Tagungsband zum 15. Kryptotag

Workshop der Fachgruppe Angewandte Kryptologie
in der Gesellschaft für Informatik
Carl von Ossietzky Universität Oldenburg

1. und 2. Dezember 2011

Carl von Ossietzky Universität Oldenburg,
Institut für Mathematik und Department für Informatik

Inhaltsverzeichnis

Vulnerable relations of prime factors in the RSA cryptosystem

Marián Kühnel

IT Security Group, RWTH Aachen, Germany

The security of the RSA cryptosystem is based on the assumption that recovering the private key from a public key pair and factoring a modulus N is a hard task. In 1990, Wiener [4] demonstrated how one can obtain the private key from the public key pair if the private key is smaller than $N^{\frac{1}{4}}$. Boneh and Durfee improved Wiener's result and presented two approaches based on lattices which reconstructed private keys smaller than $N^{0.292}$ in polynomial time [1]. The attack was further extended by de Weger to the case where the modulus is a product of primes with a small difference [5]. He derived new bounds for the two approaches of Boneh und Durfee. However, in [5] the upper bound for the second Boneh-Durfee attack was not analyzed in detail due to complicated restrictions. An adequate lattice was determined by Herrman and May [3] who introduced the technique of unravelled linearization, originally introduced for exploiting output bits in power generators [2]. Here, the adapted unravelled linearization technique performed a linearization on the modular equation and so exploited induced relations of the linearization itself.

We show that the recent bound on small private key can be further optimized with respect to small prime difference. Therefore, we generate a set of coprime polynomials where the underlying polynomial needed for the basis matrix generation will be the one used by Boneh and Durfee [1]. Then, we join together the monomials of the underlaying bivariate polynomial and adapt the technique of unravelled linearization for constructing lattices as in [3]. We effectively reveal sublattices for small prime difference with a triangular structure needed for a trivial determinant calculation. Next, we use basis reduction algorithms and root finding techniques to reveal the exact roots. Finally, we explain the concrete advantage compared to [1], [5] and [3] and depict the current boundary function for the private key and small prime difference.

References

[1] Boneh, D., Durfee, G.: Cryptanalysis of RSA with Private Key d Less Than $N^{0.292}$, Advances in Cryptology – EUROCRYPT??99, Lecture Notes in Computer Science 1592, Berlin: Springer 1999, pp. 1–11

[2] Herrmann, M., May, A.: Attacking Power Generators Using Unravelled Linearization: When Do We Output Too Much?, Proceedings of the 15th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology In Advances in Cryptology (Asiacrypt 2009), Lecture Notes in Computer Science 5912, Heidelberg:Springer 2009, pp. 487–504

[3] Herrmann, M., May, A.: Maximizing Small Root Bounds by Linearization and Applications to Small Secret Exponent RSA, In Practice and Theory in Public Key Cryptography (PKC 2010), Lecture Notes in Computer Science 6056, Berlin:Springer-Verlag 2010, pp. 53–69

[4] Wiener, M.: Cryptanalysis of short RSA secret exponents, IEEE Transactions on Information Theory **36**, 553–558 (1990)

[5] De Weger, B.: Cryptanalysis of RSA with small prime difference, Applicable Algebra in Engineering, Communication and Computing, Vol. **13(1)**, 17??-28 (2002), Berlin:Springer-Verlag

Analyzing standards for RSA integers

Daniel Loebenberger

Universität Bonn, BIT

The key-generation algorithm for the RSA cryptosystem is specified in several standards, such as PKCS#1, IEEE 1363-2000, FIPS 186-3, ANSI X9.44, or ISO/IEC 18033-2. All of them substantially differ in their requirements. This indicates that for computing a "secure" RSA modulus it does not matter how exactly one generates RSA integers. In this talk we show that this is indeed the case to a large extend: First, we give a theoretical framework that will enable us to easily compute the entropy of the output distribution of the considered standards and show that it is comparatively high. To do so, we compute for each standard the number of integers they define (up to an error of very small order) and discuss different methods of generating integers of a specific form. Second, we show that factoring such integers is hard, provided factoring a product of two primes of similar size is hard.

Faire teilbare elektronische Geldsysteme mit Observern

Patrick Märtens

Justus-Liebig-Universität Gießen

Seit dem ersten elektronischen Geldsystem von Chaum, Fiat und Naor [CFN89] werden diese, insbesondere deren Effizienz betreffend, stets weiter verbessert. Im Jahr 2005 wurde in [CHL05] erstmals ein *kompaktes* Geldsystem vorgestellt, welches die Komplexität des Abhebeprotokolls stark reduziert. Noch effizienter sind *teilbare* Geldsysteme (z.B. [CG10]). Hier hebt jeder Kunde eine teilbare Münze mit dem Wert 2^L ab und teilt diese beim Bezahlen in eine (Teil-)Münze mit einem Wert $2^\ell, 0 \leq \ell \leq L$. Dadurch werden effiziente Abhebe- und Bezahlprotokolle realisiert.

Eine elementare Voraussetzung elektronischer Geldsysteme ist, dass kein Kunde mehrmals mit der gleichen Münze bezahlen und kein Händler eine Münze mehrmals einlösen kann. Ein weiteres zentrales Sicherheitsziel ist die Anonymität der Kunden.

Da sich eine Mehrfachausgabe durch rein kryptografische Mittel aber nicht verhindern lässt, wurde in [CP93] erstmals eine zusätzliche, manipulationssichere Hardware, ein sogenannter *Observer*, in ein elektronisches Geldsystem integriert. Durch die Beteiligung des Observers am Abhebe- und Bezahlprotokoll kann so die mehrfache Ausgabe von Münzen unmittelbar verhindert werden.

Um den in [SN92] aufgezählten kriminellen Aktivitäten, wie Erpressung und Geldwäsche entgegenzuwirken, ist eine *aufhebbare* Anonymität notwendig. Je nach Szenario kann die Bank mit Hilfe einer weiteren Partei, der sogenannten *Trusted-Third-Party* (TTP), den Besitzer einer bestimmten Münze identifizieren (Kunden-Tracing), oder den Ausgabeort einzelnen Münzen bestimmen und diese ggf. sperren (Münz-Tracing). Ein solches Geldsystem wird als *fair* bezeichnet (z.B. [FTY98]).

Ob und wie die beiden Zusatzeigenschaften Fairness und Observer effizient in teilbare elektronische Geldsysteme integriert werden können, ist Gegenstand meiner aktuellen Forschung. Ich werde darstellen, wie ein Kunden-Tracing mit einfachen kryptografischen Bausteinen ohne Effizienzverlust in ein teilbares Geldsystem integriert werden kann. Des weiteren werde ich zeigen, wie ein effizientes Münz-Tracing realisiert werden kann, so dass alle Teil-Münzen einer bestimmten teilbaren Münze verfolgt werden können. Aktuell befasse ich mich damit, ein Münz-Tracing zu integrieren, welches ermöglicht nur bestimmte Teil-Münzen zu verfolgen, während andere anonym bleiben.

Literatur

[CFN89] David Chaum, Amos Fiat und Moni Naor. Untraceable Electronic Cash. In *Advances in Cryptology - Crypto '88*, Bd. 403 (LNCS), S. 319 - 327. Springer. 1989.

[CG10] Sébastien Canard und Aline Gouget. Multiple Denominations in E-cash with Compact Transaction Data. In *Financial Cryptography '10*, Bd. 6052 (LNCS), S. 82 - 97. Springer. 2010.

[CHL05] Jan Camenisch, Susan Hohenberger und Anna Lysyanskaya. Compact E-Cash. In *Advances in Cryptology - Eurocrypt '05*, Bd. 3494 (LNCS), S. 302 - 321. Springer. 2005.

[CP93] David Chaum und Torben P. Pedersen. Wallet Databases With Observers. In *Advances in Cryptology - Crypto '92*, Bd. 740 (LNCS), S. 89 - 105. Springer. 1993.

[FTY98] Yair Frankel, Yiannis Tsiounis und Moti Yung. Fair Off-Line e-Cash made easy. In *Advances in Cryptology - Asiacrypt '98*, Bd. 1514 (LNCS), S. 257 - 270. Springer. 1998.

[SN92] Sebastiaan von Solms und David Naccache. On Blind Signatures and Perfect Crimes. In *Computers and Security '92*, Bd. 11, Nr. 6, S. 581 - 583. 1992.

Homomorphic Encryption with a Double Decryption Mechanism based on Elliptic Curves over Rings

Andreas Peter

Technische Universität Darmstadt & CASED
Security Engineering Group, Germany

We consider the following setting of a company where each employee has his own secret key, say for e-mail communication, while the head of the company (or some other master authority) always needs to be able to decrypt any e-mail even in case an employee lost his secret key. Certainly, for large companies to be practical, we would like the master authority to have a *single* master secret that is independent of the secret keys (and in particular, independent of the amount) of the individual employees. Encryption schemes providing such a functionality are called *public-key encryption schemes with a double decryption mechanism* (DD-PKE). More importantly, in certain situations it is useful to have such a public-key encryption scheme to be also *group homomorphic*, i.e., its decryption procedure is a group homomorphism. To the author's knowledge, there are currently only two schemes of this kind. One was proposed by Bresson, Catalano and Pointcheval [2] which itself is a variant of a scheme by Cramer and Shoup [3].

In this talk, we present for the first time such a scheme (being *both* homomorphic *and* having a double decryption mechanism) which works over points on some elliptic curve. More precisely, we work on elliptic curves over the ring $\mathbb{Z}_{N^2}$ where $N = pq$ is some RSA-modulus. Our proposed scheme can be seen as an elliptic curve analogon to the already existing homomorphic DD-PKE scheme [2] by Bresson, Catalano and Pointcheval. Although it uses similar structures [2] and particularly requires factoring N to be computationally infeasible, it has some advantages over the original scheme. For one, being a scheme with a double decryption mechanism, [2]'s master entity decryption procedure requires the computation of so-called *Partial Discrete Logarithms*. The corresponding decryption procedure of our scheme is much simpler and does not require these computations. Additionally, we achieve higher security than [2] while taking the same security parameter (here, this is the bit length of the prime p) – unfortunately this goes on the cost of efficiency. It should not be swept under the carpet that our scheme is also very interesting from a theoretical point of view, since it constitutes another example on the power and usability of elliptic curves in cryptography. Interestingly enough, we show our scheme to be semantically secure *if and only if* the elliptic curve analogon of the Decision Diffie-Hellman Assumption over $\mathbb{Z}^*_{N^2}$ as introduced in [2] is hard. We do so by working with the generic framework for group homomorphic encryption schemes introduced by Armknecht, Peter, and Katzenbeisser [1].

References

[1] Frederik Armknecht, Andreas Peter, and Stefan Katzenbeisser. A cleaner view on ind-cca1 secure homomorphic encryption using soap. Cryptology ePrint Archive, Report 2010/501, 2010.

[2] Emmanuel Bresson, Dario Catalano, and David Pointcheval. A simple public-key cryptosystem with a double trapdoor decryption mechanism and its applications. In Chi-Sung Laih, editor, *ASIACRYPT*, volume 2894 of *Lecture Notes in Computer Science*, pages 37–54. Springer, 2003.

[3] Ronald Cramer and Victor Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In Lars R. Knudsen, editor, *EUROCRYPT*, volume 2332 of *Lecture Notes in Computer Science*, pages 45–64. Springer, 2002.

MinRank Attacks revisited

Enrico Thomae and Christopher Wolf

Horst Görtz Institute for IT-security
& Faculty of Mathematics
Ruhr-University of Bochum, 44780 Bochum, Germany

The MinRank problem is a well known mathematical problem which is proven to be NP-complete [1]. In the context of Cryptography this problem typically appears for layer-based primitives like the Rainbow Signature Scheme. In the past years many MinRank instances deduced from cryptographic primitives were easily solvable. Thus the so called MinRank attack is an established tool of cryptanalysis which should be taken into account by designers of new schemes.
We first show that there still exists schemes vulnerable to MinRank attacks - namely Double-Layer Square and Square+ [2]. After that we revisit techniques to attack MinRank [3, 4] using the example of the Rainbow Signature Scheme. We show that there is still some structure left, not used for the attack until now. How to make use of it is part of ongoing research. One of the main open questions is, how we can obtain good upper bounds on the degree of regularity for overlapping blocks of bihomogeneous equations. For *one* block of bihomogeneous equations this problem was solved by Faugère *et al.* [5].

References

[1] Jonathan F. Buss, Gudmund Skovbjerg Frandsen, and Jeffrey Outlaw Shallit. The computational complexity of some problems of linear algebra. Research Series RS-96-33, BRICS, Department of Computer Science, University of Aarhus, September 1996. `http://www.brics.dk/RS/96/33/`, 39 pages.

[2] Enrico Thomae and Christopher Wolf. Roots of square: Cryptanalysis of double-layer square and square+. In *PQCrypto '11: Proceedings of the 4th International Workshop on Post-Quantum Cryptography*, 2011.

[3] Olivier Billet and Henri Gilbert. Cryptanalysis of rainbow. In *SCN*, volume 4116 of *Lecture Notes in Computer Science*, pages 336–347. Springer, 2006.

[4] Jean-Charles Faugère, Françoise Levy dit Vehel, and Ludovic Perret. Cryptanalysis of minrank. In David Wagner, editor, *CRYPTO*, volume 5157 of *Lecture Notes in Computer Science*, pages 280–296. Springer, 2008.

[5] Jean-Charles Faugère, Mohab Safey El Din, and Pierre-Jean Spaenlehauer. Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1,1): Algorithms and complexity. *J. Symb. Comput.*, 46:406–437, April 2011.

ECM mit OpenCL

Wilke Trei

Carl von Ossietzky Universität Oldenburg

Eine der größten Herausforderungen für die moderne Computeralgebra ist das Akquirieren neuer Technologien für mathematische Algorithmen. Dabei spielt zunehmend die Parallelisierung existenter Algorithmen eine große Rolle, da die technologischen Fortschritte im Bereich der Einzelkernprozessoren seid Jahren stagniert. In diesem Vortrag soll anhand einer Implementierung von Lenstras Elliptische Kurven Faktorisierung (ECM) das Konzept von OpenCL einem offenen Programmierstandard für parallele Berechnungen auf verschiedenster Hardware vor gestellt werden und dabei sowohl die Chancen als auch die Probleme bei der effizienten Implementierung zahlentheoretischer Algorithmen auf moderner Hardware diskutiert werden.

Teilnehmer

Name	Einrichtung
Marie A. van Amelsvoort	Universität Bremen
Hartje Bruns	BOS Bremen
Christina Delfs	Carl von Ossietzky Universität Oldenburg
Maria Hahn	Carl von Ossietzky Universität Oldenburg
Florian Heß	Carl von Ossietzky Universität Oldenburg
Stefan Hellbusch	Carl von Ossietzky Universität Oldenburg
Christian Janson	Universität Bremen
Max Kronberg	Carl von Ossietzky Universität Oldenburg
Marian Kühnel	TU Aachen
Daniel Loebenberger	Universität Bonn
Patrick Märtens	Justus Liebig Universität Giessen
Felix Braun Munziger	Carl von Ossietzky Universität Oldenburg
Heinz-Georg Quebbemann	Carl von Ossietzky Universität Oldenburg
Jan Pelz	BOS Bremen
Andreas Peter	TU Darmstadt
Christopher Schael	Universität Bremen
Uli Schlachter	Carl von Ossietzky Universität Oldenburg
Valentin Spreckels	Carl von Ossietzky Universität Oldenburg
Andreas Stein	Carl von Ossietzky Universität Oldenburg
Sandra Stein	Carl von Ossietzky Universität Oldenburg
Enrico Thomae	Ruhr Universität Bochum
Wilke Trei	Carl von Ossietzky Universität Oldenburg
Osmanbey Uzunkol	Carl von Ossietzky Universität Oldenburg
Elke Wilkeit	Carl von Ossietzky Universität Oldenburg

http://KryptoTag.de

Der Kryptotag ist eine zentrale Aktivität der GI-Fachgruppe „Angewandte Kryptologie“. Er ist eine wissenschaftliche Veranstaltung im Bereich der Kryptologie und von der organisatorischen Arbeit der Fachgruppe getrennt. Grundgedanke des Kryptotages ist, dass er inklusive Anreise wirklich nur einen Tag dauert und Nachwuchswissenschaftlern, etablierten Forschern und Praktikern auf dem Gebiet der Kryptologie die Möglichkeit bieten, Kontakte über die eigene Universität hinaus zu knüpfen.

Die Vorträge können ein breites Spektrum abdecken, von noch laufenden Projekten, die ggf. erstmals einem breiteren Publikum vorgestellt werden werden, bis zu abgeschlossenen Forschungsarbeiten, die zeitnah auch auf Konferenzen präsentiert wurden bzw. werden sollen oder einen Schwerpunkt der eigenen Diplomarbeit oder Dissertation bilden. Die eingereichten Abstracts werden gesammelt und als technischer Bericht veröffentlicht. Es handelt sich damit um eine zitierfähige Arbeit. Sie können von den Seiten der Fachgruppe herunter geladen werden.

Bisherige Kryptotage

15. Kryptotag 1. und 2. Dezember 2011, Carl von Ossietzky Universität Oldenburg, Institut für Mathematik und Department für Informatik. Kontakt: Florian Heß

14. Kryptotag 21. und 22. März 2011, Horst Görtz-Institut für IT-Sicherheit, Ruhr-Universität Bochum, Kontakt: Christopher Wolf.

13. Kryptotag 5. November 2010, Security Engineering Group, TU-Darmstadt, Kontakt: Andreas Peter.

12. Kryptotag 9. April 2010, Institut für Kryptographie und Sicherheit, KIT, Kontakt: Willi Geiselmann, Prof. Dr. Jörn Müller-Quade.

11. Kryptotag 30. November 2009, Lehrstuhl für Informationssicherheit und Kryptographie, Universität Trier, Kontakt: Prof. Dr. Ralf Küsters.

10. Kryptotag 20. März 2008, Institut für Mathematik, TU-Berlin, Kontakt: Florian Heß.

9. Kryptotag 10. November 2008, Fachhochschule Gelsenkirchen, Kontakt: Markus Linnemann.

8. Kryptotag am 11. April 2008 Universität Tübingen, WSI für Informatik, Diskrete Mathematik. Kontakt: Michael Beiter, Claudia Schmidt, Anja Korsten.

7. Kryptotag am 9. November 2007 Bonn-Aachen International Center for Information Technology. Kontakt: Michael Nüsken und Daniel Loebenberger.

6. Kryptotag am 19. Februar 2007. Universität des Saarlandes, Information Security and Cryptography Group und Sirrix AG. Kontakt: Michael Backes und Ammar Alkassar.

5. Kryptotag am 11. September 2006. Universität Kassel, Fachbereich Mathematik/Informatik, Theoretische Informatik. Kontakt: Heiko Stamer.

1. Kryptowochenende am 1.–2. Juli 2006. Tagungszentrum Kloster Bronnbach der Universität Mannheim. Kontakt: Frederik Armknecht und Dirk Stegemann.

4. Kryptotag am 11. Mai 2006. Ruhr Universität Bochum, Horst-Görtz Institut. Kontakt: Ulrich Greveler.

3. Kryptotag am 15. September 2005. Technische Universität Darmstadt, Theoretische Informatik. Kontakt: Ralf-Philipp Weinmann.

2. Kryptotag am 31. März 2005. Universität Ulm, Abteilung für Theoretische Informatik. Kontakt: Wolfgang Lindner und Christopher Wolf.

1. Kryptotag am 1. Dezember 2004. Universität Mannheim, Theoretische Informatik. Kontakt: Stefan Lucks und Christopher Wolf.

Innerhalb der Fachgruppe für Angewandte Kryptologie sind Stefan Lucks (Bauhaus-Universität Weimar) und Frederik Armknecht (Universität Mannheim) verantwortlich für die Organisation der Kryptotage. Für eventuelle Rückfragen bitte an sie wenden.