CASA UNIVERSE

THE SECRETS OF HUBA AND THE TRACES OF THE COOKIES

A JOURNEY THROUGH THE FUTURE OF CRYPTOGRAPHY AND THE EXCITING RESEARCH WORLD OF CASA
THE SECRETS OF HUBA AND THE TRACES OF THE COOKIES

A JOURNEY THROUGH THE FUTURE OF CRYPTOGRAPHY AND THE EXCITING RESEARCH WORLD OF CASA
CASA

Cyber Security in the Age of Large-Scale Adversaries

Outstanding scientists within the Cluster of Excellence “CASA - Cyber Security in the Age of Large-Scale Adversaries” research and develop strong and sustainable countermeasures against powerful cyber attackers, with a particular focus on nation-state attackers. Research in CASA is characterized by a highly interdisciplinary approach that examines not only technical issues, but also the interplay between human behavior and IT security. This unique, holistic approach forms the basis for excellent IT security research.

CASA unites four main research areas:

**HUB A** “Future Cryptography”: Researching future cryptography and developing quantum-resistant approaches with provable security.

**HUB B** “Embedded Security”: Tackling the task of strengthening the security of embedded systems at the hardware level by investigating the interaction of security systems with their physical environment.

**HUB C** “Secure Systems”: Developing secure and efficient systems at the software level. Machine Learning is one of the many methods used to explore and expand this field.

**HUB D** “Usability”: Focusing on usable security and privacy and researching the interface between humans and technology.

Each HUB addresses specific major research challenges that have been carefully selected to address security issues critical to the protection against large-scale attackers. The challenges of HUB A are:

**Research Challenge 1**: Cryptography Against Mass Surveillance
**Research Challenge 2**: Quantum-Resistant Cryptography
**Research Challenge 3**: Foundations of Privacy
The winter has been cold and going on for months. Whitfield the fox is hungry and bored. He is naturally drawn to the delicious smell of cookies and lured into an adventure...

A witty fox like Whitfield is very curious about all that can be found out there. Who knows... Cookies might not be the only thing that he brings home.

I wonder what they have baking in the ovens here...
WELCOME TO RESEARCH HUB A
**CHALLENGE 1**
*Cryptography Against Mass Surveillance*
How can we develop new cryptographic solutions that protect against mass surveillance?

**CHALLENGE 2**
*Quantum-Resistant Cryptography*
Can we find practical encryption and signature schemes that offer provable security against quantum computers?

**CHALLENGE 3**
*Foundations of Privacy*
How can we use cryptography to protect our privacy when Big Data is stored in the Cloud?

**CASA BACKGROUND**
CASA stands for ‘Cyber Security in the Age of Large-Scale Adversaries’ and is funded as a Cluster of Excellence (EXC) within the Excellence Strategy of the DFG in Germany. Its goal is to enable sustainable security against sophisticated large-scale attacks. Therefore, an interdisciplinary team explores not only technical, but also social factors and implications. The Cluster of Excellence is located at Ruhr University Bochum.

casa.rub.de
AND THE SMELL SEEMS TO BE COMING RIGHT OUTTA THE WALL. BUT I CAN’T SEE ANY ENTRANCE. MY NOSE NORMALLY DOESN’T LET ME DOWN.

AHA! HERE IS A BACKDOOR - QUITE WELL HIDDEN. AND LUCKY ME HERE ARE THE COOKIES. OH, THANK YOU, WONDERFUL NOSE.

OH, YES!

THE FRONT DOOR IS LOCKED!

OH, YES!

Hey! You!

Hey! You!

HUH?

DID YOU THINK YOU COULD JUST WALK IN HERE AND NICK THE SWEETS FOR TONIGHT’S CELEBRATION WITHOUT BEING NOTICED?

I’M MONI, BY THE WAY. AND IT JUST SO HAPPENS THAT WE WORK ON HIDDEN BACKDOORS IN SOFTWARE AND ELECTRONIC DEVICES HERE AT HUB A.

Ehm, well... I came through the hidden backdoor and I just followed the trace of the cookies.

Do you know the Snowden Documents? They proved that nation states have been exploiting technology to perform mass surveillance on both their own and other states’ citizens. Some of their actions concern the domain of cryptography.

Wow, that’s a big stack of documents. Can you give me the gist?
THE INTELLIGENCE AGENCIES PROACTIVELY HELPED IMPLEMENT WEAK CRYPTOGRAPHIC STANDARDS. THESE TENDED TO REMAIN UNNOTICED, BECAUSE THEY FELL OUTSIDE THE REALM OF TRADITIONAL SECURITY MODELS. PRIVATE COMMUNICATION IS AN ESSENTIAL CIVIL RIGHT AND CRUCIAL FOR AN OPEN SOCIETY. THUS, RESEARCH ON BACKDOOR-FREE CRYPTOGRAPHY IS OF GREAT IMPORTANCE — AND GREAT FUN.

TO BE VERY HONEST WITH YOU, I ONLY CAME FOR THE DELICIOUS TREATS. BUT NOW I HAVE A FEW QUESTIONS AND WANT TO LEARN MORE ABOUT WHAT YOU PEOPLE ARE DOING HERE AT HUB A OF CASA.

WITH PLEASURE! YOU HAVE ENTERED THE CHALLENGE 1 BUILDING, HERE YOU WILL FIND THE FIRST OF THE THREE HUB A CHALLENGES. WE HAVE THREE KEY OBJECTIVES HERE:

1 We will study on how to guarantee that cryptographic standards are backdoor free.

2 We will study past and ongoing cryptographic standards to identify adversarially planted backdoors.

3 We will develop novel approaches for safe parameter generation that can provably withstand parameter subversion attacks and backdoors.

WOW, THERE IS QUITE A LOT ON YOUR LIST! HOWEVER, I AM NOT AN EXPERT. WHAT ARE YOU CELEBRATING TONIGHT, BY THE WAY?

YOU WILL SEE LATER. BUT FOR NOW, KEEP YOUR PAWS AWAY FROM THE COOKIES, OK?

NOW, THAT YOU’VE SNUCK IN... LET ME SHOW YOU WHY I’M SENSITIVE TO THE SUBJECT OF BACKDOORS.

GREAT, MY EARS ARE PRICKED.

CASA WIKI

Backdoors allow access to computer systems without the owner’s permission. They can result from faulty programming or be intentionally built into software and hardware.

Cryptography is about secure electronic communication in the presence of malicious third parties. The most commonly used cryptography is encryption and signatures.

Cryptographic standards are technical standards that help to maximize the compatibility, interoperability, and security of encryption.
BACKDOORS ALLOW YOU TO GAIN ACCESS TO A SYSTEM BY BYPASSING THE NORMAL AUTHENTICATION PROCESS OR CRYPTOGRAPHY. DELIBERATELY WEAKENED ENCRYPTIONS ARE OF GREAT INTEREST IN POLITICAL DISCUSSION ON LAW ENFORCEMENT.

THE DESIGN OF SUCH BACKDOORS IN (SYMMETRIC) CRYPTOGRAPHIC PROTOCOLS HAS A LONG HISTORY AND IS A PRESSING RESEARCH TOPIC.

NOW I UNDERSTAND THE PRACTICAL RELEVANCE OF YOUR WORK. IT'S ABOUT THE FUNDAMENTAL TRUSTWORTHINESS OF SYSTEMS.

A Long Disreputable Story
Among the most famous examples are the block cipher DES, for which the key size was deliberately weakened to 56 bits, and the pseudorandom number generator Dual EC DRBG, which was equipped with a backdoor – accessed through a specific selection of its parameters.

IT LOOKS PRETTY SECURE TO ME.

IT DOES! BUT IN BOTH CASES, WHAT LOOKED SECURE COULD EASILY BE UNDERMINED.

HA! THEY LEFT A BACKDOOR!

THAT'S AS EASY AS π.
NOW LET'S GO EXPONENTIAL!

WEAK ENCRYPTION IS LIKE FANCY GIFT WRAPPING. IT LOOKS PRETTY, BUT DOES LITTLE FOR THE SECURITY OF THE CONTENT. LIKE A HOLE IN A FENCE, WEAK ENCRYPTION CAN BE USED OR ABUSED.

SURE, NOT ONLY THE GOOD GUYS CAN USE IT. AND WHAT ABOUT PRIVACY IN GENERAL?
In 2015, WikiLeaks presented evidence that the NSA had been wire-tapping the mobile phone of former chancellor Angela Merkel since 2002. The spying operation was also not restricted to her: the phones of 125 high-ranking politicians and advisors were also tapped.

The encryption algorithm GeA-1 was implemented in mobile phones in the 1990s to encrypt data connections. Since then, it has been kept secret. Although the vulnerability is still present in many modern mobile phones, according to the researchers, it no longer poses any significant threat to users. GEA-1 is so easy to break that it must be a deliberately weak encryption built in to provide a backdoor to mobile phone data.

A research team from CASA with colleagues from France and Norway, has analyzed the algorithm and has come to the following conclusion: GeA-1 is so easy to break that it must be a deliberately weak encryption built in to provide a backdoor to mobile phone data. However, the team has not yet discovered the weaknesses that are supposed to remain hidden.

Hey team, this could be interesting for us.

Although the vulnerability is still present in many modern mobile phones, according to the researchers, it no longer poses any significant threat to users.
A backdoor allows an attacker who knows of the weakness to break the encryption. A backdoor reduces the size of the set of possible keys that could be used to unlock the encryption.

Weak design can make it more than one million times faster to guess the correct key. Now just imagine an old weak design in the face of increasing computing power!

Oh, no – it actually fits.

Now, that we've discovered the backdoor, it's time to fix it. Unfortunately, this is often a lengthy process and requires more than a simple patch.

Let's have a look at the screen.

Symmetric Encryption uses the same key for encryption and decryption. It is well suited for bulk encryption as it is fast and needs few resources.

NIST is the US-based National Institute of Standards and Technology.

Good Symmetric Encryption
- Everything is known about the algorithm but the key.
- Without the key, no information about the plaintext can be gained from the ciphertext.
- The number of keys is too large to be guessed.
In the concrete case of GEA-1, we initiated a responsible disclosure process. Through the mobile phone association GSMA, the Bochum based group contacted the manufacturers before publishing their data to give them the opportunity to remove GEA-1 through software updates. In addition, they advocated for the removal of the successor GEA-2. ETSI, the organization responsible for telecommunications standards, decided that henceforward, smartphones should no longer support GEA-2.

Why Transparency helps Security

In general, cryptographic algorithms should not be developed in secret and with unclear design components. NIST has lead the way in their process of selecting the Advanced Encryption Standard (AES) and upcoming post-quantum algorithms: using open design competitions followed by public discussions and analysis. It sounds contradictory but security gets better the more it is developed in public.

Good Job, Team!

Before you dive into Challenge 2, here’s the recipe for the cookies. See you later at the party!

Thanks!

I wonder if they can get rid of this sneaky backdoor problem... I wish them all the best.

Wow, this is a pretty fast ride. What will come next?
HuH, THIS ROOM HAS HARDLY ANY CORNERS.

HUH, THIS ROOM HAS HARDLY ANY CORNERS.

YEP, THAT’S TRUE. IT SUITS OUR WORK. WE FIND OURSELVES IN ELLIPTIC CURVES A LOT. HI, I AM SHAHI.

YEAP, THAT’S TRUE. IT SUITS OUR WORK. WE FIND OURSELVES IN ELLIPTIC CURVES A LOT. HI, I AM SHAHI.

WOW, THEN IT’S A COOL DESIGN BY THE ARCHITECT. MY NAME IS WHITFIELD.

WOW, THEN IT’S A COOL DESIGN BY THE ARCHITECT. MY NAME IS WHITFIELD.

LET’S DIVE RIGHT INTO THE TOPIC. I WAS INFORMED YOU WERE COMING!

LET’S DIVE RIGHT INTO THE TOPIC. I WAS INFORMED YOU WERE COMING!

SO, THERE IS ONE THING WE THINK A LOT ABOUT HERE AT CHALLENGE 2. CERTAIN CRYPTOGRAPHIC SCHEMES ARE THE BASIS OF NOTHING LESS THAN THE SECURITY OF OUR CURRENT DIGITAL COMMUNICATION SYSTEM. CONSEQUENTLY, IT’S SUPER IMPORTANT TO MAKE THESE SCHEMES WATERTIGHT.

FOR EXAMPLE, ASYMMETRIC ENCRYPTION AND DIGITAL SIGNATURES. THEY DERIVE THEIR SECURITY FROM THE FACT THAT IT IS HARD TO FACTOR LARGE INTEGERS AND TO COMPUTE SO-CALLED DISCRETE LOGARITHMS OVER ELLIPTIC CURVES.

WHAT KIND OF SCHEMES?

WHAT KIND OF SCHEMES?

HOWEVER, ALREADY IN THE 1990S, PETER SHOR PUBLISHED A SEMINAL PAPER SHOWING THAT THESE PROBLEMS BECOME FAIRLY EASY TO SOLVE FOR ATTACKERS Equipped WITH A LARGE QUANTUM COMPUTER. THAT WOULD MEAN ALL PERSONAL SECRETS AND DATA – BOTH PAST AND PRESENT – WOULD IMMEDIATELY BECOME PUBLIC!

OH NO! ALL OUR SECRETS ARE AT RISK!

OH NO! ALL OUR SECRETS ARE AT RISK!

WELL, THAT DOESN’T SOUND TOO PROMISING...
A **Quantum Computer** is a computer that exploits the laws of quantum mechanics in order to solve certain problems faster. For example, it could quickly break all currently deployed asymmetric cryptography. Scalable quantum computers do not yet exist but the larger research community is making great progress in building them.

**Post-Quantum Cryptography** refers to cryptographic systems that can withstand attackers equipped with quantum computers.

**Shor's algorithm** is an algorithm designed by Peter Shor in 1994 that can efficiently factor large integers and compute discrete logarithms over elliptic curves: Thus, essentially providing the framework to break all currently deployed public-key cryptography schemes.

**Asymmetric Cryptography** uses a public key for encryption and a private key for decryption. It is mostly used for key agreement between parties that have not previously met.
THE CHALLENGE IS TO BUILD SUITABLE REPLACEMENTS FOR TODAY'S SCHEMES THAT CAN RESIST ATTACKS THAT MAKE USE OF QUANTUM COMPUTING POWER. LET ME SHOW YOU OUR MAIN RESEARCH PROJECT. MY COLLEAGUE JOAN IS THE PERFECT PERSON TO DECRYPT OUR WORK FOR YOU.

FUNNY, YOU STILL WORK ON CHALK BOARDS?! I DIDN'T EXPECT THAT.

RESEARCH PROJECT

Post-Quantum Cryptography

HEY JOAN, WE HAVE A VISITOR. THIS IS WHITFIELD. COULD YOU EXPLAIN A BIT ABOUT YOUR RESEARCH TO HIM?

SURE! GREAT TO HAVE YOU VISIT US HERE. SO, TO TRY AND PUT IT SIMPLY, AS YOU HAVE SEEN, THE FACTORING-RACE IS GOING TO BE DOMINATED AND REVOLUTIONIZED BY THE QUANTUM COMPUTER SOON. THEREFORE, WE NEED TO DEVELOP A MATHEMATICAL PROBLEM WHICH IS HARD TO SOLVE, EVEN FOR QUANTUM COMPUTERS. THE ONE WE CHOSE IS BASED ON LATTICES.
A lot of post-quantum cryptography is based on mathematical lattices. A lattice is a discrete subgroup of a multi-dimensional space.

PuH – I am sorry, but is there any other way to explain this? I am just a little fox and not exactly a math genius...

**Lattice-Based Cryptography**

Picture a chain-link fence – this is a two-dimensional lattice. The lattice points are the intersection points of the chain-links in the fence (we call these links vectors). It is extremely mathematically demanding to try to find a ‘short vector’ in a high-dimensional lattice; i.e., a chain link close to the origin of the graph.

If I put a red nose on one of these short chain-link lattice vectors, it might take you a while to find it, but eventually if you were patient enough you would succeed. In a high-dimensional lattice, it is mathematically very difficult and time consuming to find such a vector – even for a quantum computer. Post-quantum secure cryptography is based on the difficulty of finding short vectors in high-dimensional lattices.

This is only three dimensions. Our new post-quantum cryptography relies on the difficulty of finding one specific intersection in a 500-dimensional lattice! Holy guacamole! This is impressive.
SO, WE WILL ONLY NEED THIS IN SOMETHING LIKE 15 YEARS TO PROTECT OUR COMMUNICATION?

NO! WE NEED TO USE THIS NOW, SO THAT TODAY’S COMMUNICATION REMAINS PRIVATE EVEN IN 15 YEARS.

THAT’S WHY IMMEDIATE ACTION IS REQUIRED: OUR DATA ENCRYPTED TODAY STILL HAS TO BE SECURE IN 10 TO 20 YEARS!

REAL LIFE STORY

The American National Institute for Standards and Technology (NIST) has recognized the risks for secure data encryption posed by quantum computers and, in 2016, started a process to standardize post-quantum cryptography. 69 proposals were submitted from the research community worldwide which were evaluated in a public process. In July 2022, four of these were selected to be standardized by NIST: three digital signature schemes and one public-key encryption system. CASA researchers contributed to three of the four systems: CRYSTALS-Dilithium, SPHINCS+ and CRYSTALS-Kyber.

WHAT A GREAT SUCCESS FOR CASA! AND SUCH IMPORTANT WORK. CONGRATULATIONS!

THANK YOU!
WE ARE VERY PROUD! ALL SUBMISSIONS WERE SCRUTINIZED VERY CAREFULLY. SOME, HOWEVER, WERE NOT AS SAFE AS THE APPLICANTS THOUGHT.

A little over four hours after NIST published the specifications of all submitted algorithms, Lorenz Panny, at the time Ph.D. student at TU Eindhoven, already presented a full break of the candidate “Guess Again”. The attack software required less than 30 lines of code and is called “guessed once”.

UH, NICE, THE NEW NIST PROPOSALS ARE ONLINE! I’LL JUST HAVE A LOOK AT ONE OF THEM WHILE HAVING MY MORNING COFFEE.

NOW I UNDERSTAND WHY YOU ARE CELEBRATING!

TAKE THIS HAT FOR THE PARTY LATER. I THINK THAT NOW YOU HAVE GOT A PRETTY GOOD OVERVIEW OF WHAT WE DO AT CHALLENGE 2. I KNOW, IT IS SUCH A HUGE TOPIC IN SUCH A SHORT TIME. BUT YOU CAN ALWAYS COME BACK AND LEARN MORE.

WE’RE ALWAYS HAPPY TO GIVE VISITORS A GLIMPSE INTO OUR EXCITING RESEARCH!

THANK YOU! I AM NOT USED TO THAT MUCH THEORY THOUGH I DEFINITELY LEARNED A LOT.
WHOW! THAT WAS SOME PRETTY COMPLEX AND THEORETICAL STUFF. I'M GLAD FOR THIS LITTLE BREAK IN THE CHAIRLIFT.

BUT I WONDER HOW THIS IS ALL REALLY USED AND WHAT EFFECT IT HAS ON MY DAILY LIFE?

THEY HAVE CCTV HERE?

As already mentioned intelligence services perform mass surveillance...

THAT DOESN'T FEEL NICE.

...on both their own and other states’ citizens.

OH, A LETTER! FOR ME?

WHAT?! IT'S FROM MY AUNTY!

META DATA
Sender: Aunty Fox
Receiver: Whitfield Fox
Date sent: 4 days ago
Date received: Right now
Carrier Material: Paper
Format: SnailMail
Transferred by: US Postal
Volume: 3 pages
Language: Fox-Vox-en-us
Encryption: Envelope

Even if the content of a message is encrypted, the sender and recipient can be identified during transmission.

This so-called “meta data” contains lots of valuable information.
Dear Whitfield!
Since you are at CASA, I thought this might interest you: I just received an encrypted e-mail from your cousin in Australia. He’s a journalist, as you know, and he says that the government has been spying on him. Maybe your new friends know how to help him? Love from your concerned Aunty

Also on your way to the party? So sorry for the rough welcome to Challenge 3. We just want to convey how important privacy is. We also work on finding solutions here, with a main goal being the creation of a secure model for cryptographic key agreement.

Yes! The so called "TOR" Network, or "Onion Routing", provides a solution.

We want to create a fast and simple model, made up of multiple, secure nodes. And finally, we want to implement it in a way that anyone can use it. Here's the idea it's based on...

An Onion?

TOR is the acronym for “The Onion Router”. The message including meta data is encrypted with three layers. Let's take a closer look...

In 2016, Paul Farrell researched detention camps for refugees on the island Nauru, where the poor, inhumane conditions have been harshly criticized. Based on the government’s Data Retention Act laws, the Australian Police were legally allowed to obtain and study all of his communication; under the grounds of identifying his sources and procuring information about potential whistle blowers. They also collected the meta data from Farrell’s mobile phone and analyzed data from his e-mail account.

If such an invasion of private space is allowed in democracies, what kind of things are happening in authoritarian regimes?

Dear Whitfield!
Since you are at CASA, I thought this might interest you: I just received an encrypted e-mail from your cousin in Australia. He’s a journalist, as you know, and he says that the government has been spying on him. Maybe your new friends know how to help him? Love from your concerned Aunty

Also on your way to the party? So sorry for the rough welcome to Challenge 3. We just want to convey how important privacy is. We also work on finding solutions here, with a main goal being the creation of a secure model for cryptographic key agreement.

Yes! The so called "TOR" Network, or "Onion Routing", provides a solution.

We want to create a fast and simple model, made up of multiple, secure nodes. And finally, we want to implement it in a way that anyone can use it. Here's the idea it's based on...

An Onion?

TOR is the acronym for “The Onion Router”. The message including meta data is encrypted with three layers. Let's take a closer look...

In 2016, Paul Farrell researched detention camps for refugees on the island Nauru, where the poor, inhumane conditions have been harshly criticized. Based on the government’s Data Retention Act laws, the Australian Police were legally allowed to obtain and study all of his communication; under the grounds of identifying his sources and procuring information about potential whistle blowers. They also collected the meta data from Farrell’s mobile phone and analyzed data from his e-mail account.

If such an invasion of private space is allowed in democracies, what kind of things are happening in authoritarian regimes?
The message is sent to an entry node of the network. This one peels off one layer of encryption and sends it to a relay node. This one does the same and sends it to the exit node. Here the last encryption layer is removed and the message is redirected to the recipient. None of the nodes has the full information about the sender or the receiver.

**Entry node**

**Relay node**

**Exit node**

**Message**

**Entry node key**

**Relay node key**

**Exit node key**

OK, NOW I UNDERSTAND THE COMPARISON WITH AN ONION. EVERY LAYER IS AN ADDITIONAL ENCRYPTION.

LIKE YOUR NAMESAKE WHITFIELD DIFFIE, YOU SEEM TO BE A CLEVER ONE. THE DECISION TO HAVE THREE NODES WITHIN A TOR SYSTEM HAS BEEN MADE TO KEEP A GOOD BALANCE BETWEEN SPEED AND SAFETY.

As it takes time to peel an onion, Tor is slower than regular Internet traffic - which means it’s not much fun gaming via Tor. It is important to know that Tor is also not 100% secure, as so called “traffic correlation attacks” can endanger the anonymity of Tor users. These attacks try to observe as many Tor nodes as possible, in order to find patterns in the timing, size or delay of incoming and outgoing communication. Such attacks can utilize machine learning to reveal the user's information.

OMG! THAT'S MORE THAN FIVE EYES. MORE LAYERS COULD BE A SOLUTION, BUT IT MAKES THINGS EVEN SLOWER.

Even hidden nodes can be detected. Some Tor-specific code can be recognized using deep package inspection if a message is sent. Once the hidden node is known, it can be blocked. For example, China blocks all attempts to access entry nodes from within the country.
Defenses

So path “A” depicts traditional Onion Routing and uses only three different nodes. Our solution is path “B”: it takes a longer route over more nodes and therefore is slower. But the network plays a role as well. With each additional node, the amount of unique paths a message can take grows exponentially—while also increasing the effort required to simply observe each of the Tor nodes in the chain.

RESULT: The letter came faster over path “A”, but is ripped open. Via path “B” it took longer, but the letter is still encrypted. I’d go with “B” then.

Commander! We can’t find our ships due to our secure routing!

Layer 1

Fun Fact

Despite its apparent enmity with Tor, the U.S. government played a pivotal role in its creation. Onion Routing, in its most basic form, was developed by the U.S. Navy in the 1990s to protect intelligence communications. Also, the U.S. Department of State Bureau of Democracy, Human Rights and Labor is among Tor’s financial backers.

Let’s get the crypto-party started!

I hope that you are able to take something home with you—and I mean more than just a cookie!
CHEERS TO YOU! YOU HAVE DONE A GREAT JOB WITH LISTENING AND UNDERSTANDING OUR WORK!

WELL, I GUESS IT’S PROBABLY JUST THE TIP OF THE ICEBERG, ISN’T IT?

OH, AND BY THE WAY, I GOT THIS LETTER FROM MY AUNTY. SHE IS ASKING FOR SOME ADVICE.

LET ME SEE...

HMM. I THINK YOUR COUSIN ALREADY MADE THE FIRST STEP BY USING ENCRYPTED E-MAIL. HE SHOULD USE A TOR BROWSER AND SECURE MESSENGER AS WELL. EVEN NOW, CERTAIN SECURITY AND PRIVACY MECHANISMS CAN BE VERY INCONVENIENT TO USE - BUT OUR COLLEAGUES AT HUB D ARE WORKING ON THAT! MAYBE YOU SHOULD VISIT THEM SOMETIME TOO.

HEY, YOU TWO! STOP TALKING AND JOIN OUR BREAK-DANCE BATTLE!

IT SOUNDS REALLY TEMPTING, BUT I’LL HAVE TO PASS. MY AUNTY IS PROBABLY STARTING TO GET REALLY WORRIED.

SO, NOW I HAVE A BAG FULL OF COOKIES, MY HEAD FULL OF KNOWLEDGE AND EVEN SOME ANSWERS AND ADVICE FOR AUNTY. SHE WILL BE PROUD. AFTER ALL, I HAVE LEARNED THAT SECURITY IS NOT A STATE BUT A CONTINUOUS PROCESS. YOU HAVE TO TAKE FUTURE POSSIBILITIES INTO ACCOUNT. IT’S GOOD THAT THE PEOPLE AT CASA ARE TAKING CARE OF IT.
CASA: Cyber Security in the Age of Large-Scale Adversaries was established in 2019. It is the only Cluster of Excellence in the field of computer security in Germany. CASA is funded by a grant from the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) worth about 30 million Euros, which ensures excellent research conditions.

CASA brings together a core group of principal investigators, chosen with a strong focus on security and privacy, with selected top-level researchers from highly relevant neighboring disciplines. The team covers the full scope needed to tackle the challenging research problems in modern computer security; namely computer science, mathematics, electrical engineering, and psychology.

CASA is hosted by the Horst Görtz Institute for IT Security (hgi.rub.de/en), a pioneering research center in Germany. Furthermore, CASA collaborates strongly with the Max Planck Institute for Security and Privacy in Bochum (mpi-sp.org) and several other institutes and universities.

What is a “Cluster of Excellence”? With the funding line “Clusters of Excellence”, internationally competitive research centers at universities or university alliances in Germany are provided with project-based funding for a period of 7 years. Within the clusters, scientists from different disciplines and institutions work together on a research project. The funding gives them the opportunity to concentrate intensively on their research goal, to train young scientists and to recruit international top researchers.

casa.rub.de

### TECHNICAL BACKGROUND

The concepts and methods presented in this comic were developed by researchers involved in the Cluster of Excellence CASA. If you are interested in more details, you can find the original publications online. These scientific papers explain the results in more detail. For many publications we also publish the source code and other research artifacts. Please reach out to us, if you have questions: info@casa.rub.de

### PUBLICATIONS

Christof Beierle, Tim Beyne, Patrick Felke, Gregor Leander: *Constructing and Deconstructing Intentional Weaknesses in Symmetric Ciphers*, CRYPTO, 2022

Christof Beierle, Patrick Derbez, Gregor Leander, Gaëtan Leurent, Håvard Raddum, Yann Rotella, David Rupprecht, Lukas Stennes: *Cryptanalysis of the GPRS Encryption Algorithms GEA-1 and GEA-2*, EUROCRYPT, 2021


CASA HUB A

2nd edition 2023
Copyright 2022
All contents, especially texts and graphics
are protected by copyright. All rights,
including reproduction, publication,
editing and translation, are reserved,
Cluster of Excellence CASA.

Editorial team
Annika Gödde (CASA/Ruhr-Universität Bochum)
Niels Jansen (Ellery Studio)
Eike Kiltz (CASA/Ruhr-Universität Bochum)
Gregor Leander (CASA/Ruhr-Universität/Bochum)
Peter Schwabe (CASA/Max Planck Institute
for Security and Privacy)
Jörg Schwenk (CASA/Ruhr-Universität Bochum)
Christian Mainka (CASA/Ruhr-Universität Bochum)

Ellery Studio
Art Direction and Design: Luca Bogoni
Illustrations: Lucia Cordero,
Hannah Schrage, David Ramirez Fernandez
Project Management: Martin Steffens

Cover image
Hannah Schrage

Printed at
Schmidt, Ley + Wiegandt GmbH + Co. KG,
Lünen, www.slw-medien.de

Published by
CASA: Cyber Security in the Age
of Large-Scale Adversaries
Universitätsstraße 150
44780 Bochum

hgi-presse@rub.de
casa.rub.de

Scan to access the digital version of our comic:
WHAT IS SAFE TODAY MAY BE AN OPEN SECRET TOMORROW. THIS IS ESPECIALLY TRUE IN THE DIGITAL SPHERE: FROM MASS SURVEILLANCE AND POST-QUANTUM CRYPTOGRAPHY TO SAFE ROUTING AND ENCRYPTION.

FOLLOW THE CURIOUS LITTLE FOX WHITFIELD ON HIS CHASE THROUGH HUB A. WILL HE MANAGE ALL THE TWISTS AND TURNS ALONG THE WAY?

FIND OUT MORE!