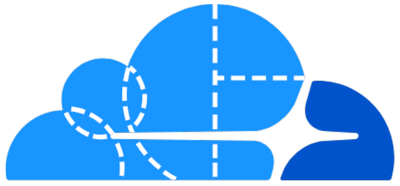
Not-So-Low Hanging Fruit

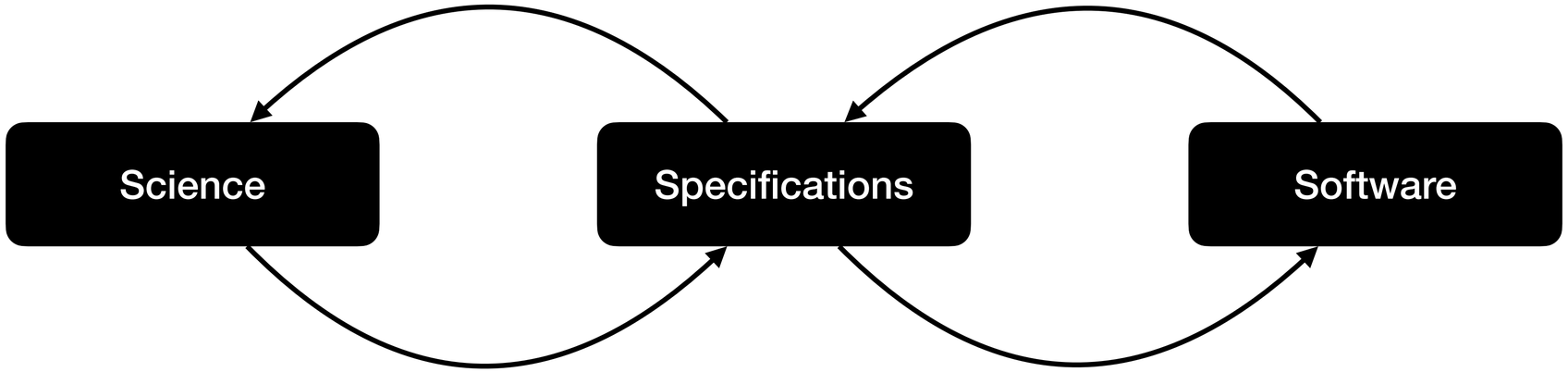
Security and Privacy Research Opportunities for IETF Protocols

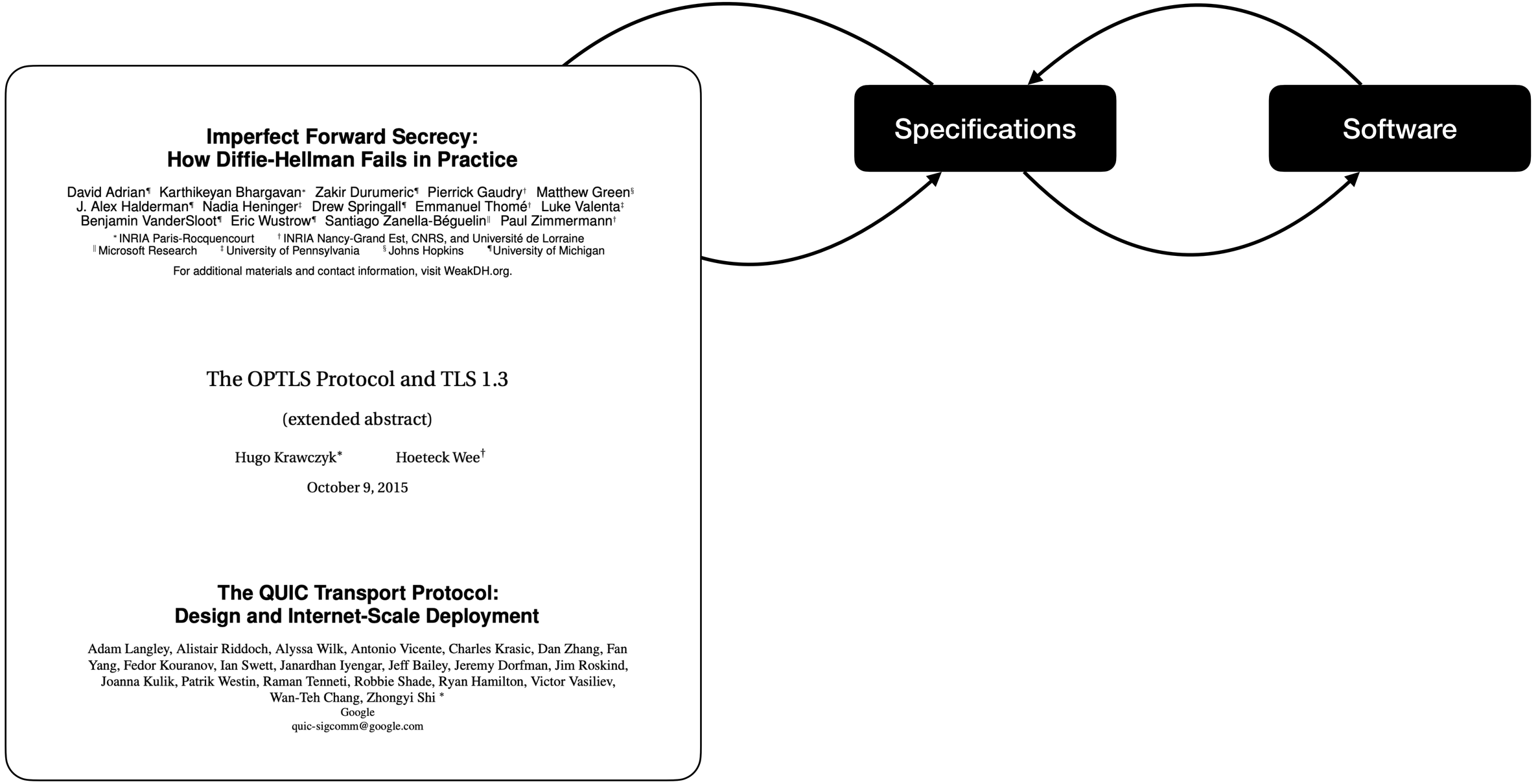
Christopher A. Wood
Research Lead, Cloudflare



Cloudflare
Research

IETF 117 - Applied Networking Research Workshop 2023


Science
Specifications
Software


Specifications
Software
Imperfect Forward Secrecy:
How Diffie-Hellman Fails in Practice
David Adrian¶ Karthikeyan Bhargavan* Zakir Durumeric¶ Pierrick Gaudry† Matthew Green§
J. Alex Halderman¶ Nadia Heninger‡ Drew Springall¶ Emmanuel Thomé† Luke Valenta‡
Benjamin VanderSloot¶ Eric Wustrow¶ Santiago Zanella-Béguelin‖ Paul Zimmermann†
* INRIA Paris-Rocquencourt † INRIA Nancy-Grand Est, CNRS, and Université de Lorraine
‖ Microsoft Research ‡ University of Pennsylvania § Johns Hopkins ¶ University of Michigan
For additional materials and contact information, visit WeakDH.org.
The OPTLS Protocol and TLS 1.3
(extended abstract)
Hugo Krawczyk* Hoeteck Wee†
October 9, 2015
The QUIC Transport Protocol:
Design and Internet-Scale Deployment
Adam Langley, Alistair Riddoch, Alyssa Wilk, Antonio Vicente, Charles Krasic, Dan Zhang, Fan
Yang, Fedor Kouranov, Ian Swett, Janardhan Iyengar, Jeff Bailey, Jeremy Dorfman, Jim Roskind,
Joanna Kulik, Patrik Westin, Raman Tenneti, Robbie Shade, Ryan Hamilton, Victor Vasiliev,
Wan-Teh Chang, Zhongyi Shi *
Google
quic-sigcomm@google.com

Science

Software

Internet Engineering Task Force (IETF)
Request for Comments: 9000
Category: Standards Track
Published: May 2021
ISSN: 2070-1721

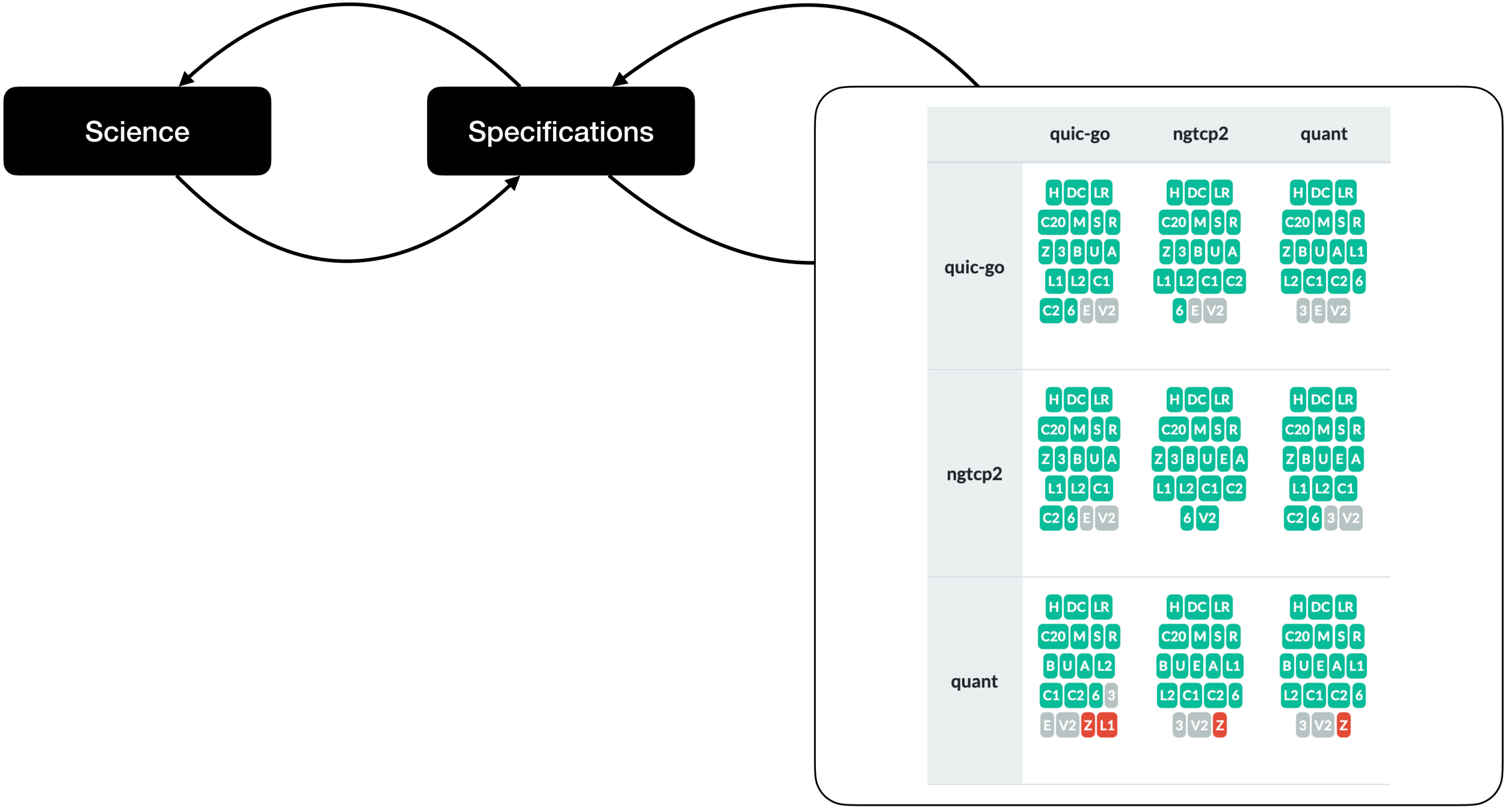
J. Iyengar, Ed.
Fastly
M. Thomson, Ed.
Mozilla

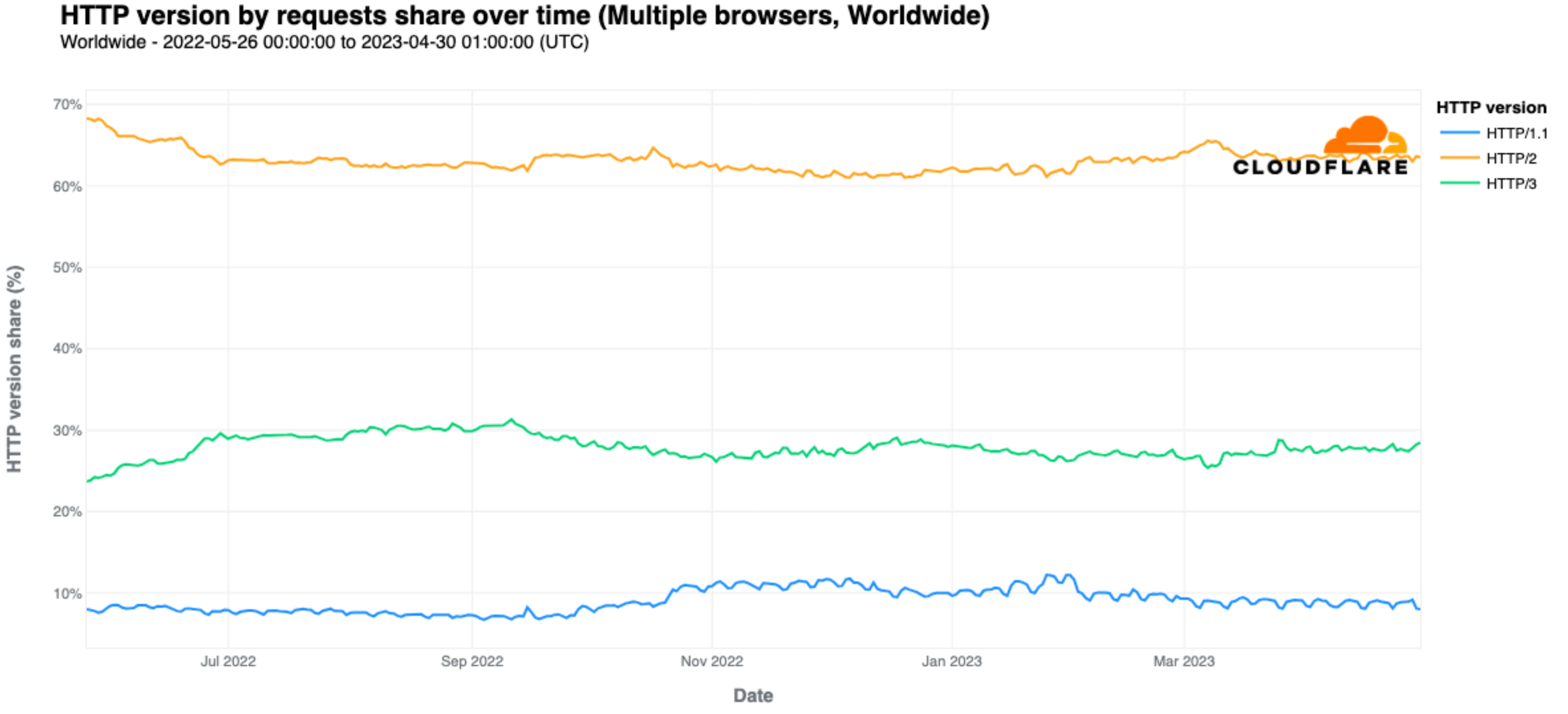
QUIC: A UDP-Based Multiplexed and Secure Transport

Internet Engineering Task Force (IETF)
Request for Comments: 9001
Category: Standards Track
Published: May 2021
ISSN: 2070-1721

M. Thomson, Ed.
Mozilla
S. Turner, Ed.
sn3rd

Using TLS to Secure QUIC


Science
Specifications
quic-go
ngtcp2
quant
quic-go
H DC LR C20 M S R Z 3 B U A L1 L2 C1 C2 6 E V2
H DC LR C20 M S R Z 3 B U A L1 L2 C1 C2 6 E V2
H DC LR C20 M S R Z B U A L1 L2 C1 C2 6 3 E V2
ngtcp2
H DC LR C20 M S R Z 3 B U A L1 L2 C1 C2 6 E V2
H DC LR C20 M S R Z 3 B U E A L1 L2 C1 C2 6 V2
H DC LR C20 M S R Z B U E A L1 L2 C1 C2 6 3 V2
quant
H DC LR C20 M S R B U A L2 C1 C2 6 3 E V2 Z L1
H DC LR C20 M S R B U E A L1 L2 C1 C2 6 3 V2 Z
H DC LR C20 M S R B U E A L1 L2 C1 C2 6 3 V2 Z



https://blog.cloudflare.com/http3-usage-one-year-on/


TLS


ACME


QUIC


MLS


MASQUE

Specifications at the IETF

Specifications transfer science to software (theory to practice)

- Clear descriptions for target algorithm, protocol, or system
- Basis for implementations and deployments
- Targets for verification and analysis

Specifications encourage open collaboration and build communities

Software at the IETF

Software is a primary input and output of the IETF

- Rough consensus ***and running code***
- Standards service interoperable deployments of protocols

Shipping software reveals new insights and unearths new challenges

Science at the IETF

Science is a valuable part of shipping IETF protocols

- Advances our understanding of problem and solution space
- Improves confidence in what we ship

Science has transitive effects on other parts of the process

- Progress creates opportunities for more research

Multiparty Computation

Multiparty Computation Overview

Multiparty Computation (MPC) is technique for computing (arbitrary) functions over private inputs

- Privacy-preserving measurement (PPM)
- Privacy-preserving ad-click attribution (IPA)

Specialized MPC protocols are being standardized and deployed today

- Distributed Aggregation Protocol (draft-ietf-ppm-dap)
- Verifiable Distributed Aggregation Protocol (draft-irtf-cfrg-vdaf)

Lightweight Techniques for Private Heavy Hitters

Dan Boneh, *Stanford*
Elette Boyle, *IDC Herzliya*
Henry Corrigan-Gibbs, *EPFL and MIT CSAIL*
Niv Gilboa, *Ben-Gurion University*
Yuval Ishai, *Technion*

Verifiable Distributed Aggregation Functions

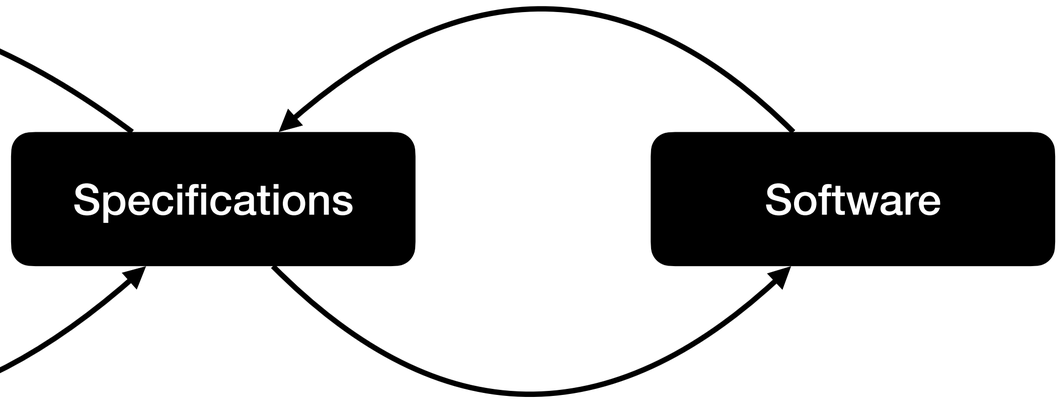
Hannah Davis, *University of California, San Diego*
Christopher Patton, *Cloudflare*
Mike Rosulek, *Oregon State University*
Phillipp Schoppmann, *Google*

2023/07/12

PLASMA: Private, Lightweight Aggregated Statistics against Malicious Adversaries with Full Security

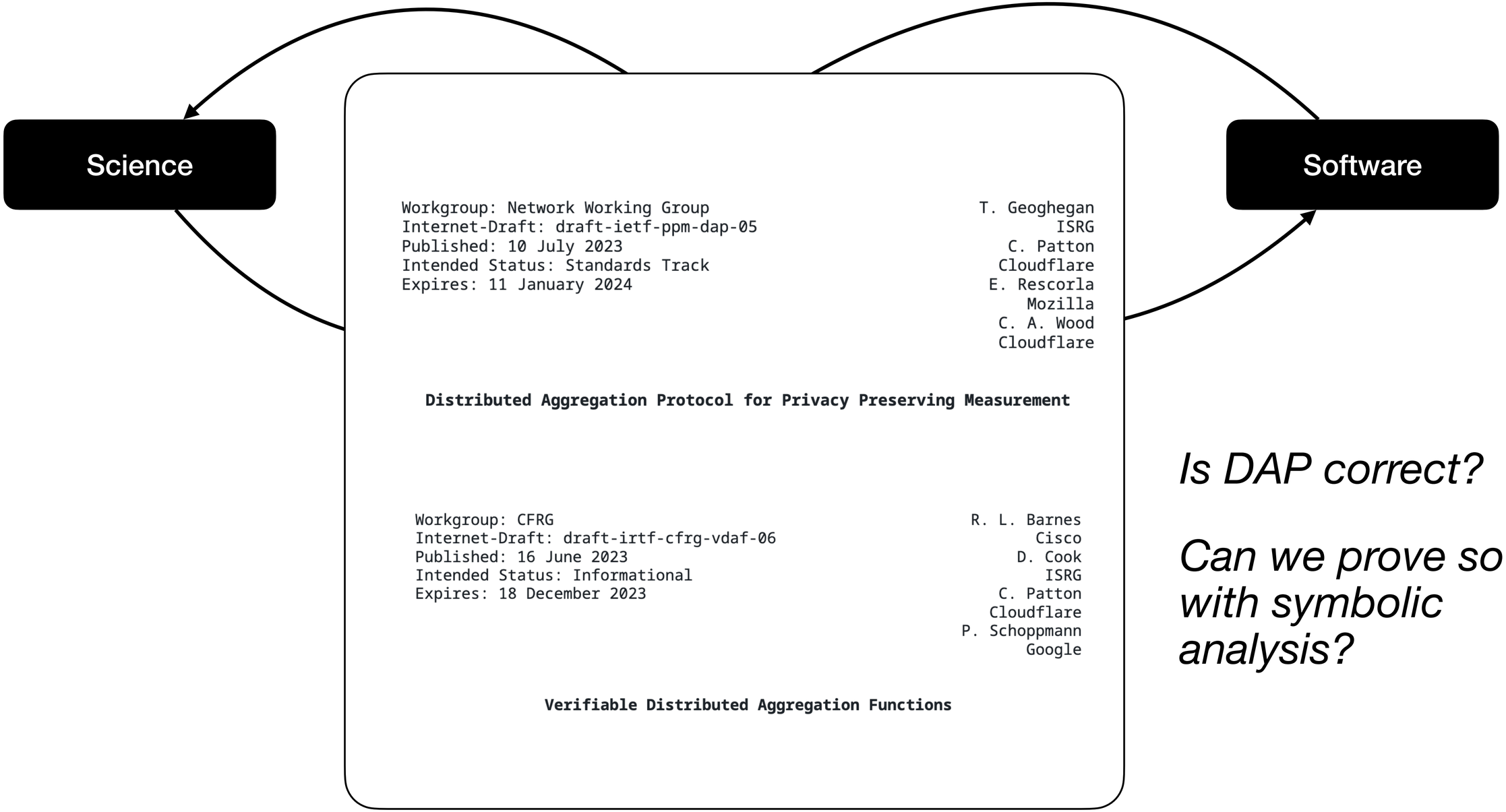
Dimitris Mouris[1]*, Pratik Sarkar[2]*, and Nektarios Georgios Tsoutsos[1]

[1] University of Delaware
{jimouris, tsoutsos}@udel.edu
[2] Boston University
pratik93@bu.edu



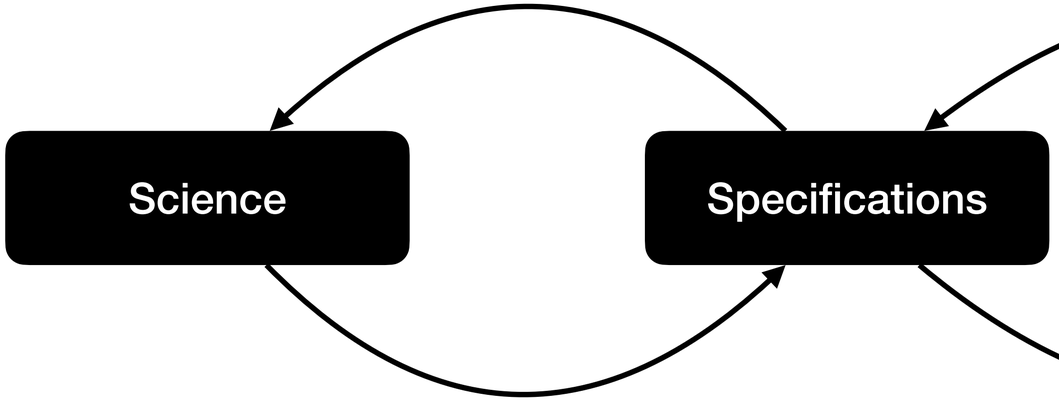
Are there more performant heavy hitter protocols?

How do we helpfully compose differential privacy with these protocols?



Is DAP correct?

Can we prove so with symbolic analysis?



Can we formally verify VDAF implementations?

Can we provide guidance for users of these protocols and libraries in practice?

janus

ci-build passing

Janus is an experimental implementation of the Distributed Aggregation Protocol (DAP) specification. Currently it supports VDAFs with trivial aggregation parameters only, e.g. Prio3. VDAFs with nontrivial aggregation parameters (e.g. Poplar1) are not yet supported.

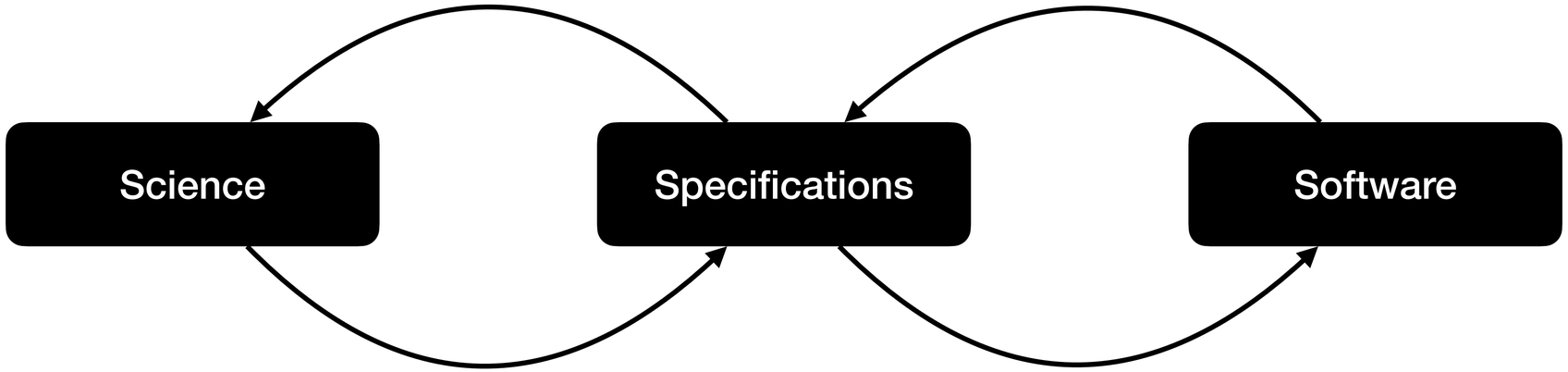
Janus is currently in active development.

Daphne

Daphne is a Rust implementation of the Distributed Aggregation Protocol (DAP) standard. DAP is under active development in the PPM working group of the IETF.

Other Research Opportunities

- Anonymous credentials
  - Post quantum cryptographic solutions
  - Formal verification of existing implementations
  - Deployable generic anonymous credentials
- Zero-knowledge proof (systems)
  - Building blocks for higher-level protocols (API models and reusable abstractions)
  - Formally verified and reference implementations for experimentation
  - New protocol embeddings

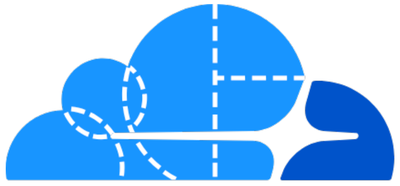

Science
Specifications
Software

Questions?
Comments?

Not-So-Low Hanging Fruit

Security and Privacy Research Opportunities for IETF Protocols

Christopher A. Wood
Research Lead, Cloudflare



Cloudflare
Research

IETF 117 - Applied Networking Research Workshop 2023