From Math to the C-Suite

Talking about Enterprise Security in the Quantum Age

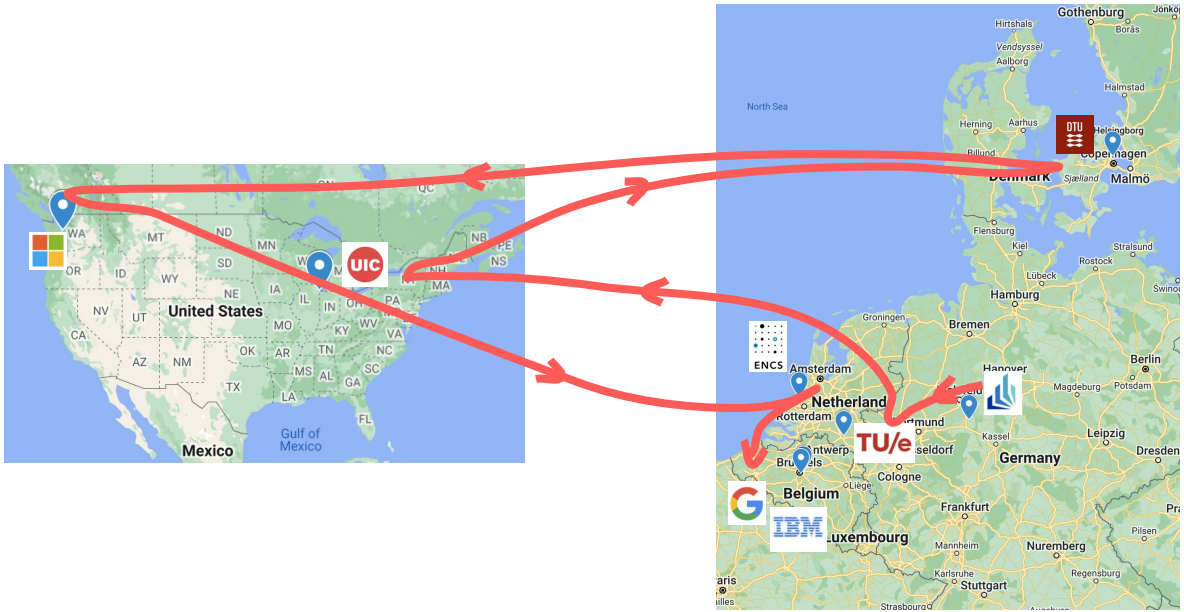
High Tech Women Conference 2024, Darmstadt, 25-Sep-2024

Christiane Peters
cbcrypto.org
https://www.linkedin.com/in/christianepeters/
chrpet@google.com

Disclaimer

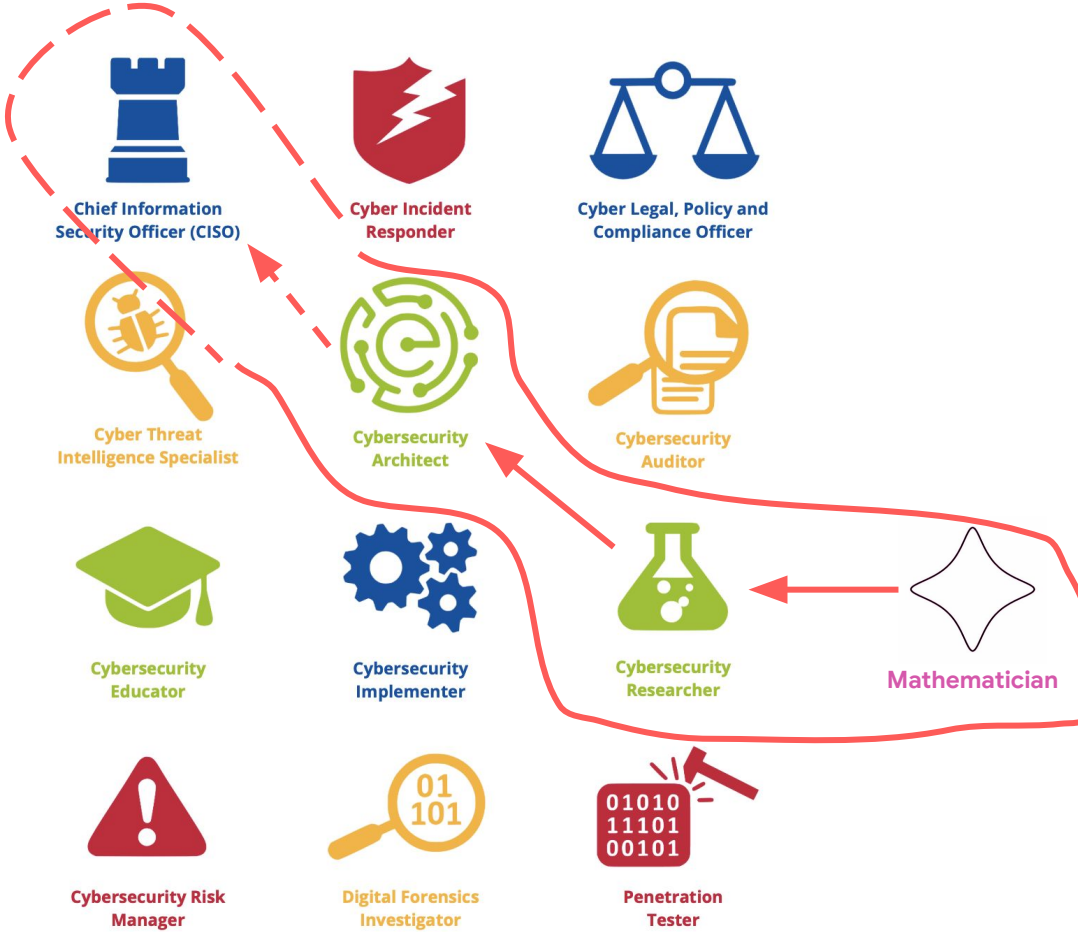
The views and opinion expressed in this presentation belong to the presenter and do not necessarily reflect the position of her employer.

How to move 400 km from Germany to Belgium in 8 years.



Paderborn, DE - Eindhoven, NL - Chicago, IL - Copenhagen, DK - Redmond, WA - The Hague, NL - Brussels, BE

How to move from math to C-level discussions.



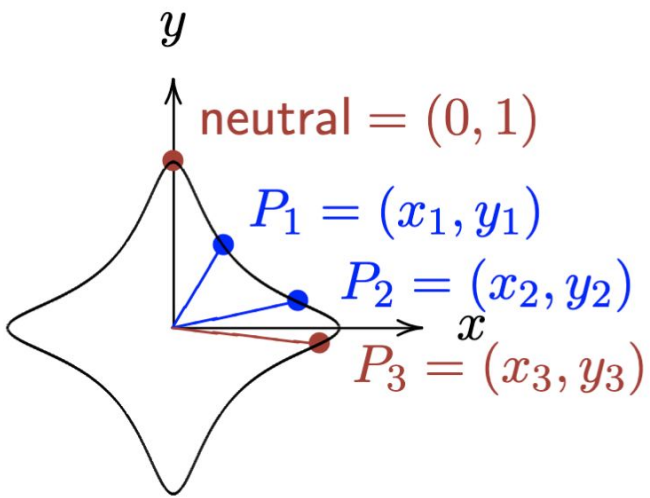
https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

Math

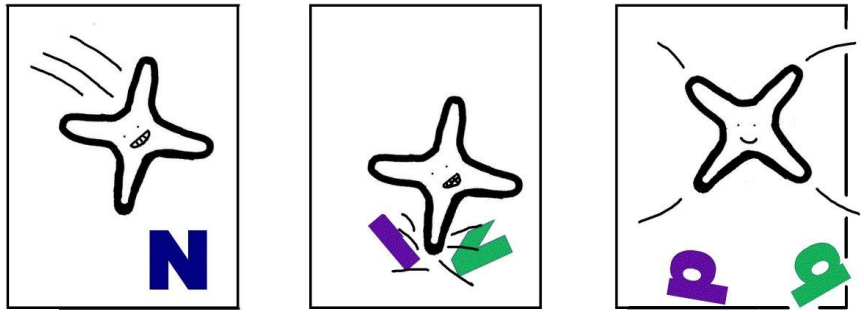
2007

(Twisted) Edwards Curves

Mathematician



https://eprint.iacr.org/2008/013

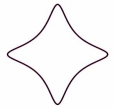


https://eprint.iacr.org/2008/016

“IBM is going to build a large quantum computer in the next 6-10 years”

(and is going to break elliptic-curve cryptography)

2007



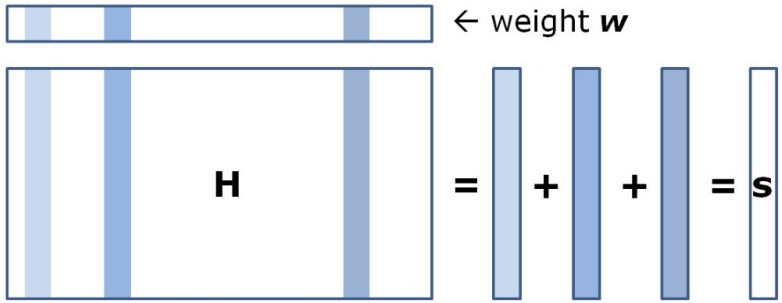
Mathematician

Entering the world of post-quantum cryptography

Attacking and Defending the McEliece Cryptosystem

Together with DJ Bernstein and Tanja Lange, we broke the original McEliece parameters by decrypting a McEliece ciphertext in 14 days on a cluster of 100 computers.

https://eprint.iacr.org/2008/318



Syndrome Decoding Problem

The attack made “headlines” in the Netherlands and internationally

McEliece original system broken

Daniel J. Bernstein, Christiane Peters and I improved an attack on the McEliece cryptosystem which made it feasible to attack the original parame
(from the 1978 paper). We wrote an optimized implementation and used our computers and quite a few more machines worldwide to actually exec
the attack; thanks to everybody who contributed! The attack succeeded in decrypting a challenge ciphertext in 8000 core-days. The paper describi
background appeared at the second PQCrypto workshop.
Christiane gave the presentation, her slides give more details about the actual attack and the computation power used. We intend to put more mate
online once we find the time.

Our press release, October 20th, 2008:

Cryptographers crack internet encryption of the future
A cryptosystem proposed in 1978, one of the leading candidates for "post-quantum cryptography," has been broken by researchers at TU/e.
Physicists have been racing to build quantum computers that would break the public-key cryptosystems used to protect Internet commerce today, s
as RSA and elliptic-curve cryptography. However, quantum computers are not believed to affect the "McEliece cryptosystem" published thirty yea
ago.
Professor Tanja Lange (EIPSI), in a joint paper with her Ph.D. student Christiane Peters and with Professor Daniel J. Bernstein visit
University of Illinois at Chicago, described a way to speed up attacks against the McEliece cryptosystem. The researchers wrote sof

NEWS RELEASE 31-OCT-2008

Eindhoven researchers crack Internet security of the future

Peer-Reviewed Publication

EINDHOVEN UNIVERSITY OF TECHNOLOGY

https://hyperelliptic.org/tanja/press/mceliece.html

ScienceDaily

Your source for the latest research news

Mathematician

New! Sign up for our free **email newsletter**.

S_D Health Tech Enviro Society Quirky

Science News *from research organizations*

Quantum Computers? Internet Security Code Of The Future Cracked

Date: November 1, 2008

Source: Eindhoven University of Technology

Summary: Computer science experts have managed to crack the so-called McEliece encryption system. This system is a candidate for the security of Internet traffic in the age of the quantum computer -- the predicted super-powerful

CONNECT

Lees Pro met een account

Business Maatschappij Tech & Toekomst Carrière

Nieuws • Automatisering Gids +

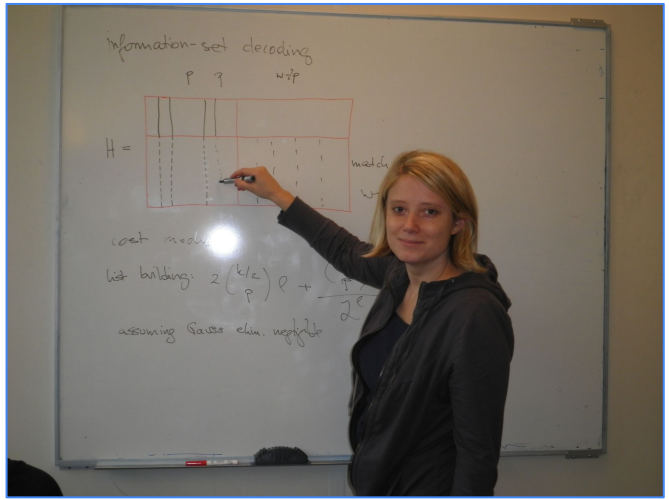
23 oktober 2008 leestijd 1 minuut 0 reacties

TU Eindhoven kraakt zware encryptie

Onlangs is de aanval gelukt met hulp van enkele tientallen gekoppelde

We also proposed new parameters for code-based cryptography

which ended in 2017 in the Classic McEliece submission to NIST's PQC standardization program



Mathematician

Off-Shor

Christiane Peters

Technische Universiteit Eindhoven

JQI/NIST Quantum Information Workshop

October 28, 2010

Classic McEliece

Intro | Comparison | Implementation | Specification | NIST
ISO | Papers | Talks | People | Credits

Dedicated to the memory of Robert J. McEliece, 1942–2019

https://classic.mceliece.org/

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

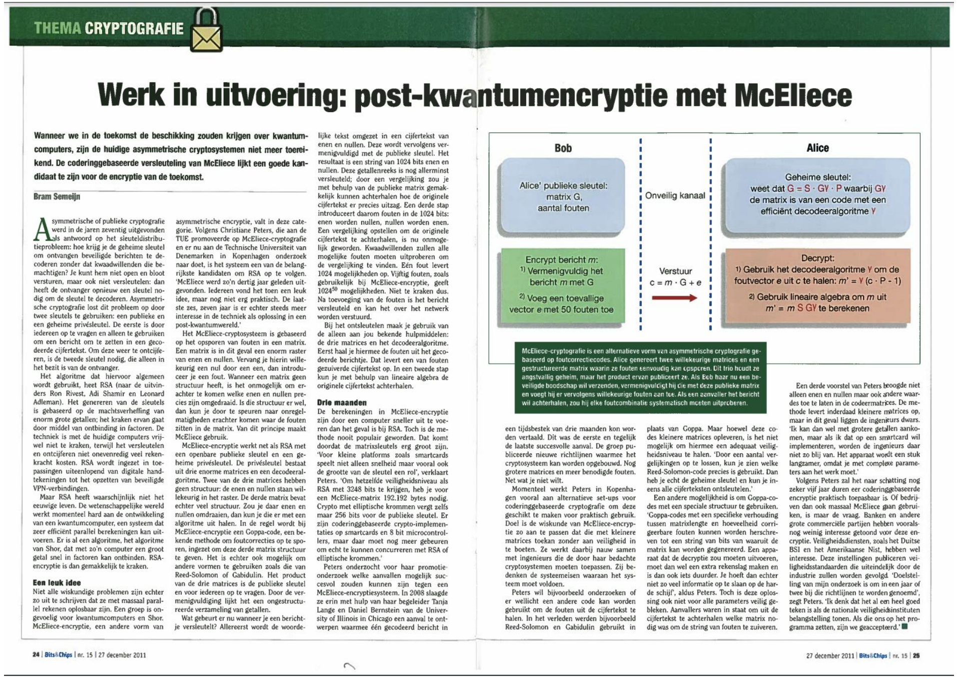
PROJECTS

Post-Quantum Cryptography PQC

https://csrc.nist.gov/projects/post-quantum-cryptography

It was an awesome time

Learn to talk to science journalists


THEMA CRYPTOGRAFIE

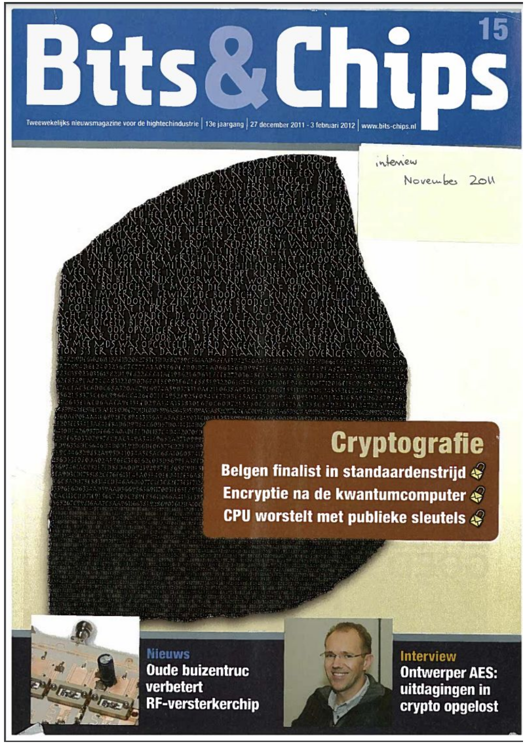
Werk in uitvoering: post-kwantumencryptie met McEliece

Wanneer we in de toekomst de beschikking zouden krijgen over kwantumcomputers, zijn de huidige asymmetrische cryptosystemen niet meer toereikend. De coderinggebaseerde versleuteling van McEliece lijkt een goede kandidaat te zijn voor de encryptie van de toekomst.

Bram Semeijn

24 | Bits&Chips | nr. 15 | 27 december 2011

27 december 2011 | Bits&Chips | nr. 15 | 25



https://bits-chips.nl/

Mathematician

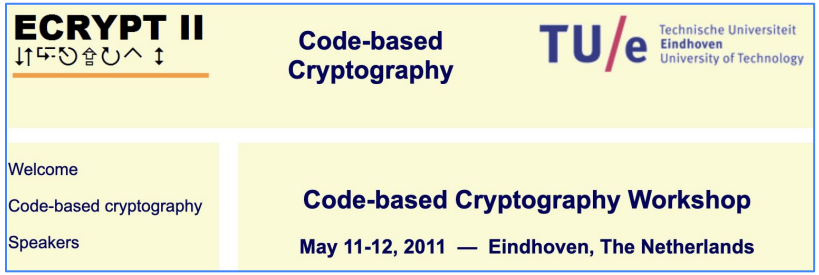
Meet other young women in research

(Google Anita Borg Scholarship 2009)

Consider applying as well: https://buildyourfuture.withgoogle.com/scholarships/

https://googleblog.blogspot.com/2009/05/announcing-2009-anita-borg-scholars-and.html

Bringing Researchers Together



CrossFyre 2011 & 2012

Dagstuhl Seminar 16032 - Privacy and Security in Smart Energy Grid 2016

Mathematician

“Post-Ph.D. Depression”

This quantum computer thing - is it ever gonna happen?

I’m “only a mathematician”

What's the point anyway?

Moving to Industry

2013

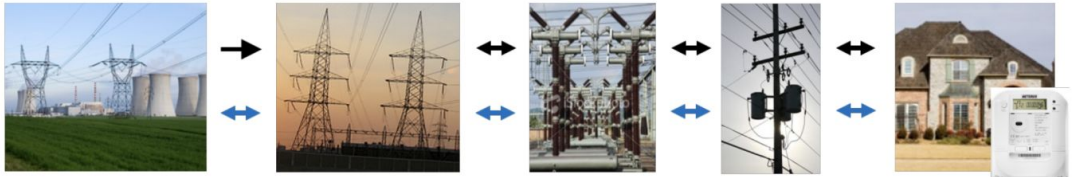
Critical Infrastructure Security Research & Consulting

Cybersecurity Researcher

Smart Grid 101

ENCS

- Energy and information flows in many directions: from generation to grid or building, from utility to customers, etc.



- Utilities collect smart meter data for billing, grid management, etc

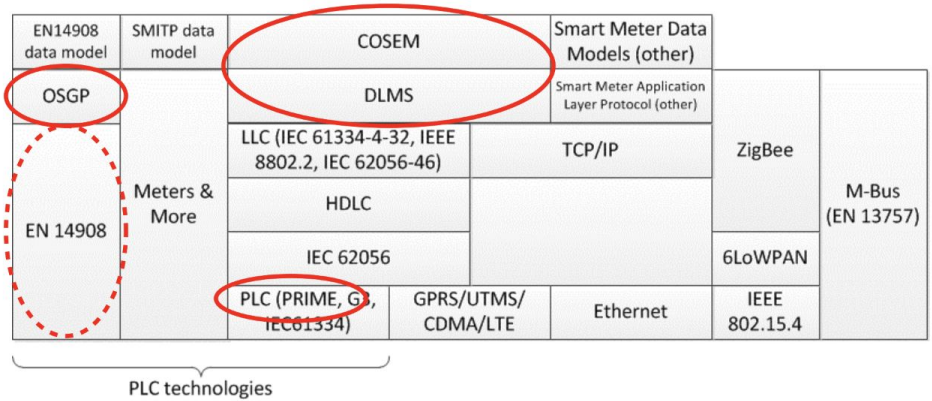
7

Many early smart meter protocols were poor

Cybersecurity Researcher

Smart Meter Protocol Stacks*

ENCS



(* Disclaimer: this is a selection of possible stacks; not complete)

Klaus Kursawe, Christiane Peters. **Structural Weaknesses in the Open Smart Grid Protocol.** Best Paper Award ARES 2015. https://eprint.iacr.org/2015/088

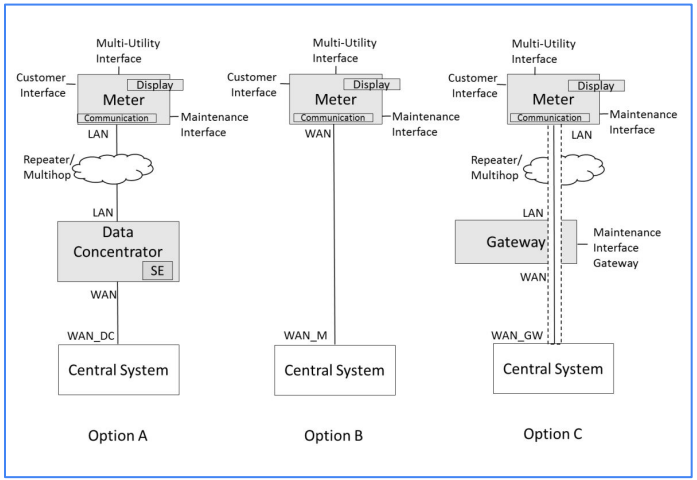
“Attacking and Defending” all over again

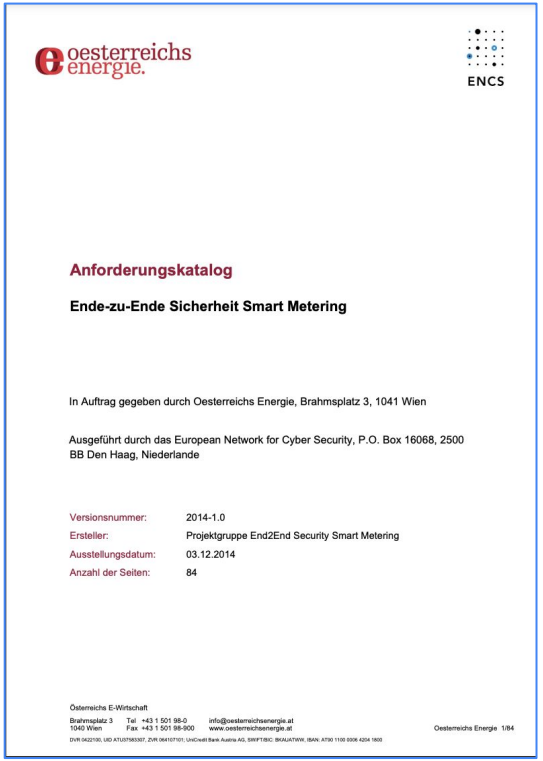
How to make things better?

End-to-end Security Solution Architecture for Smart Meters

2014: EU member states started roll out of smart electricity meters

Working on secure designs for smart grid devices and comms protocols





oesterreichs energie.

ENCS

Anforderungskatalog

Ende-zu-Ende Sicherheit Smart Metering

In Auftrag gegeben durch Oesterreichs Energie, Brahmsplatz 3, 1041 Wien

Ausgeführt durch das European Network for Cyber Security, P.O. Box 16068, 2500 BB Den Haag, Niederlande

Versionsnummer:	2014-1.0
Ersteller:	Projektgruppe End2End Security Smart Metering
Ausstellungsdatum:	03.12.2014
Anzahl der Seiten:	84

Is there more out there?

Moving to Enterprise Security

2015

Working with Financial Services Organizations on Getting Cryptography Right

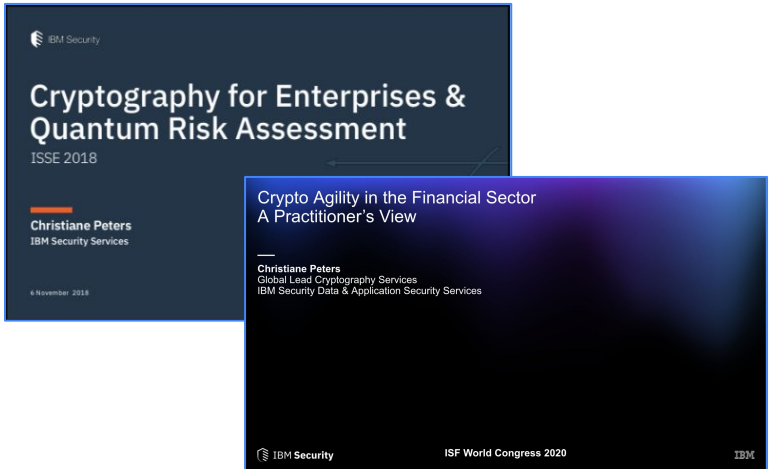
Cybersecurity Architect

Christiane Peters, Tiago Teles. **Implementing a Crypto Services Strategy at ABN AMRO Bank**. Real World Crypto 2020. New York, NY, United States.

IBM Global Cryptography Services Lead

Cybersecurity Architect

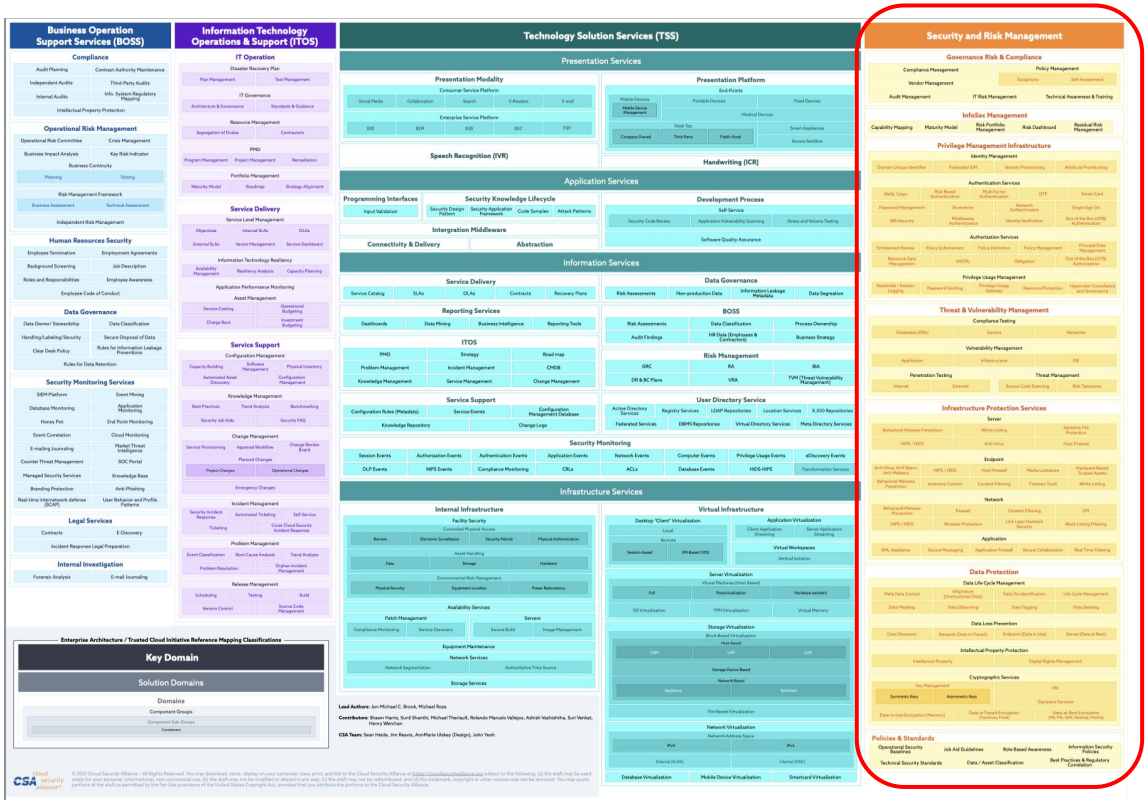
I defined and led the **Cryptography Services consulting & system integration practice** as part of the Global IBM Security Services Center of Competence.



https://securityintelligence.com/posts/how-to-make-cryptography-services-work-for-your-organization/

Going beyond Cryptography

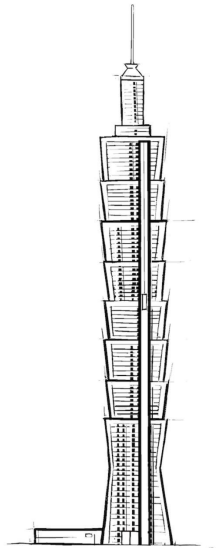
Cloud Security Alliance - Enterprise Reference Architecture



Security and Risk Management is part of the overall architecture framework, not a siloed architecture by itself

Source:
https://cloudsecurityalliance.org/artifacts/enterprise-architecture-reference-diagram/

Becoming an Enterprise Security Architect



Tall buildings need someone to ride the elevator

*"Modern architects **align organization and technology**, reduce friction, and **chart transformation journeys**.*

*Such architects ride the Architect Elevator from the penthouse, where the **business strategy** is set, to the engine room, where the **enabling technologies are implemented**.*

*They shun popular buzzwords in favor of a clear strategy defined by **conscious decision making.**"*

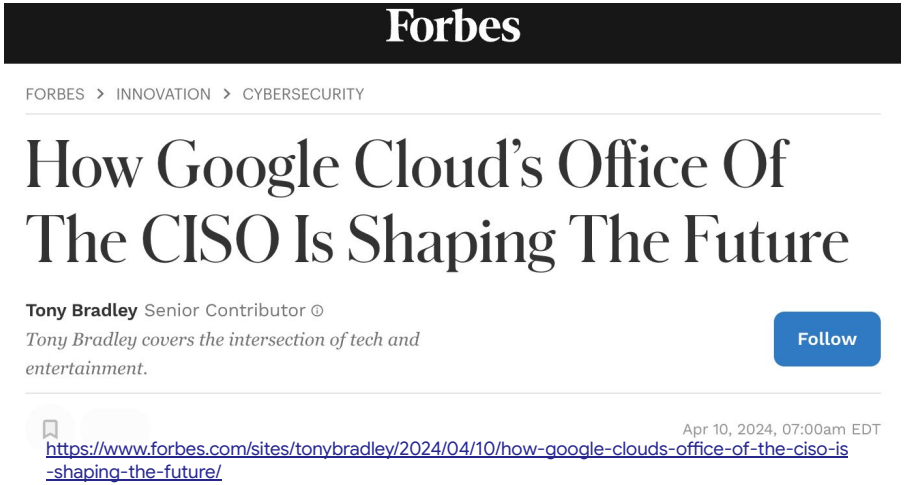
Gregor Hohpe, https://architectelevator.com/

Working with the C-Level

Today I work in Google Cloud's Office of the CISO

We primarily do Security Strategy Consulting.

We work with Cloud Customers on all executive levels, including CEOs, CFOs, CIO/CTOs, and of course CISOs.



Forbes

FORBES > INNOVATION > CYBERSECURITY

How Google Cloud's Office Of The CISO Is Shaping The Future

Tony Bradley Senior Contributor

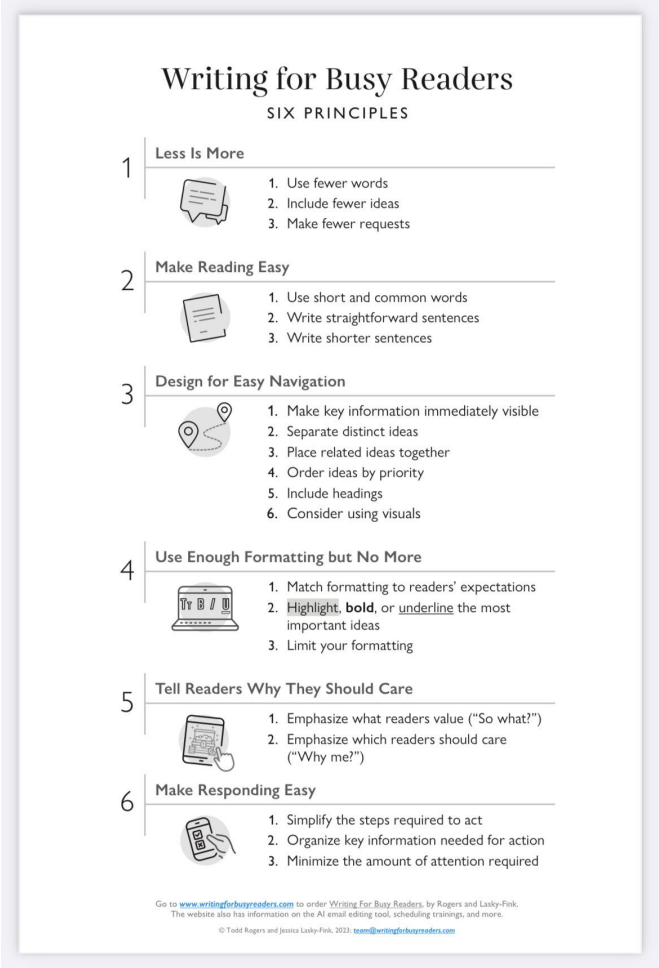
Tony Bradley covers the intersection of tech and entertainment.

Follow

Apr 10, 2024, 07:00am EDT

https://www.forbes.com/sites/tonybradley/2024/04/10/how-google-clouds-office-of-the-ciso-is-shaping-the-future/

Communicating with the Executive Level



Writing for Busy Readers

SIX PRINCIPLES

1 Less Is More

1. Use fewer words
2. Include fewer ideas
3. Make fewer requests

2 Make Reading Easy

1. Use short and common words
2. Write straightforward sentences
3. Write shorter sentences

3 Design for Easy Navigation

1. Make key information immediately visible
2. Separate distinct ideas
3. Place related ideas together
4. Order ideas by priority
5. Include headings
6. Consider using visuals

4 Use Enough Formatting but No More

1. Match formatting to readers' expectations
2. Highlight, **bold**, or underline the most important ideas
3. Limit your formatting

5 Tell Readers Why They Should Care

1. Emphasize what readers value ("So what?")
2. Emphasize which readers should care ("Why me?")

6 Make Responding Easy

1. Simplify the steps required to act
2. Organize key information needed for action
3. Minimize the amount of attention required

Go to www.writingforbusyreaders.com to order Writing For Busy Readers, by Rogers and Lasky-Fink. The website also has information on the AI email editing tool, scheduling trainings, and more.

https://writingforbusyreaders.com/

Talking about PQC to CISOs

Questions you get:

“How much will it cost?”

“Is there a tool to ‘get PQC done’?”

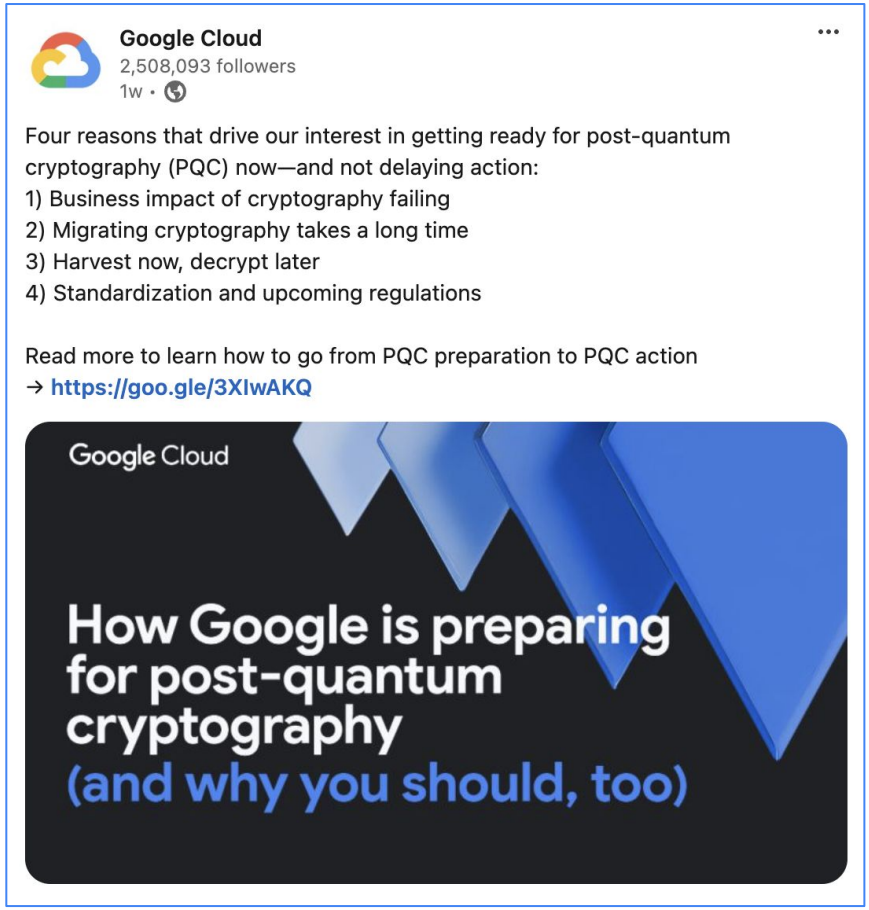
“What’s the risk?”

“What’s the benefit?”

“How will this increase our revenue?”

More than 17 years after starting my Ph.D. on PQC there’s still a lot of work to do.

Stay tuned.



https://cloud.google.com/security/resources/post-quantum-cryptography

What did I learn?

Think about both “attacking and defending”.

Be humble. Show responsibility to others.

Find your own path. Do what you enjoy.

Thank you

Christiane Peters
https://www.linkedin.com/in/christianepeters/
cbcrypto.org
chrpet@google.com