RSA 40 years later: A historical perspective

Paris May 30 2018

Jacques Stern
École normale supérieure
Summary

1. RSA before RSA
2. Did RSA prove secure enough?
3. Did RSA prove versatile enough?
4. Did RSA change our lives?
New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

Abstract—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

I. INTRODUCTION

WE STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of me-

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

R.L. Rivest, A. Shamir, and L. Adleman*

Abstract

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:
1976: Asymmetric Cryptography

- Whitfield Diffie and Martin Hellman 1976
- Secret key exchange

\[ g^x \mod p \quad \rightarrow \quad g^{xy} \mod p \quad \rightarrow \quad g^y \mod p \]

(common key)

Private key
1976 -> 1984: From DH to EG

- El Gamal 1984
- Encrypt by producing $g^r \mod p$ and using ephemeral key as mask for message: $m.h^r \mod p$
1976-1978 From PKC to RSA

- 1976: Invention of PKC (Public Key Cryptography) by Diffie, Hellman
- 1978: The RSA cryptosystem and signature scheme by Rivest, Shamir, Adleman

\[ y = x^e \mod n \]
\[ n = pq \text{ } p, q \text{ prime} \]
RSA yields signatures

- Because E and D commute (known to DH)
- Apply D to message m to create signature
- Verify using public key only
1763 -> 1978: 215 years

- Novi Commentarii Academiae Scientiarum Petropolitanae 8, 1763, 74-104

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

R.L. Rivest, A. Shamir, and L. Adleman

Abstract

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:
Euler 1763

- Page 83: the numbers of integers prime to $n$ is equal to $\phi(n) = (p-1)(q-1)$
NOVA METHODO DEMONSTRATA. 99

Coroll. 2.

49. Contra autem iam supra vidimus productum ex duobus pluribusque residuis in classe residuorum repetituri. Vide sequitur ex quo non residuo et quocunque residuis in classe non residuorum occurriere debere.

Scholion.

50. Vis huius demonstrationis ideo nititur fundamento, quod si inter residua occurring partes $x, a, b, c, d$, etc. ad divisiorem primo, atque $a$ fuerit etiam pars ad divisiorem prima in his residuis non contenta, tum producida omnia $aa, ab, ac, ad, etc.$ non forem in residuis non occurriere, quod quidem per se demonstratum, sed etiam ea esse partes ad divisiorem N primus, omnesque inter se diversas; sed si ea per N, actu dividantur, relinqui residua diversa. Illud quidem per se est peripicum; cum enim $a, b, c, d$, etc. sint numeri ad N primi, etiam eorum producta ad N prima sint necesse est. Quod autem producita $aa, ab, ac, ad$, etc. sint omnia ad N relatae inter se diversae, intelligitur, quod si verbi gratia duo $aa$ et $ab$ per N divisa pari darent residua, eorum differentia $ab - a = (b - a)$ per N esset divisibilis, ideoque et $b - a$; id quod hypothesi, quod $a$ et $b$ sint diversae partes ad N primae, repugnat.

Theoremata 10.

51. Exponentes minimae potestatis $x^n$, quae per numerum $N$ ad $x$ primum divisa unitatem relinquit, $N = 2$ vel

THEOREMATI ARITHMETICA.

vel est aequalis numero partium ad $N$ primarum, vel huius numeri semissis, aliaque eius pars aliquota.

Demonstratio.

Sit $n$ numerus partium ad $N$ primarum, quam cum $v$ constituant residua, erit numerus non residuum $\equiv n - v$. Vidimus autem haec numerum esse vel $\equiv 0$, vel $\equiv v$, vel $\equiv 2v$, vel aliis cuipiam multiplo exponentis $v$. Sit ergo $n - v = (m - x)v$, ita vt $m$ denotet vel unitatem, vel alium quemuis numerum integrum, atque hic obtinebimus $n = mv$ et $v = \frac{n}{m}$; ita de patet exponentem minimae potestatis ipius $x$, quae per $N$ divisa unitatem relinquit, esse vel $\equiv n$, si $m = x$, vel $\equiv x$, si $m = 2$, vel in generis eis partem quamquam aliquotam numeri $n$, qui exprimit multitudinem partium ad divisiorem $N$ primarum. Q. E. D.

Coroll. 1.

52. Si $x^n$ fuerit minima potestatis, quae per numerum $N$ ad $x$ primum divisa unitatem relinquit, sequenter potestates idem residuum relinquentes sunt $x^{n'}$, $x^{n''}$, $x^{n'''}$, etc. neque praeter illae aliae dantur, quae per $N$ divisa unitatem relinquant.

Coroll. 2.

53. Exponentes ergo huius potestatis minimae semper cum numero partium ad divisiorem $N$ primarum, ita connectitur, vt sit vel illi ipse, vel cuipiam eius partis aliquotae, aequalis.

Scholion.
1978: what is the future of RSA

• Will RSA prove secure enough? Or shall we give it up?
• Will RSA prove versatile enough? Or shall we need alternatives?
• Will RSA change our lives?
First ten years: textbook attacks

- Small message space attack: exhaustively compute $E_K(m_i)$ until correct message is found
- Broadcast attack: obtain encryption of an identical message under various public keys (Hastad)
- Solve equations by chinese remaindering

\[
x^3 = c \mod N_1 \\
\ldots \\
x^3 = c \mod N_3
\]
First 10 years: factoring

- Factor and combine congruences to yield $x^2 = y^2 \mod N$
  
  Pomerance, Eurocrypt 84, Paris

THE QUADRATIC SIEVE FACTORING ALGORITHM

by

Carl POMERANCE

Department of Mathematics
University of Georgia
Athens, Georgia 30602 USA

The quadratic sieve algorithm is currently the method of choice to factor very large composite numbers with no small factors. In the hands of the Sandia National Laboratories team of James Davis and Diane Holdridge, it has held the record for the largest hard number factored since mid-1983. As of this writing, the largest number it has cracked is the 71 digit number $(10^{71} - 1)/9$, taking 9.5 hours on the Cray XMP computer at Los Alamos, New Mexico. In this paper I shall give some of the history of this algorithm and also describe some of the improvements that have been suggested for it.
First 10 years: factoring

- Also from Eurocrypt 84

Status Report on Factoring
(At the Sandia National Laboratories)*

James A. Davis, Diane B. Holdridge and Gustavus J. Simmons

Sandia National Laboratories
Albuquerque, New Mexico 87185
1988: a breaking point

- A 6 pages manuscript by John Pollard circulated in August 1988.
- Published a few years later in : The Development of the Number Field Sieve Lenstra, Arjen K., Lenstra, Hendrik W.Jr. (Eds.)

FACTORIZING WITH CUBIC INTEGERS

J. M. POLLARD

Summary. We describe an experimental factoring method for numbers of form $x^3 + k$; at present we have used only $k = 2$. The method is the cubic version of the idea given by Coppersmith, Odlyzko and Schoeppel (Algorithmica 1 (1986), 1–15), in their section ‘Gaussian integers’. We look for pairs of small coprime integers $a$ and $b$ such that:

i. the integer $a + bx$ is smooth,

ii. the algebraic integer $a + bz$ is smooth, where $z^3 = -k$. This is the same as asking that its norm, the integer $a^3 - kb^3$ shall be smooth (at least, it is when $k = 2$).

We used the method to repeat the factorisation of $F_7$ on an 8-bit computer ($2F_7 = x^3 + 2$, where $x = 2^{43}$).
Second 10 years: factoring

RSA-100
Factors: 40094690950920881030683735292761468389214899724061 * 3797522793694367392280887275545627854565536638199
Date: April 1, 1991
Method: pmpqs
Time: Approx. 7 MIP-Years
Name: Mark Manasse, Arjen K. Lenstra
Email: msm@src.dec.com, lenstra@flash.bellcore.com
Recd: April 1, 1991

We are happy to announce that
RSA-129 = 1143816257578388667669235779976146612010218296721242362562618429\ - 35706935245733397830597123563958705058998075147599290026879543541 = 3490529510847650949147849619903898133417764638493387843990820577 * 3276913299326670954996199811908344614317764296799294253979828853

The encoded message published was
968696137546220614724092225935882905759911245743198746951209309162\ 9822514570835693147662283989628013391990551829945157815154

This number came from an RSA encryption of the 'secret' message using the public exponent 9007. When decrypted with he 'secret' exponent
1066986143685780024426637713269201547807099066393786280126262496631\ 0631258911774470873340168559796230653965845513277109085360695
this becomes
2008050013010709030023151804190001180500019172105011309190800151919090\ 618010705

Using the decoding scheme 01=A, 02=B, ..., 26=Z, and 00 a space between words, the decoded message reads

THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE
1993: Engineering (PKCS#1 v 1.5)

Used in SSL v3.0
Algebraic attacks revisited

- Tool: method to solve a low degree polynomial equation $P(x) = 0 \mod N$, when suitable approximation of a root is given (Coppersmith 94)
- Applies to factoring when partial information is known
- Also applies to small message space with random padding: Randomness should not be too small
1994: the quantum threat

- Proceedings of the 35th FOCS, Santa Fe, NM, Nov. 20--22, 1994

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.
1998: The oracle threat

Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1

Daniel Bleichenbacher
Bell Laboratories
700 Mountain Ave.
Murray Hill, NJ 07974
E-mail: bleichen@research.bell-labs.com

Abstract. This paper introduces a new adaptive chosen ciphertext attack against certain protocols based on RSA. We show that an RSA private-key operation can be performed if the attacker has access to an oracle that, for any chosen ciphertext, returns only one bit telling whether the ciphertext corresponds to some unknown block of data encrypted using PKCS #1. An example of a protocol susceptible to our attack is SSL V.3.0.

- To decrypt c, submit ciphertext $c^e$
- Usually not PKCS#1 compliant
- if accepted reveal 7 bit of info
- Repeat cleverly
- cleartext is recovered after a few thousand calls
- plausible in SSL setting
Third 10 years : factoring

- August 22, 1999, 512 bits!

RSA-155
Factors:
102639592829741105772054196573991675900716567808038066803341933521790711307779
* 106603488380168454820927220360012878679207958575989291522270603237193062808643
Date: August 22, 1999
Method: the General Number Field Sieve, with a polynomial selection method of Brian Murphy and Peter L. Montgomery, with lattice sieving (71%) and with line sieving (29%), and with Peter L. Montgomery's blocked Lanczos and square root algorithms;

- December 3, 2003

RSA-576 has 174 decimal digits (576 bits), and was factored on December 3, 2003 by J. Franke and T. Kleinjung from the University of Bonn. factorization.
The value and factorization are as follows:

\[
\text{RSA-576} = 18819881292060796383697239461650439807163563379417382700763356422988859715234665485319 \\
0606065047430453173880113033967161996923212057340318795506569966221305168759307650257059
\]

\[
\text{RSA-576} = 39807508642406493739712550550386491199064362342526708406385189575946388957261768583317 \\
\times 472772146107435302536223071973048224632914695302097116459852171130520711256363590397527
\]
The factorization was found using the general number field sieve algorithm.
Third 10 years : provable security

- Provide a mathematical proof that formatted RSA is “as secure” as full-size “raw” RSA
- Hash functions are treated as purely random
- Adversary is extensively allowed to query decryption of related (but distinct from target) ciphertexts [CCA attack]
- Still unable to get one bit of information on target
1994: OAEP (Bellare Rogaway)

random seed | fixed | 00...00 | 01 | Data block

G

Mask 1

+ H

Mask 2

00 S T
2001: The OAEP saga

- OAEP Believed to withstand CCA attacks,
- Paper by Shoup showing proof invalid
- Repaired by FOPS same year

OAEP Reconsidered*
Victor Shoup
IBM Zurich Research Lab, Säumerstr. 4, 8803 Rüschlikon, Switzerland
sho@zurich.ibm.com
September 18, 2001

Abstract
The OAEP encryption scheme was introduced by Bellare and Rogaway at Eurocrypt '94. It converts any trapdoor permutation scheme into a public-key encryption scheme. OAEP is widely believed to provide resistance against adaptive chosen ciphertext attack. The main justification for this belief is a supposed proof of security in the random oracle model, assuming the underlying trapdoor permutation scheme is one way.
This paper shows conclusively that this justification is invalid. First, it observes

RSA–OAEP is Secure under the RSA Assumption*
Eiichiro Fujisaki and Tatsuaki Okamoto
NTT Labs, 1-1 Hikarino-oka
Yokosuka-shi, 239-0847 Japan.
E-mail: {fujisaki,okamoto}@isl.ntt.co.jp

David Pointcheval and Jacques Stern
Département d’Informatique – Ecole Normale Supérieure
45, rue d’Ulm – 75230 Paris Cedex 05 – France.
E-mail: {David.Pointcheval,Jacques.Stern}@ens.fr
URL: http://www.di.ens.fr/users/{pointche,stern}
Fourth 10 years : factoring

- December 12, 2009 « halfway » to 1024 bits !
- Later: smaller sizes

<table>
<thead>
<tr>
<th>RSA</th>
<th>Bits (q)</th>
<th>Bits (n)</th>
<th>Date</th>
<th>Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA-704 [*]</td>
<td>212</td>
<td>704</td>
<td>July 2, 2012</td>
<td>Shi Bai, Emmanuel Thomé and Paul Zimmermann</td>
</tr>
<tr>
<td>RSA-230</td>
<td>230</td>
<td>762</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSA-232</td>
<td>232</td>
<td>768</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSA-768 [*]</td>
<td>232</td>
<td>768</td>
<td>December 12, 2009</td>
<td>Thorsten Kleinjung et al.</td>
</tr>
</tbody>
</table>
Quantum factoring

● Still not competing

<table>
<thead>
<tr>
<th>Number</th>
<th># of factors</th>
<th># of qubits needed</th>
<th>Algorithm</th>
<th>Year implemented</th>
<th>Implemented without prior knowledge of solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>2</td>
<td>8</td>
<td>Shor</td>
<td>2001 [2]</td>
<td>×</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>8</td>
<td>Shor</td>
<td>2007 [3]</td>
<td>×</td>
</tr>
<tr>
<td>21</td>
<td>2</td>
<td>10</td>
<td>Shor</td>
<td>2009 [5]</td>
<td>×</td>
</tr>
<tr>
<td>143</td>
<td>2</td>
<td>4</td>
<td>minimization</td>
<td>2012 [1]</td>
<td>✓</td>
</tr>
<tr>
<td>56153</td>
<td>2</td>
<td>4</td>
<td>minimization</td>
<td>2012 [1]</td>
<td>✓</td>
</tr>
<tr>
<td>291311</td>
<td>2</td>
<td>6</td>
<td>minimization</td>
<td>not yet</td>
<td>✓</td>
</tr>
<tr>
<td>175</td>
<td>3</td>
<td>3</td>
<td>minimization</td>
<td>not yet</td>
<td>✓</td>
</tr>
</tbody>
</table>

High-fidelity adiabatic quantum computation using the intrinsic Hamiltonian of a spin system: Application to the experimental factorization of 291311

Zhaokai Li, Nikesh S. Dattani, Xi Chen, Xiaomei Liu, Hengyan Wang, Richard Tanburn, Hongwei Chen, Xinhua Peng, Jiangfeng Du

(Submitted on 26 Jun 2017)

In previous implementations of adiabatic quantum algorithms using spin systems, the average Hamiltonian method with Trotter's formula was conventionally adopted to generate an effective instantaneous Hamiltonian that simulates an adiabatic passage. However, this approach had issues with the precision of the effective Hamiltonian and with the adiabaticity of the evolution. In order to address these, we here propose and experimentally demonstrate a novel scheme for adiabatic quantum computation by using the intrinsic Hamiltonian of a realistic spin system to represent the problem Hamiltonian while adiabatically driving the system by an extrinsic Hamiltonian directly induced by electromagnetic pulses. In comparison to the conventional method, we observed two advantages of our approach: improved ease of implementation and higher fidelity. As a showcase example of our approach, we experimentally factor 291311, which is larger than any other quantum factorization known.

Subjects: Quantum Physics (quant-ph)
Cite as: arXiv:1706.08061 [quant-ph]
(or arXiv:1706.08061v1 [quant-ph] for this version)

Submission history
From: Jiangfeng Du [view email]
[v1] Sun, 25 Jun 2017 08:53:02 GMT (1279kb,D)
Beyond provable security

- Verify cryptographic proofs formally
- Active research
- Many success with proof assistants

Beyond Provable Security
Verifiable IND-CCA Security of OAEP

Gilles Barthe¹, Benjamin Grégoire², Yassine Lakhnech³, and Santiago Zanella Béguelin¹

¹ IMDEA Software
² INRIA Sophia Antipolis-Méditerranée
³ Université Grenoble 1, CNRS, Verimag

Abstract. OAEP is a widely used public-key encryption scheme based on trapdoor permutations. Its security proof has been scrutinized and amended repeatedly. Fifteen years after the introduction of OAEP, we present a machine-checked proof of its security against adaptive chosen-ciphertext attacks under the assumption that the underlying permutation is partial-domain one-way. The proof can be independently verified by running a small and trustworthy proof checker and fixes minor glitches that have subsisted in published proofs. We provide an overview of the proof, highlight the differences with earlier works, and explain in some detail a crucial step in the reduction: the elimination of indirect queries made by the adversary to random oracles via the decryption oracle. We also provide—within the limits of a conference paper—a broader perspective on independently verifiable security proofs.
Back in 1978: RSA versatile?

- CANNOT provide short keys
- CANNOT allow to use email address as PK
- CANNOT allow to perform Crypto-computing

- Fostered 40 years of research on alternatives
1985: Shorter keys via EC

- Shorter keys due to less efficient attacks
- Miller
- Koblitz

Use of Elliptic Curves in Cryptography

Victor S. Miller

Exploratory Computer Science, IBM Research, P.O. Box 218, Yorktown Heights, NY 10598

ABSTRACT

We discuss the use of elliptic curves in cryptography. In particular, we propose an analogue of the Diffie-Hellmann key exchange protocol which appears to be immune from attacks of the style of Western, Miller, and Adleman. With the current bounds for infeasible attack, it appears to be about 20% faster than the Diffie-Hellmann scheme over GF(p). As computational power grows, this disparity should get rapidly bigger.

Elliptic Curve Cryptosystems

By Neal Koblitz

This paper is dedicated to Daniel Shanks on the occasion of his seventieth birthday

Abstract. We discuss analogs based on elliptic curves over finite fields of public key cryptosystems which use the multiplicative group of a finite field. These elliptic curve cryptosystems may be more secure, because the analog of the discrete logarithm problem on elliptic curves is likely to be harder than the classical discrete logarithm problem, especially over GF(2^n). We discuss the question of primitive points on an elliptic curve modulo p, and give a theorem on nonsmoothness of the order of the cyclic subgroup generated by a global point.
1984: ID based

- PK related to ID
- Generated by Trusted third Party
- Proposed for signatures

IDENTITY-BASED CRYPTOSYSTEMS AND SIGNATURE SCHEMES

Adi Shamir

Department of Applied Mathematics
The Weizmann Institute of Science
Rehovot, 76100 Israel

THE IDEA

In this paper we introduce a novel type of cryptographic scheme, which enables any pair of users to communicate securely and to verify each other's signatures without exchanging private or public keys, without keeping key directories, and without using the services of a third party. The scheme assumes the existence of trusted key generation cen-
A One Round Protocol for Tripartite Diffie–Hellman

Antoine Joux

SCSSI, 18, rue du Dr. Zamenhoff
F-92131 Issy-les-Mv Cedex, France
Antoine.Joux@ens.fr

Abstract. In this paper, we propose a three participants variation of the Diffie–Hellman protocol. This variation is based on the Weil and Tate pairings on elliptic curves, which were first used in cryptography as cryptanalytic tools for reducing the discrete logarithm problem on some elliptic curves to the discrete logarithm problem in a finite field.
1940 -> 2000 Pairings

- Introduced by Weil 1940

- Used in Crypto to spot “weak” elliptic curves where DLP is easier

- Reversed by Joux 2000
A One Round Protocol for Tripartite Diffie–Hellman

Antoine Joux
SCSSI, 18, rue du Dr. Zamenhoff
F-92131 Issy-les-Mx Cedex, France
Antoine.Joux@ens.fr

Abstract. In this paper, we propose a three participants variation of the Diffie–Hellman protocol. This variation is based on the Weil and Tate pairings on elliptic curves, which were first used in cryptography as cryptanalytic tools for reducing the discrete logarithm problem on some elliptic curves to the discrete logarithm problem in a finite field.

Identity-Based Encryption from the Weil Pairing

Dan Boneh∗
dabo@cs.stanford.edu

Matthew Franklin†
franklin@cs.ucdavis.edu

Abstract
We propose a fully functional identity-based encryption scheme (IBE). The scheme has chosen ciphertext security in the random oracle model assuming a variant of the computational Diffie–Hellman problem. Our system is based on bilinear maps between groups. The Weil pairing on elliptic curves is an example of such a map. We give precise definitions for secure identity based encryption schemes and give several applications for such systems.
From TDH to ID-based

$$h = H(id)$$

$$g^r$$

$$k = e(h, g)^rz$$

$$(g^r, m.k)$$

- Encrypts $m$ as
ON DATA BANKS AND PRIVACY HOMOMORPHISMS

Ronald L. Rivest
Len Adleman
Michael L. Dertouzos

Massachusetts Institute of Technology
Cambridge, Massachusetts

I. INTRODUCTION

Encryption is a well-known technique for preserving the privacy of sensitive information. One of the basic, apparently inherent, limitations of this technique is that an information system working with encrypted data can at most store or retrieve the data for the user; any more complicated operations seem to require that the data be decrypted before being operated on.
Homomorphic encryption

- Many schemes have “somewhat homomorphic” properties
- Based on encrypting with noise and decrypting with trapdoor
- Too many operations on encrypted data does not allow to recover error
Bootstrapping

- Breakthrough by Gentry 09

- Used ideal lattices in $\mathbb{Z}[X]/f$

Fully Homomorphic Encryption Using Ideal Lattices

Craig Gentry
Stanford University and IBM Watson
cgentry@cs.stanford.edu

ABSTRACT

We propose a fully homomorphic encryption scheme – i.e., a scheme that allows one to evaluate circuits over encrypted data without being able to decrypt. Our solution comes in three steps. First, we provide a general result – that, to construct an encryption scheme that permits evaluation of arbitrary circuits, it suffices to construct an encryption scheme that can evaluate (slightly augmented versions of) its own decryption circuit; we call a scheme that can evaluate its (augmented) decryption circuit bootstrappable.

Produced by Rivest, Adleman and Dertouzos [54] shortly after the invention of RSA by Rivest, Adleman and Shamir [55]. Basic RSA is a multiplicatively homomorphic encryption scheme – i.e., given RSA public key $pk = (N,e)$ and ciphertexts $\{\psi_i \leftarrow \pi_i^e \mod N\}$, one can efficiently compute $\prod_i \psi_i \equiv (\prod_i \pi_i)^e \mod N$, a ciphertext that encysts the product of the original plaintexts. Rivest et al. [54] asked a natural question: What can one do with an encryption scheme that is fully homomorphic: a scheme $E$ with an efficient algorithm Evaluate that, for any valid public key $pk$, any circuit $C$ (not just a circuit consisting of multiplication...
Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes

Nigel P. Smart and Frederik Vercauteren

1 Dept. Computer Science,
University of Bristol,
Merchant Venturers Building,
Woodland Road,
Bristol, BS8 1UB,
United Kingdom
nigel@cs.bris.ac.uk

2 COSIC - Electrical Engineering,
Katholieke Universiteit Leuven,
Kasteelpark Arenberg 10,
B-3001 Heverlee,
Belgium
fvercaut@esat.kuleuven.ac.be

Abstract. We present a fully homomorphic encryption scheme which has both relatively small key and ciphertext size. Our construction fol-

Implementing Gentry’s Fully-Homomorphic Encryption Scheme

Craig Gentry* and Shai Halevi*

IBM Research

Abstract. We describe a working implementation of a variant of Gentry’s fully homomorphic encryption scheme (STOC 2009), similar to the variant used in an earlier implementation effort by Smart and Vercauteren (PKC 2010). Smart and Vercauteren implemented the underlying “somewhat homomorphic” scheme, but were not able to implement the bootstrapping functionality that is needed to get the complete scheme to work. We show a number of optimizations that allow us to implement all aspects of the scheme, including the bootstrapping functionality.

Fully Homomorphic Encryption over the Integers

Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan

1 MIT CSAIL
2 IBM Research

Abstract. We construct a simple fully homomorphic encryption scheme, using only elementary modular arithmetic. We use Gentry’s technique to construct a fully homomorphic scheme from a “bootstrappable” somewhat homomorphic scheme. However, instead of using ideal lattices over a polynomial ring, our bootstrappable encryption scheme merely uses addition and multiplication over the integers. The main appeal of our scheme is the conceptual simplicity.
HE over the integers

- Simpler construction
- Security based on the “approximate GCD” problem \([\text{find an integer } p \text{ from approximations of several multiples of } p]\)
- Seems familiar to cryptanalysts …
The two faces of lattices

The Two Faces of Lattices in Cryptology

Phong Q. Nguyen and Jacques Stern

École Normale Supérieure, Département d’Informatique,
45 rue d’Ulm, 75005 Paris, France
pnguyen@ens.fr and http://www.di.ens.fr/~pnguyen/
stern@di.ens.fr and http://www.di.ens.fr/~stern/

Abstract. Lattices are regular arrangements of points in $n$-dimensional space, whose study appeared in the 19th century in both number theory and crystallography. Since the appearance of the celebrated Lenstra-Lenstra-Lovász lattice basis reduction algorithm twenty years ago, lattices have had surprising applications in cryptology. Until recently, the applications of lattices to cryptology were only negative, as lattices were used to break various cryptographic schemes. Paradoxically, several positive cryptographic applications of lattices have emerged in the past five years: there now exist public-key cryptosystems based on the hardness of lattice problems, and lattices play a crucial rôle in a few security proofs. We survey the main examples of the two faces of lattices in cryptology.

A method to break the approximate gcd problem (using orthogonal lattices see NS 2001)
A method to achieve HE
Alternatives in 2018

- Practicality is improving
- Balance between design and cryptanalysis not always clear
- Additional research needed
Cryptanalysis takes time

FLASH, a fast multivariate signature algorithm
http://www.minrank.org/flash/

Jacques Patarin, Nicolas Courtois and Louis Goubin

Bull CP8
68 route de Versailles – BP45
78431 Louveciennes Cedex
France
J.Patarin@frlv.bull.fr, courtois@minrank.org, Louis.Goubin@bull.net

Abstract. This article describes the particular parameter choice and implementation details of one of the rare published, but not broken signature schemes, that allow signatures to be computed and checked by a low-cost smart card. The security is controversial, since we have no proof of security, but the best known attacks require more than $2^{80}$ computations. We called FLASH our algorithm and we also proposed SFLASH, a version that has a smaller public key and faster verification though one should be even more careful about it’s security.

FLASH and SFLASH have been accepted as submissions to NESSIE (New European Schemes for Signatures, Integrity, and Encryption), a project within the Information Societies Technology (IST) Programme of the European Commission.

– 2001

2007

Practical Cryptanalysis of SFLASH

Vivien Dubois¹, Pierre-Alain Fouque¹, Adi Shamir¹,², and Jacques Stern¹

¹ École normale supérieure
Département d’Informatique 45, rue d’Ulm
75230 Paris cedex 05, France
Vivien.Dubois@ens.fr,
Pierre-Alain.Fouque@ens.fr, Jacques.Stern@ens.fr
² Weizmann Institute of Science
Adi.Shamir@weizmann.ac.il

Abstract. In this paper, we present a practical attack on the signature scheme SFLASH proposed by Patarin, Goubin and Courtois in 2001 following a design they had introduced in 1998. The attack only needs the public key and requires about one second to forge a signature for any message, after a one-time computation of several minutes. It can be applied to both SFLASH¹ which was accepted by NESSIE, as well as to SFLASH² which is a higher security version.
Did RSA change our lives?

- As a community YES
- Gathered smart researches
- Fostered progress in crypto
- Also in related fields: quantum, DPA, formal security …
Did RSA change our lives?

- As individuals ALSO YES
- Improved security of the Internet (SSL)
- Laid foundations for the future (signatures, blockchains …)
- Still challenges for use for confidentiality and privacy
RSA in 2018

- Security well understood and discussed
- RSA is here to last
- Provided we keep an eye on cryptanalysis
- And on Quantum machines
- Still work on alternatives should go on
- And care should be exercised!
Oracles strike again

The ROBOT Attack

Return Of Bleichenbacher’s Oracle Threat
Hanno Böck, Juraj Somorovsky (Hackmanit GmbH, Ruhr-Universität Bochum), Craig Young (Tripwire VERT)

Return Of Bleichenbacher’s Oracle Threat (ROBOT)
https://robotattack.org/

Hanno Böck, Juraj Somorovsky$^{1,2}$, and Craig Young$^3$

$^1$Ruhr-Universität Bochum
$^2$Hackmanit GmbH
$^3$Tripwire VERT

December 12, 2017