Bol. Soc. Paran. Mat.
©SPM –ISSN-2175-1188 ON LINE
SPM: www.spm.uem.br/bspm

(3s.) **v. 38** 2 (2020): 75–82.
ISSN-00378712 IN PRESS
doi:10.5269/bspm.v38i2.38218

R-prime Numbers of Degree k *

Abdelhakim Chillali

ABSTRACT: In computer science, a one-way function is a function that is easy to compute on every input, but hard to invert given the image of a random input. Here, "easy" and "hard" are to be understood in the sense of computational complexity theory, specifically the theory of polynomial time problems. Not being one-to-one is not considered sufficient of a function for it to be called one-way (see Theoretical Definition hereinafter). A twin prime is a prime number that has a prime gap of two, in other words, differs from another prime number by two, for example the twin prime pair $(5, 3)$. The question of whether there exist infinitely many twin primes has been one of the great open questions in number theory for many years. This is the content of the twin prime conjecture, which states: There are infinitely many primes p such that $p + 2$ is also prime. In this work we define a new notion: "r-prime number of degree k" and we give a new RSA trap-door one-way. This notion generalized a twin prime numbers because the twin prime numbers are 2-prime numbers of degree 1.

Key Words: RSA, Prime Number, One-Way function, Cryptography.

Contents

1. Introduction

A one-way function is a function that is easy to compute on every input, but hard to invert given the image of a random input. Here, "easy" and "hard" are to be understood in the sense of computational complexity theory, specifically the theory of polynomial time problems. Not being one-to-one is not considered sufficient of a function for it to be called one-way (see Theoretical Definition, below), [6, 7].

Definition 1.1. *A one-way function f is a function that is easy to compute but computationally hard to reverse.*
1. Easy to calculate $f(x)$ from x
2. Hard to invert, to calculate x from $f(x)$

* USMBA, LSI, FP, Taza, Morocco
2010 *Mathematics Subject Classification:* 11T71, 14G50, 94A60.
Submitted July 15, 2017. Published June 14, 2017

Definition 1.2. *A trapdoor one-way function is a one-way function with an additional requirement. Informally, a one-way function might be described as a function for which evaluation in one direction is straightforward, while computation in the reverse direction is far more difficult. Such a function becomes a trapdoor one-way function when one adds the requirement that computation in the reverse direction becomes straightforward when some additional (trapdoor) information is revealed.*

Remark 1.3. *$f : D \to R$ is a trapdoor one way function if there is a trapdoor s such that:*
1. Without knowledge of s, the function f is a one way function
2. Given s, inverting f is easy.

2. The R-prime numbers

A twin prime is a prime number that has a prime gap of two, in other words, differs from another prime number by two, for example the twin prime pair $(41, 43)$. The question of whether there exist infinitely many twins primes has been one of the great open questions in number theory for many years. This is the content of the twin prime conjecture, which states: There are infinitely many primes p such that $p + 2$ is also prime. In 1849 de polygonal made the more general conjecture that for every natural number k, there are infinitely many prime pairs p and p' such that $p' - p = 2k$. The case $k = 1$ is the twin prime conjecture. Cousin prime numbers are prime numbers that differ by four.

Lemma 2.1. *Let p and q are two odd prime numbers, such that $p < q$. Then there exists a number $s \in \mathbb{N}$ such that $q - p = 2s$.*

Proof: As a prime p and q are odd, then $q - p$ is an even number. □

Remark 2.2. *If $N = pq$ is an RSA number. Then there exists a number $s \in \mathbb{N}$ such that $N = p(p + 2s)$, we have:*

$$p = \sqrt{(N + s^2) - s}$$

and

$$q = \sqrt{(N + s^2) + s}$$

Definition 2.3. *Let r is a prime number. Two numbers prime p and q, such that $p < q$ are r-prime numbers, if there exists a number $k \in \mathbb{N}$ such that $q - p = 2r^k$. The prime number p is said, in this case, r-prime number of degree k.*

Remark 2.4. *1. The twin prime numbers are 2-prime numbers of degree 1.*

2. The cousin prime numbers are 2-prime numbers of degree 2.

3. Results and discussion

Let $n \in \mathbb{N}$ and r a prime integer. Let $a_n^{(r)}$ is the number of primes in the set $[[r^n, r^{n+1}]]$, $b_n^{(r)}$ is the number of r-prime numbers of degree k in the set $[[r^n, r^{n+1}]]$ and $c_n^{(r)} = \dfrac{b_n^{(r)}}{a_n^{(r)}}$.

We consider the following sequences $(a_n^{(r)})_{n\in\mathbb{N}}$, $(b_n^{(r)})_{n\in\mathbb{N}}$ and $(c_n^{(r)})_{n\in\mathbb{N}}$. Where $k = 0$ and $r = 2$, we have the first 21 values of these sequences grouped in the following table:

Table 1: THE FIRST 21 VALUES OF THE SEQUENCES

n	$a_n^{(r)}$	$b_n^{(r)}$	$c_n^{(r)}$
0	1	0	0
1	2	1	0,5
2	2	1	0,5
3	2	0	0
4	5	1	0,2
5	7	2	0,2857142857142860
6	13	5	0,3846153846153850
7	23	4	0,1739130434782610
8	43	8	0,1860465116279070
9	75	14	0,1866666666666670
10	137	28	0,2043795620437960
11	255	41	0,1607843137254900
12	464	72	0,1551724137931030
13	872	122	0,1399082568807340
14	1612	228	0,1414392059553350
15	3030	362	0,1194719471947190
16	5709	656	0,1149062883166930
17	10749	1187	0,1104288771048470
18	20390	2087	0,1023540951446790
19	38635	3776	0,0977352141840300
20	73586	6812	0,0925719566221836

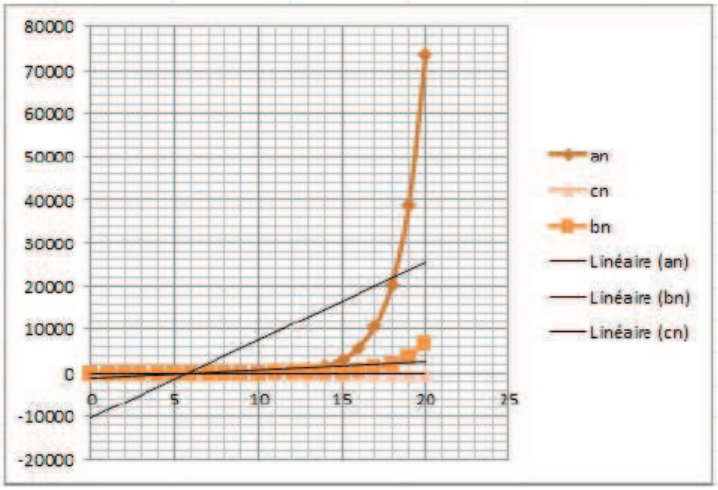

Figure 1: The graphical representation of the sequences

Conjecture:
Let r be a nonzero integer number. There are infinite r-prime of degree k.
The sequence $(c_n^{(r)})_{n\in\mathbb{N}}$ converges to 0.

4. New RSA attack

In this section we assume that $N = p(p + 2r^k)$, is an RSA number, where p is r-prime number of degree k. We have, (see Remark 2.2):

$$p = \sqrt{(N + r^{2k}) - r^k}$$

RSA Algorithm: (see [1], [2])

1. Bob chooses p, secret r-prime number of degree k, and sets that $N = p(p + 2r^k)$
2. Bob chooses e with $gcd(e, \phi(N)) = 1$
3. Bob computes d so that $de = 1 \mod \varphi(N)$
4. Bob makes N and e public but keeps p, r, k and d secret
5. Alice encrypts m as $c = m^e \mod N$
6. Bob decrypts c as $m = c^d \mod N$

Chillali Attack:

1. Chillali knows that $p = \sqrt{(N + r^{2k}) - r^k}$, he takes N
2. Calculate with Maple:
   $> n$:=length(convert(N,binary));
   for k from 1 to n do
   if (isprime(sqrt$(N + r^(2 * k)) - r^k$)=true) then Return($[k, sqrt(N + r^(2 * k)) - r^k, sqrt(N + r^(2 * k)) + r^k]$)
   else end if;
   end do;

Finally, Chillali calculate p and $q = p + 2r^k$, after that factorize N.
Example: N:=2310501570502116935114428835902727936928233422203780506836918401360209156387113823567886794794408316945179243147692904156065277247629000001688200665366006126547704450909752445235424454270043561406355457531409462197089658183068665148887199576619654058510244919785197474628931176170439210846727815909788055653525417625389491831606186567565302609395548314272614438073332602941867076943075860873447304529609874560137578430615911151215956186784810364685787541278027369009940034928892978482670780557590120980157413626601247164765931150430447551152983365696720388212474437558047923651526803288274197476734709278639566434182849560033079262675130481975311521969028178915983208036678315576628089654197704971314421249733020746867021544719220820929509904673538579960295837702450740924668594109950540607709194449721253948881610539655118578099642226407270852393184174948572076101203976602808776563920044581325487813000623500819081914679873052185577110786273344706416835360001373806544220736866697893870000303656801853743691684751394401424575504470497533620522381258815741459433555964881989113629386638773983278926154652271755166202423701850418454138763251189158550257592769954911319907755229794010185568927411774220699743869415856293813933733201943967049676734793814210906360031156612319005023449953081549898022457687685228111867515619929773144423178353712326891915259746696391030100957262657223415457228448973485524630257308086133483541660308753416229307708587311346451027770820896525763754653964585252840557344960656563518617825355794546844653227990543842433737768903559552587119635963477902306666054508942133868391841175906310569297684515397794748485029085348783413039486936987679550121423453363688354363692292702929007128661753341236438377354937510191281844863699911416356073985166579173879015593266552677622863214860142920836671054887611659283264418544314568418102475594638125901730757130114439683560329978850822854141911814604806376460076009313512904291484058317632871941228115236989721210162843531576964089925867361332192877107048896703135024419322206204106303529804463262309084155818764791926881726382257560385594683273910401501315201574756898280633054925430955644149070319842772552144365963164177741517576482245257348649796699104895786560188192257402380454372534838415765101683020880813145136387077662967899010303392119382394401168898157713299945189826055268147166910791226688478293966582067419703485512921684376520043791321730578268474930861222410500438244177732415865420961

42545008362692644603319019822350057408247949948178033155734213742694604
64683129585171581552542234865987608871199079412384256552908397685702979
22041596224541874514397435783611066323734003448300258673551201248275950
20710360022446683113131806169483371526741281720911526354654806876601646
88248156915664213123858997965815068095425233075877617726803742635717625
07159628529747347251413158307289338011987404435024741362131016095680669
07615343746051283727645706670045385354373738064205590434595173445877051
34528581605348270829397366336756125838019035939179671758414901218987995
87071931336041936682752284045334186639120873647553637002540518051734196
93326749559050205367382988606045857619643573299938466447955392471483265
95284667753546009598754789720143821641755006445897246304310495086049810
31772852762360022422195649470208324644395676231701237807779388978343161
44456252295923758436591945974586378826106762195428797200286806944150816
40915223256053884861125327221746007682648938345006209114894195028685586
40368599632233170253974032281689273785347114135137924970075797157453139
01491144418647705957576874486830114146340571230690197310970369185189618
31741642143412124020201290224363093409901847631917823468792306821721320
87221782111843278544783174227538657131087505793176001.

p:=10443888814131525066917527107166243825799642490473837803842334832
83953907971557456848826811934997558340890106714439262837987573438185793
60726323608785136527794595697654370999834036159013438371831442807001185
59462263763188393977127456723346843445866174968079087058037040712840487
40118609114467977783598029006686938976881787785946905630190260940599579
45343282346930302669644305902501597239986771421554169383555988529148631
82379144344967340878118726394964751001890413490084170616750936683338505
51032972088269550769983616369411933015213796825837188091833656751221318
49284636812555022599830041234478486259567449219461702380650591324561082
57318353800876086221028342701976982023131690176780066751954850799216364
19370285375124784014907159135459982790513399611551794271106831134090584
27288427979155484978295432353451706522326906139490598769300212296339568
77828789484406160074129456749198230505716423771548163213806310459029161
36926708342856440730447899971901781465763473223850267253059899795996090
79946920177462481771844986745565925017832907047311943316555080756822184
65717463732968849128195203174570024409266169108741483850784119298045229
81857338977648103126085903001302413467189726673216491511131602920781738
03343609024380470834040315419209 7.

q:=22123000461052396300949980998377306929368108700408171024880396070
30594706308528699609927451156519227304929012295618862153402576648997071
29727684600752063778727863167653029811001452412580528071420983756084893
09180536668659968880129659834397222332464847994781289335628495373320168
91201579033534315162059194255916786734094941260689076533414272188890713
46753073863774447155764711093604167689543607055127510364613253246652709
03661807447176302368144397196068371897929698555147237167618426748896515
67689771506035588261566493053025353700061442029161099191377524177377375
88597059735745331080362036268448863892078508213332597025459352395852905

588979821890138561413325863973188620567854068718552437782229256516406843973252564097752210574685523155902225773560340254851526099685886528323515799686197670674244538668451013585735375988136548297852376643115167931821632983352957819985122607955403696137801533681595146870666730812929487161058786892625858758338536196873670536437494002613393324969750667790112286794114822609118897738868141237037222648305993868907421342346839456247376781941947379642554301738192292455375064590019675679893764900323870026457579854503805963580090994214240686076075971778066104438302498457893013942764692579476294767934973539488721698812561224290897186328578957149528704489009505275466255391835168302142474888523080080820943046563554614838883198398132177767880678349380363182698199951297101602422600327105232467230392307404369723817279170096636346282586171975978384603027476095019737165278994149366727220879809970971168328270306867405363048274505788933711073472293374004525879941041154716905027086495391676016247956826397770894247379846145085518233639094020645027657936505491618119225852364140443604317833556441673015875151720469180343215070058247911021077721712932677561049832191340400275422142880411127801571486543090928761606542324761475056577915724741935128018818601048997551136367676034625487710938458394825474127368379771431005780525584362598369417793875401651599691032130823728277712284810578453031198824020933630934041210741528244128530305039790423844249715307050289300808126732127578861263462554965378967279618821095848009324869878631942886634190665302550137898941289734340687649784135376844000894058400790333992612021797470307112698708685506611296588513807964563636385304443439083093127164196722091056206737940991919929378508930350532645273319009017301363353900975196823726838956212893061697455914643854922135886874844006792372454381035535704185613034293926310058726027113443 3.

Execution time:= 11.107

Table 2: COMPLEXITY OF CALCULUS

The number r	Size of N	Executed Time
2	12393	11.107
3	10241	13.245
31	10469	58.345
41	13422	121.556
101	33403	1367.942

Conclusion:

In this work we could factor a number of 33403 size, in a time of 1367,942 second. So if you know a trap for RSA, its security is broken, for the one must seek another useful encryption, which will be safer.

Acknowledgments

The author gratefully acknowledges that his research is supported by Sidi Mohamed Ben Abdellah University, Polydisciplinary Faculty of Taza (FPT), and the Laboratory of Engineering Sciences (LSI) at FP, Taza, Morocco. We thank the referee by your suggestions.

References

1. Rivest, R.; Shamir, A.; Adleman, L., *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM 21 (2): 120–126, (1978).
2. Boneh Dan, *Twenty Years of attacks on the RSA Cryptosystem*, Notices of the American Mathematical Society 46 (2): 203–213,(1999).
3. A. Chillali, *Cryptography over elliptic curve of the ring*, World Academy of Science, Engineering and Technology, (2011).

Abdelhakim Chillali,
Sidi Mohamed Ben Abdellah University,
FP, LSI, Taza, Morocco.
E-mail address: abdelhakim.chillali@usmba.ac.ma