Scientometrics (2015) 105:179–202
DOI 10.1007/s11192-015-1661-z

Scientometric dimensions of cryptographic research

Jiban K. Pal[1]

Received: 11 July 2015 / Published online: 23 August 2015

Abstract Information security has been a crucial issue in modern information management; thus cryptographic techniques have become inevitable to safeguard the digital information assets as well as to defend the invasion of privacy in modern information society, and likely to have far reaching impact on national security policies. This paper demonstrates the intellectual development of cryptographic research based on quantifiable characteristics of scholarly publications over a decade of the present century (2001 to 2010). The study critically examines the publication growth, authorship pattern, collaboration trends, and predominant areas of research in cryptology. Rank list of prolific contributors, productive institutions, and predominant countries have been carried out using fractional counting method. Strenuous efforts have been made to perform the activity index (performance indicator) of JOC, to determine the degree of collaboration in quantitative terms, to ascertain the collaboration density, as well as to test the empirical validation of Lotka's law in this scientific specialty. Major findings reveal that performance of JOC in cryptographic research corresponds precisely to the growth of world's publication activity (activity index = 1.1) over a decade of time; single-authored papers count only 25 % and average authorship accounts for 2.4 per paper; an increasing trend of multi-authored publications and a significant degree of collaboration (DC = 0.74) implies that cryptographers prefer to work in highly collaborative manner; author productivity distribution data partially fits the Lotka's law, when the value of α (productivity parameter) approximated to 2.35 (instead of 2) and the number of articles does not exceed two. While large majority of collaborations constituted across the countries (56 %), then adequate amount of inter-country bilateral and multilateral collaboration signifies higher density or greater strength in the research network; most of the potential collaborators are emanated from 10 institutions of 5 different countries; however, cryptographic research is dominated by USA and Israel. More interestingly, vast majority among top-twenty ranked productive authors are

✉ Jiban K. Pal
jiban@isical.ac.in

[1] Library, Documentation and Information Science Division, Indian Statistical Institute, 203, B. T. Road, Kolkata 700108, India

affiliated in USA and Israel; *Yehuda Lindell* is found to be the most prolific author followed by *Rosario Gennaro* (USA), *Tamir Tassa* (Israel), *Jonathan Katz* (USA), etc.; Anglo-American institutions are more open than their overseas competitors; University of California (six centers) is placed on the top of the productive institutions. The study entails distinct subject clusters (research streams); and author-assigned keyword frequencies revealed that cryptanalysis, discrete logarithm, elliptic curve, block cipher, provable security, cryptography, secure computation, oblivious transfer, public-key encryption, zero-knowledge are more prevalent and active topics of research in cryptology. The implications of empirical results to the field are discussed thoroughly, and further analyzes are proposed to visualize this assessment in a better way.

Keywords Cryptography research · Scientometrics · Activity index · Authorship pattern · Productivity distribution · Collaboration density · Productive institutions · Prevalent topics in cryptology · Scientific visualization

Introduction

Information is the basic ingredient for all kinds of activities in our civilized society. It is treated as marketable commodity. Now a day, information generation and access-to-information is being considered as an indicator to measure the social progress of a country. In fact, Internet has wrought a dramatic change in accessing and transferring information; thereby offer us a powerful means of managing information in modest way. However, phenomenal increase of digital information assets drastically changes the information behavior. But opportunities and complications are two sides of a coin. Indeed, a new information society has formed exploiting efficient technologies, and further development of these technologies have been aggravated many ills of information handling activities by means of hacking, cracking, phishing, spying, DNS poisoning, IP spoofing, virus infection, and so many (*read as cybercrime*). Thus Internet often misleads users, and creates a hurdle in transferring authentic information securely through distributed network environment. Therefore, Information security has been a crucial issue in modern information management.

"Cryptography" is the science of information security, closely related to the cryptanalysis. The word is derived from the Greek *kryptós*, means hidden. Thus cryptography refers to numerous ways to hide information in storage or transit; often associated with the process of encryption and decryption. In particular, Cryptology is the science of secret messages that underpins *cryptography*, which concerns designing cryptosystems for coding and decoding messages; and more glamorous *cryptanalysis*, which is concerned with breaking cryptosystems, or deciphering messages without prior detailed knowledge of the cryptosystem (Dooley 2013). The first known use of a modern cipher was by Julius Caesar (100 BC to 44 BC), who did not trust his messengers when communicating with his governors and officers; thereby, he created a system in which each character in his messages was replaced by a character three positions ahead of it in the Roman alphabet.

Modern cryptography is concerned with the cryptosystems, refers to the art of keeping messages secure using mathematical procedures and computer programs, includes regulation of human behavior. Thus, it enables the users to communicate securely over an insecure channel in a way that guarantees their transmissions' privacy and authenticity

(Coron 2006). Therefore, the ability to store and transfer sensitive information securely has become a critical issue in achieving required success in cryptology. In fact, it has turned into a battleground of the world's best mathematicians and computer scientists. The field has expanded to encompass many others—including information theory, communication theory, number theory, discrete mathematics, algebraic geometry, application of algorithms, provable security, advanced protocols, social engineering, etc.

Attaining information security had been one of the major policy issues for many nations since last two decades. Owing to the vision of all our technocrats' and great leaders, India has made immense progress towards information security over the last decade. The country is now focusing on DNS security and testing of hardware to minimize the tampering of devices. Recently, it has introduced National Cyber Security Policy (NCSP-2013), released on 2 July 2013. The President of India, Shri Pranab Mukherjee, in his speech at the 48th Convocation of Indian Statistical Institute, Kolkata (on 10 January 2014), had accorded the importance to information security. He stated that "ISI is involved in developing technologies and theories in the areas of cryptology and information security that are likely to have far reaching impact on national security policies".

Realizing the growing importance of information security, Government of India (Ministry of Communication and Information Technology) regularly conducts Information Security Education and Awareness (ISEA) Programme to create awareness among social commons, on how to protect our information in the cyber space. In no doubt, cryptography is becoming increasingly important as the Internet and other forms of electronic communications (via e-mail, e-voting, digital coins, e-shopping, e-commerce, credit card, etc.) have become more prevalent; thereby, application of cryptographic techniques has become inevitable to safeguard the digital information assets and to defend the invasion of privacy in every sphere of the modern society (Blanchette 2013).

Quantitative studies are more prevalent among scientific disciplines (*read as scientometrics*), often used to evaluate the trends-in-research of a discipline confined to an emerging area. Numerous studies have been carried out in multiple dimensions in order to understand the growth of research, prolific contributors, potential collaborators, active subdomains of research, and to track many other issues (Anyi et al. 2009). In reverse, mapping of literature of a particular discipline over a period of time depicts the changes in cognitive structure and scientific behaviour of that discipline. In fact, various bibliometric methods are extensively used for nurturing scientific information and research domains are increasingly evaluated based on the publication count and related indices. Essentially such counting is predominant by means of publications in a premier scholarly journal of the discipline concerned—since an esteemed journal is considered as sample representative of all scientific communications in a particular domain.

Indeed an assessment of cryptographic research becomes imperative over other disciplines, as cryptography has emerged as an indispensible tool for provable security and technological applications. However, scientometric analysis on this area of research has not been published as yet. Therefore, an attempt has been made to analyze the trends in cryptographic research through scholarly publications of the Journal of Cryptology (JOC). This paper is hence interesting in providing a systematic and comprehensive survey of cryptography using quantitative methods and techniques; which empirically access the research impact (Glänzel and Moed 2002), analyze emerging trends of the given field of research (Chen et al. 2012).

Certainly the study will provide useful information on research performance of an academia; stimulates visualization of esteemed institutions, prolific authors, and core journals by depicting citation behavior of this field of knowledge. Thus it enables researchers to identify the gaps and research frontiers to carry out in future, so as to insist aspiring researchers in their career planning. No doubt, this work will be useful for better research governance through capacity building by means of resource allocations, and collection development of this scientific specialty.

Scope and objectives

The study is confined to the scholarly literatures published in the Journal of Cryptology (ISSN: 0933-2790) over a decade of the present century i.e. from 2001 to 2010. It is a premier international scholarly journal, published by the International Association for Cryptologic Research (IACR) since June 1988. Currently it is technically co-sponsored by Springer-Verlag Publisher (New York, USA) available both in print and online.

The journal, founded under the editorship of Ernest F. Brickell (a celebrated cryptographer), emerged to extend the unique perceptions, both in theoretical results and application standards. It carries much of the path-breaking research works of eminent scientists in the field, thereby illustrates original contributions in cryptology and allied areas of modern information security to pursue vigorous research activities (Brickell 1988).

However, it provides an excellent communication channel for exchanging innovative ideas in different dimensions of cryptology and intends to serve a broad readership; which makes the journal an effective and reliable representation of modern cryptographic research. The journal, thus, has played a decisive role to the advancement and dissemination of cryptographic information worldwide; thereby well regarded by the peers.

Further the study is conducted purely based on the research articles of cryptology (includes cryptography, cryptanalysis, and allied areas of research); therefore the communications like a few preface, editorial note, erratum, book reviews, letter to editor, corrigendum, obituary, etc. (those have lesser research impact) are discarded from the purview of this study. Indeed, a scientometric analysis of scholarly articles appeared during a decade would certainly be indicative for analyzing current trends of cryptographic research.

Objectively, the study is intended to investigate the recent trends in cryptographic research for enabling better research governance and monitoring academic administration of this scientific specialty; thereby could be utilized as a tool for capacity building, resource allocations, and collection development as well. Thus academic administrators could be able to compare their peers, policymakers could identify relative strengths or weakness in strategically important research areas, and funding agencies could be able to predict their possible areas of investments.

It is also conducted with the following specific objectives.

(a) to understand the growth of cryptographic research by analyzing JOC's performance compare with the world's cryptographic publications over a passage of time.
(b) to examine the authorship pattern and degree of collaboration as well as collaboration density in the research of this scientific specialty.
(c) to prepare a rank list of prolific contributors and to test the empirical validation of Lotka's law for author productivity within the scope of this study.
(d) to determine the potential collaborators of cryptographic research and extent of collaborative research across institutions and countries.
(e) to analyze the scattering of publications into various subject-clusters and to identify high-score keywords for detecting active areas or topics of research in cryptology.

Justification of the study

On its' twenty-five years journey, JOC has undergone radical changes in quality, visibility, and readership of cryptographic research; thus it accommodated several thought-breaking research publications. It also compensates an endless diversification among the facets in cryptology that are related symbiotically, thereby theory and applications became increasingly blurred over the journal issues. Reportedly scientometric studies are more frequent in emerging areas of science, but no such study has been traced on Cryptology. In fact, JOC being top grade channel of research with international recognition makes extra significance to conduct such a study for representing current trends in cryptographic research—hence the quest is pursued.

However, over the passage of time, JOC has created significant queries among the cryptographers as well as scientometricians—how far the Journal is being pursued the trends of current cryptographic research in terms of coverage, internationality, authorship, collaboration, interdisciplinary approach, proactive areas, etc. as envisaged by the IACR? Indeed appropriate to look back a decade of twenty-first century for accessing the trends in cryptographic research and set the course of future direction in this scientific specialty.

Data source and methodology

In order to achieve the aforesaid objectives, primary data of the study has been collected from MathSciNet (1940–2014). It enables web access to Mathematical Reviews (MR) database via multiple mirror sites and offers excellent content with powerful search functionality and timely updates. It's dynamic search interface provides diverse searchable fields including author affiliations, institution-code, country code, classification code, and source journal name that could be useful to identify the articles of a particular journal across different time-frame. In fact, Boolean operators can effectively create different combinations among the fields. Therefore, bibliographic data of the articles having source-journal as *Journal of Cryptology* in the byline and published during 2001 to 2010 were retrieved from the MathSciNet database. Search string used for "(Journal = (Journal of Cryptology) NOT MR Number = (MR2371222) AND Publication Type = (Journals)) AND pubyear in [2001 2010]". Complete searching displayed 167 hit records (excluding an erratum in vol. 20, no. 3, 2007), thus found a reasonable sample size for the purpose of the study.

Prior to tabulation, retrieved data set is verified with the physical volumes of the journal available in ISI library collection. Thereafter, necessary bibliographic elements of each article like title, author(s) name with affiliation, publication year, volume, issue, pages, mathematics subject classification (primary), reviewer name, etc. were tabulated in the corresponding data sheets using MS-Excell. However, the data relating to number of references, author-assigned keywords of each publication were collected directly from the electronic version of the articles. Ultimately, various scientometric techniques are applied to determine the authorship patterns of publications and the extent of collaborations across the institutions of various geographical boundaries, and to trace many other issues; subsequently analyzed for making observations and interpretations.

Chronological distribution of cryptographic contributions (JOC vs. World-total) has been performed, and activity index (AI) has been calculated to analyze how JOC's performance changed with the world's cryptographic research over a passage of time; using the indicator as studied by Bujdosó and Braun (1983). Collaboration trend of research has been assessed by means of proportion of non-collaborative versus collaborative (having two or more authors) papers; extent of collaborative research is determined on the basis of lateral relations within the collaborative publications both institution-wise and country-wise; thereby unilateral, bi-lateral and multilateral collaborations were traced out. In addition, strength in collaboration by means of degree of collaboration (DC) has been estimated using Subramanyam's formula (Subramanyam 1983). Strenuous efforts have been made for empirical validation of Lotka's law (Lotka 1926). Worthy to mention, instead of commonly used inverse square law, a generalized form of the law (referred to inverse power law) as presented by Bookstein (1976) is applied and tested. A rank list of prolific contributors has been prepared on the basis of weighted values of the publications using adjusted or fractional counting method (Van-Hooydonk 1997).

Geographical diversity in authorship is considered as an indicator to measure the internationality of cryptographic publications; thereby a rank list of institutions as well as countries has been prepared based on the weighted value of contributions. Weighted value (actual share) has been calculated using fractional counting method, i.e. considering proportionate representation of authorship in contributions produced by a particular institution or country. It has resulted more distinct list for determining the ranks.

Scattering of publications across sub-domains are examined on the basis of AMS classification code in two, three, even five-digit-level; thus active areas of research in Cryptology were detected.

Therefore, a thorough analysis of collected data has been worked out in different dimensions using quantitative techniques. However, necessary data sheets are presented in tables and graphs for better interpretation.

Quantitative analysis and empirical findings

A detailed analysis of collected data; duly illustrated by tables and graphs, revealed lots of information to answer various interesting questions and interpreted towards decision-making, which are presented in the following sections.

Chronological distribution of contributions

Table 1 presents year wise distribution of 167 articles published in the journal over 10 volumes consisting 40 issues, during the study period. It appears that the number of contributions increased consistently over the years (except in 2003 and 2004), and an average of 4 articles is contributed to each issue of this journal. Significantly the activity of this journal founds very much precious to the cryptographic publications produced worldwide over the same period, as shown in the table and Fig. 1.

World contributions to cryptology research (given under World-total) has been obtained from MathSciNet database using search expression *"(MSC Primary = (94A60 or 94A62 or 11T71 or 14G50 or 68P25 or 81P94) AND Publication Type = (Journals)) AND pubyear = 2001"*. In the above expression *MSC Primary* denotes the subject-codes primarily assigned for cryptography and related sub-domains in the mathematics subject

Table 1 Year-wise distribution of contributions (JOC vs. World-total)

Year	Vol. (issue)	JOC articles	Cu.%	(Jy/Jt)	World total	Cu.%	(Wy/Wt)	AI
2001	14 (1–4)	15	8.98	0.09	163	4.11	0.04	2.19
2002	15 (1–4)	16	18.56	0.10	228	9.86	0.06	1.67
2003	16 (1–4)	12	25.75	0.07	297	17.34	0.07	0.96
2004	17 (1–4)	13	33.53	0.08	312	25.20	0.08	0.99
2005	18 (1–4)	17	43.71	0.10	495	37.68	0.12	0.82
2006	19 (1–4)	17	53.89	0.10	508	50.48	0.13	0.80
2007	20 (1–4)	17	64.07	0.10	448	61.77	0.11	0.90
2008	21 (1–4)	20	76.05	0.12	578	76.34	0.15	0.82
2009	22 (1–4)	20	88.02	0.12	439	87.40	0.11	1.08
2010	23 (1–4)	20	100.00	0.12	500	100.00	0.13	0.95
Total		167			3968			1.11

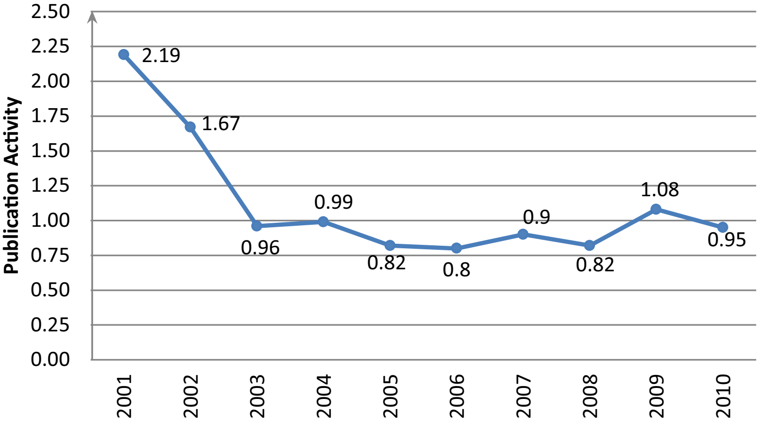


Fig. 1 Activity index of JOC during 2001–2010

classification of AMS; whereas publication type indicates the cryptology literatures published in journals during specified year, within the scope of the source database.

The AI characterizes the relative research efforts of a journal in the given subject or scientific specialty (Bujdosó and Braun 1983). Here, AI has been calculated for different years to analyze how JOC's performance changed with the world's research performance over a passage of time, using the formula; Activity Index = [{(JOC's output in a particular year)/(JOC's total output during study period)}/{(World's cryptology publication output in a particular year)/(World's total cryptology publication output during study period)}].

$$\text{Symbolically it can expressed as, AI} = [(\text{Jy}/\text{Jt})/(\text{Wy}/\text{Wt})]$$

Activity index (AI) equals to 1 indicates that JOC's research effort in the given field corresponds precisely to the world's average; while AI greater than 1 reflects higher activity. Here, average AI is derived 1.1, invariably means the research activity of the JOC is almost similar to this scientific specialty and could be considered as a sample

Table 2 Authorship distribution of JOC publications

Year	Number of Articles	Authorship value					Occurrence of authors	Average authorship
		Solo	Two	Three	Four	Five or more		
2001	15	4	6	5	0	0	31	2.07
2002	16	4	9	3	0	0	31	1.94
2003	12	5	5	1	1	0	22	1.83
2004	13	7	1	3	1	1^5	27	2.08
2005	17	5	6	4	1	1^6	39	2.29
2006	17	2	5	6	2	1^5, 1^7	50	2.94
2007	17	4	5	4	4	0	42	2.47
2008	20	6	8	2	2	1^7, 1^{10}	53	2.65
2009	20	2	6	9	2	1^6	55	2.75
2010	20	4	4	7	5	0	53	2.65
Total	167	43	55	44	18	7 ($2^5 + 2^6 + 2^7 + 1^{10}$)	403	**2.4**

representative of this domain of research. Therefore, a consistent growth with steady increasing pace has been maintained in JOC when compared to the world average. However, as reflected the values, JOC's efforts in cryptology research were much higher than the world average in the first two years and it was at peak in 2001 (AI = 2.19), which implies the authoritativeness of this journal in this scientific specialty.

Authorship pattern

Table 2 presents the authorship pattern observed in the contributions of JOC during 2001–2010. The study shows a total of 403 occurrences of authors counted in 167 articles produced during the period, thus average authorship obtained 2.4 for each publication. It is also observed that a quarter of the publications (25.75 %) produced under single-authorship; rests in collaboration—either by two-authors or three, four, five, six, seven, even by ten-authors. Thus contributors of this scientific specialty are mostly preferred to work in collaborative manner. Collaboration among two-authors (33 %) is predominant, followed by three authors (26 %), and four authors (11 %), etc.

The study depicts an increasing trend of multi-authored publications (46 % in 2004 and 90 % in 2009) has been observed in agreement with many other disciplines (Bandyopadhyay 2001). Such a trend of collaboration among the researchers is perhaps due to increased complexity in research activities, technological expositions combined with more specializations, cost of modern investigations, impact on citations, and often interdisciplinary research areas have been forcing the researchers to share their expertise in producing their output.

Research collaboration

Research collaboration has become prevalent in many scientific specialties and highly practiced in twenty-first century. Huang et al. (2014) noted that multi-authored publications have been increased steadily in post-web era. Collaboration is an intense form of interaction that allows for effective communication as well as sharing of competence and other resources. However, multiple-authorship in different dimensions (say for inter-

Table 3 Collaboration trend and degree of collaboration

Year	Non-collaborative (N_s)	%	Collaborative (N_m)			%	DC
			Domestic	International	Total		
2001	4	26.67	4	7	11	73.33	0.733
2002	4	25.00	4	8	12	75.00	0.750
2003	5	41.67	5	2	7	58.33	0.583
2004	7	53.85	1	5	6	46.15	0.462
2005	5	29.41	5	7	12	70.59	0.706
2006	2	11.76	9	6	15	88.24	0.882
2007	4	23.53	7	6	13	76.47	0.765
2008	6	30.00	6	8	14	70.00	0.700
2009	2	10.00	6	12	18	90.00	0.900
2010	4	20.00	7	9	16	80.00	0.800
Total	43	25.75	54	70	124	74.25	**0.742**

department, inter-institute, inter-country, etc.) provides a measure of intensity in collaborations. Indeed lateral relationship among the collaborated authors might be considered as viable indicator to determine the intensity in research collaboration.

Table 3 depicts the collaboration scenario among the authors in different two levels—namely *Domestic* (co-authors are from the same country), and *International* (collaboration occurs within two or more authors of different countries). Out of 124 collaborative contributions domestic collaboration constituted only 44 %, while 56 % contributions are collaborated among cryptologists across the countries. Thus it brings out the prevalence of team research and the scientists working in this field prefer to conduct research in collaboration.

In order to measure the degree of collaboration (DC) in quantitative terms, the formula given by Subramanyam (1983) can be useful. He worked out the DC, which is determined by the ratio of number of collaborative publications and total number of publications during certain period of time. That can be expressed as,

$$\mathrm{DC} = \frac{N_m}{N_m + N_s} = \frac{124}{124 + 43} = 0.742$$

where N_m refers to multi-authored (two or more) contributions and N_s denote the number of single-authored contributions published in the journal during study period. Thus, average degree of collaboration is found to be 0.74 and quite significant. The extent of collaboration distribution over the period is presented in Fig. 2. Clearly it indicates the prevalence of collaborative research (74.25 %) over the solo research (25.75 %) in the specialty studied here, as envisaged in the contributions of JOC.

Collaboration density (bilateral and multilateral)

Table 4 reveals further distribution of collaborative contributions in order to map the lateral relations among co-authors. The lateral relationship among co-authors can be studied under three different levels of aggregation; namely *unilateral*, *bilateral*, and *multilateral*. Unilateral collaboration is described when co-authorship of a publication occurs within a link, whereas bilateral collaboration implies the co-authorship occurs

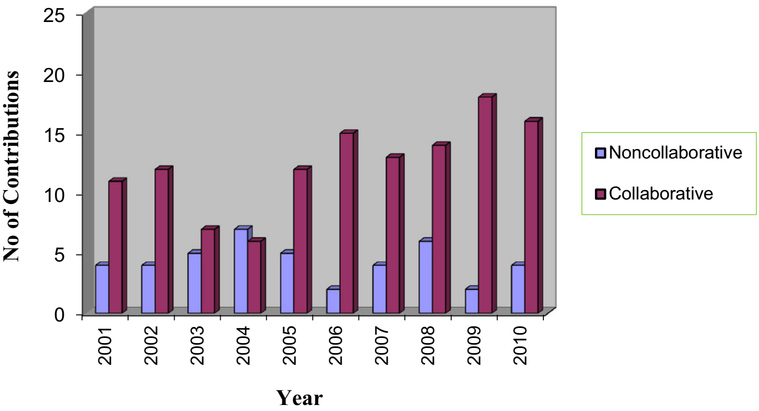


Fig. 2 Collaboration trend over the years (single vs. multi-authors)

Table 4 Lateral relations among co-authors

Year	Collaborative contributions	Domestic collaboration				International collaboration			
		Uni-	Bi-	Multi-	Total	Uni-	Bi-	Multi-	Total
2001	11	1	2	1	4	0	6	1	7
2002	12	3	1	0	4	0	6	2	8
2003	7	3	2	0	5	0	2	0	2
2004	6	1	0	0	1	0	3	2	5
2005	12	2	3	0	5	0	4	3	7
2006	15	3	2	4	9	0	5	1	6
2007	13	2	4	1	7	0	5	1	6
2008	14	2	4	0	6	0	6	2	8
2009	18	3	3	0	6	0	12	0	12
2010	16	3	3	1	7	0	3	6	9
Total	124	23	24	7	54	00	52	18	70

between two (only two) different links. Multilateral collaboration indicates the participation of co-authors from two or more different links for producing an article.

However, collaborative contributions are viewed laterally in two different angles to determine the intensity in collaboration, viz. *Domestic* (within the country, institute-wise linkage) and *International* (cross-country collaboration). So, domestic collaboration of a publication happens to be made by the co-authors from the same country; either from the same institute (unilateral) or two different institutes (bilateral), otherwise may be from more than two different institutes. Similarly, International (inter-country) multilateral collaboration of a publication implies that author's affiliated institutes are located in three or more different countries.

While multilateral collaboration have more intent over the bilateral collaboration, then cross-country collaboration identifies greater intensity in compare to domestic collaborations—thus defines *collaboration density*. Such indicator helps to determine the strength of

Table 5 Top-twenty productive authors (based on weighted value of contributions)

Rank	*Author name* (affiliation code)	Share value of contributions by authorship								Total Cont.	Weighted value
		Full	1/2	1/3	1/4	1/5	1/6	1/7	1/10		
1	*Lindell*, *Yehuda* (IL-BILN-C)	4	7	2	–	–	–	–	–	13	8.17
2	*Gennaro*, *Rosario* (1-IBM)	1	2	2	2	–	–	–	–	7	3.17
3	*Tassa*, *Tamir* (IL-The Open University, Ra'anana, Israel)	2	2	–	–	–	–	–	–	4	3.00
4	*Katz*, *Jonathan* (1-MD-C)	–	3	3	1	–	1	–	–	8	2.92
5	*Knudsen*, *Lars R.* (DK-TUD-M)	1	3	–	1	–	–	–	–	5	2.75
6	*Vaudenay*, *Serge* (CH-LSNP)	2	1	–	–	–	–	–	–	3	2.50
7	*Shoup*, *Victor* (CH-IBM)	1	1	2	1	–	–	–	–	5	2.42
8	*Bellare*, *Mihir* (1-UCSD-CS)	1	1	1	1	–	–	–	1	5	2.18
9	*Goldreich*, *Oded* (IL-WEIZ-CS)	1	2	–	–	–	–	–	–	3	2.00
10	*Pinkas*, *Benny* (1-HP Labs, Princeton, USA)	–	3	1	–	–	–	–	–	4	1.83
11	*Rogaway*, *Phillip* (1-CAD-C)	–	3	–	1	–	–	–	–	4	1.75
12	*Beimel*, *Amos* (IL-BGUN-C)	–	2	1	1	–	–	–	–	4	1.58
13	*Ishai*, *Yuval* (IL-TECH-C)	–	–	4	–	1	–	–	–	5	1.53
14	*Håstad*, *Johan* (S-RIT-C)	1	1	–	–	–	–	–	–	2	1.50
	Joux, *Antoine* (F-DCSSI Crypto Lab, France)	1	1	–	–	–	–	–	–	2	1.50
	Vadhan, *Salil* P. (1-HRV)	1	1	–	–	–	–	–	–	2	1.50
	Verheul, *Eric R.* (NL-PricewaterhouseCoopers, GRMS Crypto Group, The Netherlands)	1	1	–	–	–	–	–	–	2	1.50
15	*Biham*, *Eli* (IL-TECH-C)	–	1	2	–	1	–	–	–	4	1.37
16	*Lu*, *Chi-Jen* (RC-AST-I)	1	–	1	–	–	–	–	–	2	1.33
	Teske, *Edlyn* (3-WTRL-B)	1	–	1	–	–	–	–	–	2	1.33
17	*Naor*, *Moni* (IL-WEIZ-AC)	–	2	–	1	–	–	–	–	3	1.25
18	*Boneh*, *Dan* (1-STF-C)	–	1	2	–	–	–	–	–	3	1.17
	Shamir, *Adi* (IL-WEIZ-CS)	–	1	2	–	–	–	–	–	3	1.17
19	*Coppersmith*, *Don* (1-IBM)	1	–	–	–	–	–	1	–	2	1.14
	Jutla, *Charanjit* (1-IBM)	1	–	–	–	–	–	1	–	2	1.14
20	*Black*, *John* (1-CO–C)	–	1	1	1	–	–	–	–	3	1.08
	Namprempre, *Chanathip* (1-UCSD-CS)	–	1	1	1	–	–	–	–	3	1.08
	Ostrovsky, *Rafail* (1-UCLA-C)	–	1	1	1	–	–	–	–	3	1.08
21-	Rest 245 unique authors having 295 occurrences in different combinations-of-authorship, thus each of them carrying out the weighted value 1 or less.	22	68	105	60	8	11	12	9	295	112.06
Total	273 unique authors	43	110	132	72	10	12	14	10	403	167

a research network, where international multilateral has greater strength than domestic multilateral collaboration. A considerable number of bilateral and multilateral collaboration signifies that intellectual perceptions of authors from diverse origin have been used to produce the research outputs in this scientific specialty.

Ranking of prolific authors

Table 5 depicts the ranking of prolific authors based on the weighted value of their contributions (by authorship) in JOC during the study period. Weighted value of contributed articles has been calculated using fractional counting method; where total weight of an article always considered 1, which is distributed equally among the authors responsible for the article. Such a ranking method entails more accurate values in making the differences with finer tunes; thus removes anonymous ranking of authors, as yielded from direct counting method (Egghe et al. 2000). For instance, authors produced 5 articles each would come to the same rank in direct counting method; but they can be ranked more appropriately having different weighted values of their shared contributions, if fractional counting method is applied.

Out of 273 unique authors having 403 occurrences of authorship in 167 contributions; 28 prolific contributors ranked within top-twenty, as presented in Table 5. It is observed that top-ten authors received a total weighted score of 31 (out of 167) by contributing in 57 articles. Other listed authors carrying out the score within 1.08 to 1.75. Yehuda Lindell (Department of Computer Science, Bar-Ilan University, Israel) is found to be the most prolific author; followed by Rosario Gennaro (IBM, Thomas J. Watson Research Center, USA), Tamir Tassa (Open University, Israel), Jonathan Katz (Department of Computer Science, University of Maryland, USA), Lars R. Knudsen (Department of Mathematics, Technical University of Denmark), Serge Vaudenay (Swiss Federal Institute of Technology, Switzerland), etc. Rest 245 unique authors, who received the weighted score ≥ 1 is not revealed in the ranked list.

More interestingly, vast majority of the top-twenty ranked researchers come largely from Anglo-American countries. In fact 12 productive authors affiliated in USA, 8 in Israel, 2 in Switzerland, 1 in Denmark, 1 in Canada, 1 in France, 1 in Netherlands, etc.

Empirical validation of Lotka's law

Lotka's empirical law of scientific productivity states that y number of authors each credited with x number of papers is inversely proportional to x, which is the output of individual author. Thus relation is expressed as (Lotka 1926),

$$x^n \alpha \frac{1}{y} \quad \text{or} \quad x^n y = C[n \text{ and } C \text{ are two constants}] \tag{1}$$

There has been a considerable literature on the empirical validation of Lotka's law. Several studies have reported that Lotka's law is applicable for the productivity trend distributions of well-recognized disciplines. Usually such disciplines follow the distribution patterns that conform Lotka's law in its original form with exponent value of 2. While some other investigations found that the value of exponent n is not always 2, rather a variable value around 2.

Murphy (1973) in a study applied the Lotka's law appropriately in the field of humanities, without any statistical test to check the degree of significance. Pao (1985) presented the application process of Lotkás law (step by step) deducing the values of constant and exponent based on the method as same as Lotka, and tested the degree of significance. Later she applied this procedure over 48 groups of authors (representing 20 scientific disciplines) and found that in most of the cases the original law of Lotka holds good (Pao 1986). Nicholls (1986) has conducted studies on 15 different datasets of humanities, social sciences, and sciences for testing the empirical validation of the Law. He observed that the studies on their majority are conflicting, incomparable, and inconclusive; thus do not provide any clear-cut validation of the Lotka's law. Such inconsistencies in validation of the Law are perhaps due to a steady increase of co-authored publications over the time. Potter (1981) noted that Lotka credited only the senior author for each contribution ignoring all co-authors, as multi-authorship contribution was less common in Lotka's time. However, a number of studies showed that using total or even fractional counting of authorship lead to a breakdown of Lotka's law (Rousseau 1992).

Therefore, instead of commonly used inverse square law, Lotka's formulation can be observed as inverse power law in general, i.e. $x^n \cdot y = C$. The exponent (n) and the constant (C) can be estimated from the given set of author productivity data. A generalized form of Lotka's law (referred to inverse power law) as devised by Bookstein (1976) could be useful.

$$a_n = \frac{C}{n^\alpha} \quad \text{for} \quad n = 1, 2, 3\ldots \quad \text{and} \quad C > 0 \tag{2}$$

where a_n represents the probability of authors producing n contributions each and C and α are two parameters to be estimated for a specific set of data. The value of productivity constant (α) or characteristic exponent can be determined by considering the values of n (1, 2, 3…) applying either graphical or mathematical method.

Now, an attempt has been made to predict simply on the applicability of Lotka's law for author productivity in the dataset studied here; and to what extent author's productivity conforms to Lotka's law has also been carried out. Table 6 shows the author productivity considering all the authors; where 204 authors have one paper each, 40 authors produced only two papers each, 17 authors contributed three papers each, 5 authors have four papers each to their credit, and so on. Maximum number of papers that have been credited to an individual author is found as 13. Now considering the observed data (204 authors have produced 1 paper each), anyone can easily derive the value of C from the Eq. (2).

Table 6 Author productivity in JOC during 2001–2010 (*all authors considered*)

No of articles (A)	No. of authors Observed (B)	Percentage (%)	Authorship ($A \times B$)	Percentage (%)	No. of authors expected when $\alpha = 2$	No. of authors expected when $\alpha = 2.35$
1	204	74.725	204	50.620	204	204
2	40	14.652	80	19.851	51	40.0
3	17	6.227	51	12.655	23	15.5
4	5	1.831	20	4.962	13	7.8
5	4	1.465	20	4.962	8	4.6
7	1	0.366	7	1.736	4	2.1
8	1	0.366	8	1.985	3	1.5
13	1	0.366	13	3.225	1	0.5
Total	273	100	403	100	307	276

$$a_n = \frac{C}{n^\alpha} \quad \text{or,} \quad 204 = \frac{C}{1^\alpha} \quad \text{or,} \quad C = 204$$

Subsequently, taking the expected value of α as 2 and putting the derived value of C as well as values of n (1, 2, 3, 4,…) in the above equation, corresponding values of expected authors (a_n) are obtained. Result shows (Table 6) a considerable variation in the expected values when compare to observed values. So, the Law does not fit in this case and a violation is clearly observed.

It is also evident from the table, when the value of α (productivity parameter) approximated to 2.35 (instead of 2) then the expected values of a_n are quite close to the observed values, still a meaningful distance exists therein.

$$a_n = \frac{C}{n^\alpha} \quad \text{or} \quad n^\alpha = \frac{C}{a_n} \quad \text{or} \quad \log n^\alpha = \log \frac{C}{a_n} \quad \text{or} \quad \alpha \log n = \log \frac{C}{a_n} \quad \text{or} \quad \alpha = \frac{\log \frac{C}{a_n}}{\log n}$$

$$\text{or} \quad \alpha = \frac{\log \frac{204}{40}}{\log 2} \quad \text{or} \quad [\text{for}\, C = 204,\, a_n = 40,\, n = 2] \quad \text{or} \quad \alpha = \frac{0.70757}{0.30103} = 2.350$$

Putting the values of n (1, 2, 3, 4,…) and calculated value of α as 2.35 following values of a_n are derived.

$$a_n = \frac{C}{n^\alpha} = \frac{204}{1^{2.35}} = 204; \frac{204}{2^{2.35}} = \frac{204}{5.0982} = 40.01; \frac{204}{3^{2.35}} = \frac{204}{13.22} = 15.43; \ldots$$

It is therefore observed that, productivity distribution data (as shown in Table 6) partially fits the Lotka's law in its original form with a calculated value of exponent $\alpha = 2.35$; while the number of contributions (articles) does not exceed two. The law does not hold-good beyond this value. Noteworthy is the fact, larger the value of α, greater is the gap between the productivity of individual groups of authors contributing n number of papers each. Practically a larger value of α implies the proportion of highly productive authors is decreased (Gupta 1995). Further statistical tests (viz. Chi-square of goodness-of-fit and *K–S* test) could be useful to confirm the applicability of this Law at an appropriate level of significance.

Geographical diversity of contributions

Table 7 shows the geographical distribution of contributing authors in JOC during the study period. Country names have been identified from the author-affiliations corresponding to their publications, which was primarily available within the 'institution code' data-field of MathSciNet. Tabulated data shows that a total of 403 occurrences of authors from 29 countries took part in producing 167 publications. Authors from diverse geographical locations (numerous countries) represented for contributing their research endeavors to JOC, implies that the journal considerably gained diverse experiences and opinions in publishing those articles. Such geographical diversity in authorship could be considered as an indicator to measure the internationality of a journal (Perneger and Hudelson 2007). Obviously, the source journal deserves the status of an international channel of research communications.

A rank list of participating countries has been prepared on the basis of weighted value of contributions (by authorship) from respective countries, thereby using fractional counting method. USA received the maximum weight by carrying out a score of 57.53 (out of 167), affiliating 149 occurrences of authors in different authorship positions; followed by Israel

Table 7 Rank list of countries (based on weighted value of contributions)

Country name (code)	Share value of contributions by authorship								Total Cont.	Weighted value
	Full	1/2	1/3	1/4	1/5	1/6	1/7	1/10		
USA (1-)	12	34	53	32	4	8	3	3	149	57.53
ISRAEL (IL-)	8	29	20	7	3	2	–	–	69	31.85
FRANCE (F-)	4	6	11	4	–	–	3	2	30	12.30
CANADA (3-)	5	2	12	1	1	–	–	–	21	10.45
GERMANY (D-)	2	9	1	6	–	–	–	–	18	8.33
UNITED KINGDOM (4-)	3	1	7	5	–	–	–	1	17	7.18
SWITZERLAND (CH-)	2	3	5	3	–	1	–	–	14	6.08
SWEDEN (S-)	2	2	3	–	–	–	–	–	7	4.00
DENMARK (DK-)	1	4	–	2	1	1	–	–	9	3.87
ITALY (I-)	–	5	–	3	–	–	–	1	9	3.35
THE NETHERLANDS (NL-)	1	1	3	1	–	–	–	2	8	2.95
REPUBLIC OF KOREA (KR-)	1	–	–	–	–	–	7	–	8	2.00
BELGIUM (B-)	–	2	2	–	–	–	–	1	5	1.77
JAPAN (J-)	–	–	3	3	–	–	–	–	6	1.75
AUSTRALIA (5-)	–	2	2	–	–	–	–	–	4	1.67
TAIWAN—R.O.C. (RC-)	1	–	1	–	–	–	–	–	2	1.33
NORWAY (N-)	–	2	–	1	–	–	–	–	3	1.25
SINGAPORE (SGP-)	–	1	2	–	–	–	–	–	3	1.17
LUXEMBOURG (LUX-)	–	2	–	–	–	–	1	–	3	1.14
GREECE (GR-)	–	–	–	4	–	–	–	–	4	1.00
PEO. REP. OF CHINA (PRC-)	–	–	3	–	–	–	–	–	3	1.00
RUSSIA (RS-)	–	2	–	–	–	–	–	–	2	1.00
TURKEY (TR-)	1	–	–	–	–	–	–	–	1	1.00
POLAND (PL-)	–	1	–	–	1	–	–	–	2	0.70
IRELAND (IRL-)	–	–	2	–	–	–	–	–	2	0.67
MEXICO (MEX-)	–	1	–	–	–	–	–	–	1	0.50
THAILAND (THA-)	–	1	–	–	–	–	–	–	1	0.50
BRAZIL (BR-)	–	–	1	–	–	–	–	–	1	0.33
PORTUGAL (P-)	–	–	1	–	–	–	–	–	1	0.33
Total 29 countries contributed	43	110	132	72	10	12	14	10	403	**167**

(31.85), France (12.30), Canada (10.45), and others. It also found that top ten countries are having a total 343 (out of 403) occurrences of authors in various authorship positions, thus carrying an weighted score of 145 (about 87 %). Rest of the weight is eventually distributed over 19 countries, as shown in the Table 7. This indicator helps to find out the partner countries having similar research interests and extent of their involvement in recognizing the international repute of the subject.

Institution-wise diversity of publications

Table 8 depicts the distribution of authors made their contribution to JOC from various institutions of different countries. Distributed data presents a total of 136 individual

Table 8 Rank list of productive institutes (based on weighted value of contributions)

Rank	*Institute name* (code)	Share value of contributions by authorship								Total freq.	Total weight
		Full	1/2	1/3	1/4	1/5	1/6	1/7	1/10		
1	*University of California, USA*. [Six Centers] Berkeley (1-CA-), Davis (1- CAD-), Irvine (1- CA3-), Los Angeles (1- UCLA-), San Diego (1-UCSD-), Santa Cruz (1-UCSC-).	3	9	3	6	2	1	–	1	25	10.67
2	*Weizmann Institute of Science*, Israel (IL-WEIZ-)	3	7	2	3	–	1	–	–	16	8.08
3	*Bar-Ilan University*, Israel (IL-BILN-)	3	8	2	–	–	–	–	–	13	7.67
4	*IBM Research Centers*, USA (1-IBM-)	3	2	5	4	1	–	3	–	18	7.30
5	*Technion—Israel Inst. of Tech.*, Israel (IL-TECH-)	–	1	10	1	3	–	–	–	15	4.68
6	*University of Maryland*, USA (1-MD-)	–	3	6	2	–	4	–	–	15	4.67
7	*Ecole Normale Superieure*, Paris, France (F-ENS-)	1	2	4	3	–	–	1	1	12	4.33
8	*University of Bristol*, England (4-BRST-)	1		6	4	–	–	–	–	11	4.00
9	*University of Waterloo*, Canada (3-WTRL-)	2	1	3	1	–	–	–	–	7	3.75
10	*Stanford University*, USA(1-STF-)	–	1	6	3	–	–	–	–	10	3.25
11	*Harvard University, USA* (1-HRV-)	1	2	2	2	–	–	–	–	7	3.17
12	*Ben Gurion Univ. of the Negev, Israel* (IL-BGUN-)	–	4	1	2	–	–	–	–	7	2.83
	Royal Institute of Technology (KTH), Sweden (S-RIT-)	2	1	1	–	–	–	–	–	4	2.83
13	*Technical Univ. of Denmark, Denmark* (DK-TUD-)	1	2	–	2	–	–	–	–	5	2.50
	Open Univ. of Israel, Raanana, Israel (IL-OPENR-)	2	1	–	–	–	–	–	–	3	2.50
14	*Swiss Federal Inst. of Tech., Switzerland* (CH-LSNP-)	1	1	2	1	–	–	–	–	5	2.42
15	*Massachusetts Institute of Technology*, USA(1-MIT-)	1	2	1	–	–	–	–	–	4	2.33
	Ecole Polytechnique, France (F-POLY-)	1	–	4	–	–	–	–	–	5	2.33
17	*IBM Zurich Research Lab., Switzerland* (CH-IBM-)	1	1	2	–	–	–	–	–	4	2.17
18	*University of Calgary, Canada* (3-CALG-)	1	–	3	–	–	–	–	–	4	2.00
	TU Darmstadt, Germany (D-DARM-)	1	2	–	–	–	–	–	–	3	2.00

Table 8 continued

Rank	*Institute name* (code)	Share value of contributions by authorship								Total freq.	Total weight
		Full	1/2	1/3	1/4	1/5	1/6	1/7	1/10		
19	*Boston University*, *USA*(1-BOST-)	–	–	1	4	–	3	–	–	8	1.83
	Tel Aviv University, *Israel* (IL-TLAV-)	–	3	1	–	–	–	–	–	4	1.83
	DCSSI Crypto Lab, *France* (F-DCSSI-C-)	1	1	1	–	–	–	–	–	3	1.83
20	*Columbia University*, *New York*, *USA* (1-CLMB-)	–	2	1	1	1	–	–	–	5	1.78
21	*Katholieke Universiteit Leuven*, *Belgium* (B-KUL-)	–	2	2	–	–	–	–	1	5	1.77
22	*Universita di Salerno*, *Italy* (I-SLRN-)	–	2	–	3	–	–	–	–	5	1.75
	Royal Holloway and Bedford New College, *Univ. of London, England, UK* (4-LNDHB-)	1	1	–	1	–	–	–	–	3	1.75
23	*Haifa University*, *Israel* (IL-HAIF-)	–	1	2	1	–	1	–	–	5	1.58
24	*PriceWaterhouseCoopers*, *GRMS Crypto Group*, *The Netherlands* (NL-PWC)	1	1	–	–	–	–	–	–	2	1.50
25	*University of Colorado*, *USA* (1-CO-)	–	1	2	1	–	–	–	–	4	1.42
26	*Aarhus University*, *Denmark* (DK-ARHS-)	–	2	–	–	1	1	–	–	4	1.37
27	*Center for Math. and Com. Sc.*(*CWI*), *The Netherlands* (NL-MATH-)	–	–	3	1	–	–	–	1	5	1.35
28	*Universitat Duisburg-Essen*, *Germany* (D-DUES2-)	–	1	1	2	–	–	–	–	4	1.33
	Hebrew University, *Jerusalem*, *Israel* (IL-HEBR-)	–	2	1	–	–	–	–	–	3	1.33
	Macquarie University, *Sydney*, *Australia* (5-MCQR-)	–	2	1	–	–	–	–	–	3	1.33
	Academia Sinica, Taiwan (*R.O.C.*)(RC-AST-)	1	–	1	–	–	–	–	–	2	1.33
	University of Toronto, *Canada* (3-TRNT-)	1	–	1	–	–	–	–	–	2	1.33
29	*Telcordia Technologies Inc.*, *NJ*, *USA* (1-TELC-)	–	–	3	1	–	–	–	–	4	1.25
30	*Eidgenossische TH Zurich*, *Switzlerland* (CH-ETHZ-)	–	1	–	2	–	1	–	–	4	1.17
31	*Centre Universitaire de Luxembourg*, (LUX-CUL-)	–	2	–	–	–	–	1	–	3	1.14
32-	Rest 95 Institutes contributed through 132 occurrences of authors in different authorship-positions, thus each of them carrying out the weighted score 1.00 or less.	10	36	48	21	2	–	9	6	132	51.54
Total	136 Institutions contributed	43	110	132	72	10	12	14	10	403	**167**

institutions were involved in generating 167 publications of JOC during the study period. These institutions appeared in the publications through 403 occurrences of authors in various authorship positions, as well as share values. A rank list of participating institutions has been prepared based on the weighted value of the contributions (by authorship) from respective institutions. Weighted value (actual share) has been calculated using fractional counting method, i.e. considering proportionate representation of authorship in contributions produced by a particular institution. It has resulted more distinct list for determining the ranks of the contributed institutions.

The University of California (six centers), USA is appeared on the top; which is followed by Weizmann Institute of Science, Israel (IL-WEIZ), Bar-Ilan University, Israel (IL-BILN), IBM Research Centers, USA (1-IBM-), Technion—Israel Institute of Technology, Israel (IL-TECH-), University of Maryland, USA (1-MD-), Ecole Normale Superieure, Paris, France (F-ENS-), University of Bristol, England, UK (4-BRST-), etc. Though a few institutes contributed equal number of publications (say 15 each by IL-TECH & 1-MD), but ranked differently due to unequal share value (score 4.68 and 4.67) of their contributions, as shown in Table 8. Active participation of various institutions across geographical boundaries implies the recognition and authoritativeness of this journal in this specialty of research.

Top 10 institutions are carrying about 35 % of the total score (58 out of 167), by affiliating 35 % of the total occurrences of authors (142 out of 403) with various authorship positions. However, first forty-one institutions contributed through 271 occurrences of authors, received a total score 115. Rest of the weight is eventually distributed over 95 institutes, thus each of them received the weighted score ≥ 1 is not revealed in the ranked list.

Subject clusters of cryptographic research

Objectively the study ascertains the subject clusters that are predominating in this scientific specialty. Thus it analyzes the scattering of publications into different sub-domains to detect the active areas of research in Cryptology. In view of this objective, subject areas pertaining to the articles are identified based on the primary subject code (assigned for each article using Mathematics Subject Classification of AMS) in two-digit level, available from MathSciNet. Distribution of JOC publications into broad subject clusters and their sub-clusters (two, three or five-digit-level) are presented in Table 9. Evidently the subject cluster Communication Information and Circuits (94- including cryptography) covers almost 87 % of contributed articles in JOC; essentially required to pursue the research on modern information security, as committed by the International Association for Cryptologic Research.

Further distribution of contributions has been made to identify the active sub-domains in this scientific specialty. These sub-clusters have been determined by the MSC primary codes in five-digit level, as shown in the Table 10.

Sub-domain wise distribution shows that contributors have pursued their research mostly in the areas of Cryptography (94A60) and Authenticated and secret sharing (94A62) followed by coding theory and cryptography (14G50), curves over finite and local fields (11G20), primality in number theory (11Y11), data encryption (68P25), and algebraic coding theory (11T71). Such a simple indicator could help academic administrators to identify potential and allied areas of research in order to pursue their academic endeavors.

Table 9 Domain-wise distribution of JOC publications

Domains of research	Sub-domains (*MSC Code*)	Freq.	Sub-total	%
Communication, information and circuits (94-)	Cryptography (94A60)	110	145	86.83
	Authentication and secret sharing (94A62)	33		
	Communication theory (94A05)	1		
	Switching theory, Boolean functions (94C10)	1		
Number theory and diophantine geometry (11-)	Curves over finite and local fields (11G20)	3	11	6.59
	Primality in number theory (11Y11)	3		
	Algebraic coding theory (11T71)	2		
	Elliptic curves over global fields (11G05)	1		
	Structure theory (11T30)	1		
	Algorithms and complexity (11Y16)	1		
Theory of computing and computer system orgn. (68-)	Network design and communication (68M10)	1	6	3.59
	Network protocols (68M12)	1		
	Information storage and retrieval (68P20)	1		
	Data encryption (68P25)	2		
	Complexity classes (68Q15)	1		
Algebraic Geometry (14-)	Coding theory and cryptography (14G50)	4	4	2.40
Quantum theory and axiomatic (81-)	Quantum computation (81P68)	1	1	0.60

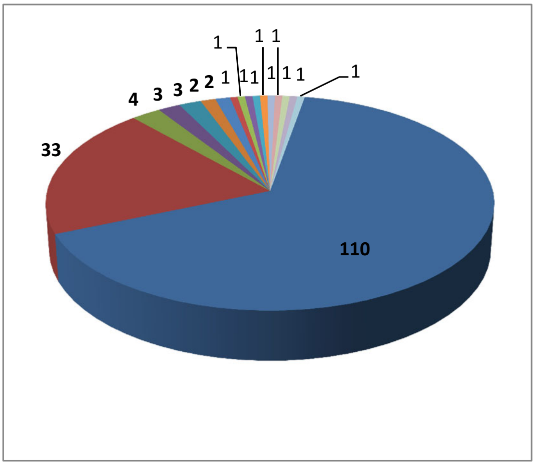
Analysis of author-assigned keywords

Keywords are supposed to be one of the best indicators to understand and grasp the thought content of the contributions and specific areas of research addressed. Thus analysis of keywords could be useful for researchers to reflect the precision of subject declaration and choice-of-terms. In this study, a total of 747 keywords (author-assigned) are found in 167 articles of JOC, of which 510 unique keywords are soughed and enumerated. Notably the occurrence frequency of keywords was highly uneven.

Plural form of a term is treated equally with the singular, such as—adversary versus adversaries, cipher versus ciphers, Isogeny versus Isogenies. Coherent terms (either similar in meaning or semantically related) represented by different wordings are treated separately; in order to express the existence of inter-author inconsistencies for choice-of-terms. For instance Elliptic curve, Elliptic curves cryptography, ECC, Elliptic curve cryptosystem, etc. Therefore, metamorphic terms of a concept (e.g. Diffie–Hellman) could be appeared in different alphabetic positions of the keyword list, as given below;

- Diffie–Hellman
- Strong Diffie–Hellman
- Diffie–Hellman problem
- Gap Diffie–Hellman problem
- Twin Diffie–Hellman problem
- Decision Diffie–Hellman problem
- Tripartite Diffie–Hellman key exchange

Table 10 Sub-categories of the publications

Sub-domain	Freq.	%	Cu %	
94A60	110	65.87	65.87	
94A62	33	19.76	85.63	
14G50	4	2.40	88.03	
11G20	3	1.80	89.82	
11Y11	3	1.80	91.62	
11T71	2	1.20	92.82	
68P25	2	1.20	94.01	
11G05	1	0.60	94.61	
11T30	1	0.60	95.21	
11Y16	1	0.60	95.81	
68M10	1	0.60	96.41	
68M12	1	0.60	97.01	
68P20	1	0.60	97.61	
68Q15	1	0.60	98.21	
81P68	1	0.60	98.80	
94A05	1	0.60	99.40	
94C10	1	0.60	100	
	167	100		

The study reveals an indiscriminate use of keywords by the authors, thus addressed wide range of research topics on cryptology and allied areas. A long list invariably declares the lack of practicing standard-vocabulary for assigning the keywords of scholarly articles. It has been found that 413 keywords appeared only once during a decade-long study period and many of them are meaningfully same. It implies the author's freedom or uniqueness of using terms, rather to maintain standard-vocabulary in order to describe neo micro-thoughts. Author hereby suggests for developing a faceted schema of standard terminologies and its' widespread implementation for authority control while assigning keywords (or subject headings) in this scientific specialty. A truncated list of highly-cited keywords and their corresponding frequencies are presented in Table 11.

Not surprisingly, Cryptanalysis listed as the most frequent keyword appeared in 17 articles, followed by Discrete logarithm, Elliptic curve, Block cipher, Provable security, Cryptography, Secure computation, Oblivious transfer, Public-key encryption, Zero-knowledge, etc.

Active topics of research in Cryptology

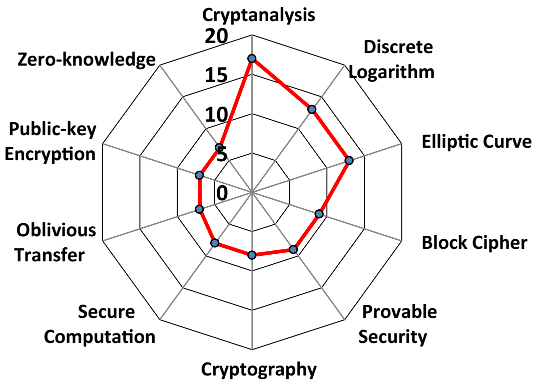
Among the ranked list, top-ten keywords covered almost 13 % of the total keywords cited by the authors, thus presents the concentrated areas (active topics) of research in Cryptology, as shown in Fig. 3. However the frequency of first 43 keywords cumulated as 226, thereby covered almost 30 % of the total keywords appeared in the list.

So the study reveals the research focuses in this scientific field. Indeed, the analysis of keywords could bring an insight to the authors for identifying less-covered or active areas of research, and making strategies of pursuing further research in cryptology.

Table 11 Highly cited author-assigned keywords

Sl	Keywords	Frequency	Cu-Freq.	Cu %
1	Cryptanalysis	17	17	2.276
2	Discrete logarithm	13	30	4.016
3	Elliptic curve (-curves)	13	43	5.756
4	Block cipher (-ciphers)	9	52	6.961
5	Provable security	9	61	8.166
6	Cryptography	8	69	9.237
7	Secure computation—multiparty	8	77	10.308
8	Oblivious transfer	7	84	11.245
9	Public-key encryption	7	91	12.182
10	Zero-knowledge	7	98	13.119
11	Elliptic curve cryptography (ECC)	6	104	13.922
12	Key exchange	6	110	14.726
13	Secure computation	6	116	15.529
14	Secure computation—twoparty	6	122	16.332
15	Bounded-storage model	5	127	17.001
16	Privacy	5	132	17.671
17	RSA	5	137	18.340
18	Secure function evaluation	5	142	19.009
19	Digital signature	4	146	19.545
20	Encryption	4	150	20.080
21	Modes of operation	4	154	20.616
22	One-way function	4	158	21.151
23	Pseudorandomness	4	162	21.687
24	Public-key cryptography	4	166	22.222
25	Signatures	4	170	22.758
26	Unconditional security	4	174	23.293
27	Universal composability	4	178	23.829
28–43	16 keywords having	3 each	226	30.254
44–97	54 keywords having	2 each	334	44.712
98–**510**	413 keywords having	1 each	**747**	100.000

Fig. 3 Active topics of research in cryptology (2001–2010)



Further research

The study could be useful to track many other issues on the growth of cryptographic research, thereby stimulate further studies on citation behavior and collaboration network; which are most desirable by the community-experts and scholars as a research tool. Therefore, the analyses can be made for determining citation patterns, tracking citation networks, justifying self-citation rate, enumerating source-materials cited, calculating mean-age of cited references, identifying core journals, plotting Bradford's bibliograph on cited journals, and so on. Notably, Lindsey (1989) reported a couple of problems to be involved in using citation counts as a measure of quality in science.

Subsequently assessment of internationality and scientific value of the publications could be the probable areas of research in this direction. Simpson (1949) estimator can be applied towards measuring the concentration and geographical diversity of the cryptographic publications, an indicator to visualize the internationality.

However, a detailed correlation analysis of the publications may be observed between multi-authorship and corresponding citation rates (based on SCI), as viewed by Lindsey (1978). Thus one might easily compute whether and how strongly these pairs of variables are associated (i.e. influencing each other) using Pearson's correlation coefficient.

Conclusion

This study examined quantitatively the cryptographic research by analyzing publications growth, authorship pattern, collaboration trend, and predominant areas of cryptographic research using well-established scientometric techniques. It also prepared a rank list of prolific contributors, productive institutions and predominant countries using fractional counting method; as well as active topics of research in cryptology are detected. Intrinsic effort has been made to calculate the AI of JOC and to test the empirical validation of Lotka's law for author productivity. The analysis tracked many other issues for intellectual developments of cryptographic research and to enable better research governance and monitoring academic endeavors as well.

Findings reveal that—research effort of JOC conforms to the growth of world's cryptographic research over a decade of time. As the average AI is derived more than 1 (AI = 1.1), invariably means the research activity of the JOC is at par, even greater than the world's publication activity in cryptographic research. Otherwise, a consistent growth with steady increasing pace has been maintained in JOC when compared to the world average. Therefore, implies the authoritativeness of the JOC to be considered as representative sample of this scientific specialty.

In a straightway, this study entails an increasing trend of multi-authored publications (46 % in 2004 and 90 % in 2009); thus promotes collaboration in agreement with many other disciplines. Average degree of collaboration in quantitative terms i.e. DC derived as 0.74 is quite significant. So the prevalence of team research is clearly observed. Such a trend of collaboration is perhaps due to increased complexity in research activities, technological expositions desire more specializations, and often interdisciplinary research areas are forcing the researchers to share their expertise.

In terms of collaboration density—while multi-authored publications constituted 74 %, then cross-country or international collaboration (56 %) is far beyond the domestic collaborations (44 %). Again a considerable number of inter-country bilateral (52) and multilateral (18) collaboration signifies greater intensity over the domestic collaborations. Indeed, cross-country multilateral collaborations have more intent over the bilateral collaboration, thus defines the strength of research network. So it implies that intellectual perceptions of the cryptographers from diverse origin (across the countries) have been accumulated to produce the research outputs in this scientific specialty.

During last decade of this century, cryptographic research was dominated by USA and Israel. USA received the maximum weighted score (57.53) by affiliating 149 occurrences of authors in different authorship positions; followed by Israel (31.85), France, Canada, Germany, UK, and others. More interestingly, vast majority among top-twenty ranked productive authors are affiliated in USA and Israel. *Yehuda Lindell* is found to be the most prolific author affiliated to the Department of Computer Science, Bar-Ilan University, Israel; followed by *Rosario Gennaro* (USA), *Tamir Tassa* (Israel), *Jonathan Katz* (USA), etc. However, it is observed that author productivity is not in agreement with Lotka's law. But productivity distribution data partially fits the Law when the value of α (productivity parameter) approximated to 2.35 (instead of 2), provided the number of contributions (articles) does not exceed two. The Law does not hold-good beyond this value.

In view of research collaboration network, Anglo-American institutions were more open than their overseas competitor. Among the most productive institutions University of California (six centers), USA is appeared on the top; which is followed by Weizmann Institute of Science (Israel), Bar-Ilan University (Israel), IBM Research Centers (USA), Technion—Israel Institute of Technology (Israel), University of Maryland (USA), Ecole Normale Superieure, Paris (France), University of Bristol (UK), University of Waterloo (Canada), etc. Although a few institutions are earmarked their positions through active participation, but the contributions are eventually made from as many as 136 institutions across geographical boundaries; which implies the authoritativeness and international recognition of JOC in cryptographic research.

The study ascertained broad subject cluster as communication information and circuits, as well as distinct research streams (sub-clusters) such as cryptography, authenticated and secret sharing. However, coding theory, primality in number theory, algorithms and complexity, curves over finite and local or global fields, data encryption, and network protocols are found to be predominating areas of research. Author-assigned keyword frequencies revealed that cryptanalysis, discrete logarithm, elliptic curve, block cipher, provable security, cryptography, secure computation, oblivious transfer, public-key encryption, zero-knowledge, etc. are active topics of research in cryptology. Therefore, the scholars have been paid more concentration on the aforesaid issues to pursue their research on modern information security.

Invariably this study has revealed much information in multiple dimensions, which might be supportive to the scholars, academic administrators, decision makers, and library managers to formulate strategies by means of capacity building, resources allocation, fund allocation, and collection development in libraries for enhancement of cryptographic research.

References

Anyi, K. W. U., Zainab, A. N., & Anuar, N. B. (2009). Bibliometric studies on single journals: A review. *Malayasian Journal of Library and Information Science, 14*(1), 17–55.

Bandyopadhyay, A. K. (2001). Authorship patterns in different disciplines. *Annals of Library and Information Studies, 48*(4), 139–147.

Blanchette, Jean-François. (2013). *Burdens of proof: Cryptographic culture and evidence law in the age of electronic documents*. Cambridge, MA: MIT Press.

Bookstein, A. (1976). The bibliometric distribution. *Library Quarterly, 46*(4), 416–423.

Brickell, Ernest F. (1988). Editorial. *Journal of Cryptology, 1*(1), 1.

Bujdosó, E., & Braun, T. (1983). Publication indicators of relative research efforts in physics subfields. *Journal of the American Society for Information Science, 34*(2), 150–155.

Chen, C., Hu, Z., Liu, S., & Tseng, H. (2012). Emerging trends in regenerative medicine: A scientometric analysis in CiteSpace. *Expert Opinion on Biological Therapy, 12*(5), 593–608.

Coron, J. S. (2006). What is cryptography? *Security and Privacy Magazine, IEEE, 4*(1), 70–73.

Dooley, John F. (2013). *A brief history of cryptology and cryptographic algorithms*. New York: Springer International Publishing.

Egghe, L., Rousseau, R., & Van-Hooydonk, G. (2000). Methods for accrediting publications to authors or countries: Consequences for evaluation studies. *Journal of the American Society for Information Science, 52*(2), 145–157.

Glänzel, W., & Moed, H. F. (2002). Journal impact measures in bibliometric research. *Scientometrics, 53*(2), 171–193.

Gupta, D. K. (1995). Authorship trend and application of Lotka's law: Early literature of computer based storage and retrieval of geoscientific data and information. *IASLIC Bulletin, 30*(1), 13–22.

Huang, M. H., Wu, L. L. & Wu, Y. C. (2014). A study of research collaboration in the pre-web and post-web stages: a coauthorship analysis of the information systems discipline. *Journal of the Association for Information Science and Technology* (preprint).

Lindsey, D. (1978). *The scientific publication system in social science: A study of the operation of leading professional journals in psychology, sociology, and social work*. San Francisco: Jossey-Bass.

Lindsey, D. (1989). Using citation counts as a measure of quality in science measuring what's measurable rather than what's valid. *Scientometrics, 15*(3), 189–203.

Lotka, A. J. (1926). The frequency distribution of scientific productivity. *Journal of the Washington Academy of Science, 16*, 317–323.

MathSciNet (1940–2014). Mathematical reviews on the net. American Mathematical Society (AMS), Providence, USA. http://www.ams.org/mathscinet. Accessed on 12 May 2014.

Murphy, L. J. (1973). Lotka's law in the humanities. *Journal of the American Society for Information Science, 24*(6), 461–462.

NCSP-2013. National Cyber Security Policy: (2013). Ministry of communication and information technology, Government of India (released on 2nd July 2013). https://www.dsci.in/node/1453. Accessed on 12 September 2014.

Nicholls, P. T. (1986). Empirical validation of Lotka's law. *Information Processing and Management, 22*(5), 417–419.

Pao, M. L. (1985). Lotka's law: A testing procedure. *Information Processing and Management, 21*(4), 305–320.

Pao, M. L. (1986). An empirical examination of Lotka's law. *Journal of the American Society for Information Science, 37*(1), 26–33.

Perneger, T. V., & Hudelson, P. M. (2007). How international is the international journal for quality in health care? *International Journal for Quality in Health Care, 19*(6), 329–333.

Potter, W. G. (1981). Lotka's law revisited. *Library Trends, 30*(1), 21–39.

Rousseau, R. (1992). Breakdown of the robustness property of Lotka's law: The case of adjusted counts for multiauthorship attributions. *Journal of the American Society for Information Science, 43*(10), 645–647.

Simpson, E. H. (1949). Measurement of diversity. *Nature, 163*, 688. doi:10.1038/163688a0.

Subramanyam, K. (1983). Bibliometric studies of research in collaboration: A review. *Journal of Information Science, 6*(1), 33–38.

Van-Hooydonk, G. (1997). Fractional counting of multiauthored publications: Consequences for the impact of authors. *Journal of the American Society for Information Science, 48*(10), 944–945.