Google | Privacy, Safety & Security

Updates on Google's PQC migration

Sophie Schmieg, Google

RWPQC, March 08, 2026

The four main areas of cryptography

Asymmetric Encryption

Used mainly for encryption in transit, allows sending confidential messages to another party, by negotiating a shared key.

Digital Signatures

Used very widely, allows for proof of documents being genuine.

Symmetric Cryptography

Used very widely, especially for encryption at rest and for actually transferring data for encryption in transit, allows to encrypt data with a key.

Fancy Cryptography

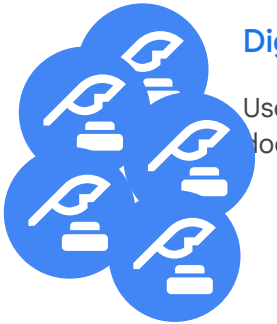
Various other uses of cryptography, often to accomplish complicated privacy guarantees.

The four main areas of cryptography

Asymmetric Encryption

Used mainly for encryption in transit, allows sending confidential messages to another party by negotiating a shared key.

Vulnerable to Store Now Decrypt Later



Digital Signatures

Used very widely, allows for proof of documents being genuine.

Symmetric Cryptography

Used very widely, especially for tion at rest and for actually rring data for encryption in t, allows to encrypt data with a key.

Fancy Cryptography

Various other uses of cryptography, often to accomplish complicated privacy guarantees.

?

What is new? Encryption in transit

- Internal production traffic encryption in transit ✅ (2023)

What is new? Encryption in transit

- Internal production traffic encryption in transit ✅ (2023)
- TLS Consumer facing encryption in transit ✅ (2024)

What is new? Encryption in transit

- Internal production traffic encryption in transit ✅ (2023)
- TLS Consumer facing encryption in transit ✅ (2024)
- SSH ✅ (2025)

What is new? Encryption in transit

- Internal production traffic encryption in transit ✅ (2023)
- TLS Consumer facing encryption in transit ✅ (2024)
- SSH ✅ (2025)
- TLS Customer facing encryption in transit ✅ (February 2026)

What is new? Encryption in transit

- Internal production traffic encryption in transit ✅ (2023)
- TLS Consumer facing encryption in transit ✅ (2024)
- SSH ✅ (2025)
- TLS Customer facing encryption in transit ✅ (February 2026)
- Long tail remains ❌

Example Long Tail

 *

Corp X25519MLKEM768

* This is not a yak. It is a bison, for copyright reasons.

Example Long Tail

Corp X25519MLKEM768

Windows DirectAccess

only supports RSA

* Yaks might be more closely related to bison than to domestic cattle, so it's not that bad.

Example Long Tail

Corp X25519MLKEM768

Windows DirectAccess only supports RSA

RSA-PSS mistake in TPM 2.0 spec *

* Do not attempt to shave bisons. They will kill you.

Example Long Tail

Corp X25519MLKEM768

Windows DirectAccess only supports RSA

RSA-PSS mistake in TPM 2.0 spec

TLS 1.3 only supports RSA-PSS for client certs *

* No seriously, do not approach the danger cow.

Example Long Tail

Corp X25519MLKEM768

Windows DirectAccess only supports RSA

RSA-PSS mistake in TPM 2.0 spec

TLS 1.3 only supports RSA-PSS for client certs

TLS and DirectAccess share credentials *

* This picture was taken with a telelens. No cryptographers were harmed.

Example Long Tail

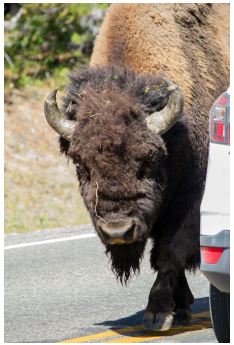
Corp X25519MLKEM768

Windows DirectAccess only supports RSA

RSA-PSS mistake in TPM 2.0 spec

TLS 1.3 only supports RSA-PSS for client certs

TLS and DirectAccess share credentials



Credentials are stored in TPM *

* No bisons were harmed either.

Example Long Tail

*

In conclusion: No X25519MLKEM768 due to lacking RSA-PSS support in a ten year old spec

* Yes, I took more than one bison picture.

What is new? Digital Signatures

- Cloud KMS (2025)

What is new? Digital Signatures

- Cloud KMS (2025)
- Prototyping MTC (2026)

What is new? Digital Signatures

- Cloud KMS (2025)
- Prototyping MTC (2026)
- Limited internal deployments

What is new? Conclusions

- ML-KEM deployment is making progress, but long tail remains

What is new? Conclusions

- ML-KEM deployment is making progress, but long tail remains
- Signature use cases are more difficult due to key management

Emergency Planning: Motivation

- Being surprised by a quantum computer is a business continuity risk

Emergency Planning: Motivation

- Being surprised by a quantum computer is a business continuity risk
- Long signature deployment timelines need special considerations

Emergency Planning: Two Scenarios

Quantum Zero Day

- Very hard to detect

Emergency Planning: Two Scenarios

Quantum Zero Day

- Very hard to detect
- String of unrelated compromises

Emergency Planning: Two Scenarios

Quantum Zero Day

- Very hard to detect
- String of unrelated compromises
- At detection likely actively exploited for some time

Emergency Planning: Two Scenarios

Quantum Zero Day

- Very hard to detect
- String of unrelated compromises
- At detection likely actively exploited for some time

Accelerated Timeline

- Informed by public statements by quantum physicists

Emergency Planning: Two Scenarios

Quantum Zero Day

- Very hard to detect
- String of unrelated compromises
- At detection likely actively exploited for some time

Accelerated Timeline

- Informed by public statements by quantum physicists
- Difficulty distinguishing signal from noise

Emergency Planning: Two Scenarios

Quantum Zero Day

- Very hard to detect
- String of unrelated compromises
- At detection likely actively exploited for some time

Accelerated Timeline

- Informed by public statements by quantum physicists
- Difficulty distinguishing signal from noise
- Public timeline might be lagging behind threat actors

Emergency Planning: Threat Model observations

many fast CRQCs

Emergency Planning: Threat Model observations

many fast CRQCs

- Threat actor will mainly focus on decryption of stored traffic

Emergency Planning: Threat Model observations

many fast CRQCs

- Threat actor will mainly focus on decryption of stored traffic
- Not directly detectable

Emergency Planning: Threat Model observations

many fast CRQCs

- Threat actor will mainly focus on decryption of stored traffic
- Not directly detectable
- Similar to Enigma cryptanalysis

Emergency Planning: Threat Model observations

many fast CRQCs

- Threat actor will mainly focus on decryption of stored traffic
- Not directly detectable
- Similar to Enigma cryptanalysis

few slow CRQCs

Emergency Planning: Threat Model observations

many fast CRQCs

- Threat actor will mainly focus on decryption of stored traffic
- Not directly detectable
- Similar to Enigma cryptanalysis

few slow CRQCs

- Threat actor will mainly focus on single powerful keys

Emergency Planning: Threat Model observations

many fast CRQCs

- Threat actor will mainly focus on decryption of stored traffic
- Not directly detectable
- Similar to Enigma cryptanalysis

few slow CRQCs

- Threat actor will mainly focus on single powerful keys
- Likely targets include CAs, CT logs, and identity provider

Emergency Planning: Threat Model observations

many fast CRQCs

- Threat actor will mainly focus on decryption of stored traffic
- Not directly detectable
- Similar to Enigma cryptanalysis

few slow CRQCs

- Threat actor will mainly focus on single powerful keys
- Likely targets include CAs, CT logs, and identity provider
- Difficult, but not impossible to detect directly

Emergency Planning: Conclusions

- Business continuity planning for PQC can inform emergency plans

Emergency Planning: Conclusions

- Business continuity planning for PQC can inform emergency plans
- Signature deployment is more important in an emergency timeline

Emergency Planning: Conclusions

- Business continuity planning for PQC can inform emergency plans
- Signature deployment is more important in an emergency timeline
- Active quantum computers are hard to detect

Thank you

Sophie Schmieg
Senior Staff Cryptography Engineer
sschmieg@google.com