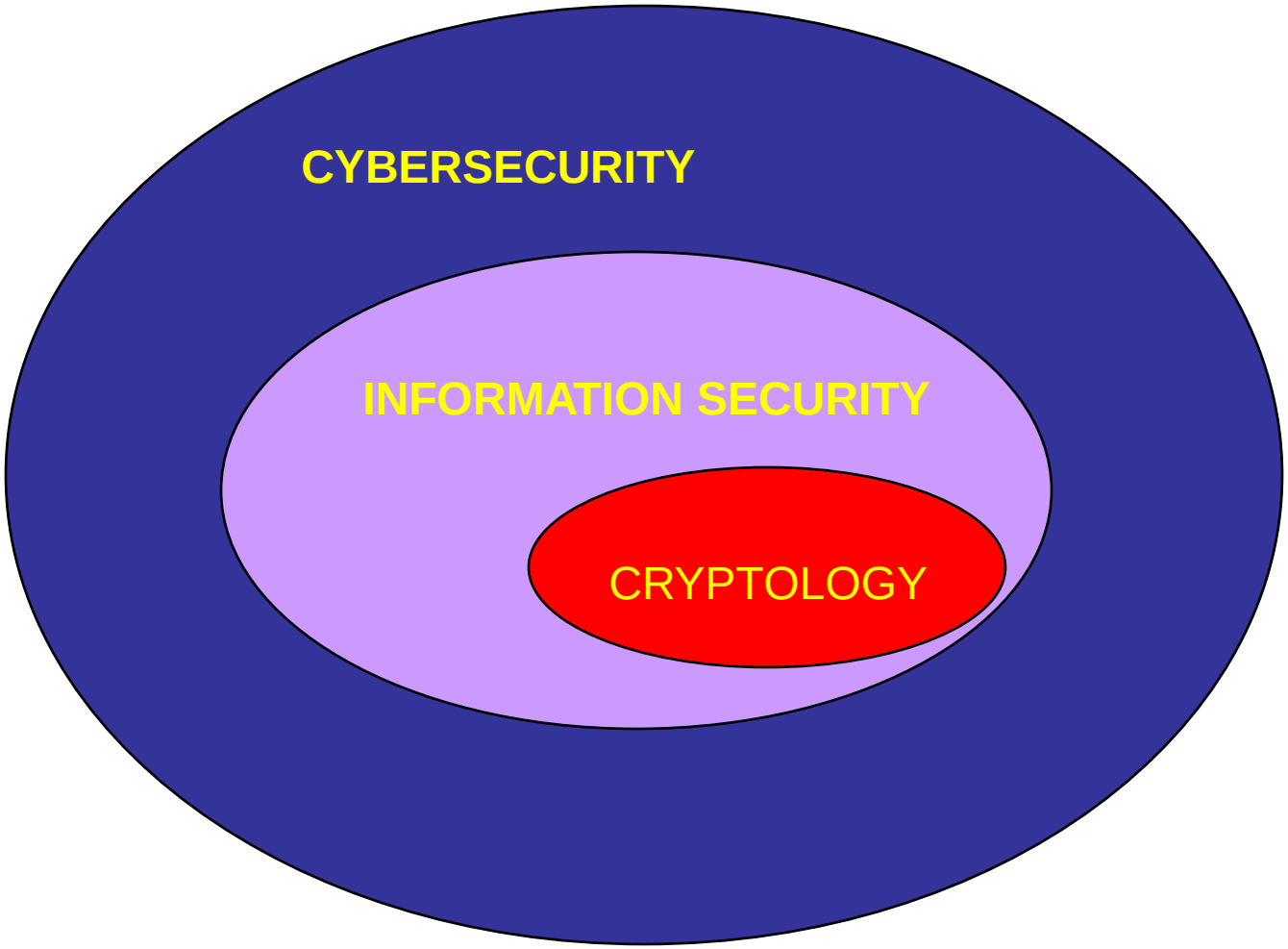
Roadmap

- Abstract of the Talk
- A Hystorical Prospective on Cryptology
- Cryptology and Information Security in MI-SANU
  - A Summary of the Achiewements
- An Illustration of Recent Results:
  - A Framework for Security Enhanced Encryption Based on Channels with Synchronization Errors
  - Information-Theoretic Security Evaluation
  - Computational-Complexity Security Evaluation
- Concluding Notes

Abstract of the Talk

Cybersecurity

jedan od ključnih izazova danas: “CyberSecurity”



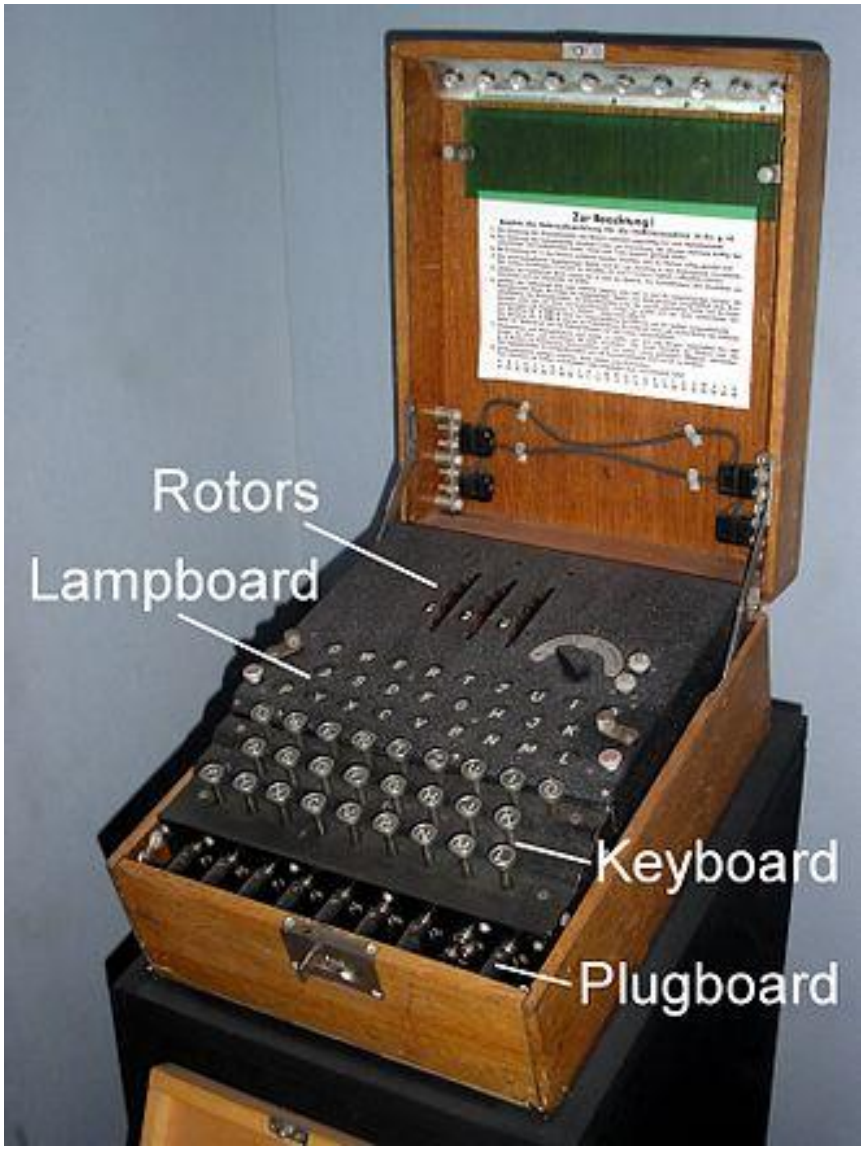
- Kriptologija je ključna matematička disciplina na osnvu koje se izgradje informaciona i sajber bezbednost.
- Ovo izlaganje sumira dostignuca tokom dve decenije razvoja kriptologije u MI-SANU.
- Ukazuje se na ostvarene rezultate u domenima osnovnih istrazivanja i tehnološki orijentisanih projekata kojima je MI-SANU postao vodeca nacionalna i regionalna institucija u oblasti kriptologije i njenih primena za ostvarivanje informacione i sajber bezbednosti.
- Posebno se ukazuje i na niz internacionalnih saradnji koje su bitno doprinele visokoj medjunarodnoj reputacji MI-SANU.

I. Jedan istorijski pogled na kriptologiju

Prvi Racunar

&

od “Veštine Tajnopisa” do Kriptologije


Rotors
Lampboard
Keyboard
Plugboard

Kriptoanaliza Enigme

Known plaintext attacking scenario

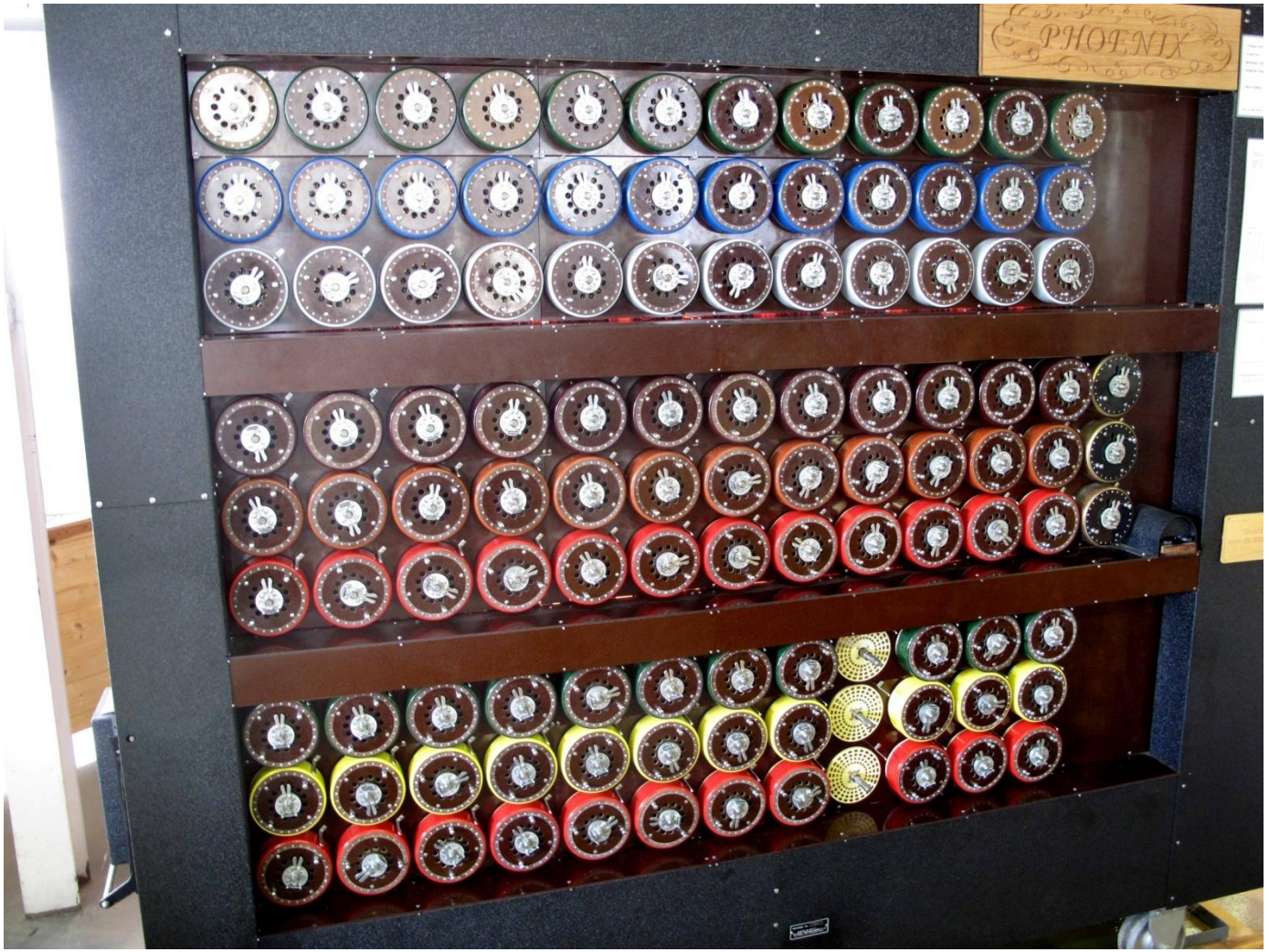
- Kako dobiti korespodentne parove otvorenog teksta i šifrata
- ...

Paradigm of Exhaustive Serach

- Kako pretraživati po prostoru mogucih hipoteza
- ...

The working rebuilt Bomb at Bletchley Park museum. Each of the rotating drums simulates the action of an Enigma rotor.

Prvi (Elektomehanicki) računar



Radjanje
Kriptologije i Teorije Informacija

Claude Shannon (1916-2001)

Teorija Informacija i Kriptologija: Novi Domeni Nauke

- **Teorija Infrmacija**
- C. E. Shannon, “**A mathematical theory of communication**”. Bell System Technical Journal, vol. 27, pp. 379–423 and 623–656, July and October 1948.

- **Kriptologija**
- C. E. Shannon "**Communication Theory of Secrecy Systems**". Bell System Technical Journal, vol. 28 (4), pp. 656–715, 1949.

Teorija Informacija i Kriptologija: Novi Domeni Nauke

- **Teorija Infrmacija**
- C. E. Shannon, “**A mathematical theory of communication**”. Bell System Technical Journal, vol. 27, pp. 379–423 and 623–656, July and October 1948.

- **Kriptologija**
- C. E. Shannon "**Communication Theory of Secrecy Systems**". Bell System Technical Journal, vol. 28 (4), pp. 656–715, 1949.

Teorija Informacija i Kriptologija: Novi Domeni Nauke

- **Teorija Infrmacija**
- C. E. Shannon, “**A mathematical theory of communication**”. Bell System Technical Journal, vol. 27, pp. 379–423 and 623–656, July and October 1948.

- **Kriptologija**
- C. E. Shannon "**Communication Theory of Secrecy Systems**". Bell System Technical Journal, vol. 28 (4), pp. 656–715, 1949.

Information and Coding Theory

Information Theory Keywords

- Entropy
- Equivocation
- Channel Capacity
- ...

Coding Theory Keywords

- Reliable Communications
- Linear Block Codes
- LDPC codes
- Decoding techniques

KRIPTOLOGIJA

Kriptografija (Cryptography)

- Tajnost
- Integritet
- Autentičnost
- Neporicivost

Kriptoanaliza (Cryptanalysis)

- Tehnike provere sigurnosti i “razbijanja” kriptografskih algoritama
- Generičke tehnike
- Prilagodjene tehnike
- Scenariji evaluacije

II. Cryptology and Information Security in MI-SANU

A Summary of the Achiewements

Kriptologija i Informaciona Bezbednost u MI-SANU

Osnovna Istraživanja

(više od 20 godina – više od 100 medjunarodnih referenci)

- Medjunarodno prepoznata kao vodeća u nacionalnim i regionalnim okvirima
- Intenzivna medjunarodna saradnja (Japan, EU, Indija, US)

Tehnička Rešenja

(više od 15 godina – više od 50 tehničkih rešenja)

- Projekti sa vodećim državnim i privrednim institucijama

Ilustrativni Naučni Radovi i Patenti

Transactions Papers

Reduced Complexity Iterative Decoding of Low-Density Parity Check Codes Based on Belief Propagation

Marc P. C. Fossorier, *Member, IEEE,* Miodrag Mihaljević, and Hideki Imai, *Fellow, IEEE*

***Abstract*—In this paper, two simplified versions of the belief propagation algorithm for fast iterative decoding of low-density parity check codes on the additive white Gaussian noise channel are proposed. Both versions are implemented with real additions only, which greatly simplifies the decoding complexity of belief propagation in which products of probabilities have to be computed. Also, these two algorithms do not require any knowledge about the channel characteristics. Both algorithms yield a good performance–complexity tradeoff and can be efficiently implemented in software as well as in hardware, with possibly quantized received values.**

***Index Terms*—APP decoding, belief propagation, block codes, four-density parity check codes, iterative decoding.**

I. Introduction

LOW-DENSITY parity-check (LDPC) codes, proposed by Gallager [1], [2], appear as a class of codes which can yield very good performance on the binary symmetric channel (BSC) as well as on the additive white Gaussian noise (AWGN) channel. Recently, it was shown that the belief propagation (BP) algorithm [3] provides a powerful tool for iterative decoding of LDPC codes, by noting that the original Gallager's iterative probabilistic decoding of LDPC codes is a particular BP-based decoding approach [5]–[8]. As in [4], this probabilistic decoding algorithm is based on evaluating the likelihood ratios associated with each information bit from information provided by disjoint parity check equations. Iterative decoding techniques in general have received significant attention recently and various results have been reported (see [5]–[18], for example).

The aim of this paper is to develop an iterative decoding algorithm for LDPC codes as an approximation of the standard BP decoding procedure, so that the modified algorithm performs close to the standard BP but with a significant reduction of complexity. Accordingly, a goal of this paper is to obtain a good performance–complexity tradeoff. First, a simplified version of the BP algorithm is considered. This modified algorithm, which corresponds to the approach taken in [12]–[14], is then further simplified so that it performs real value additions only. This second simplification, which is equivalent to the approximation presented in [19] for majority logic decoding based on the APP algorithm of [4], simply consists of expressing all the steps of the algorithm with respect to logarithms of probabilities rather than probabilities. The same standard approximation was used to derive the Max-Log-MAP algorithm from the MAP algorithm [10], [11]. This simple algorithm allows the processing of low-complexity iterative decoding of LDPC codes, but at the expense of about 1-dB degradation in error performance with respect to the BP algorithm at the bit error rate (BER) 10^{-5}. A second simplified algorithm is then considered. For this algorithm, the standard approximation is directly applied to the BP algorithm. Although not as straightforward as in the previous case, due to the fact that for the BP algorithm the probability values considered at iteration-i do not necessarily correspond to the hard decisions made at iteration-$(i-1)$, the application of the standard approximation achieves a better tradeoff between error performance and decoding complexity, with real value additions only and a performance degradation of few tenths of a decibel at the BER 10^{-5} for the LDPC codes simulated.

The paper is organized as follows. The characteristics of LDPC codes and their decoding based on BP are briefly reviewed in Section II. Then the two reduced-complexity BP-based decoding algorithms are described in Section III. Finally, these algorithms are compared with BP in Section IV and concluding remarks are given in Section V.

Paper approved by J. Huber, the Editor for Coding and Coded Modulation of the IEEE Communications Society. Manuscript received May 25, 1998; revised September 9, 1998 and November 23, 1998. This work was supported by the National Science Foundation under Grant NCR-94-15374 and Grant CCR-97-32959 and by the Japan Society for Promotion of Science (JSPS) under Contract JSPS-RFTF-96P00604.

M. P. C. Fossorier is with the Department of Electrical Engineering, University of Hawaii, Honolulu, HI 96822 USA (e-mail: marc@aravis.eng.hawaii.edu).

M. Mihaljević is with the Mathematical Institute, Academy of Science and Arts, Belgrade, Yugoslavia.

H. Imai is with the Institute of Industrial Science, University of Tokyo, Tokyo 106, Japan.

Publisher Item Identifier S 0090-6778(99)03899-4.

0090–6778/99$10.00 © 1999 IEEE

Security Evaluation of Certain Broadcast Encryption Schemes Employing a Generalized Time-Memory-Data Trade-Off

Miodrag J. Mihaljević, Marc P. C. Fossorier, and Hideki Imai

***Abstract*— In this letter a weakness of certain broadcast encryption schemes in which the protected delivery of a session key (SEK) is based on XOR-ing this SEK with the IDs of the keys employed for its encryption is addressed. The weakness can be effectively explored assuming passive attacking which in the cases corresponding to a malicious legitimate user being the attacker, is a ciphertext only attack. A dedicated algorithm for cryptanalysis is proposed based on a generalized time-memory-data trade-off approach and its main characteristics are derived. The developed algorithm points out a security weakness of employing a block cipher with block length shorter than the key length in the considered BE schemes.**

***Index Terms*— Broadcasting, conditional data access control, cryptographic key management, cryptanalysis, time-memory-data trade-off.**

I. Introduction

A CONVENTIONAL approach for access control to broadcasted (multicasted) data employs the following paradigm: the data are encrypted and only legitimate users are provided with the information on how to decrypt them. We consider schemes where the data encryption is performed based on a symmetric cipher and the updatable secret session encrypting key (SEK). To make SEK updating possible, another set of keys called the key-encrypting keys (KEKs) are involved. There are two basic approaches for establishing the required security based on the above paradigm. One approach uses static KEKs (see [9], [1] and [6], for example), and the other one employs updatable KEKs (see [10], [11], and [12], for example). BE schemes with static KEKs (stateless receivers) have the desirable feature that members do not need to be always connected online, which is especially preferable for applications over lossy channels. Since rekey messages in stateless schemes are independent of each other, members once being offline or inactive can always decrypt the latest group key instantly.

In this letter the security evaluation of certain BE schemes with static KEKs is considered. In order to enhance the security of these schemes, before the encryption, the SEK is XOR-ed with the identifier (ID) of the KEK employed for its encryption, as proposed in [6] and [9].

Manuscript received June 22, 2007. The associate editor coordinating the review of this letter and approving it for publication was Prof. Christina Fragouli.

M. J. Mihaljević is with the Mathematical Institute, Serbian Academy of Sciences and Arts, Kneza Mihaila 35, Belgrade, Serbia (e-mail: miodragm@turing.mi.sanu.ac.yu).

Marc P. C. Fossorier is with the Department of Electrical Engineering, University of Hawaii, Honolulu, HI 96822, USA.

Hideki Imai is with the Faculty of Science and Engineering, Chuo University, Tokyo, Japan, and the Research Center for Information Security (RCIS), National Institute of Advanced Industrial Science and Technology (AIST), Tokyo, 101-0021 Japan.

Digital Object Identifier 10.1109/LCOMM.2007.071029.

II. Models of Certain Broadcast Encryption and Problem Statement

Let KEK_i denote a KEK employed in the system, and let ID_i denote its name or ID, assuming that ID_i does not disclose any information on KEK_i itself. BE is based on the following approach. The system center generates all the employed KEKs. A user of the BE system is in advance provided with a subset of all KEKs employed in the system. Note that different users can have overlapping subsets of KEKs, but no pair of users have an identical subset.

In a basic BE setting, the procedures at the center and for each of the users are based on the following. When the current SEK should be updated, the center finds a subset $I = I(SEK)$ of KEKs $\{KEK_i\}_{i\in I}$ such that each of the legitimate users possesses at least one of these keys and none of the un-legitimate users possesses any of these keys. The center encrypts the data with SEK, generates all encrypted forms of SEK employing each KEK_i, $i \in I$, and broadcasts $< [header]; G_{SEK}(data) > = < [\{ (ID_i, E_{KEK_i}(SEK)) \}_{i\in I}]; G_{SEK}(data) >$, where $E(\cdot)$ and $G(\cdot)$ are certain encryption algorithms.

In order to address certain weaknesses of this basic BE model, in [6], an enhanced security approach for BE is proposed, which corresponds to the following BE header model:

$$[header] = [\{ (ID_i, E_{KEK_i}(SEK \oplus ID_i)) \}_{i\in I}], \quad (1)$$

where $\oplus$ denotes bit-by-bit XOR-ing of the vectors SEK and ID_i. This enhanced approach is employed in [1] as well.

The problem addressed in this letter is the security evaluation of the BE schemes which follow the header model specified by (1). Recently, vulnerabilities of certain BE schemes have been reported in [7] and [8] and they provide the origins for the approach given in this letter. Particularly note that a security weakness of the approach proposed in [6] is reported in [7] employing an active attack scenario, while the scope of this letter is restricted to passive attacking.

III. Scenario for the Security Evaluation

The considered settings for cryptanalysis originate from the following issues: (i) It is a realistic scenario that different schemes of the same class are deployed and are subject to malicious monitoring; (ii) In a typical BE scheme with stateless receivers KEKs are in a tamper-proof (resistant) hardware and accordingly the system should be considered as broken even if an attacker can recover only one of the KEKs employed in the system.

1089-7798/07$25.00 © 2007 IEEE

PHYSICAL REVIEW A 75, 052334 (2007)

Generic framework for the secure Yuen 2000 quantum-encryption protocol employing the wire-tap channel approach

Miodrag J. Mihaljević*
Mathematical Institute, Serbian Academy of Sciences and Arts, Belgrade, Serbia
and Research Center for Information Security, National Institute of Advanced Industrial Science and Technology, Room 1102, Akihabara Daibiru, 1-18-13 Sotokanda, Chiyoda-ku, Tokyo 101-0021, Japan
(Received 11 March 2007; revised manuscript received 9 April 2007; published 24 May 2007)

It is shown that the security, against known-plaintext attacks, of the Yuen 2000 (Y00) quantum-encryption protocol can be considered via the wire-tap channel model assuming that the heterodyne measurement yields the sample for security evaluation. Employing the results reported on the wire-tap channel, a generic framework is proposed for developing secure Y00 instantiations. The proposed framework employs a dedicated encoding which together with inherent quantum noise at the attacker's side provides Y00 security.

DOI: 10.1103/PhysRevA.75.052334 PACS number(s): 03.67.Dd

I. INTRODUCTION

The Yuen 2000 (Y00) protocol (see [1–4]) protects the data jointly employing cryptographic and physical noise: It combines quantum and stream cipher concepts yielding a randomized stream cipher. Security of the Y00 protocol has attracted significant attention and has been discussed in a number of papers. In a general setting, security of Y00 protocol has been challenged in [5–8] with the corresponding replays in [1,9–11], respectively. Discussions on security of a particular Y00 instantiation have been reported in [12–14].

This paper addresses Y00 security against known-plaintext attacks and the main goal is to provide the following: (i) a contribution to the discussions on Y00 security via an alternative approach; (ii) pointing out applicability of the wire-tap channel [15] paradigm as a background for consideration of Y00 security and developing certain families of the Y00 protocol; and (iii) proposal of a generic framework for developing secure Y00 protocol employing certain encoding dedicated to the unavoidable quantum noise which an attacker must face.

II. BACKGROUND

A. Y00 protocol and heterodyne measurements

1. Y00 quantum stream cipher

Y00 protocol employs certain results of the quantum detection theory to provide a randomized stream cipher. In Y00 protocol, a pseudorandom number generator (PRNG) with a shared key is used to make a difference in the performances of the quantum signal detection. The legitimate communicating parties, a sender and a receiver, Alice and Bob, respectively, share a secret key and the key is expanded into a long key-stream sequence or "running key" via a PRNG. Assuming that BPS and MPS mean a binary pure state and M-ary pure state, respectively, according to the quantum detection theory, we have the following property of the average error probability, $P_e(\mathrm{BPS}) < P_e(M\mathrm{PS})$. It means that if the attacker Eve does not know the key, she must detect M-ary quantum states, while Bob's detection procedure which employs the key is the binary. So, Eve must search for the data or the key based on her detection results with an unavoidable quantum error. The possibility of obtaining information-theoretic security against known-plaintext attack employing the quantum noise randomization at Eve's side was first pointed out in [1,11].

The framework of the Y00 protocol is as follows. The output bit sequence of the PRNG is divided into $\ln M$-bit segments, and each segment is considered as the running key symbol U_i which determines the basis $\{|\alpha e^{i\theta_i}\rangle, |\alpha e^{i(\theta_i+\pi)}\rangle\}$: That is, when a running key symbol U_i appears, a coherent state basis corresponding to U_i is chosen. Then, the data bit is transmitted by $|\alpha e^{i\theta_i}\rangle$ or $|\alpha e^{i(\theta_i+\pi)}\rangle$. In the basic model of the Y00 protocol, the mapping function $f(\cdots)$ of the running key symbols to the bases of coherent states is given by the following phase modulation: $\begin{matrix} U_i \\ \theta_i \end{matrix} \Big\| \begin{matrix} 1 & 2 & 3 & \cdots & M \\ \theta_1 & \theta_2 & \theta_3 & \cdots & \theta_M \end{matrix}$, where the mapping $U_i \to \theta_i$ means that U_i implies a selection of θ_i, $\theta_i+\pi$, and $\pi > \theta_{i+1} > \theta_i > 0$.

The security role of the mapper has been discussed in [1,2,13] where its significance has been pointed out. Particularly, a mapping technique which provides immunity against certain correlation attacks has been proposed in [14]. These results have been considered as a background for development of an alternative mapping approach employing the wire-tap channel [15] paradigm.

2. Heterodyne measurement

The heterodyne measurement is the key step for security evaluation of the Y00 protocol because this measurement results in a mapping of Y00 security into a cryptographic decoding problem. Via the heterodyne measurement, it is possible to obtain a noisy version of the output sequence from PRNG so that the security of the Y00 protocol reduces to recovering the secret key which controls PRNG employing its noisy output sequence.

Suppose that state $|\phi(m)\rangle$, $0 \le m < M$ is transmitted, and an eavesdropper performs a heterodyne measurement to obtain (r,θ) in polar coordinates. Based on the observed values

*Electronic address: miodragm@turing.mi.sanu.ac.yu; URL: http://www.mi.sanu.ac.yu/cv/cvmihaljevic.htm

 ©2007 The American Physical Society

Computing (2009) 85:153–168
DOI 10.1007/s00607-009-0035-x

An approach for stream ciphers design based on joint computing over random and secret data

Miodrag J. Mihaljević · Hideki Imai

Received: 31 October 2008 / Accepted: 19 February 2009 / Published online: 7 May 2009
© Springer-Verlag 2009

Abstract This paper proposes and analyzes an approach for design of stream ciphers based on joint computing over random and secret data. Feasibility of encryption/decryption computation when the ciphertext involve pure random data is shown. The core element of the proposed approach for stream ciphering is a pseudo-random embedding of the random bits into the ciphertext and this embedding plays role of a homophonic encoding. The initial ciphertext with the embedded random bits is further on intentionally degraded by its exposure to a moderate noise which can be modelled as the binary symmetric channel effect. A security evaluation of the proposed approach implies that its security appears as a consequence of hardness of the LPN problem, as well. The developed design has potential of providing that complexity of recovering the secret key in the known plaintext attack scenario is close to the complexity of recovering the secret key via the exhaustive search, i.e. close to the maximal possible one for the given size of the secret key. The proposed approach can be considered as

M. J. Mihaljević was supported by the grant ON144018 of the Ministry for Science and Tech.

M. J. Mihaljević
Mathematical Institute, Serbian Academy of Science and Arts,
Kneza Mihaila 35, Belgrade, Serbia

M. J. Mihaljević (✉) · H. Imai
Research Center for Information Security (RCIS),
National Institute of Advanced Industrial Science and Technology (AIST),
Room 1003, Akihabara Daibiru, 1-18-13, Sotokanda, Chiyoda-ku,
Tokyo 101-0021, Japan
e-mail: miodragm@mi.sanu.ac.rs

H. Imai
Faculty of Sciences and Engineering, Chuo University,
1-13-27, Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan

US008023649B2

(12) **United States Patent**
Mihaljevic et al.

(10) **Patent No.: US 8,023,649 B2**
(45) **Date of Patent: Sep. 20, 2011**

(54) **METHOD AND APPARATUS FOR CELLULAR AUTOMATA BASED GENERATION OF PSEUDORANDOM SEQUENCES WITH CONTROLLABLE PERIOD**

(75) Inventors: **Miodrag J. Mihaljevic**, Tokyo (JP); **Jouji Abe**, Kanagawa (JP)

(73) Assignee: **Sony Corporation**, Tokyo (JP)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 977 days.

(21) Appl. No.: **10/578,505**

(22) PCT Filed: **Sep. 5, 2005**

(86) PCT No.: **PCT/JP2005/016686**
§ 371 (c)(1),
(2), (4) Date: **May 5, 2006**

(87) PCT Pub. No.: **WO2006/028235**
PCT Pub. Date: **Mar. 16, 2006**

(65) **Prior Publication Data**

US 2008/0304667 A1 Dec. 11, 2008

(30) **Foreign Application Priority Data**

Sep. 6, 2004 (JP) 2004-258186

(51) **Int. Cl.**
H04L 9/26 (2006.01)
H04L 9/24 (2006.01)
H04L 9/20 (2006.01)

(52) **U.S. Cl.** **380/46**; 380/47; 380/277; 380/268; 708/250; 708/253; 708/255; 708/256

(58) **Field of Classification Search** ..... None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,331,581	A *	7/1994	Ohkubo et al.	708/253
5,511,146	A *	4/1996	Simar, Jr.	706/10
6,985,918	B2 *	1/2006	Shackleford et al.	708/250
7,389,316	B1 *	6/2008	Baetoniu	708/250
7,571,200	B2 *	8/2009	Shackleford et al.	708/250
7,634,522	B1 *	12/2009	Carter et al.	708/250
7,715,639	B2 *	5/2010	Ishikawa	382/238
7,716,100	B2 *	5/2010	Metlapalli	705/35
7,788,479	B2 *	8/2010	Ishii	713/150
7,925,014	B2 *	4/2011	Kim et al.	380/46
2003/0204541	A1 *	10/2003	Shackleford et al.	708/250
2004/0006680	A1 *	1/2004	Duncan	711/219

OTHER PUBLICATIONS

Cattell, Kevin et al., "2-by-n Hybrid Cellular Automata with Regular Configuration: Theory and Application", IEEE Transactions on Computers, vol. 48, No. 3, pp. 285-295, 1999.

Guan, Sheng-Uei et al., "An Evolutionary Approach to the Design of Controllable Cellular Automata Structure for Random Number Generation", IEEE Transactions on Evolutionary Computation, vol. 7, No. 1, pp. 23-35, 2003.

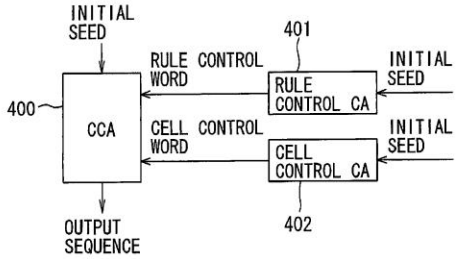
* cited by examiner

Primary Examiner — Syed Zia
(74) *Attorney, Agent, or Firm* — Oblon, Spivak, McClelland, Maier & Neustadt, L.L.P.

(57) **ABSTRACT**

A compact apparatus for generation of desired pseudorandom sequences with controllable period. The apparatus includes two-dimensional cellular automata for generating a first sequence, 2-by-L cellular automata for generating a second sequence, adders for performing bit-to-bit mod2 sum of the first sequences and the second sequences, and a buffer for buffering the resultant sequences from the adders.

15 Claims, 11 Drawing Sheets



特　許　証
(CERTIFICATE OF PATENT)

特許第４８６３２８３号
(PATENT NUMBER)

発明の名称
(TITLE OF THE INVENTION)　軽量の認証プロトコルによる認証システム

特許権者
(PATENTEE)　東京都千代田区霞が関１－３　１
独立行政法人産業技術総合研究所

発明者
(INVENTOR)　ミハイエビッチ　ミオドラッグ
渡邊　創

出願番号
(APPLICATION NUMBER)　特願２００７－０３７４８０

出願日
(FILING DATE)　平成１９年　２月１９日(February 19, 2007)

登録日
(REGISTRATION DATE)　平成２３年１１月１８日(November 18, 2011)

この発明は、特許するものと確定し、特許原簿に登録されたことを証する。
(THIS IS TO CERTIFY THAT THE PATENT IS REGISTERED ON THE REGISTER OF THE JAPAN PATENT OFFICE.)

平成２３年１１月１８日(November 18, 2011)

特許庁長官
(COMMISSIONER, JAPAN PATENT OFFICE)

岩井良行

Espacenet

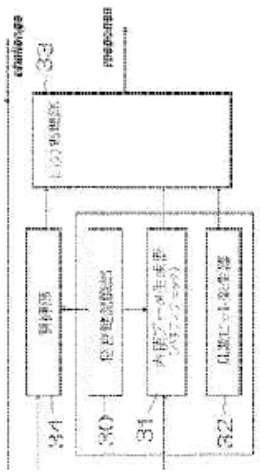
Bibliographic data: JP4863283 (B2) — 2012-01-25

AUTHENTICATION SYSTEM USING LIGHT-WEIGHT AUTHENTICATION PROTOCOL

Inventor(s):	MIHALJEVIC MIODRAG, ; WATANABE SO	
Applicant(s):	NATIONAL INSTITUTE OF ADVANCED INDUSTRIAL & TECHNOLOGY	
Classification:	- international:	***G06F21/20; G06K17/00; G06K19/07; G06K19/10; H04L9/32***
	- European:	G06F21/00N5A; H04L9/32R
Application number:	JP20070037480 20070219	
Priority number(s):	JP20070037480 20070219	
Also published as:	JP2008205675 (A) WO2008102693 (A1)	

Abstract of JP2008205675 (A)

PROBLEM TO BE SOLVED: To provide an authentication system usable for the authentication of radio tag data, using a simple protocol. SOLUTION: The authentication system includes a secret key storage for storing secret key information; an inner product generator for generating data for parity check obtained by an inner product operation between challenge data and the secret key information; a random number bit generator for generating random number bits; a controller for control processing to invert bits based on a pseudo random number bit stream generated by a key stream based on the secret key information to insert the random number bits, and to evaluate the inner product data, and by control by the controller, an output processor for outputting response data by executing processing which acts



Medjunarodna Saradnja

Research Center for Information Security (RCIS)

AIST

Notice: RCIS was reformed into RISEC on April 1, 2012.
It has been further merged into new Information Technology Research Institute on April 1, 2015.

Members

This is our member list, as of July 2010 (in alphabetical order).

- Affeldt, Reynald (Research Team for Software Security)
- Akimoto, Satoshi (ICSS Technology Team)
- Artho, Cyrille (Research Team for Software Security)
- Attrapadung, Nuttapong (Research Team for Security Fundamentals)
- Cui, Yang (JSPS Postdoctral Fellow)
- Fujiwara, Mitsuru (ICSS Technology Team)
- Hagiwara, Manabu (Research Team for Physical Analysis)
- Hanaoka, Goichiro (Research Team for Security Fundamentals)
- Hirano, Kunitake (ICSS Technology Team)
- Hori, Yohei (Research Team for Hardware Security)
- Imafuku, Kentaro (Leader, Research Team for Physical Analysis)
- Imai, Hideki (Director, Chuo Univ.)
- Inuma, Manabu (Research Team for Security Fundamentals)
- Katashita, Toshihiro (Research Team for Hardware Security)
- Kawamura, Shinichi (Deputy Director. Leader, ICSS Technology Team)
- Kimura, Gen (Research Team for Physical Analysis Aist Postdoctoral Fellow)
- Kobara, Kazukuni (Principal Research Scientist. Leader, Research Team for Security Fundamentals)
- Matsumoto, Tsutomu (Advisor, Yokohama National Univ.)
- Mihaljevic, Miodrag (Invited Senior Research Scientist, Serbian Academy of Sciences and Arts)
- Miyadera, Takayuki (Research Team for Physical Analysis)

SEMINAR TALKS
By Dr. Miodrag Mihaljevic
DATE: August 15, 2012
TIME: 11a.m.—2p.m.
WHERE: HOLMES 389

Biography:

Miodrag J. Mihaljevic has received his B.Sc. and M.S. degrees in electrical engineering from University of Belgrade, Serbia (Yugoslavia), and received his Ph.D. degree in 1990.

He is a research professor and the projects leader at the Mathematical Institute, Serbian Academy of Sciences and Arts, Belgrade. His main research areas are cryptology and information security. He has published more than 90 research papers in the leading international journals and conference proceedings (including over 50 papers in IEEE journals, J. of Cryptology, Phys. Rev., Computing, IET Inform. Sec., LNCS, IEICE Trans., Inform. Process. Lett., and as certain book chapters), and over 150 publications in total. He is co-inventor of 6 granted patents in U.S, Japan and China. His research results have been cited more than 1000 times in the leading international publications. He has served over 150 times as a reviewer for the leading international journals and conferences.

He has held long-term visiting positions at the University of Tokyo, IMAI Lab (1997-2001 and 2004-2005), Sony Computer Science Labs (2001-2002), Sony Corporation Labs. (2002-2003), Tokyo, the Research Center for Information Security (RCIS), National Institute of Advanced Industrial Science and Technology (AIST), Tokyo (2006-2012), and currently (from April 1, 2012) he holds the position of an Invited Senior Researcher at the Research Institute for Secure Systems (RISEC), National Institute AIST, Tsukuba, Japan.

Talk #1:

"On Employment Environmental Noise for Developing Dedicated Cryptographic Algorithms for Certain Smart Grid Components"

Abstract:

In certain domains of information-communications infrastructure of Smart Grid, the communications channels suffer from unavoidable and high noise. A particular example are the floating wind turbines where only wireless and power line cable (PLC) are available for communications and control purposes, and both of these channels appear as very noisy.

Accordingly, for reliable communications we need an adequate error-correction coding scheme. On the other hand it is interesting to address the issues of employment the inherent noise for design dedicated cryptographic algorithms based on which the security mechanism are built, as well as, when appropriate, to employ the available error-correction coding within a cryptographic algorithm.

This talk addresses design and analysis of cryptographic algorithms for authentication and encryption which employ the channel noise for the cryptographic security enhancement.

Talk #2:

"Information Theoretic and Computational Complexity Evaluation of Encryption Based on Pseudorandomness, Randomness and Dedicated Coding"

Abstract:

In a number of application scenarios including certain Smart Grid ones, an important request is employment of light-weight cryptographic algorithms in order to reduce the overhead to the system implied by involved cryptographic mechanisms.

At the same time, beside the light-weightiness, the employed cryptographic algorithms should be highly secure because of possible disastrous impacts of their breakability. This talk addresses a framework for enhancing security of light-weight stream ciphers employing randomness and dedicated coding. Security evaluation of the considered framework is discussed from information-theoretic and computational-complexity points of view. Regarding information-theoretic approach, the equivocation of the secret key is analyzed.

The computational-complexity evaluation approach shows that recovering of secret key appears as hard as decoding of certain general linear block codes, i.e. certain problems of learning the parity in noise (the LPN problem). The talk also discuss a problem of design appropriate linear block codes which provide joint error-correction and homophonic coding, as well as the wire-tap channel coding.

III. An Illustration of Recent Results

III.1. Introduction

Noisy Channels and Security Enhancement of Encryption

Security of Encryption and Implementation Complexity

- Mainly based on heuristic assumptions
- Particularly when the encryption is based on employment of finite state machines
- Lightweight encryption implies additional challenges

...

- Security enhancement appears as an interesting approach

...

- Asymmetric implementation complexity of encryption and decryption also appears as an interesting issue

Noisy Channels

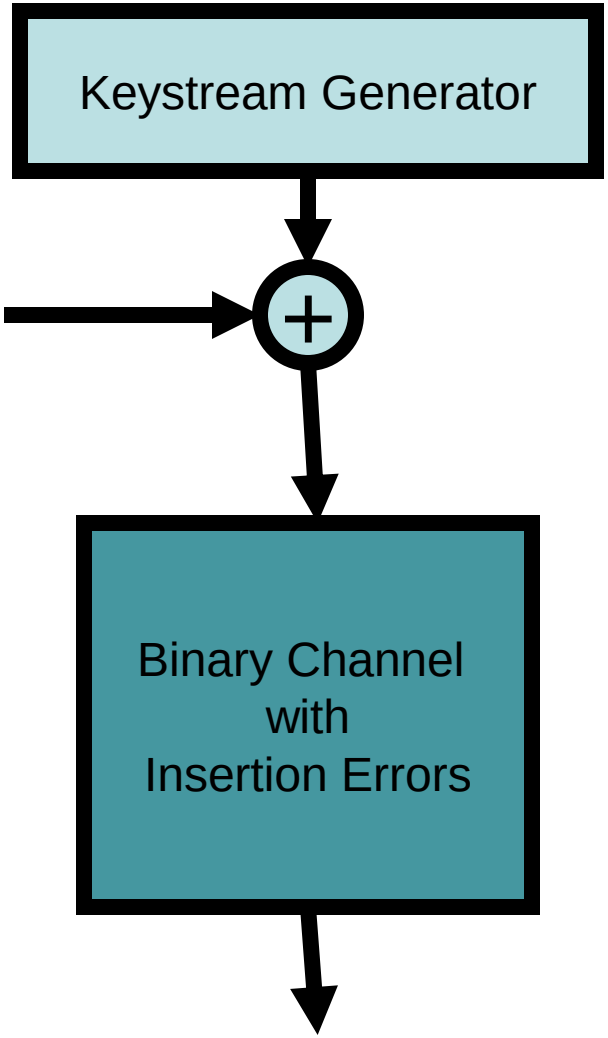
- Additive noise
- Binary Symmetric Channel
- ...

- Binary Channels with synchronization errors
- Bits deletion
- Bits insertion
- Bits Complementation

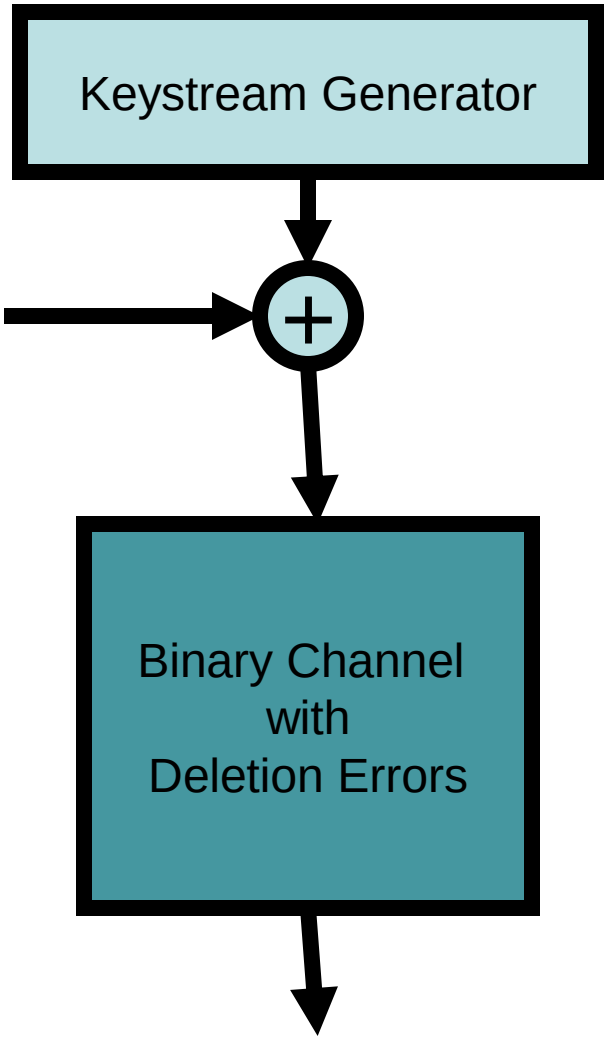
III. 2. A Framework for Security Enhancement Based on the Channels with Synchronization Errors

Desired Model of Encryption an Attacker Should Face

Encryption at Party I

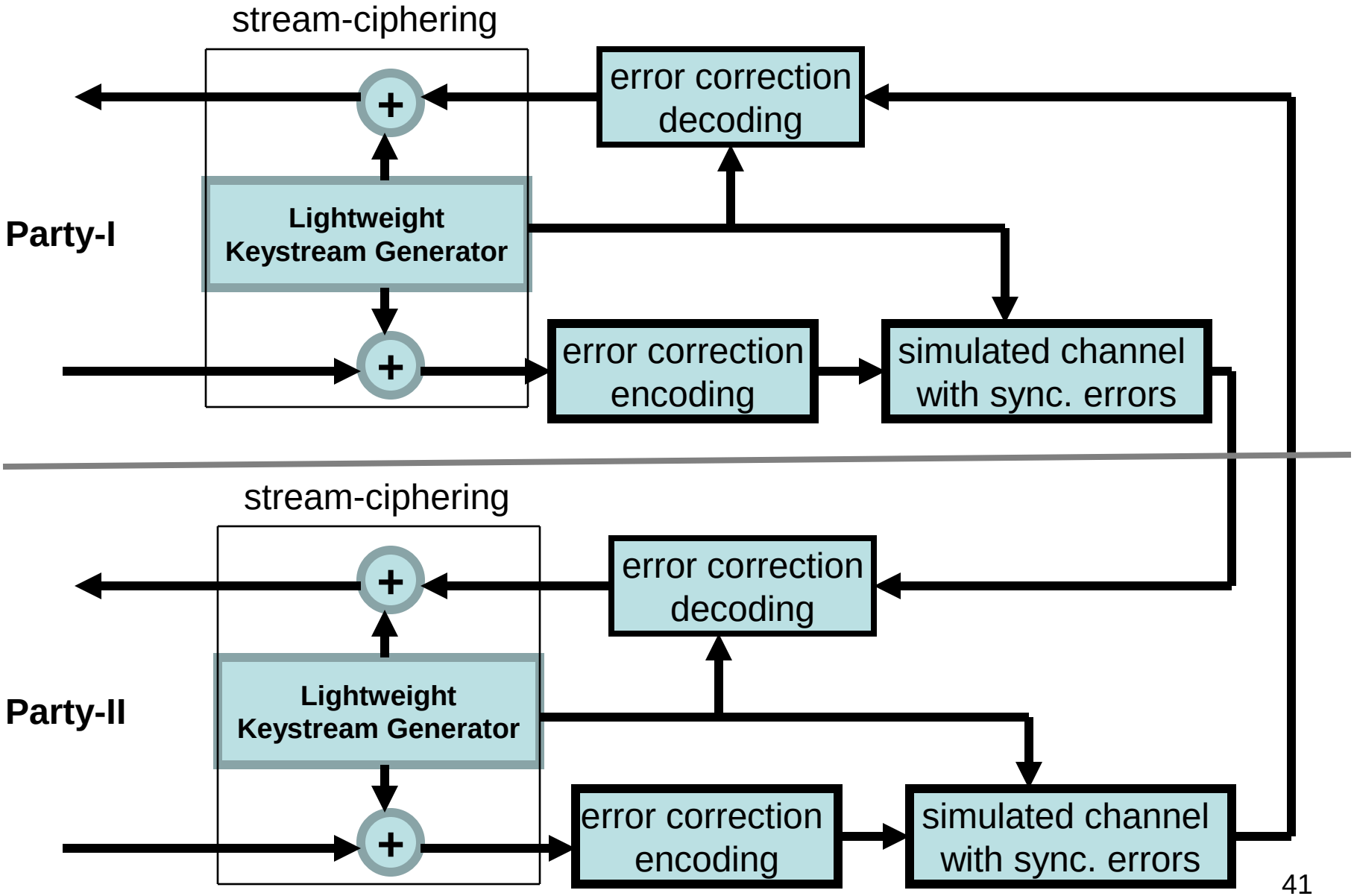


Encryption at Party II

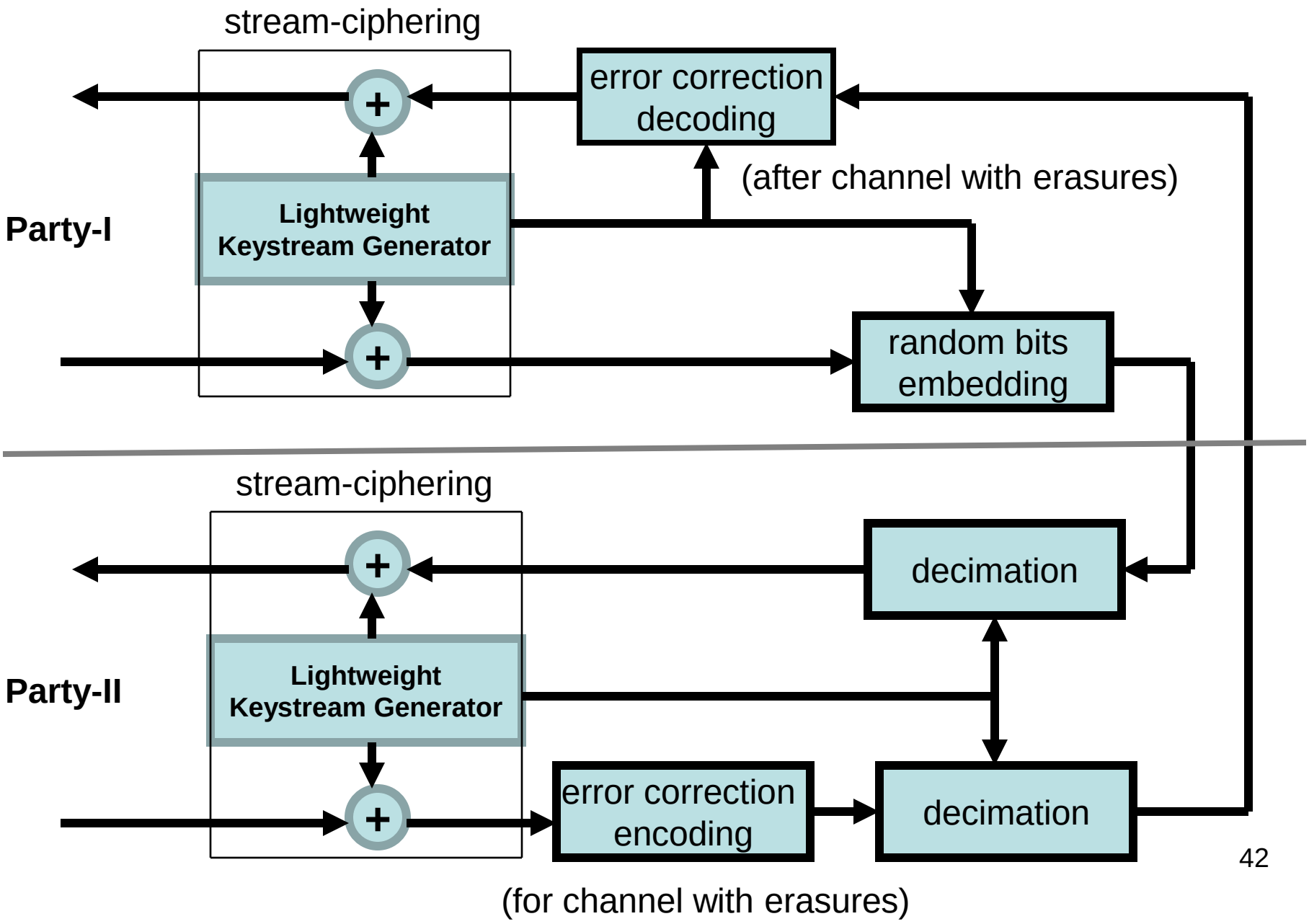


Attacker Side

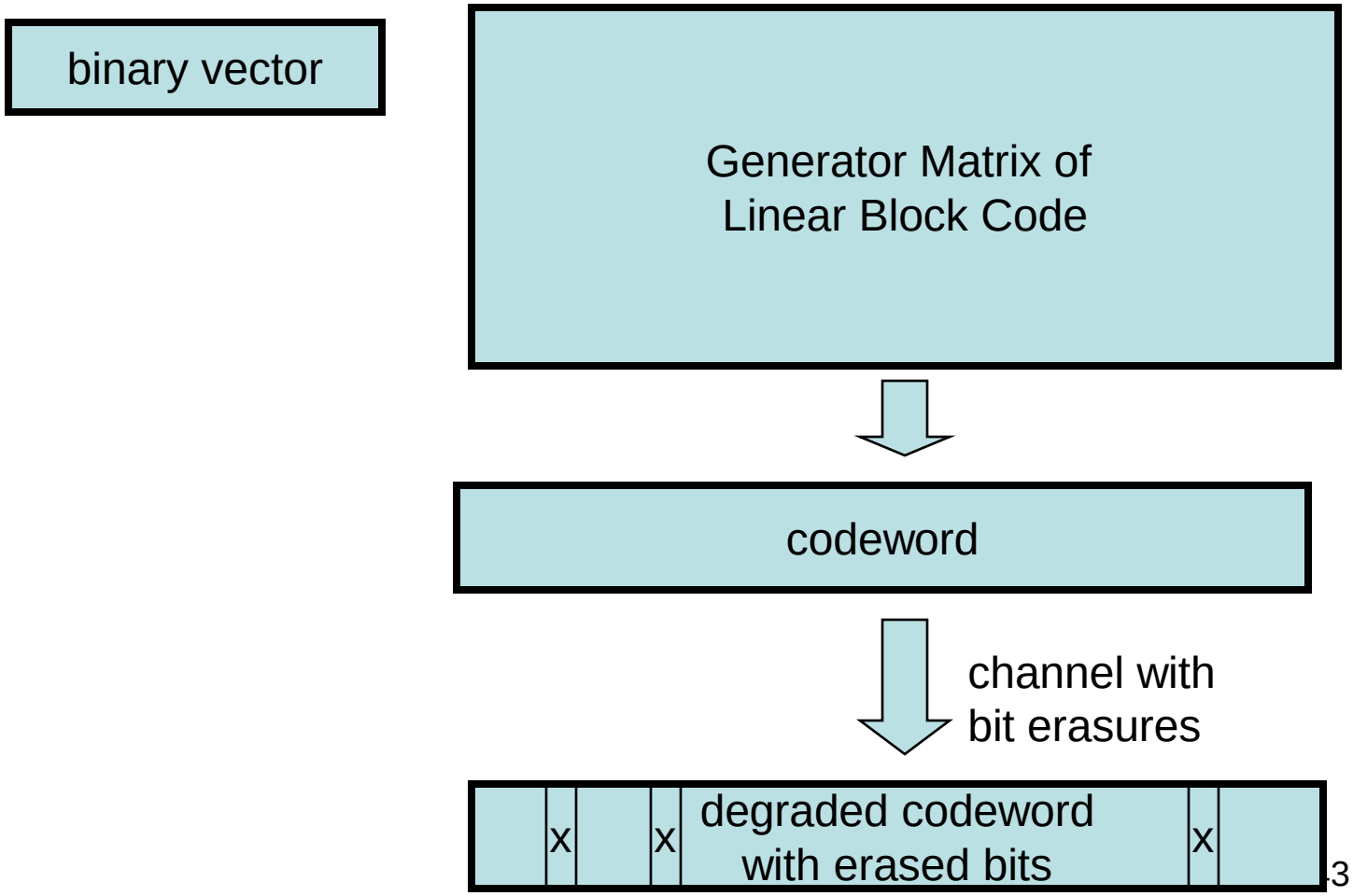
A Framework for Encryption Based on Simulated Channels with Synchronization Errors



A Framework for Encryption with Asymmetric Implementation Complexity

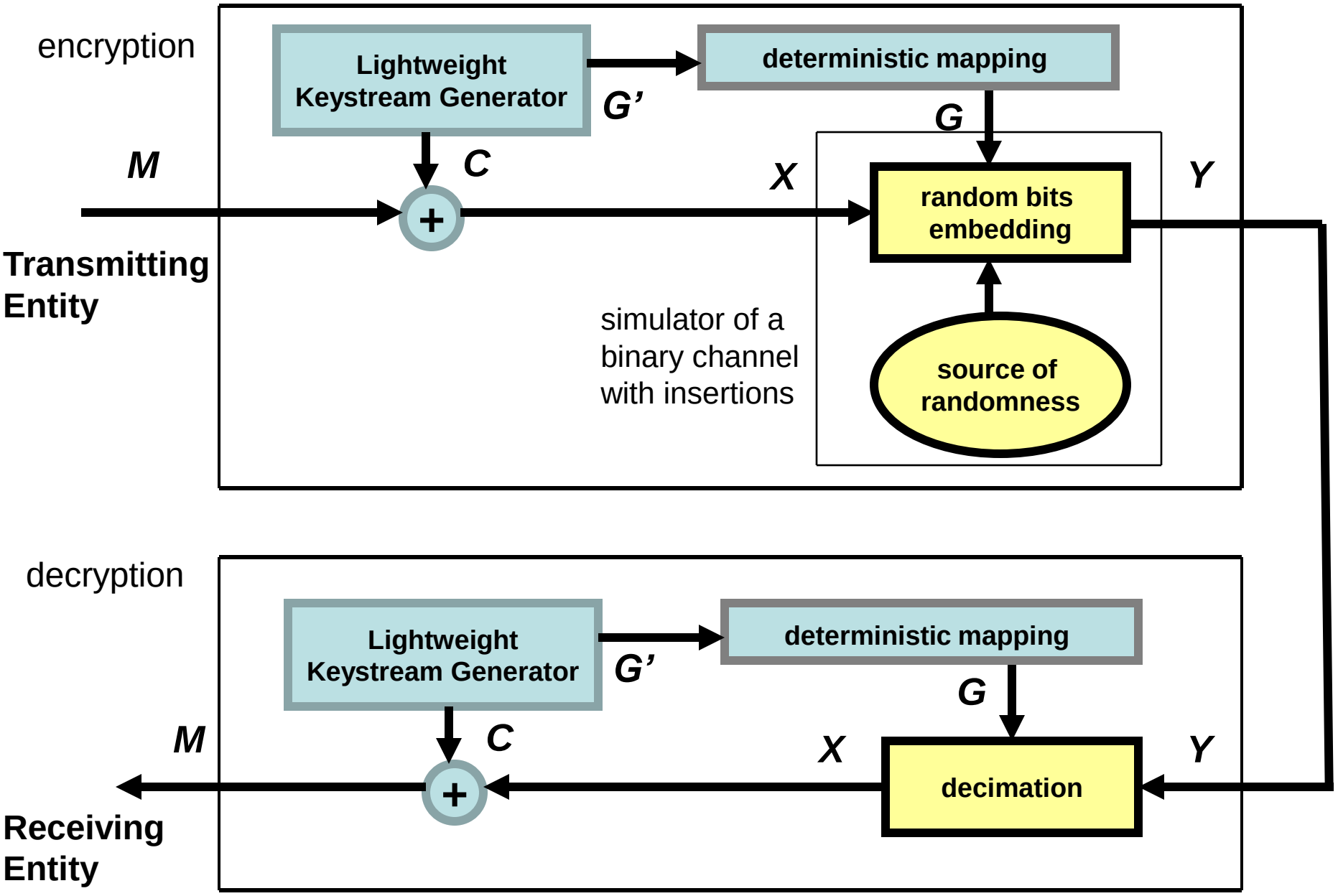


A Linear Binary Block Code Encoding Paradigm



III.3. Particular Instantiation Under Security Evaluation

A Framework for Encryption and Decryption with Asymmetric Implementation Complexity



III.4. Information-Theoretic Security Evaluation

Preliminaries

Eve (the eavesdropper) and Bob (the intended receiver) both receive the string $Y^{(n)}$ containing the randomly inserted symbols. The eavesdropper, not having access to the shared source of randomness G^n, cannot easily parse the string $Y^{(n)}$ to recover X^n. The intended receiver, on the other hand, has access to G^n, and since G_k represents the length of the inserted string between any two symbols X_k and X_{k+1}, the intended receiver (Bob) can easily remove the inserted symbols $\underline{B}_k$ from $Y^{(n)}$ (i.e., decimate $Y^{(n)}$) to recover X^n. In other words, by sharing the source of randomness G^n.

The sequence C^n is a pseudo-random sequence, but for the purpose of computing information-theoretic quantities, we assume that C^n is modeled to be statistically indistinguishable from a sequence of iid Bernoulli-$\frac{1}{2}$ random variables.

The information-theoretic quantity of interest is the *iud information rate* defined as the information rate between X^n and $Y^{(n)}$ when the symbols X_k are independent and uniformly distributed (iud)

$$\mathcal{I}_{\text{iud}}(X;Y) \triangleq \lim_{n\to\infty} \frac{1}{n} I\left(X^n; Y^{(n)}\right)\Big|_{p(x^n)=2^{-n}}.$$

The information rate $\mathcal{I}_{\text{iud}}(X;Y)$ represents the amount of information that the eavesdropper can "*learn*", on average, about X after observing Y. The information rate $\mathcal{I}_{\text{iud}}(X;Y)$ is not computable in closed-form, but is attainable using Monde-Carlo techniques.

The information rate $\mathcal{I}_{\mathsf{iud}}(X;Y)$ is not computable in closed-form, but is attainable using Monde-Carlo techniques. For example, known bounds are

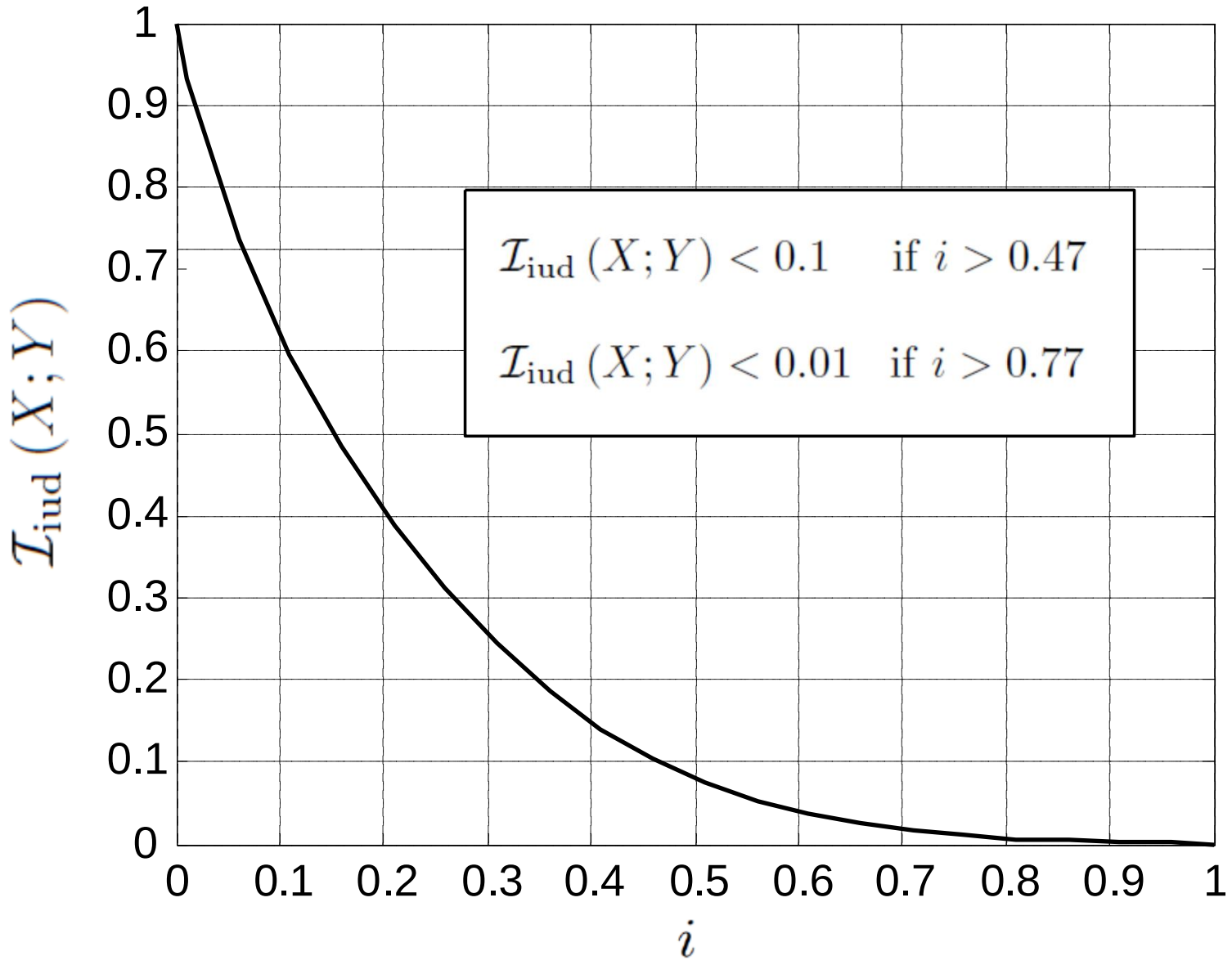
$$\mathcal{I}_{\mathsf{iud}}(X;Y) \geq \frac{1}{n} I\left(X^n; Y^{(n)}\right)\Big|_{p(x^n)=2^{-n}} - \frac{1}{n} H\left(\mathcal{L}\left(Y^{(n)}\right)\right) \quad (1)$$

$$\mathcal{I}_{\mathsf{iud}}(X;Y) \leq \frac{1}{n} I\left(X^n; Y^{(n)}\right)\Big|_{p(x^n)=2^{-n}}. \quad (2)$$

For large n, the correction term $\frac{1}{n} H\left(\mathcal{L}\left(Y^{(n)}\right)\right)$ equals

$$\frac{1}{n} H\left(\mathcal{L}\left(Y^{(n)}\right)\right) = \frac{1}{2n} \log_2\left(\frac{2\pi \mathsf{e} \cdot i \cdot n}{(1-i)^2}\right) + O\left(n^{-2}\right). \quad (3)$$

Illustrative Numerical Example



We already established that learning X after observing Y is extremely unfavorable for the eavesdropper because the information rate $\mathcal{I}_{\text{iud}}(X;Y)$ is low for large insertion probabilities i. However, the eavesdropper may adopt a strategy in which she first attempts to *learn* the sequence G^n, and then attempt to crack X^n. To study the effects of this strategy, let us define the following quantities:

$$\mathcal{I}_{\text{iud}}(G;Y) \triangleq \lim_{n\to\infty} \frac{1}{n} I\left(G^n; Y^{(n)}\right)\Big|_{p(x^n)=2^{-n}}$$

$$\mathcal{I}_{\text{iud}}(X,G;Y) \triangleq \lim_{n\to\infty} \frac{1}{n} I\left(X^n, G^n; Y^{(n)}\right)\Big|_{p(x^n)=2^{-n}}$$

$$\mathcal{I}_{\text{iud}}(X;Y|G) \triangleq \lim_{n\to\infty} \frac{1}{n} I\left(X^n; Y^{(n)}\Big| G^n\right)\Big|_{p(x^n)=2^{-n}}$$

$$\mathcal{I}_{\text{iud}}(G;Y|X) \triangleq \lim_{n\to\infty} \frac{1}{n} I\left(G^n; Y^{(n)}\Big| X^n\right)\Big|_{p(x^n)=2^{-n}}$$

Proposition 1:

$$\begin{aligned}
\mathcal{I}_{\mathsf{iud}}(G;Y) &= 0 && (1)\\
\mathcal{I}_{\mathsf{iud}}(X;Y|\,G) &= 1 && (2)\\
\mathcal{I}_{\mathsf{iud}}(X,G;Y) &= 1 && (3)\\
\mathcal{I}_{\mathsf{iud}}(G;Y|\,X) &= 1-\mathcal{I}_{\mathsf{iud}}(X;Y)\,. && (4)
\end{aligned}$$

III.5. Computational Complexity Security Evaluation

Definition 1: The Adversarial Indistinguishability Experiment consists of the following steps:

1. The adversary $\mathcal{A}$ chooses a pair of messages $(\mathbf{m}_0; \mathbf{m}_1)$ of the same length n, and passes them on to the encryption system for encrypting.

2. A bit $b \in \{0,1\}$ is chosen uniformly at random, and only one of the two messages $(\mathbf{m}_0; \mathbf{m}_1)$, precisely $\mathbf{m}_b$, is encrypted into ciphertext $\text{Enc}(\mathbf{m}_b)$ and returned to $\mathcal{A}$;

3. Upon observing $\text{Enc}(\mathbf{m}_b)$, and without knowledge of b, the adversary $\mathcal{A}$ outputs a bit b_0;

4. The experiment output is defined to be 1 if $b_0 = b$, and 0 otherwise; if the experiment output is 1, denoted shortly as the event $(\mathcal{A} \to 1)$, we say that $\mathcal{A}$ has succeeded.

Definition 2. An encryption scheme provides indistinguishable encryptions in the presence of an eavesdropper, if for all probabilistic polynomial-time adversaries $\mathcal{A}$

$$\Pr[\mathcal{A} \to 1 | \mathrm{Enc}(\mathbf{m}_b)] \leq \frac{1}{2} + \epsilon \ ,$$

where $\epsilon = \mathrm{negl}(n)$ is a negligibly small function.

Proposition 2: Let the encrypted mapping of M^n into X^n be such that $\frac{1}{2}+\epsilon$ equals the advantage of the adversary $\mathcal{A}$ (specified by Definition 2) to win the indistinguishability game (specified by Definition 1), and let the mutual information $\mathcal{I}_{iud}(X;Y)$ be known. Under these assumptions, for large n,

$$\Pr[\mathcal{A} \to 1 | Y^{(n)} = \mathbf{y}] = \frac{1}{2} + \epsilon \cdot \delta, \quad \text{where} \quad (1)$$

$$\delta \triangleq \Pr(X^n = \mathbf{x}_b | Y^{(n)} = \mathbf{y}) < \frac{1}{n} + \frac{1}{n} I\left(X^n, Y^{(n)}\right)\Big|_{p(x^n)=2^{-n}}. \quad (2)$$

Theorem 1: Let the encrypted mapping of M^n into X^n be such that $\frac{1}{2}+\epsilon$ equals the advantage of the adversary $\mathcal{A}$ (specified by Definition 2) to win the indistinguishability game (specified by Definition 1), and let the mutual information $\mathcal{I}_{iud}(X;Y)$ be known. Under these assumptions, for large n,

$$\Pr[\mathcal{A} \to 1 | Y^{(n)} = \mathbf{y}] = \frac{1}{2} + \epsilon \cdot \delta, \quad \text{where} \quad (1)$$

$$\delta < \mathcal{I}_{iud}(X;Y) + \frac{\log_2 \left[\frac{8\pi \mathrm{e} \cdot i \cdot n}{(1-i)^2} \right]}{2n} + O\left(n^{-2}\right). \quad (2)$$

Y. Liron and M. Langberg, “A Characterization of the Number of Subsequences Obtained via the Deletion Channel”, *IEEE Transactions on Information Theory*, vol. 61, no. 5, pp. 2300-2312, May 2015.

Let $D_t(\mathbf{Z})$ be a set of subsequences of $\mathbf{Z}$ that can be obtained from $\mathbf{Z}$ after t deletions. A family of strings, named unbalanced strings has been defined. A string is called unbalanced, if all of the runs of symbols in the string are of length 1, except for one run. Let $U_{\ell,r}^{(i)}$ be a binary string of length ℓ with r runs, in which all runs are of length 1, except for the i-th run which is of length $\ell - r + 1$. Due to symmetry $|D_t(U_{\ell,r}^{(1)})| = |D_t(U_{\ell,r}^{(r)})|$, and consequently define

$$u(\ell, r, t) = |D_t(U_{\ell,r}^{(1)})| = |D_t(U_{\ell,r}^{(r)})| \,. \qquad (1)$$

It has been shown that these extreme cases have the least number of subsequences among the unbalanced strings, as well as that they have the least amount of subsequences among all strings.

Y. Liron and M. Langberg, "A Characterization of the Number of Subsequences Obtained via the Deletion Channel", *IEEE Transactions on Information Theory*, vol. 61, no. 5, pp. 2300-2312, May 2015.

Theorem (Closed-Form Formula for $u(\ell, r, t)$): For all $t < \ell$, $2 < r \leq \ell$,

(i) when $r > t$:

$$u(\ell, r, t) = d(r, t) + \sum_{i=t+r-\ell-1}^{t-2} d(r-2, i) \ , \quad (1)$$

(ii) when $r \leq t$:

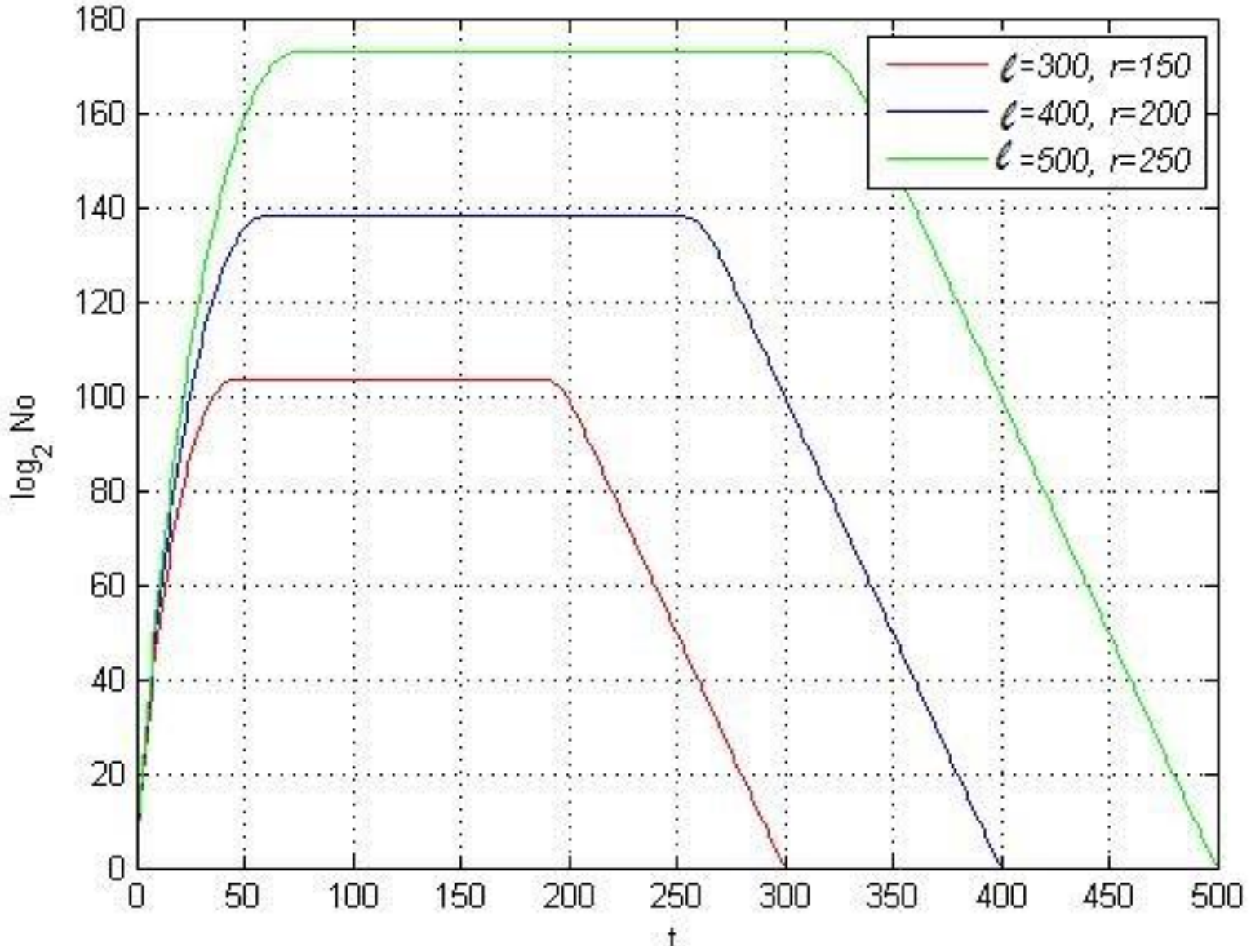
$$u(\ell, r, t) = 2 + \sum_{i=t+r-\ell-1}^{r-3} d(r-2, i) \ , \quad (2)$$

where

$$d(r, i) = |D_i(\mathbf{Z}_r^C)| = \sum_{j=0}^{i} \binom{r-i}{j} \quad (3)$$

assuming that $d(r, 0) = 1$, and for $i < 0$, $d(r, i) = 0$, and that the following conventions are employed:

$$\sum_{i=j}^{k} a_i = 0 \ \text{ when } \ j > k \ , \quad (4)$$


ℓ=300, r=150
ℓ=400, r=200
ℓ =500, r=250
log2 No
t
0
20
40
60
80
100
120
140
160
180
0
50
100
150
200
250
300
350
400
450
500

Theorem 3. Assuming that the employed keystream generator is such that the following is valid:

$$I(\mathbf{M};\mathbf{C}) = 0\ ,\ I(\mathbf{M};\mathbf{G}) = 0\ ,\ I(\mathbf{C};\mathbf{G}) = 0\ , \tag{1}$$

and

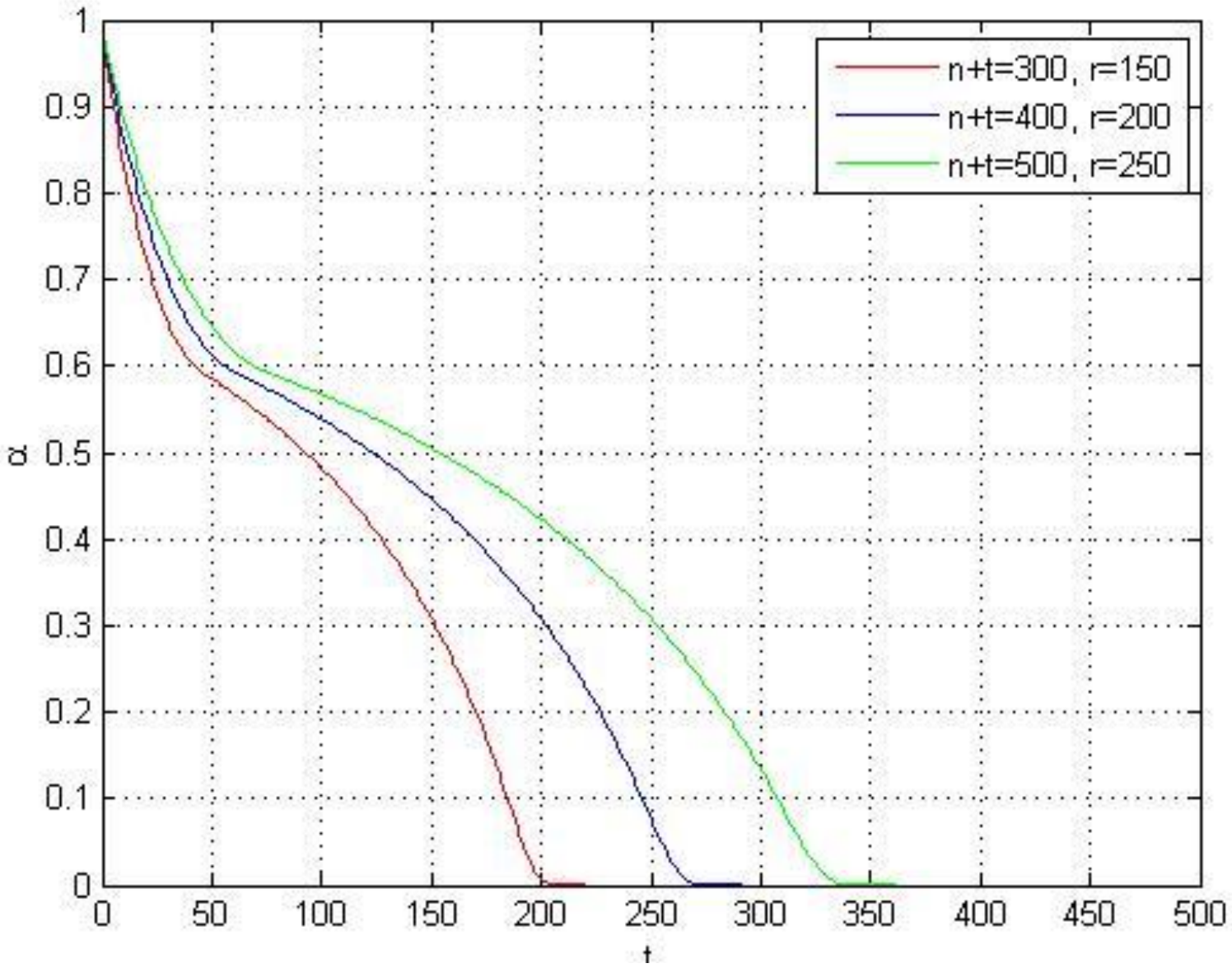
$$I(\mathbf{M};\mathbf{X}) \leq \epsilon\ . \tag{2}$$

the simulator of binary channel with random insertions provides

$$\frac{1}{n} I(\mathbf{M};\mathbf{Y}) \leq \frac{\alpha \cdot \epsilon}{n}\ , \tag{3}$$

$$\alpha = 1 - \frac{1}{n}\log_2(u(n+t,r,t))\ , \tag{4}$$

where $u(n+t,r,t)$ is number of certain equally likely subsequences.


n+t=300, r=150
n+t=400, r=200
n+t=500, r=250
α
t
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
0
50
100
150
200
250
300
350
400
450
500

Concluding Notes

Osnovne Poruke

- Pre 25 godina Kriptologija je postala jedna od disciplina koje se intenzivno neguju u MI-SANU čime se prate savremeni i najznačajniji tokovi u matematici.
- Danas u MI-SANU postoji medjunarodno respektivna kolekcija reultata u oblasti kriptologije i informacione bezbednosti koja MI-SANU čine regionalnim liderom u oblasti i partnerom vodecih svetskih centara.

Thank You Very Much for the Attention,

and

QUESTIONS Please!