

Qui a inventé le RSA ?



Jean-Jacques Quisquater
UCL Crypto Group
Louvain-la-Neuve
jjq@uclouvain.be
13 décembre 2013
Telecom Sud Paris



- de Fermat à aujourd'hui : qui a inventé le RSA ? Une histoire de clé publique.
- Nous partirons de la définition du RSA : quels sont les ingrédients nécessaires ?
- Le point de départ est Fermat. Puis ce seront Euler, Babbage, Jevons, Legendre, Hensel, Lehmer, Turing, Koenig, Squires, Ellis, Cockx, Rabin, Diffie, Hellman, Merkle, Knuth, Rivest-Shamir-Adleman ...
- Un voyage étonnant avec plusieurs grandes surprises récemment découvertes.

Ingrédients du RSA

- Système à clé publique,
- Système asymétrique,
- Fonction à sens unique,
- Calcul de l'inverse modulo,
- Exponentielle discrète efficace,
- Grands nombres premiers,
- Factorisation,
- Arithmétique des grands nombres :
 - Addition, multiplication,
 - Multiplication modulo.

Mersenne – Fermat (1643)

- 1640: Fermat proves his little theorem (a way to prove that a given integer is composite)
- 1643: Mersenne asked him if **100.895.598.169** is prime or composite (12 digits)
- Answer of Fermat: factors are **898 423** and **112 303**
- We don't know if Fermat used his published method (using difference of squares)
- Gauss was not able to do it.

... mais ...

- Il faut revenir aux textes originaux,
- Voir pourquoi Mersenne a demandé cela à Fermat,
- Tout n'est pas clarifié.

The Jevons number

- 1874: “Can the reader say what two numbers multiplied together will produce the number **8,616,460,799**? I think it unlikely that anyone but myself will ever know; for they are two large prime numbers, and can only be rediscovered by trying in succession a long series of prime divisors until the right one be fallen upon.” Only 10 digits!
- 1903: D. Lehmer shows the 2 factors during an AMS meeting (then publishing an interesting method based on continuous fractions),
- But ... 1889: Charles J. Busk publishes the factors in Nature! (hidden till last year!)
- See also <http://bit-player.org/2012/the-jevons-number>
- Golomb shows in a paper published by Cryptologia that it is in fact easy using tricks with the Fermat method.



Ajouter à ma bibliothèque

Rédiger un commentaire

Page 83



given a number of up to twenty digits, could say extremely quickly whether it was prime, though they had difficulty with elementary arithmetic. (Sacks 1985)

Frank Nelson Cole (1861–1926)

One of the most extraordinary meetings in the history of mathematics was described by E. T. Bell in *Mathematics: Queen and Servant of Science*:

At the October, 1903, meeting in New York of the American Mathematical Society, Cole had a paper on the programme with the modest title, "On the Factorization of Large Numbers." When the chairman called on him for his paper, Cole—who was always a man of few words—walked to the board and, saying nothing, proceeded to chalk up the arithmetic for raising 2 to its 67th power. Then he carefully subtracted 1. Without a word he moved over to a clear space on the boards and multiplied out, by longhand:

$$193,707,721 \times 761,838,257,287$$

The two calculations agreed. . . . Cole took his seat without uttering a word. Nobody asked him a question.

Only later did Cole admit that he had been working on this problem for the previous twenty years.

Complexity of factorization

- We don't know
- but

Feynman's Van

- 1975 Dodge Tradesman Maxivan, bought new and outfitted in Long Beach
- Had Feynman's diagrams painted
- Sold for \$1 to Leighton, who used it to transport visiting Tuvan throat singers!



+1

Like

Tweet



16 / 48

Share

Add to

Flag

Embed

Uploaded from authorPOINTLite

Views: 1050

Category: Entertainment



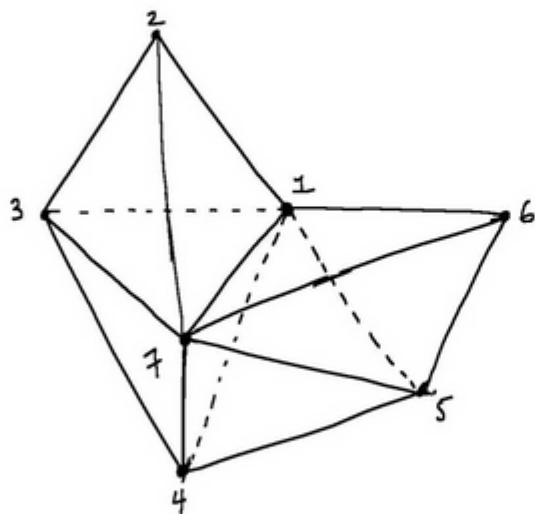
License: © All Rights Reserved

Presentation Description

Amplituhedron Drawing

Published September 13, 2013 at 640 x 708 in A Jewel at the Heart of Quantum Physics

7-point Amplituhedron in P^3



Amplitude for $[1^+ 2^+ 3^+ 4^+ 5^+ 6^+ 7^- 8^-]$

A sketch of the amplituhedron representing an 8-gluon particle interaction. Using Feynman diagrams, the same calculation would take roughly 500 pages of algebra.

Nima Arkani-Hamed

What about a factoriskedron?

- It would be the end of RSA!

“The End of RSA”



The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.”
This is in accordance with DoDI 5230.29, January 8, 2009.

Approved for Public Release, Distribution Unlimited

ISAT workshop

- Menlo Park, January 7-8, 2013
- Attendees: mathematicians, cryptographers, real-world implementers, systems analysts
 - Dan Boneh, Martin Hellman, Pete Kind, Butler Lampson, Andrew Odlyzko, Peter Weinberger, ...
- Topics:
 1. What is the state of RSA cryptanalysis?
 2. What systems rely on RSA?
 3. When RSA fails, how will we know that it has failed?
 4. How can we remediate the failure of RSA-based systems?
 5. Assuming that RSA has not yet failed, what should we do now to prepare?

Science-fiction

- In 1898 (14 years prior to the Titanic tragedy), Morgan Robertson wrote a novel called *Futility*. This fictitious novel was about the largest ship ever built hitting an iceberg in the Atlantic ocean on a cold April night. The fictional ship (named *Titan*) and the real ship *Titanic* were similar in design and their circumstances were remarkably alike. Both ships were labeled "unsinkable".

Citations Titanic

- **From Captain Smith about the Adriatic:**

"I cannot imagine any condition which would cause a ship to founder. I cannot conceive of any vital disaster happening to this vessel. Modern ship building has gone beyond that".

- **A Quote from a Titanic passenger:**

"To say a ship was unsinkable was flying in the face of God".

- **A quote from a White Star Line employee at the launch of Titanic:**

"Not even God himself could sink this ship".

Citations Factoring

- In 1976 Richard Guy wrote: "I shall be surprised if anyone regularly factors numbers of size 10^{80} without special form during the present century."
- In 1977 Ron Rivest said that factoring a 125-digit number would take 40 quadrillion years.

Rivest: prédictions en 1990

- Table 6: Rivest's Optimistic Key-Length Recommendations (In Bits)

Year	Low	Avg	High	done
1990	398	515	1289	
1995	405	542	1399	
2000	422	572	1512	512
2005	439	602	1628	640
2010	455	631	1754	768
2015	472	661	1884	
2020	489	677	2017	

Factoring

Predictions (Bruce Schneier – 1995)

Table 5:

Long-range factoring predictions

Year Key length (in bits)

1995	1024
2005	2048
2015	4096
2025	8192
2035	16,384
2045	32,768

1 Reference for the comparison

You can enter the year until when your system should be protected and see the corresponding key sizes or you can enter a key/hash/group size and see until when you would be protected.

Enter a year:

2 Compare

Method	Date	Symmetric	Asymmetric	Discrete Logarithm Key	Elliptic Curve	Hash
[1] Lenstra / Verheul	2015	82	1613 1248	145 1613	154	163
[2] Lenstra Updated	2015	78	1245 1350	156 1245	156	156
[3] ECRYPT II	2015 - 2020	96	1776	192 1776	192	192
[4] NIST	2011 - 2030	112	2048	224 2048	224	224
[5] FNISA	2010 - 2020	100	2048	200 2048	200	200
[6] NSA	-	-	-	-	-	-
[7] RFC3766	-	-	-	-	-	-
[8] BSI (signature only)	2011 - 2015	-	1976	224 2048	224	224

All key sizes are provided in bits. These are the minimal sizes for security.

samples placed in the outer slots of the prototype (giving the same transverse cross-section as the X-band waveguide) improved transmission, but with a distinct ripple, was observed over the resonance region of the arrays. Similar

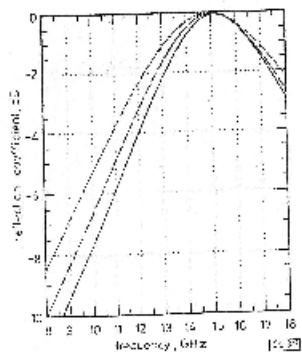


Fig. 3. Reflection response of large array for TE incidence

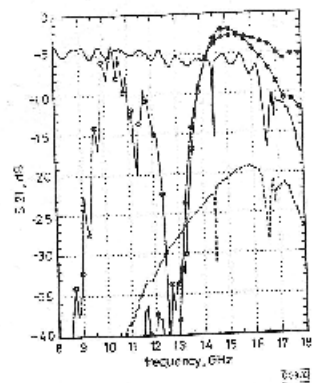


Fig. 4. Insertion loss of waveguiding system with array inserts

— no inserts
 - - - no inserts + RAM
 ○ arrays at position B
 ● inserts + RAM

results to the array/open wall case were observed when the samples were inserted into a standard X-band waveguide, showing that the close proximity of a copper wall to the array does not significantly modify the guiding effect. The null observed near 13 GHz is a filtering effect caused by a certain amount of leakage. This is outside the band of interest. There is good correlation between the infinite array reflection band and the frequency range of the wave guidance. Indeed, there was close correspondence between changes in the tripole arm length and the observed frequency shift.

Conclusions: The concept of guiding waves in a specific frequency band with resonant array inserts in a waveguide has been proposed and verified experimentally. Although in the

initial stages the guidance had a bandwidth between the -3 dB level of about 13%, coupled array designs involving double layers appear to move monotonically inwards with increasing frequency, thus moving the guide cross section to be a constant fraction of a wavelength. This effect appears to be used to design a unilobed or broadband waveguide which will be less dispersive. To achieve this a theoretical modal analysis needs to be developed to include the effect of the finite array [7] under multimode illumination.

10th August 1992

A. J. Robinson, R. D. Seager and J. C. Vardavas (Department of Electronic and Electrical Engineering, University of Technology, Loughborough, Leics. LE11 3TU, United Kingdom)

References

1. VARDAS, J. C. and SEAGER, R. D. Finite and metal insert filters with improved passband separation and increased stopband attenuation, *IEEE Trans.*, 1991, **MIT-35**, pp. 1533-1539
2. JERNILL, J. P. Finite-loss dielectric slotted waveguide filters, *Mathews & Co.*, Dec 1980, pp. 75-82
3. SEAGER, R. D. and VARDAS, J. C. Surface-coupled millimetre-wave E-plane filters, *IEEE Trans.*, 1991, **MIT-35**, pp. 1539-1542
4. SEAGER, R. D. and ADAMS, J. P. Finite lossless CAD of cross-in-aperture multi-branch coupled rectangular waveguide structures, *IEEE Trans.*, 1991, **MIT-35**, pp. 352-362
5. VARDAS, J. C., SEAGER, R. D. and ROBERTS, A. J. Waveguide and aperture filters including frequency selective surfaces, *International Patent*, 1992, Filing No. EP706169200/193
6. VARDAS, J. C. and BARTHELEMY, A. P. Resonance of two triple arm arrays as frequency selective surfaces, *Electron. Lett.*, 1984, **19**, pp. 366-368
7. STELLINGSMA, A. and VARDAS, J. C. A. Moderate convergence gradient FFT method for rapid convergence analysis of finite FSSs, *Electron. Lett.*, 1992, **28**, pp. 308-309

FACTORIZING IS POLYNOMIAL IN TIME

M. Pommerehne, J. Pollard, R.D. Seager.

Indexing terms: Number Theory, Khuritzov Fields, Krull partition theorem, Prime numbers, Error Correcting Codes, Cryptography, Security.

Introduction: We present in this letter an efficient factoring algorithm based on integer transcription via Lirpa-1 polynomials into N-KCFs (Non degenerate $\sqrt{\phi}$ -Khuritzov Colomologis Semibalanced Fields).

Our algorithm factors n bits integers in $O(n^4 \log n)$ operations. This theoretical estimate is quite well verified by extensive numerical simulations: Our Maple program factors 700 bit RSA moduli in less than 400 hours on a standard Sun WS. One of the practical consequences of our result is that factoring based cryptosystems (as for instance the RSA [1]) are no longer secure. Due to the exceptional importance of our discovery, this preliminary version is published in *Electronics Letters* whilst the full paper is under examination by the *Journal of Number Theory*.

In his milestone paper [14], Khuritzov introduced for the first time the concept of Semibalanced Colomologis Number Fields as an immediate extension of Krull's partition theorem. The connections between this result and the number-theoretical aspects of Layer-E theory were mainly [3], [6], [11], [12], [15], [17], [22] investigated in depth.

The multiquasiparabolic representation of an integer r was defined in [14] as the Semibalanced sum:

$$N(r) = \sum_{i=1}^3 N_{a_i} \cdot \left[1 \pm \left(\frac{r - r_{a_i}}{y_{a_i}} \right) \cdot \left(\frac{r_{a_i} - y_{a_i}}{r} \right)^2 \right] \quad (1)$$

David Naccache,
 une première
 nuit froide d'avril,
 imagine un polar
 crypto, à suivre ...

Grands nombres pour la crypto

- Babbage (cryptographe) imagine une machine analytique qui permet de manipuler des nombres de 40 digits, y compris leur multiplication,
- Sans décrire comment, il dit que cela peut servir pour la cryptographie ...

Legendre

- Semble être le premier à avoir décrit un algorithme pour calculer l'exponentielle discrète,
- Mais cela devait être connu bien avant sans avoir été systématisé.

Fonctions à sens unique

- Jevons
- Exemple : la factorisation !

Systemes à clé publique

- Le projet C-43,
- Turing : projet Delilah,

The
U.S. GOVERNMENT

IS ABSOLVED

FROM ANY LITIGATION WHICH MAY
ENSUE FROM THE CONTRACTORS IN -
FRINGING ON THE FOREIGN PATENT
RIGHTS WHICH MAY BE INVOLVED.

SECRET

OSRD 4573A

NATIONAL DEFENSE RESEARCH COMMITTEE
OFFICE OF SCIENTIFIC RESEARCH AND DEVELOPMENT

DIVISION 13 SECTION 3

OEMsr - 435

FINAL REPORT

ON

PROJECT C - 43

Continuation of Decoding Speech Codes

PART I — SPEECH PRIVACY SYSTEMS —

INTERCEPTION, DIAGNOSIS, DECODING, EVALUATION

"THIS DOCUMENT CONTAINS INFORMATION AFFECTING THE NATIONAL DEFENSE OF THE UNITED STATES WITHIN THE MEANING OF THE ESPIONAGE ACT, U.S.C. 50:31 AND 32, ITS TRANSMISSION OR THE REVELATION OF ITS CONTENTS IN ANY MANNER TO AN UNAUTHORIZED PERSON IS PROHIBITED BY LAW."

O.S.R.D. NO. _____ SECTION NO. _____ COPY NO. 42 DATE Oct. 12, 1944

BELL TELEPHONE LABORATORIES, INCORPORATED

NEW YORK, N. Y.

UNCLASSIFIED

AD NUMBER	
ADA800206	
CLASSIFICATION CHANGES	
TO:	unclassified
FROM:	secret
LIMITATION CHANGES	
TO:	Approved for public release, distribution unlimited
FROM:	Distribution authorized to U.S. Gov't. agencies and their contractors; Administrative/Operational Use; OCT 1944. Other requests shall be referred to Office of Scientific Research and Development, NRDC, Div. 13, Washington, DC.
AUTHORITY	
Secretary of Defense memo dtd 2 Aug 1960; Secretary of Defense memo dtd 2 Aug 1960	

THIS PAGE IS UNCLASSIFIED

Communications Division
National Defense Research Committee
of the
Office of Scientific Research and Development
Division 13 Section 3

FINAL REPORT
ON
PROJECT C-43
Continuation of Decoding Speech Codes

PART I - SPEECH PRIVACY SYSTEMS -
INTERCEPTION, DIAGNOSIS, DECODING, EVALUATION
October 12, 1944

SECRET

Contract No. : OMSr-435

Contractor: Western Electric Company Inc.
120 Broadway, New York 5, N. Y.

Project Supervisor: C. H. G. GRAY
Technical Report Prepared by: W. EDWIG

BELL TELEPHONE LABORATORIES, INC.
463 West St., New York 14, N.Y.

make speech private is to add noise or other disturbing signal to the speech and remove it at the other end, in other words, to mask the speech. He will find, however, that it is necessary to use very high levels of masking signal in order to hide the intelligibility. This of course, makes it difficult to subtract out satisfactorily; the difficulties are such that masking systems are more likely to be found on wire lines than on radio. A few speculative masking systems are outlined below.

One form of masking system is shown in figure 20. In this system, two telephone lines are used. At the sending end, noise is added to the speech in a mixing pad and the combination is sent over line 1. The noise alone is sent over a second line and it is used at the receiving end to cancel the noise transmitted with the speech by simple subtraction. This system has the advantage that the noise can be completely random. However, since the enemy might take taps from both lines and thereby be able to make the same subtraction, a variation of this system consists in distorting the noise

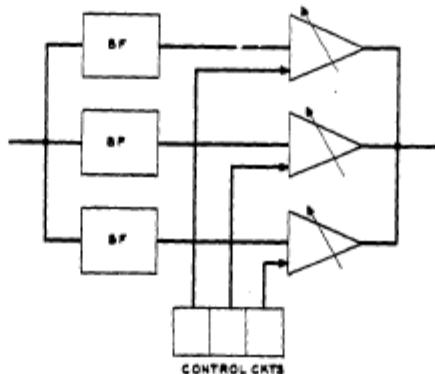


Figure 19 - Subband Level Modulation

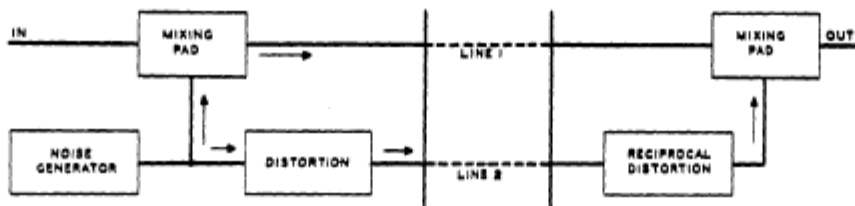


Figure 20 - Noise Masking Using Two Channels

in some predetermined manner before sending it over the second line. At the receiving end, this distortion is first nullified so that the noise may be subtracted. Naturally, the form of distortion must be unknown to the enemy. It can, of course, be varied from moment to moment.

Another masking system is shown in figure 21, which uses only one line. In this system, noise is added to the line at the receiving end instead of at the sending end. Again, the noise can be perfectly random. Since the noise is generated at the receiving end, the process of cancellation can, theoretically, be made very exact. This system, however, cannot be used for radio at all because the level of the

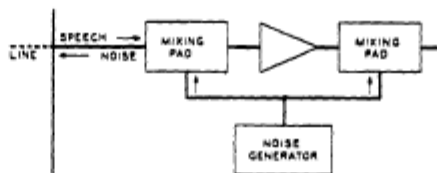


Figure 21 - Masking Noise Applied at Receiving

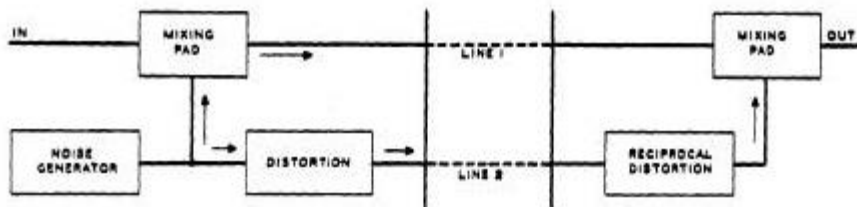
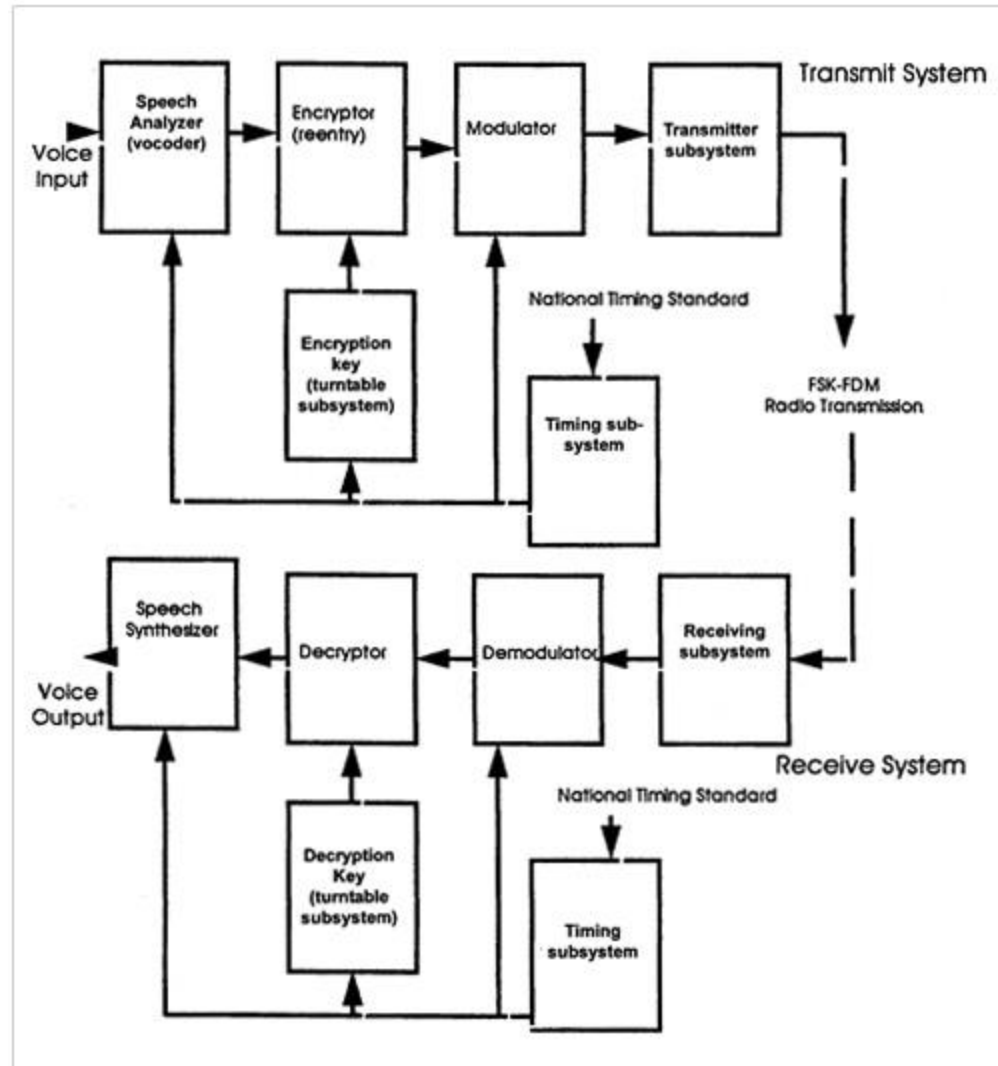


Figure 20 - Noise Masking Using Two Channels



SIGSALY <http://en.wikipedia.org/wiki/SIGSALY>

- During WWII, complete « GSM »



SIGSALY, the start of the digital revolution

see

http://www.nsa.gov/about/cryptologic_heritage/center_crypt_history/publications/sigsaly_start_digital.shtml



Firsts of SIGSALY

- The first realization of enciphered telephony
- The first quantized speech transmission
- The first transmission of speech by Pulse Code Modulation (PCM)
- The first use of companded PCM
- The first examples of multilevel Frequency Shift Keying (FSK)
- The first useful realization of speech bandwidth compression
- The first use of FSK - FDM (Frequency Shift Keying-Frequency Division Multiplex) as a viable transmission method over a fading medium
- The first use of a multilevel "eye pattern" to adjust the sampling intervals (a new, and important, instrumentation technique)
- The system can be thought of as being one of the very first successful applications of spread spectrum technology.

Delilah (Turing)



Turing

- Utilise le premier le terme de « clé publique » (expliquer),
- Imagine 2 systèmes utilisant l'arithmétique modulaire :

Stephen Squires



[Donate Now](#)

[Search](#)

[About ISOC](#)

[Publications](#)

[About the Internet](#)

[Events](#)

[Education](#)

[Public Policy](#)

[Standards](#)

[Membership](#)

[About the Internet Society](#)

[Introduction to ISOC](#)

[Mission and Strategic Plan](#)

[Initiatives](#)

[20th Anniversary](#)

[Programs](#)

[ISOC Principles and Goals](#)

[Staff and Advisors](#)

[Board of Trustees](#)

[Annual Reports](#)

[Financial Information](#)

[Media Information](#)

[Related Organisations](#)

[Awards](#)

[Career Opportunities](#)

[Identity Guidelines](#)

[Contact](#)

[Privacy Statement](#)

[Board of Trustees](#)

[2004 Board Election](#)

[Candidates](#)

Organization member candidate: Stephen Squires

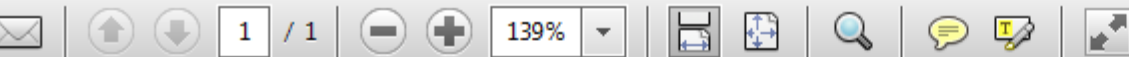
[Personal Statement](#)

The Internet has become a global phenomenon but the Internet Society is not the first organization that most people think of as a critical Internet resource. The society has not yet made the transition from an organization that serves mainly the technical community and early adopters to an organization that is capable of scaling to serve all the people who use the Internet or aspire to use it and those beyond the digital divide who may not even be aware of it. The Internet Society needs to transform into an organization for all the People of Cyber Space and provide effective ways to engage progressively wider diversities of people in the process of continuing advance of the frontier while reducing the digital divide.

Achieving the goal of having the Internet Society recognized everywhere is to have an educational mission focused on reducing barriers to learn about and access the Internet. Organizations throughout the global Internet community need to reach out to their local communities and leverage the resources to educate and enable access for future generations. Reducing the digital divide should be viewed as an Internet Society Community Service critical to bringing the power of IT to all the People.

[2004 BoT Election](#)


- [▶ Overview](#)
- [▶ Ballot](#)
- [▶ Final Nominations Committee Report](#)
- [▶ Candidates](#)
- [▶ Petitions](#)
- [▶ Election Results](#)
- [▶ Previous Elections](#)
- [▶ Current Board of Trustees](#)
- [▶ Board of Trustees Documents](#)



Squires was recruited by the National Security Agency (NSA) at age 18 while he was a freshman undergraduate electrical engineering student at Drexel University. He worked as an engineering intern in the advanced computing and communications laboratories of the NSA. Throughout his career as an electrical engineer and computer scientist at NSA, gaining early access to the full range of advanced technologies as they emerged, including many in cooperation with DARPA, such as early interactive time sharing systems with graphics, UNIX, ARPAnet, extensible programming systems, local area networks, the early Internet, personal computing, VLSI design, rapid prototyping and the highest performance information system technologies.

Squires earned his Ph.D. from Harvard University.

1 ^ | v Reply Share ›

 Guest · 3 months ago

In <http://sqgroup.iwarp.com/Kelvi...>, Stephen Squires (ex-DARPA, ex-NSA) makes the following assertion: "Shortly after returning to NSA, he [Squires] developed a prototype of the first operational public key system using advanced computational complexity theory results and that was experimentally used on the internal NSA ARPAnet based system by the mid 1970s."

It would be interesting to know how that work fits in with the early history of public key cryptography. The "advanced computational complexity results" doesn't sound much like D-H or RSA (or like Ellis, Cocks and Williamson)

^ | v Reply Share ›

 **Stephen L Squires** → Guest · 2 months ago

The computational complexity theory results were for fast multiply. The fundamentals for public key had already been developed by NSA Crypto Mathematicians by the late 1960s. A micro and nano programmable computer had been invented by Burroughs as the D-machine in the late 1960s. Using the computational complexity results for fast multiply a big number library was developed for the D-machine. In 1973 a D-machine was connected to a DEC PDP-10 in the NSA Computer Science laboratory. The system was used to prototype advanced crypto math algorithms using the D-machine big number library as an accelerator. The DEC PDP-10 with D-Machine accelerator was a node on the internal ARPAnet based network in NSA at Fort Meade. The result was a prototype public key system by 1973. With access to advanced mathematics, advanced computer science, advanced computer architectures and systems in the advanced research environment of NSA at the time -- as a kind of "time machine" -- it was easy. //SLSq

^ | v Reply Share ›

Diffie, Hellman, Merkle

- Inventent les systèmes à clé publique comme nous les connaissons, sans proposer de vrai système (mais proposent d'utiliser des matrices et des circuits booléens aléatoires ...),
- Gill propose d'utiliser le log discret
- Don Knuth propose d'utiliser la factorisation !

Michaël Rabin ?

- Voir (écouter !) mes commentaires oraux.

Conclusion : Qui a inventé le RSA ?

- Rivest, Shamir et Adelman, bien sûr, mais ils ont bien plus de précurseurs que « prévus » et nous devons sans doute attendre encore quelques années avant de tout connaître ...
- Merci de me tenir informer si vous avez des indices nouveaux ou inédits !