Post-Quantum

Cryptography Conference

Authenticity Guaranteed: Verifying Video Integrity on Consumer Devices with Post-Quantum Signatures

Ronny Döring
R&D System Engineer at Deutsche Telekom AG

KEYFACTOR CRYPTO4A SSL.com ENTRUST HID

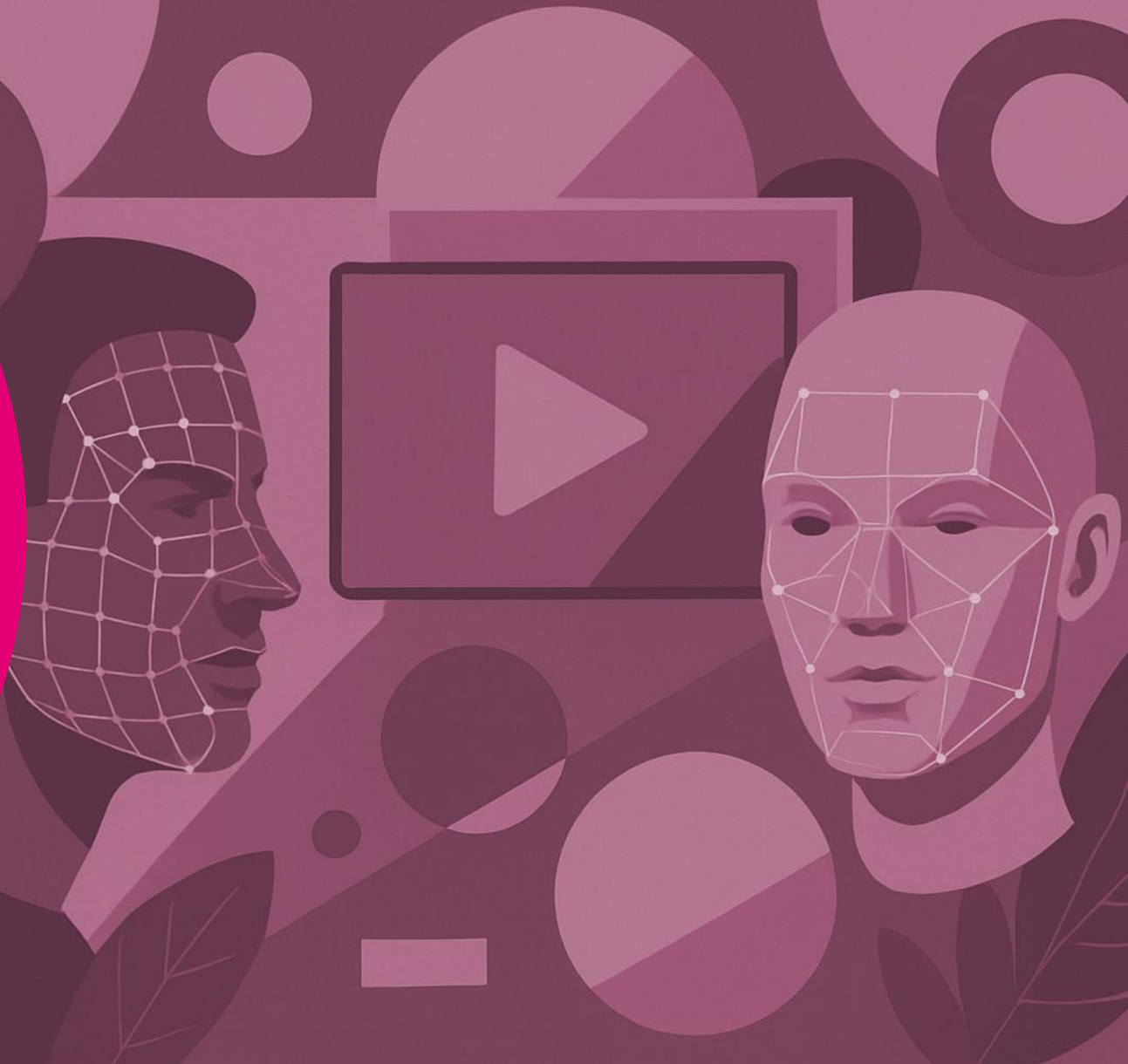
October 28 - 30, 2025 - Kuala Lumpur, Malaysia

PKI Consortium

Authenticity Guaranteed: Verifying Video Integrity on Consumer Devices with Post-Quantum Signatures

30th October 2025 | PQC Conference | Kuala Lumpur, Malaysia
Ronny Döring | T-Labs

T Labs



Contents

T-Labs – Key Facts

2004

Founded by *VISIONARIES*

Fuelled by *PIONEERS*

All of us *CONNECTED*

50+

300+
Academia, startup, and industry partners worldwide

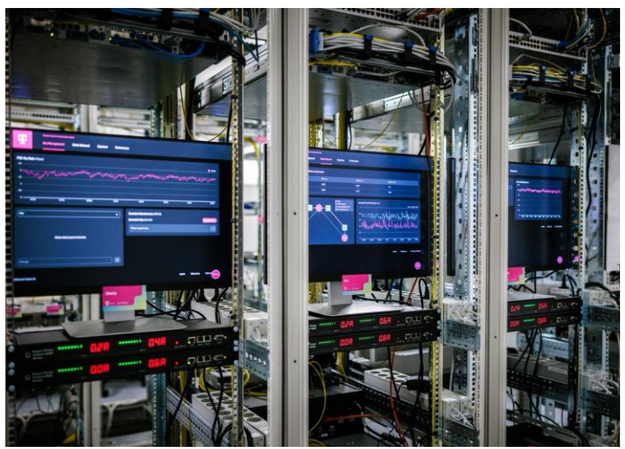
160+
Innovation projects transferred into operations, products, and services

5+
Locations in Berlin, Beer Sheva, Bonn, Dresden, Krakow and many more across the globe

1.650
Patents registered since 2004

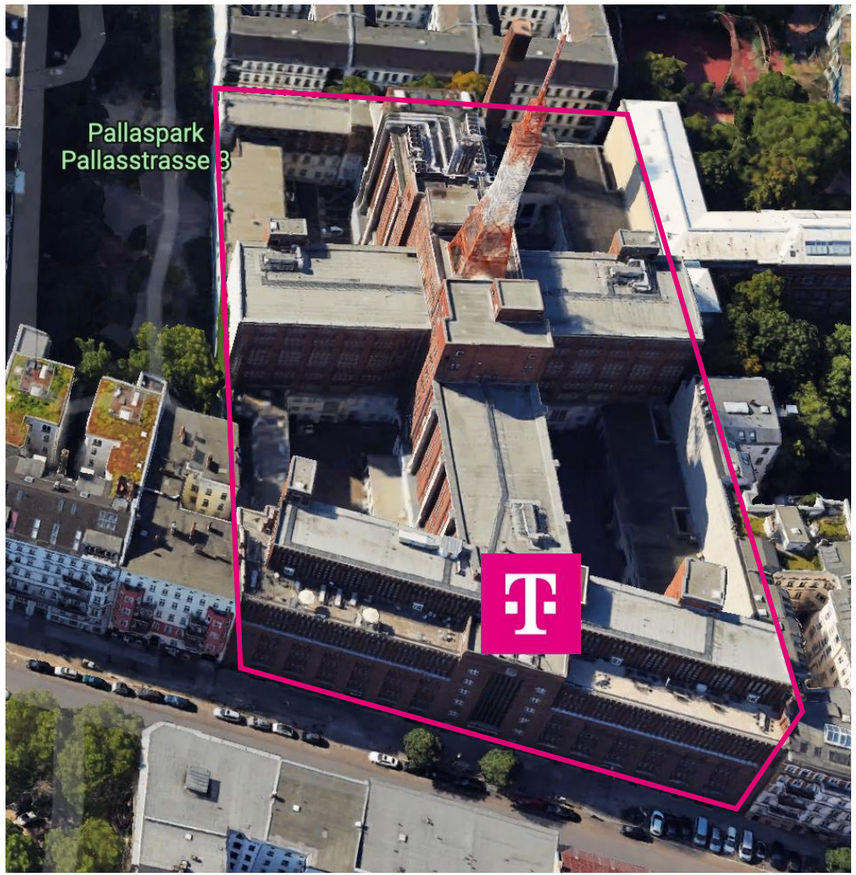
T-Labs – Applied R&D at Deutsche Telekom AG

- **Applied R&D** at DTAG
- Located in Berlin
- Research with academic partners; leveraging public programs (nat'l and EU)
- **Quantum Networks** is one of the research focus areas

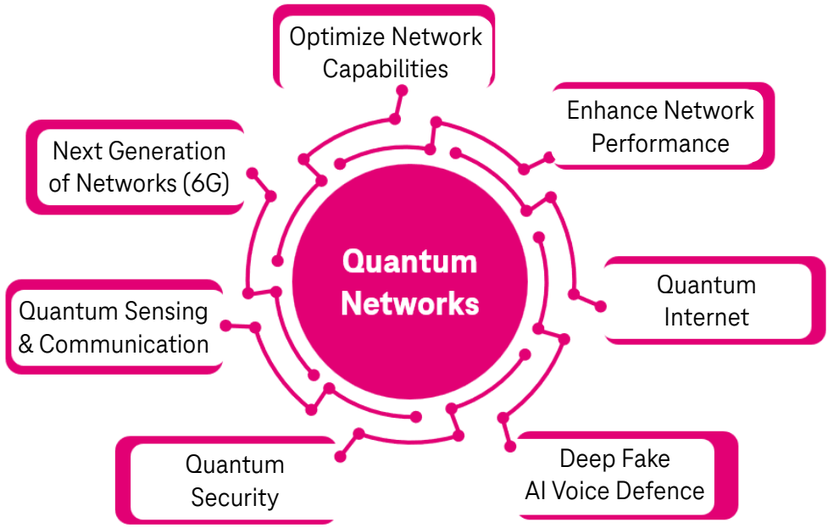


T Labs

Research. Develop. Impact.



T-Labs – Research Areas



Enhance long-term strategic position on networks

Humboldt-Universität zu Berlin · Technische Universität Dresden · Federal Ministry for Economic Affairs and Energy · TUM · Fraunhofer HHI

T Systems · GROUP TECHNOLOGY · Deutsche Telekom Geschäftskunden · Deutsche Telekom Technik

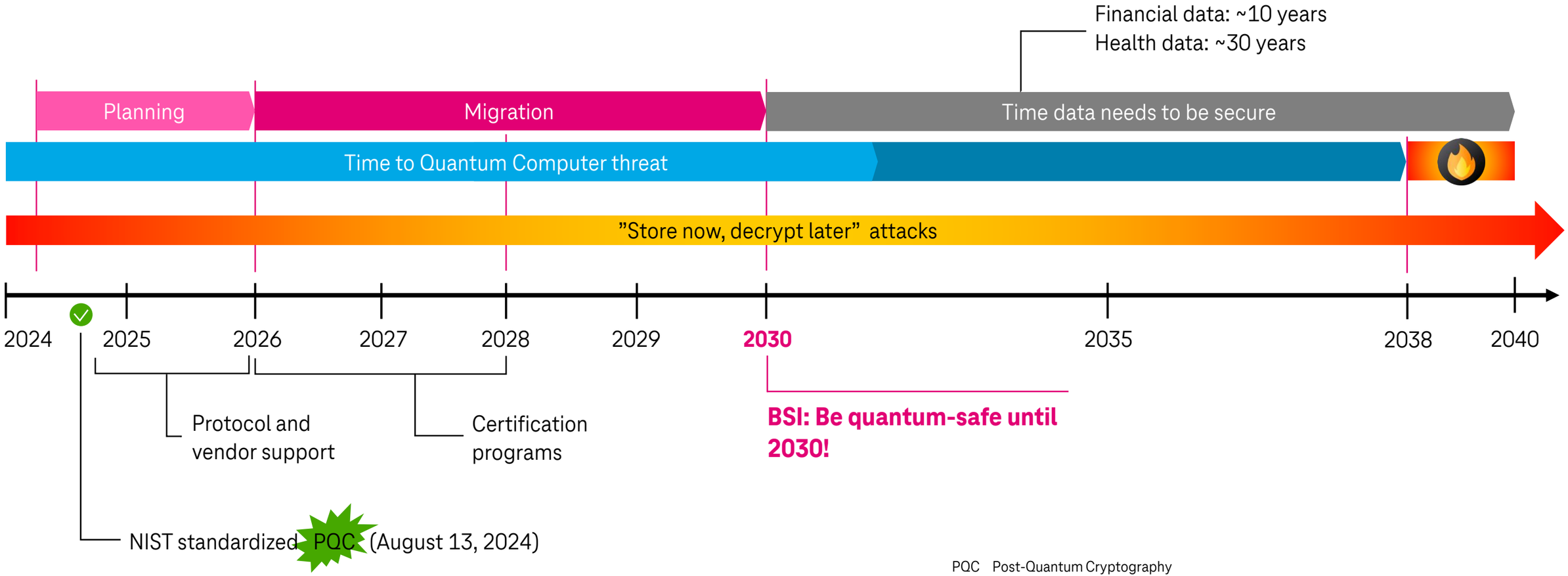
Increase revenue & product portfolio · Efficient total-cost-of-ownership · Business continuity & resilient networks

Group Technology | Portfolio | February 2025

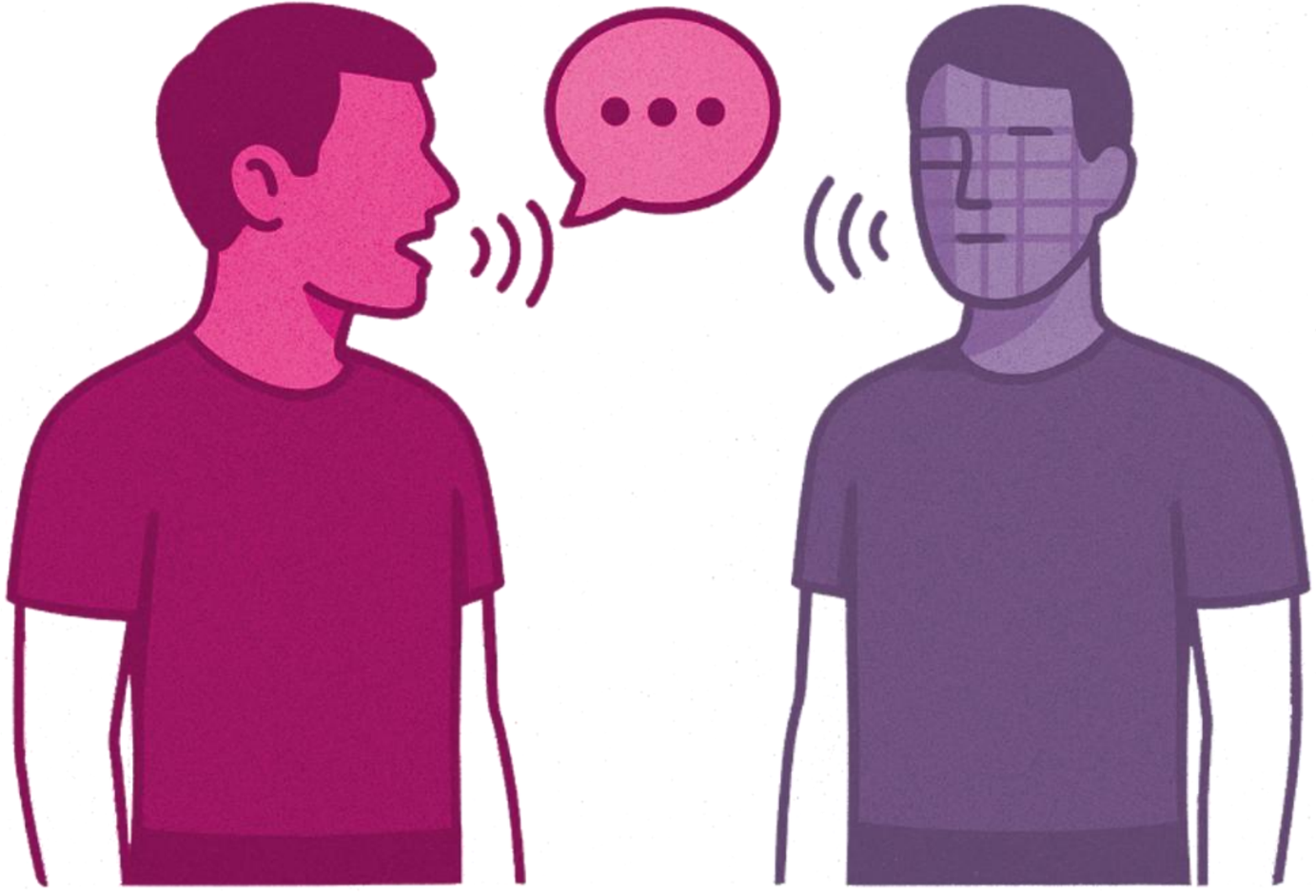
R&D Achievements

Qunnect · T Labs	Entanglement distribution in the Quantum Lab Berlin R&D TestNet with Qunnect
bdr. · T Labs · Fraunhofer HHI	Key experiment with HHI & bdr for “Forum für Quantenkommunikation in Deutschland” QKD-secured access management
SK telecom · T Labs	Multipath-based quantum-resistant WAN with SK Telecom

Quantum Security – Timeline



PQC Post-Quantum Cryptography
NIST National Institute of Standards and Technology
BSI Federal Office for Information Security (Germany)



REAL OR CLONE ?

AI or not AI?

AI or not AI?

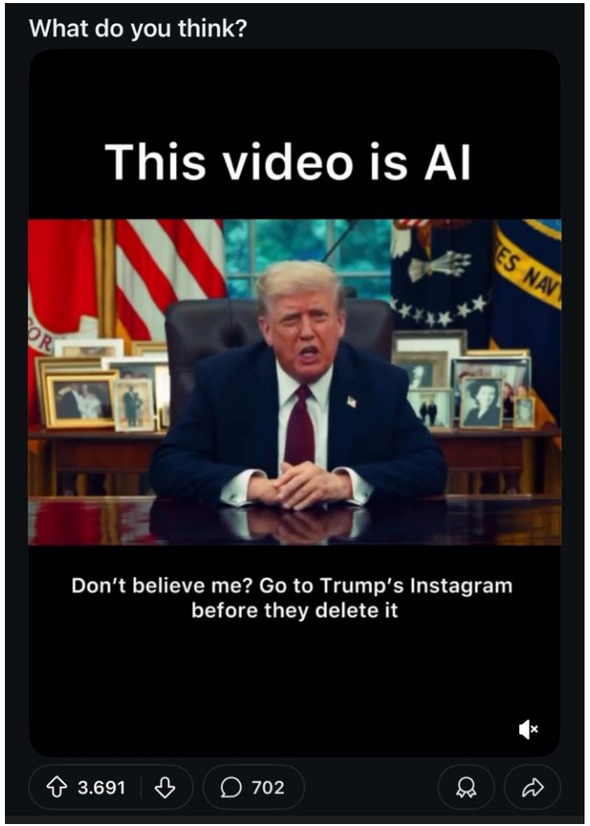
TRUTH.

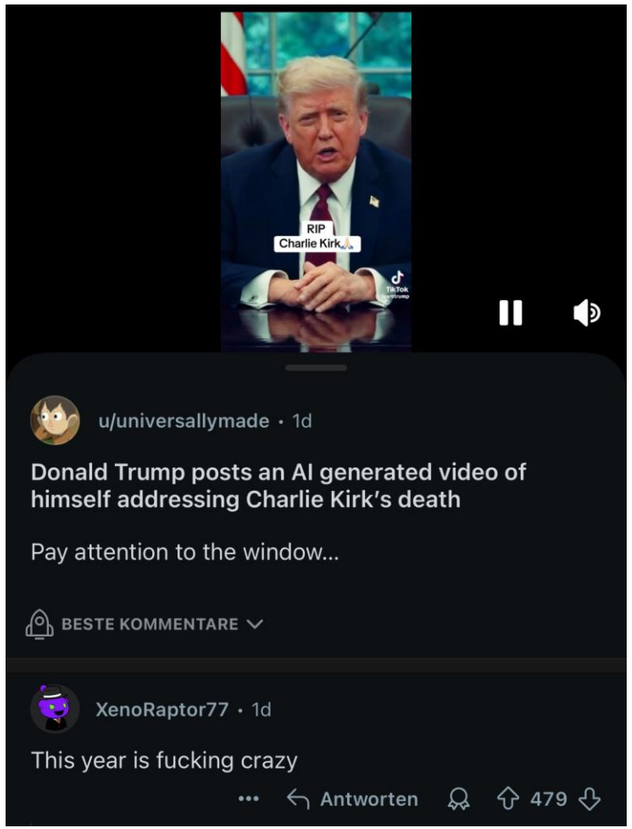
← Donald J. Trump

Donald J. Trump
@realDonaldTrump · 17h

TO MY GREAT FELLOW AMERICANS...

12.3k 30.5k 114k

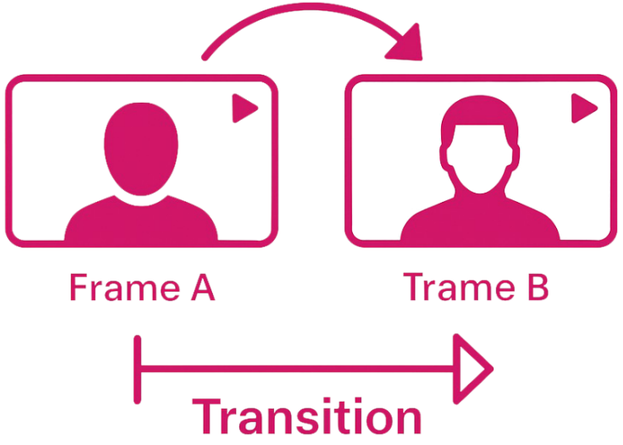


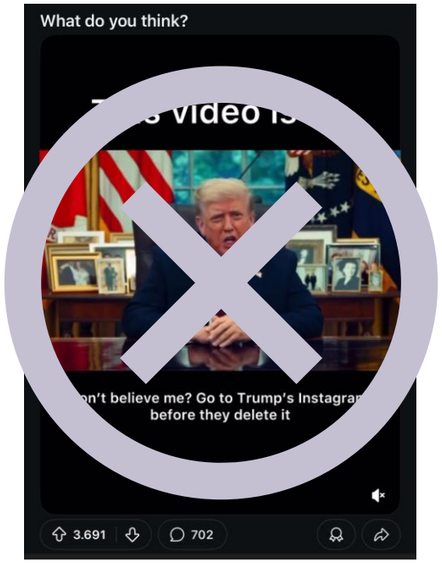


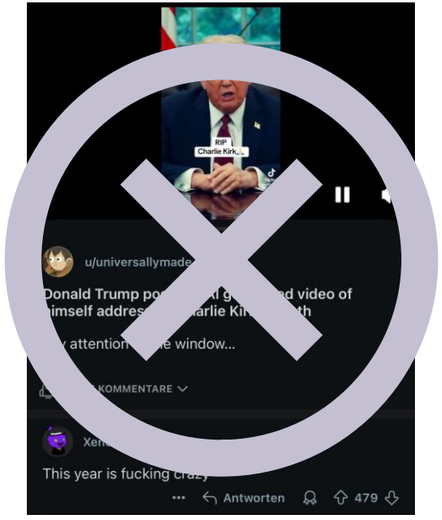
(Probably) not AI

There‘s no proof this is AI.

What seems to be a strange hand movement could be the resolve of a so called ***Morph Cut***.







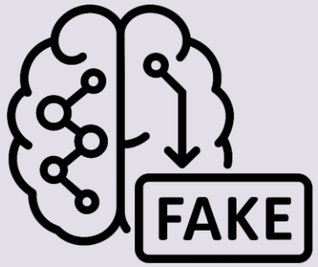
Deep Fake Detection Strategies

Watermarks

- Invisible signal or metadata (creator, model, or origin) embedded in pixels, frames, or audio spectrum.
- Detectable using dedicated verification tools.
- Enables attribution but can be removed by cropping, recompression, or noise.

Traceability through hidden patterns.

Model-Based Analysis



- Trained neural networks scan videos for visual or acoustic anomalies.
- Looks for unnatural motion, lighting, or temporal inconsistencies.
- Improves continuously as fake generation evolves.

Detection by anomaly recognition.

Watermarking helps trace AI-generated content at creation – Model-Based Analysis identifies manipulation after release.

Cryptographically Verified Video – Mechanism

Video Capture / Source

- Source can be a camera or a file.
- Group material into blocks of *n* frames.

➢ Blockwise processing

Hashing

- Create a hash of each frame.
- Concatenate frame hashes and create a block hash.

➢ Unique digital fingerprint for each block

Signing

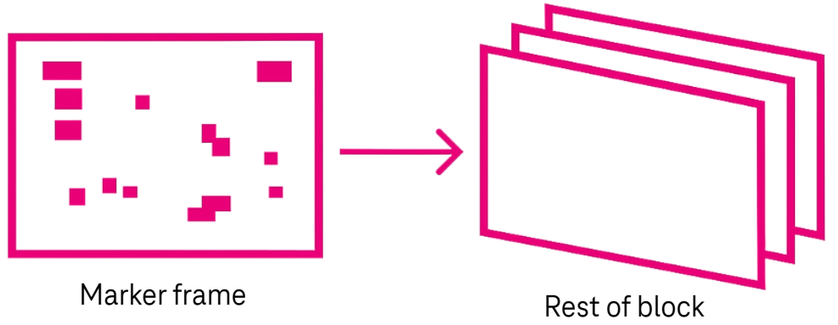
- Sign the block hash using PQC.

➢ Integrity against quantum-level attacks

Embedding

- Embed signature into a dedicated marker frame.

➢ Marker identifies each block



Verification

- Playback devices look for marker frame.
- Verify integrity using the same process but backwards.

➢ Viewer can check whether the video is from the expected source

Cryptographically Verified Video – Algorithm Selection

Algorithm	**Public Key Size** (B)	**Private Key Size** (B)	**Signature Size** (B)	**Standardized**
ML-DSA-44	1312	2560	2420	✓
SLH-DSA (PURE-SHA2-128S)	32	64	7856	✓
MAYO-2	4912	24	186	✗

Tab. 1 – PQC signature algorithms: key and signature sizes.

FIPS 204
Module-Lattice-Based Digital Signature Standard

SPHINCS+
Stateless hash-based signatures

FIPS 205
Stateless Hash-Based Digital Signature Standard

NIST
Federal Information Processing Standards (FIPS)

For this, we'll use MAYO, because it has very short signatures.

QSafePlayer

Frame: 11 | FPS: 0 | Video FPS: 30

QSafePlayer - Additional Information

Additional information

Last Signature

Last Signature Time

Signature algorithm used

Last signature was created by

Close

QSafePlayer

Frame: 9 | FPS: 0 | Video FPS: 30

QSafePlayer - Additional Information

Additional information

Last Signature

Last Signature Time

Signature algorithm used

Last signature was created by

Close

Cryptographically Verified Video – Use-Cases

Security and Critical Infrastructure

- Realtime surveillance in airports, banks, and government facilities.
- Signed streams guarantee that footage is authentic and tamper-proof.

Journalism and News Broadcasting

- Live reports from crisis zones or protests can be signed by trusted organizations.
- Ensures that video material used in news or social media is verifiably authentic.

Legal and Law Enforcement Evidence

- Court-admissible recordings (bodycams, dashcams) can be cryptographically signed.
- Guarantees full evidential integrity.

Medical and Scientific Applications

- Secure broadcast of remote medical procedures or lab experiments.
- Prevents tampering when operating or tampering with research evidence.

Cryptographically Verified Video – Pros & Cons

Advantages

Minimal Visual Impairment
Markings consist of individual pixels that are barely visible, even in stills.

Post-Quantum Signatures
Long-term protection against emerging quantum threats.

High Verification Efficiency
Modern hardware enables thousands of signature verifications per second without stuttering.

Direct Embedding with Backward Compatibility
Normal video players are supported (they are not able to verify though).

Limitations

Large Video Files
As described, the mechanism only works with uncompressed video which is unpractically large.

Delay in Livestreams
Streams will lack behind, because latency equals block size.

Verification on End-User Devices
Validation occurs locally to users – streaming platforms remain uninvolved.

No Audio Guarantee
Audio verification works very differently, so it needs to be handled separately.

T Labs

TOGETHER we drive research and development by advancing emerging technologies and inspiring innovation.

Ronny Döring