ETH zürich

D INFK

APPLIED CRYPTO GROUP

Cybersecurity - the real challenges

Professor Kenny Paterson
Applied Cryptography Group
ETH Zurich

Symposium on Privacy and Security 2021
2 September 2021, Zurich

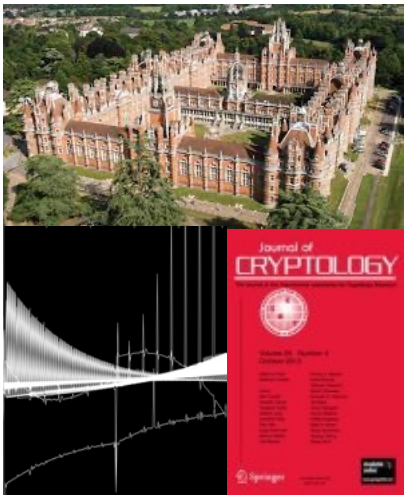
1

About the speaker

APPLIED CRYPTO GROUP

Bio sketch:

- Ph.D. in Mathematics (London, 1993).
- Postdoctoral research, 1994-1996 in Zurich and London
- HP Research Laboratories, 1996-2001: internal mathematical consulting
- Lecturer, Reader, Professor at Royal Holloway, University of London, 2001-2019
- Professor of Computer Science, ETH Zurich, 2019 – now



Main research focus: Applied Cryptography
Wikipedia: https://en.wikipedia.org/wiki/Kenny_Paterson
Research group: https://appliedcrypto.ethz.ch/
Twitter: @kennyog

ETH zürich 02/09/2021 2

2

Agenda

1. The role of cryptography in the digital society
2. Quantum computing vs. cryptography
3. Telegram and Bridgefy
4. Consuming cryptography
5. Beyond cryptography for data in transit
6. Key takeaways

ETH zürich 02/09/2021 3

3

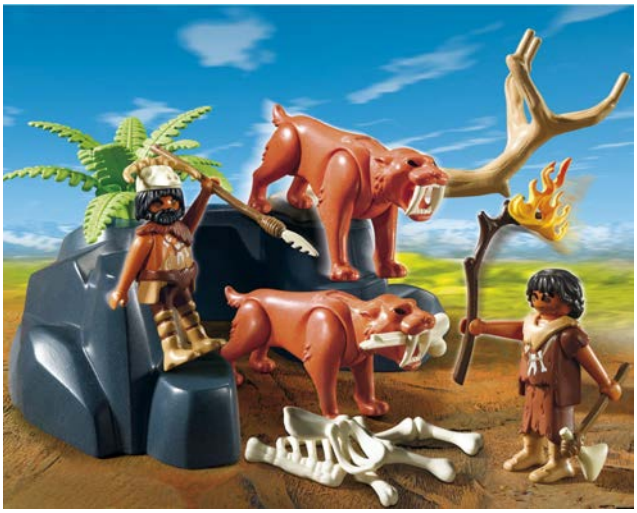
Agenda

1. **The role of cryptography in the digital society**
2. Quantum computing vs. cryptography
3. Telegram and Bridgefy
4. Consuming cryptography
5. Beyond cryptography for data in transit
6. Key takeaways

ETH zürich 02/09/2021 4

4

Then…



5

5

Now…

6

6

Cryptography everywhere

- e-commerce
- social media
- online personal banking
- debit/credit card payments
- interbank payments
- secure messaging (WhatsApp, Signal, Telegram)
- mobile telephony
- VPN/remote access
- video conferencing
- secure cloud data storage
- privacy-preserving contact tracing (GAEN, DP3T)
- Cryptocurrencies
- military and government communications systems

ETH zürich

7

7

Now…

Messaging

Cloud

Cryptocurrency

FHE and MPC startups

8

8

Cryptography ∩ politics ≠ ∅

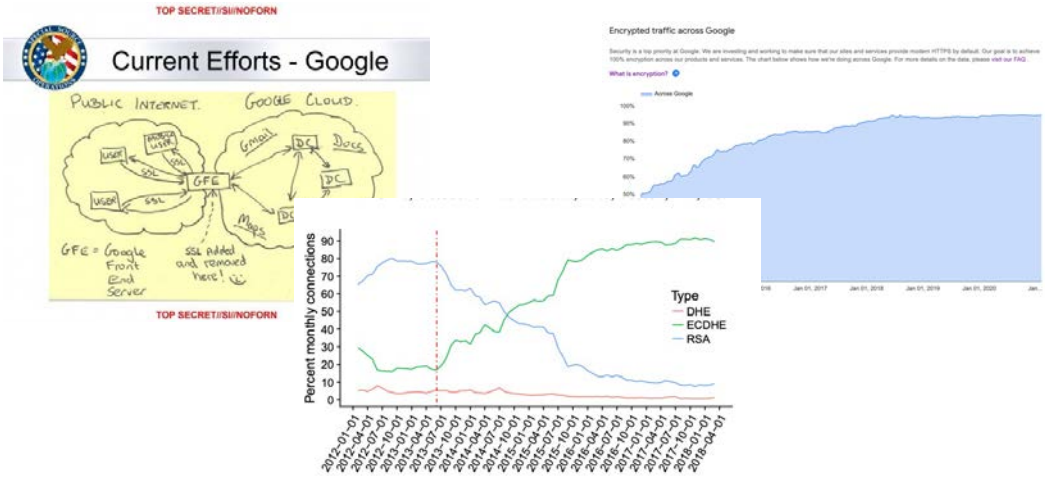


Figure 8: Negotiated RSA and forward secret connections. Dotted line shows the date of first Snowden revelations.

9

9

Agenda

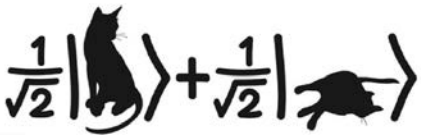
1. The role of cryptography in the digital society
2. **Quantum computing vs. cryptography**
3. Telegram and Bridgefy
4. Consuming cryptography
5. Beyond cryptography for data in transit
6. Key takeaways

ETH zürich 02/09/2021 10

10

Quantum Computing

Basic tenet of quantum physics: superposition.



Qubit: basic unit of quantum computation, loosely a superposition of classical "0" and "1" bits.

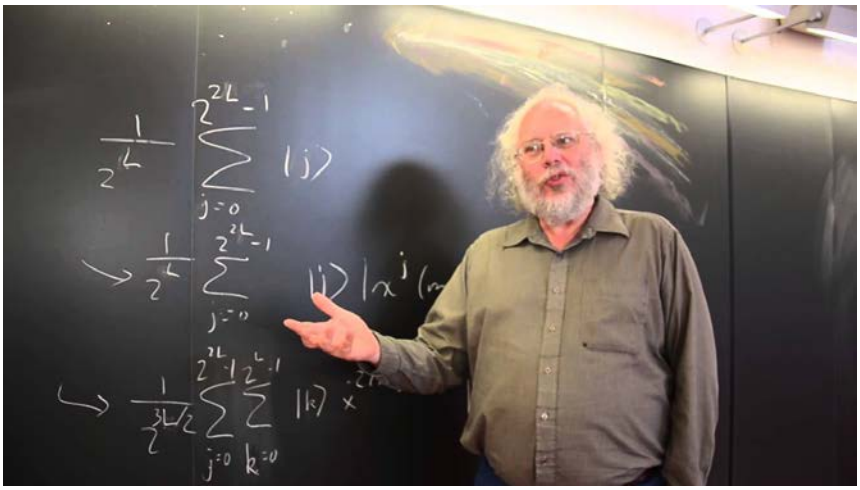
Quantum gates: analogues of classical computing gates – AND, NOT, etc – acting on qubits.

Quantum computing: execution of a sequence of quantum gates on "all possible classical states in parallel".

11

11

Shor's Algorithm Breaks Classical Public Key Cryptography



https://www.youtube.com/watch?v=hOlOY7NyMfs

12

12

Quantum Supremacy

APPLIED CRYPTO GROUP

Article

Quantum supremacy using a programmable superconducting processor

https://doi.org/10.1038/s41586-019-1666-5
Received: 22 July 2019
Accepted: 20 September 2019
Published online: 23 October 2019

Frank Arute[1], Kunal Arya[1], Ryan Babbush[1], Dave Bacon[1], Joseph C. Bardin[1,2], Rami Barends[1], Rupak Biswas[3], Sergio Boixo[1], Fernando G. S. L. Brandao[1,4], David A. Buell[1], Brian Burkett[1], Yu Chen[1], Zijun Chen[1], Ben Chiaro[5], Roberto Collins[1], William Courtney[1], Andrew Dunsworth[1], Edward Farhi[1], Brooks Foxen[1,5], Austin Fowler[1], Craig Gidney[1], Marissa Giustina[1], Rob Graff[1], Keith Guerin[1], Steve Habegger[1], Matthew P. Harrigan[1], Michael J. Hartmann[1,6], Alan Ho[1], Markus Hoffmann[1], Trent Huang[1], Travis S. Humble[7], Sergei V. Isakov[1], Evan Jeffrey[1], Zhang Jiang[1], Dvir Kafri[1], Kostyantyn Kechedzhi[1], Julian Kelly[1], Paul V. Klimov[1], Sergey Knysh[1], Alexander Korotkov[1,8], Fedor Kostritsa[1], David Landhuis[1], Mike Lindmark[1], Erik Lucero[1], Dmitry Lyakh[9], Salvatore Mandrà[2,10], Jarrod R. McClean[1], Matthew McEwen[5], Anthony Megrant[1], Xiao Mi[1], Kristel Michielsen[11,12], Masoud Mohseni[1], Josh Mutus[1], Ofer Naaman[1], Matthew Neeley[1], Charles Neill[1], Murphy Yuezhen Niu[1], Eric Ostby[1], Andre Petukhov[1], John C. Platt[1], Chris Quintana[1], Eleanor G. Rieffel[3], Pedram Roushan[1], Nicholas C. Rubin[1], Daniel Sank[1], Kevin J. Satzinger[1], Vadim Smelyanskiy[1], Kevin J. Sung[1,13], Matthew D. Trevithick[1], Amit Vainsencher[1], Benjamin Villalonga[1,14], Theodore White[1], Z. Jamie Yao[1], Ping Yeh[1], Adam Zalcman[1], Hartmut Neven[1] & John M. Martinis[1,5*]

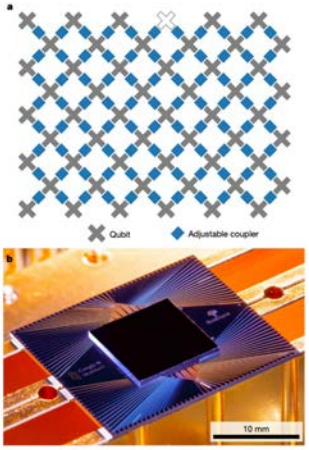


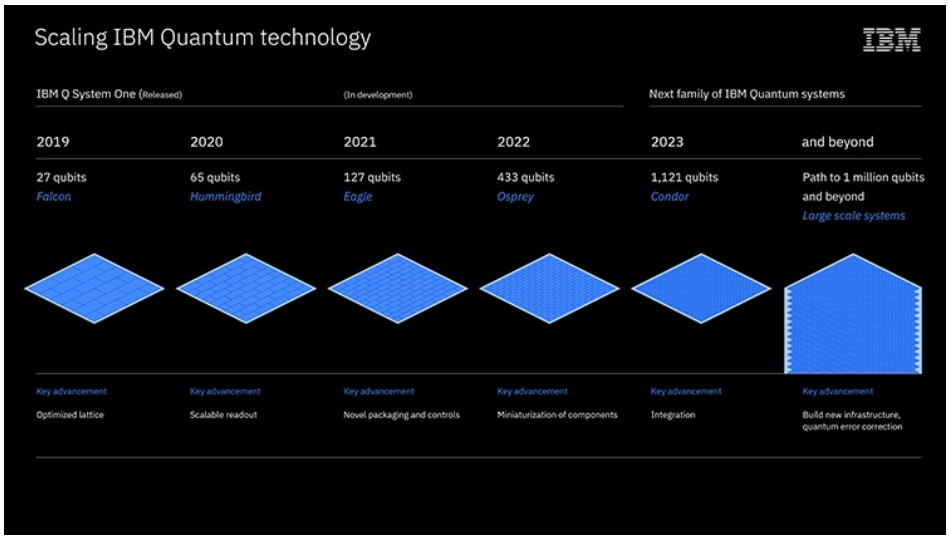
Fig. 1 | The Sycamore processor. a, Layout of processor, showing a rectangular array of 54 qubits (grey), each connected to its four nearest neighbours with couplers (blue). The inoperable qubit is outlined. **b**, Photograph of the Sycamore chip.

13

13

Quantum Computing's Prospects According to IBM

APPLIED CRYPTO GROUP



https://www.ibm.com/blogs/research/2020/09/ibm-quantum-roadmap/
February 2021

14

14

Responding to the CryptApocalypse

More usefully:

- Design new cryptosystems that we believe resist attack by quantum computers.
- **Post-quantum cryptography.**
- Aka quantum-resistant or quantum-immune cryptography.

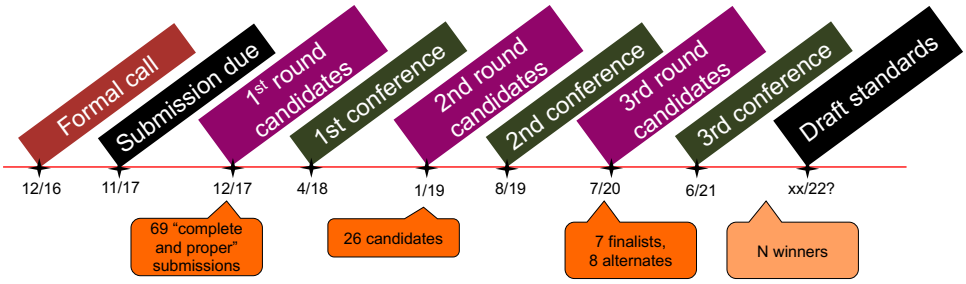
15

15

PQC and NIST

NIST competition, 2016 – 2023(ish) for standardising post-quantum public key algorithms.

- http://csrc.nist.gov/groups/ST/post-quantum-crypto/
- **Formal project start:** 2012.
- **Evaluation criteria**: security, cost, flexibility/simplicity/adoptability.
- **Process (5-7 years)**:



16

16

Agenda

1. The role of cryptography in the digital society
2. Quantum computing vs. cryptography
3. **Telegram and Bridgefy**
4. Consuming cryptography
5. Beyond cryptography for data in transit
6. Key takeaways

ETH zürich 02/09/2021 17

17

Telegram and Bridgefy

Telegram
a new era of messaging

Telegram for iPhone / iPad

General Questions

Q: What is Telegram? What do I do here?
Telegram is a messaging app with a focus on speed and security, it's super-fast, simple and free. You can use Telegram on all your devices **at the same time** — your messages sync seamlessly across any number of your phones, tablets or computers. Telegram has over **500 million** monthly active users and is one of the **10 most downloaded apps** in the world.

bridgefy

OFFLINE MESSAGING

Bridgefy is the app that lets you send offline text messages when you don't have access to the Internet, by simply turning on Bluetooth. Perfect for connecting with others during natural disasters, at large events, and at school!

Download on the App Store | GET IT ON Google Play

ETH zürich 02/09/2021 18

18

Bridgefy actively promote their app for use by higher risk protest groups

Myanmar Flocks to Bridgefy to Challenge Military Coup

• THE BRIDGEFY APP IN REAL LIFE 05/13/2021

Probably inspired by previous movements, Myanmar massively downloaded the Bridgefy App after the military took the government.

Hong Kong Protesters Adopt Bridgefy amid Sophistication of Techniques

• THE BRIDGEFY APP IN REAL LIFE 05/13/2021

Hong Kong protesters adopted the Bridgefy App to escape potential Internet shutdowns as one of several techniques that impressed the

Nigeria Protesters Adopt Bridgefy to Tackle Potential Internet Shutdown

• THE BRIDGEFY APP IN REAL LIFE 05/13/2021

Fearing a potential Internet shutdown, Nigerian protesters adopted Bridgefy to tackle it during the #EndSARS demonstrations.

ETH 19

19

So how secure are Telegram and Bridgefy?

Four Attacks and a Proof for Telegram

Martin R. Albrecht*, Lenka Mareková*, Kenneth G. Paterson† and Igors Stepanovs†
*Information Security Group, Royal Holloway, University of London, {martin.albrecht,lenka.marekova.2018}@rhul.ac.uk
†Applied Cryptography Group, ETH Zurich, {kenny.paterson,istepanovs}@inf.ethz.ch

https://mtpsym.github.io/

Mesh Messaging in Large-Scale Protests: Breaking Bridgefy

Martin R. Albrecht, Jorge Blasco, Rikke Bjerg Jensen, and Lenka Mareková(✉)

Royal Holloway, University of London, London, UK
{martin.albrecht,jorge.blascoalis,rikke.jensen,lenka.marekova}@rhul.ac.uk

https://eprint.iacr.org/2021/214

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Breaking Bridgefy, again

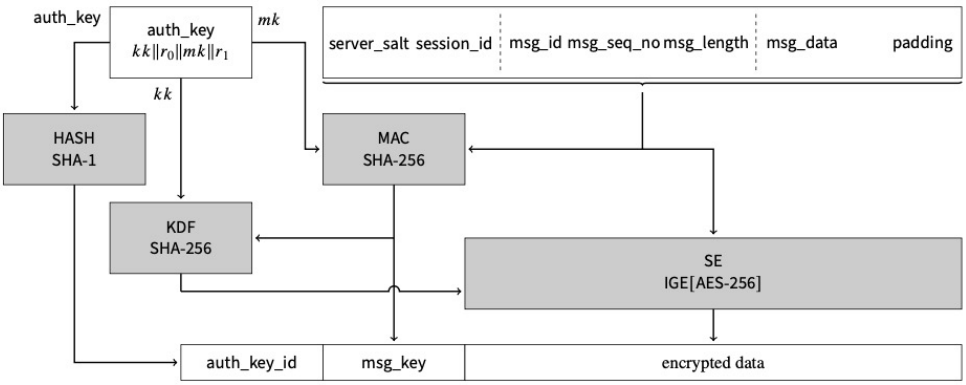
Master Thesis
Raphael Eikenberg
September 1, 2021

Advisors: Prof. Dr. Kenny Paterson, Prof. Dr. Martin Albrecht
Applied Cryptography Group
Institute of Information Security
Department of Computer Science, ETH Zürich

ETH zürich 02/09/2021 20

20

Symmetric cryptography in Telegram



ETH zürich 02/09/2021 21

21

Breaking Bridgefy, again

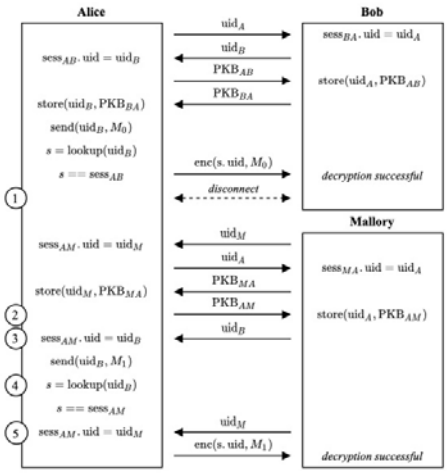
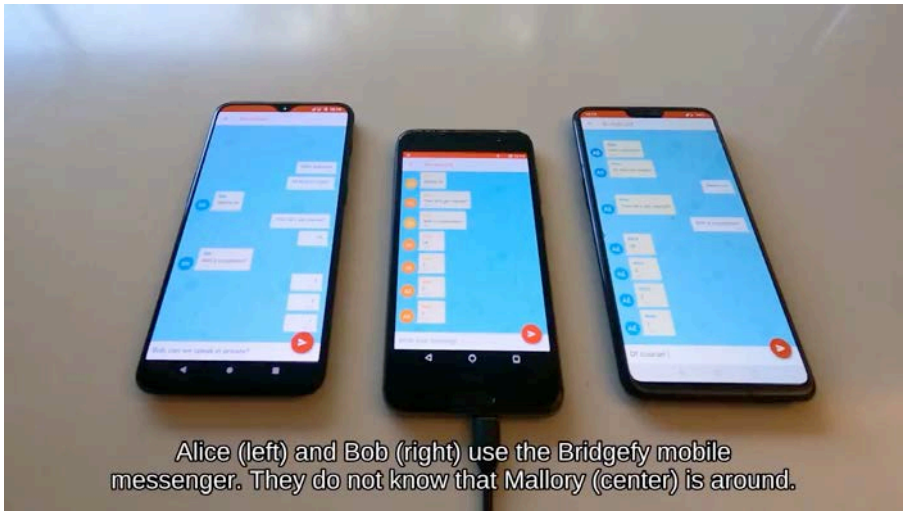


Figure 5.1: The packet flow of our TOCTOU attack on Bridgefy. Alice sends a message to Bob twice: the first message M_0 is sent to Bob only, but Mallory can decrypt the second message M_1, even though it was intended for Bob.

ETH zürich 02/09/2021 22

22

Breaking Bridgefy, again – demo



ETH zürich 02/09/2021 23

23

Telegram and Bridgefy – Common themes

- Reliance on non-standard or known-to-be-weak components
- Improper combination of components resulting in an insecure system
- Over-confidence in own level of cryptographic expertise
- Lack of process to enable smooth vulnerability disclosure
- Unwillingness to announce security issues to users

- **All this for the simplest cryptographic application: secure communication.**

ETH zürich 02/09/2021 24

24

Agenda

1. The role of cryptography in the digital society
2. Quantum computing vs. cryptography
3. Telegram and Bridgefy
4. **Consuming cryptography**
5. Beyond cryptography for data in transit
6. Key takeaways

ETH zürich 02/09/2021 25

25

Consuming cryptography

- Be aware of the Dunning-Kruger effect – it's alive and well in cryptography.
- There is no free lunch.
- Learn to detect snake-oil.

ETH zürich 02/09/2021 26

26

Four golden rules for consuming cryptography – going beyond “Don’t roll your own”

1. Large companies, or smaller ones for whom cryptography is a core technology, should **employ qualified cryptographers** and give them a role in system specification and development.
2. Developers should rely on **existing algorithms** packaged in cryptographic **libraries**.
3. Developers should rely on **existing design patterns and standards** for more complex cryptographic systems/protocols.
4. When a new application demands a new cryptographic system or protocol, and expertise is not locally available, **seek external advice**.

From: https://www.cybok.org/media/downloads/Applied_Cryptography_v1.0.0.pdf

ETH zürich 02/09/2021 27

27

CyBoK: The Cyber Body of Knowledge

https://www.cybok.org/

ETH zürich 02/09/2021 28

28

Agenda

1. The role of cryptography in the digital society
2. Quantum computing vs. cryptography
3. Telegram and Bridgefy
4. Consuming cryptography
5. **Beyond cryptography for data in transit**
6. Key takeaways

ETH zürich 02/09/2021 29

29

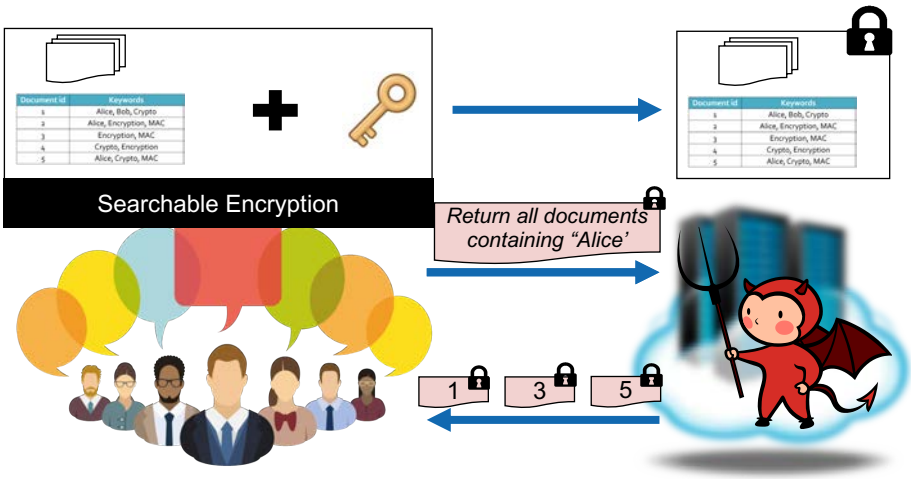
Beyond cryptography for data in transit

1. Cryptography for data at rest
2. Cryptography for data under computation
   - Searchable encryption
   - Secure multi-party computation
   - Fully homomorphic encryption
3. Cryptography for cryptocurrencies
   - Threshold techniques
   - Advanced signature schemes
   - Zero-Knowledge proofs

ETH zürich 02/09/2021 30

30

Example: searchable encryption



SE allows the server to process queries and updates "directly" on encrypted data without the need for decryption

ETH zürich Slide by Sikhar Patranabis 02/09/2021 31

31

Beyond cryptography for data in transit

Those who cannot remember the past are condemned to repeat it.

George Santayana

ETH zürich 02/09/2021 32

32

Agenda

1. The role of cryptography in the digital society
2. Quantum computing vs. cryptography
3. Telegram and Bridgefy
4. Consuming cryptography
5. Beyond cryptography for data in transit
6. **Key takeaways**

ETH zürich 02/09/2021 33

33

Key takeaways

- Cryptography has become a pervasive technology.
- Cryptography is powerful yet imperfect.
- Cryptography, like most technologies, can be used for good or ill.

- Cryptography has been protecting data in transit for thousands of years.
- Now it is increasingly being used to protect data at rest and under computation.
- Novel applications like cryptocurrencies are spurring innovation in research and deployment of cryptography.

- New technologies bring new risks and opportunities for cryptography: quantum computation, cryptocurrencies,…
- At ETH we are in the forefront of researching these topics.

ETH zürich 34

34

ETH zürich

APPLIED CRYPTO GROUP

Contact:
Professor Kenny Paterson
Applied Cryptography Group

Department of Computer Science
Universitätstrasse 6
8092 Zurich, Swizterland

https://appliedcrypto.ethz.ch/
kenny.paterson@inf.ethz.ch
@kennyog

APPLIED CRYPTO GROUP

35

APPLIED CRYPTO GROUP

Photo by Wilhelm Gunkel on Unsplash

ETH zürich

36

36