Cryptacus Newsletter

September-October 2018 Cryptacus Newsletter

Welcome to the September-October 2018 edition of the Cryptacus.eu newsletter, offering a glimpse into recent developments in the cryptanalysis of IoT & related areas. Send your comments & feedback at cryptacus.newsletter@irisa.fr

News from the Chair

by GILDAS AVOINE

Dear Cryptacus Members,

Welcome back everyone after the summer break. I hope you enjoyed your holidays and you are well rested.

First of all, the ERC published in July 2018 the list of awarded starting grant applicants.

Among them, several Cryptacus' MC Members. I would so like to kindly congratulate Billy Brumley from Tampere University of Technology (Finland), Claudio Orlandi from Aarhus University (Denmark), and Peter Schwabe from Radboud Universiteit Nijmegen (The Netherlands), who are laureates of ERC Starting Grants. Congrats!

As you may know, Cryptacus will finish in December 2018, after four years of exciting collaborations.

The final conference will be hold on September 18-20, 2018, in Rennes, France, with a great program that includes prestigious speakers. The website of the conference is available here: `www.cryptacus.eu/en/conference`

About 50 MC Members and Invited Speakers will join the conference.

Also, a social event will be organized in Mont Saint Michel on September 19th.

This conference will also be an opportunity to present the Cryptacus' book, which will be published by the end of the year by Springer: the chapter authors will have a 5-minute slot to present their chapter.

Finally, you still have time to apply for an STSM, which must be finished by December 11th, i.e., the last day of the Action.

There is still budget for STSMs, but do not wait too much, and apply soon on the Cryptacus' website!

I'm looking forward to see you in Rennes.

Gildas Avoine

Recommended Reading: Prime and Prejudice: Primality Testing Under Adversarial Conditions and the latest Tesla hack

Our first piece of recommended reading this month is *Prime and Prejudice: Primality Testing Under Adversarial Conditions* by Martin R. Albrecht, Jake Massimo, Kenneth G. Paterson and Juraj Somorovsky.

This work has been accepted to CCS2018, and a preprint is available at `https://eprint.iacr.org/2018/749`.

They provide a groundbreaking set of new results against the primality testing schemes implemented by

multiple libraries that will force developers to seriously reconsider their implementations to defend against this adversarial attacks.

Some highlights are that they are able to construct 2048-bit composites classified as prime with probability 1/16 by OpenSSL's in its default configuration or 1024-bit composites that always pass the primality test of GNU GMP.

In addition, they can create adversarial composites that always pass the primality tests of libraries such as Cryptlib, LibTomCrypt, JavaScript Big Number, and WolfSSL.

Library	Rounds of MR testing	Baillie-PSW?	Documented Failure Rate	Our Highest Failure Rate
OpenSSL 1.1.1-pre6	Default bit-size based	No	$< 2^{-80}$	1/16
GNU GMP 6.1.2	User-defined t	No	$(1/4)^t$	100% for $t \leq 15$
GNU Mini-GMP 6.1.2	User-defined t	No	$(1/4)^t$	100% for $t \leq 101$
Java 10	User-defined t	Yes (≥ 100 bits)	$< (1/2)^t$	0% for ≥ 100 bits
JSBN 1.4	User-defined t	No	$< (1/2)^t$	100%
Libgcrypt 1.8.2	User-defined t	No	Not given	1/1024[†]
CryptoJS 3.1.4	User-defined $t \leq 100$	No	Not given	100%
LibTomMath 1.0.1	User-defined $t \leq 256$	No	$(1/4)^t$	100%
LibTomCrypt 1.18.1	User-defined $t \leq 256$	No	$(1/4)^t$	100%
WolfSSL 3.13.0	User-defined $t \leq 256$	No	$(1/4)^t$	100%
Bouncy Castle C# 1.8.2	User-defined t	No	$(1/4)^t$	$(1/4)^t$
Botan 2.6.0	User-defined t	No	$\leq (1/2)^t$	$(1/4)^t$
Crypto++ 7.0	2 or 12	Yes	Not given	0%
GoLang 1.10.3	User-defined t	Yes	$< (1/4)^t$	0%
GoLang pre-1.8	User-defined t	No	$< (1/4)^t$	100% for $t \leq 13$

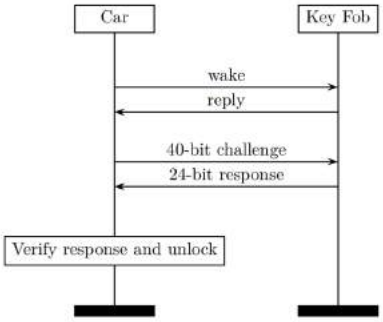
[†] When calling the `check_prime` function as opposed to `gcry_prime_check` (or calling `gcry_prime_check` in versions prior to 1.3.0).

These are fantastic and very surprising results that should radically change how we approach and implement primality testing from now on.

It's impressive that one of the most basic requisites for modern cryptography can be fooled in such a brutal way.

Fortunately, the authors offer a glimmer of hope in the form of the Baillie-PSW primality test, which they conjecture to be robust against adversarial attacks like the ones they present in here and, at the same time, efficient.

Our second piece of recommended reading is titled Fast, Furious and Insecure: Passive Keyless Entry and Start In Modern Supercars, and has been covered in news media all across the World as the latest Tesla hack, although it may affect other companies as well such as McLaren, Karma and Triumph.



Tesla has recently been short of good news, after a series of twitter tirades and some odd behaviour by Elon Musk has sent the stock value down repeatedly.

This piece of news will not contribute to Musk well known sleeping problems, but at least the seemed to have been more serious and responsive in their reaction to the discovery that other car manufacturers.

The KU Leuven team behind this work has received $10,000 as part of Tesla's bounty program.

At the core of this SNAFU is the use of an old, small and insecure proprietary cipher called DST40 that was already broken pretty badly in 2005.

Currently, the only available countermeasure for Tesla S owners is to disable passive entry and enable the pin to drive feature.

We were fortunately enough to capture the very moment Elon Musk decided in favour of using the DST40 cipher to protect Tesla cars.

The authors first publicly presented their findings during the CHES 2018 rump session, in Amsterdam.

Open Positions

Please send us any employment opportunities you may want to publicize in the newsletter.

- Lecturer or Senior Lecturer in Cyber Security (2 positions), at the Department of Computer Science, Electrical and Electronic Engineering and Engineering Maths of the University of Bristol. Salary: £36,613-£41,212 (Grade J), £42,418-£47,722 (Grade K), or £50,618-£56,950 (Grade L). These are full-time, permanent positions in a very prestigious UK University that is hiring new staff and reinventing itself after the departure of Nigel Smart. A good destination if Brexit is not a concern for you, for some obscure reason. Deadline for applications is the 31st October. Candidates are particularly sought in the areas of Security of cyber-physical systems, Human factors in cyber security and Software security.

- Lecturer (for the Smart Card and IoT Security Centre), at the very prestigious Information Security Group of Royal Holloway, University of London. The position is based at Egham and the starting salary is £42,926 to £50,811 per annum - including London allowance. This position is also full-time and permanent. Deadline for applications is the 30th September.

- Full Professor of Ubiquitous Computing at TU Wien (Vienna University of Technology). For a start in October 2019, and with a deadline of 22 October 2018, this is an excellent opportunity at the Faculty of Informatics.
  They want somebody working on "next generation ubiquitous computing systems and their application in authentic real world settings. Particular research topics of interest include sensor-rich environments; interactive and smart spaces; new interaction paradigms; Internet of Things; mobile and context-aware computing; awareness and privacy; and tangible, situated and embodied interaction." Salary starts at €70K. For more info, check `https://goo.gl/5FUzSt`

- Professor of Cybersecurity at the College of Engineering, Mathematics and Physical Sciences of the University of Exeter. Full time and permanent position, stating at around £65,000.
  Exeter is a very good UK University, belonging to the Russell Group, that has arrived late to cybersecurity research and has been unsuccessful for a while despite its best efforts, to hire anybody for leading its new and coming group. This may be a good opportunity, again if you are Brexit-neutral and like Devon. Deadline for applications is the 30th September.

For other interesting positions all across Europe, please check the recently revamped "Researchers in Motion" portal at `https://euraxess.ec.europa.eu/`.

It currently has close to 80 open positions in computer security and related areas, including in Poland, the UK, Finland, Slovenia, Italy, Norway, Switzerland, and even in Spain!

Welcome

Proposals for STSMs

By now, you should be already familiar with what Short Term Scientific Missions (or STSMs, for short) are.

Please make your willingness to receive STSMs proposals known by sending me an email. Take into account that STSMs will be more competitive in this last period of the Action.

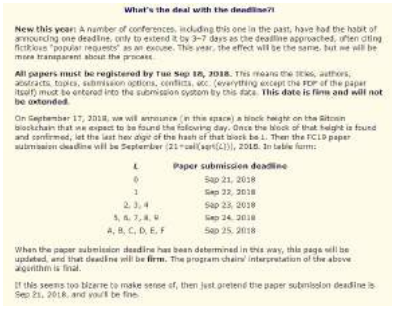
Until I do not have any more, I'll just publish mine:

- I will be very happy to receive anyone interested in investigating randomness generation and testing, particularly on constrained, embedded, IoT devices.

Event calendar

The always exotic Financial Cryptography Conference will take place this year in St. Kitts.

The deadline for paper submission has created some controversy, particularly within the numerous members of the crypto community that have developed uncontrollable allergic reactions and/or spams to the word 'blockchain' as it will depend on the value of a block on the bitcoin blockchain.


What's the deal with the deadline?!

New this year: A number of conferences, including this one in the past, have had the habit of announcing one deadline, only to extend it by 3–7 days as the deadline approached, often citing fictitious "popular requests" as an excuse. This year, the effect will be the same, but we will be more transparent about the process.

All papers must be registered by Tue Sep 18, 2018. This means the titles, authors, abstracts, topics, submission options, conflicts, etc. (everything except the PDF of the paper itself) must be entered into the submission system by this date. **This date is firm and will not be extended.**

On September 17, 2018, we will announce (in this space) a block height on the Bitcoin blockchain that we expect to be found the following day. Once the block of that height is found and confirmed, let the last hex digit of the hash of that block be L. Then the FC19 paper submission deadline will be September (21+sell(sqrt(L))), 2018. In table form:

L	Paper submission deadline
0	Sep 21, 2018
1	Sep 22, 2018
2, 3, 4	Sep 23, 2018
5, 6, 7, 8, 9	Sep 24, 2018
A, B, C, D, E, F	Sep 25, 2018

When the paper submission deadline has been determined in this way, this page will be updated, and that deadline will be **firm.** The program chairs' interpretation of the above algorithm is final.

If this seems too bizarre to make sense of, then just pretend the paper submission deadline is Sep 21, 2018, and you'll be fine.

For now the only thing I can say is that it will be sometime between the 21st and 25th of September, with the probability severely skewed in favour of the 24th or 25th.

The organisers helpfully added "If this seems too bizarre to make sense of, then just pretend the paper submission deadline is Sep 21, 2018, and you'll be fine."

The 'IoT Autentication 2018' Conference will take place in Melbourne, Australia on November 28-30, 2018.

It will feature invited presentations from Auto-ID Labs, IoT Alliance Australia, IoT (Internet of Things) Security, Prof. Michael Sheng, Prof. Margreta Kuijper, Dr. Omid Kavahei, Prof. Seng Loke,and Prof. Lejla Batina.

The Keynote speaker is Dr. Veena Pureswaran from IBM. If you want to attend, check `http://www.authiot2018.conferences.academy/`.

Eurocrypt 2019 is the 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques.

Eurocrypt is one of the three flagship conferences of the International Association for Cryptologic Research (IACR).

Eurocrypt 2019 will take place in Darmstadt, Germany on May 19-23 2019.

It is organized by the Cryptoplexity group of TU Darmstadt and its deadline is the 4th of October.

Last but not least, another truly interesting event this autumn, on October 10 in Milano.
Joan Daemen, together with Stelvio Cimato, Silvia Mella, and Gilles Van Assche are organizing a one-day workshop on *Advances in permutation-based cryptography* in the center of Milano.

In the last decade it has become clear that permutation-based crypto is highly competitive in terms of performance and resource usage when compared to classical block ciphers and their modes.

The workshop is intended to provide an introduction to the subject for academics (PhD students, Post-Docs and Professors) as well as people from industry and will address cryptanalysis, modes, protocols and implementations in a sequence of talks by top researchers in the domain.

Visit the workshop web at `http://permutationbasedcrypto.org` for the program and the practical details.

See you all back in November!

Best,
Julio Hernandez-Castro