

CAST-Workshop

2025-05-15



Sicherheit²

Das Zusammenspiel von Safety & Security im Fokus der Kryptoagilität

Karolin Varner & Wanja Zaeske

<https://rosenpass.eu>



Der Plan

- 1. Wir stellen uns vor**
- 2. Safety & Security: Kulturelle Aspekte**
- 3. Kryptografie und Avionik im Dialog**
- 4. Kryptoagilität als Prozess**



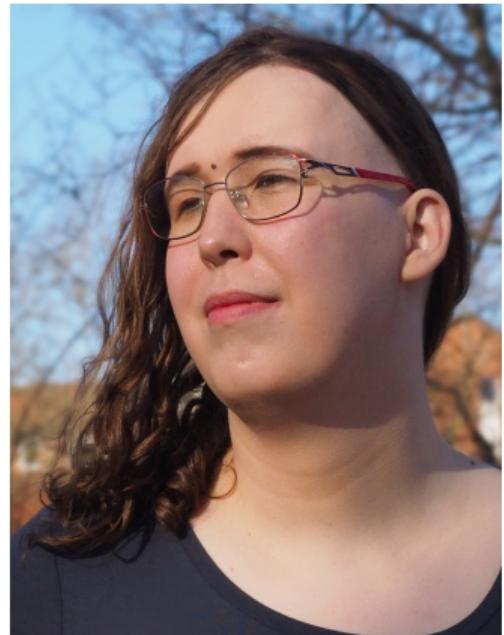
Zum Mitschauen:

[github.com/rosenpass/slides/blob/main/ 2025-05-15-cast/slides.pdf](https://github.com/rosenpass/slides/blob/main/2025-05-15-cast/slides.pdf)

Karolin Varner



- Software-Entwicklerin & Kryptografin
- 11 Jahre in der Industrie bei Startups und Konzernen
- Seit 2024 am Max-Planck-Institut für Sicherheit und Privatsphäre
- Initiatorin & Leiterin des Rosenpass e.V.
- Arbeit an weiteren Projekten wie zum Beispiel der X-Wing KEM





Wanja Zaeske



- Researcher & Software-Entwickler
- 4 Jahre Forschung im Deutsches Zentrum für Luft- und Raumfahrt (DLR)
- Schwerpunkte: Moderne Softwaretechnologien in die Avionik bringen
- Mitgründer von RoRosenpass

Rosenpass e.V.



- 2023 gegründet zur Betreuung des gleichnamigen Projekts
- Absicherung von WireGuard gegen Attacken durch Quantencomputer mittels Protokol-Level Hybridisierung
- Institution für Translationsforschung in der Kryptografie
- Schnittstelle zwischen Forschung, Industrie und Gesellschaft

rosenpass.eu



Safety & Security

Kulturelle Aspekte





Safety & Security in Computersystemen

Safety

- Schutz von Lebewesen

Security

- Schutz von Informationen
 - Information vor Dritten geheimhalten
 - Information vor Manipulation durch Dritte schützen



Problemstellungen & Rahmenbedingungen

	Safety	Security
Fehlerauftreten	Zufällig	Gezielt (durch Angreifer)
Fehlerbehandlung	Weiterbetrieb notwendig	System stoppen
Zieldefinition	Stabil (Physik bleibt gleich)	In Bewegung (Angreifer lernen)
Abgehängene Sofware	Stabil!	Unsicher?
Validierungsprozess	Normiert	Dynamisch



Vertrauen schaffen: Akzeptanzkriterien

	Safety		Security	
	Konfidenz	Verbreitung	Konfidenz	Verbreitung
Praktische Tests	●	●	○	●
Proven-in-use	○	○	-	○
Mathematische Beweise	●	-	●	●
Externe Audits	○	●	●	●

Verbreitung Häufigkeit als tragendes Argument im Assurance-Case
Konfidenz Vertrauen in das Kriterium



Ingenieurskulturen

Safety \Rightarrow Konservativ

- Menschen Sterben bei Versagen
- Probleme sind Verstanden und Stabil

Security \Rightarrow Progressive

- Versagen erzeugt eher finanziellen Schaden
- Problemtypen sind dynamisch und ändern sich dauernd

Security + Safety \Leftrightarrow Konservativ $\not\Leftarrow$ Progressiv

- Menschen sterben bei Versagen
- Probleme sind dynamisch, Zielsetzung in Bewegung



Safety + Security: Checkliste

1. Hohe Zuverlässigkeit []
2. Klarheit über Systemziele
3. Umfassende Validierung
4. Unabhängiges Review
5. Analyse von Softwaresystemen in reeller Hardware
6. Redundante Systeme
7. **Kryptoagilität**



Die vier Domänen der Sicherheit sind...

Luftfahrt

Automobile

Medizintechnik

Automatisierung

Kryptografie in der Avionik

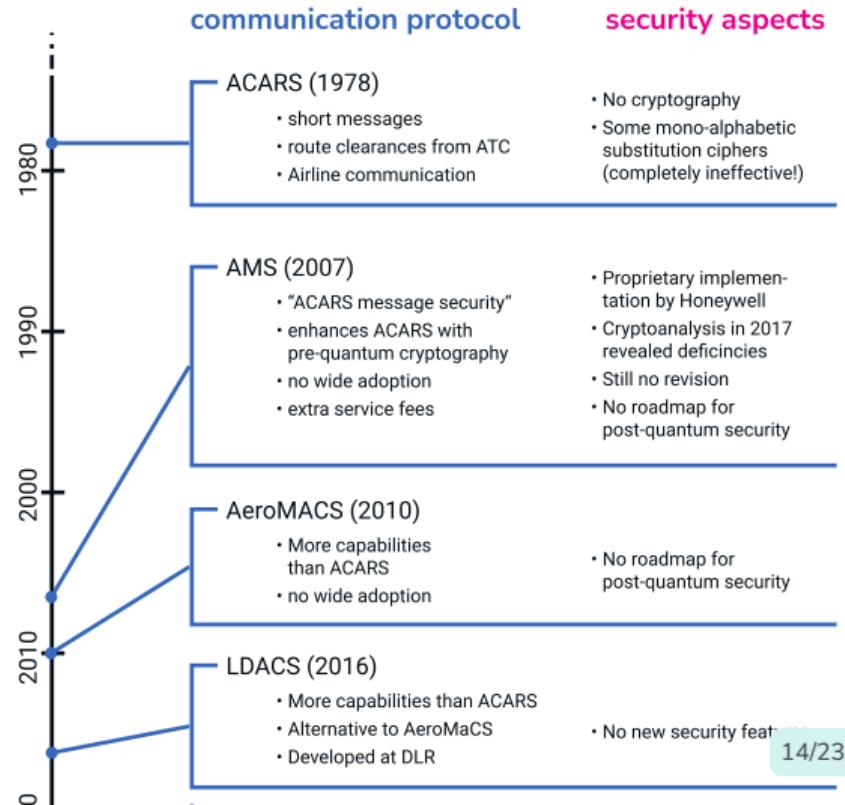


Sichere Kryptografie in der Avionik

(Gähnende Leere)



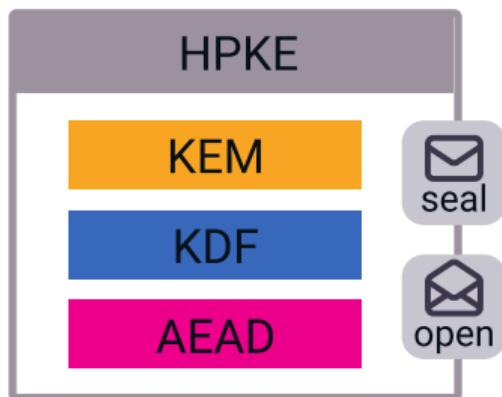
Zum Erschrecken aller...



...wird in der Luftfahrt heutzutage keine sichere Kryptografie eingesetzt.

Kryptographie in der Avionik: Unser Ansatz

- Kryptographischer Standard:
Hybride Public Key Encryption (HPKE)
- Schnittstelle aus HPKE
 - Seal: Nachricht verschlüsseln (und signieren)
 - Open: Nachricht entschlüsseln (und prüfen)





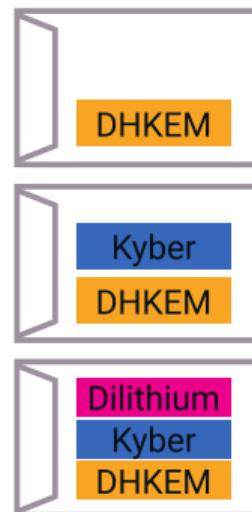
Flexible Einsatzszenarien, gleiche Schnittstelle

- Pre oder post-Quantum?
- Mehr oder weniger Speicherbedarf?
- Schnell oder langsam?
- Post-quantum Authentisierung?

HPKE Diffie-Hellman based AKEM (Authenticated Key Encapsulation Method)
x25519HkdfSha256

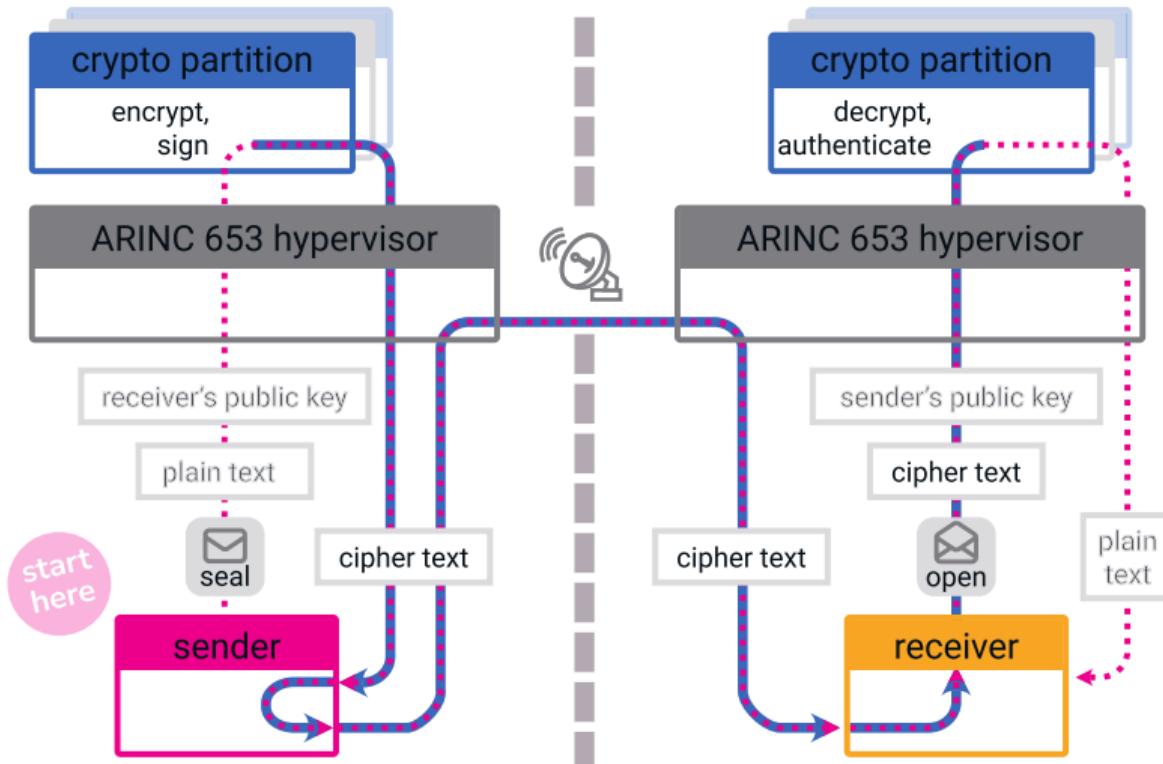
KEM
(Key Encapsulation Method)
Kyber768

signature scheme
Dilithium3



		confidentiality		authenticity	
		classic	post-quantum	classic	post-quantum
	DHKEM	✓	✗	✓	✗
	Kyber	✓	✓	✓	✗
	Dilithium	✓	✓	✓	✓
	Kyber				
	DHKEM				

Partitionen zur Integration in die Avionik



Erkenntnisse

Kryptoagilität als Prozess





Technik

- Klare Zielsetzung
 - Modularisierung reduziert Scope, ermöglicht Fokus
 - Tiefgreifendes Problemverständnis, Schutz wie und wogegen?
- Spielraum
 - Infrastruktur für Continuous Delivery
 - Freiheit, technische Neuerungen zu integrieren



Prozess

- Knowledge-Management
 - Dokumentation von Anforderungen und Entscheidungen
- Change-Management
 - Incident Response
 - Neue mit alten Anforderungen zusammenführen
- Continuous ...
 - ...Development
 - ...Delivery
 - ...Deployment

Kultur

- Fehlerkultur
 - Vorrausschauend
 - Rapid-Response
 - Verheimlichung
 - Fahrlässigkeit
- Oversight
 - Zweischneidige Klinge; "Verpflichtung zur Mittelmäßigkeit"
 - Peer Review
 - Forderungen ⇔ Förderungen
 - sonst Wettbewerbsnachteil
 - Compliance-Tools
 - Methoden-Forschung
 - Chiffren-Wettbewerbe



Kryptoagilität

Leitmotiv



Fortschritt benötigt fortschrittliche Prozesse

- Aviate
 - Modularisierung
 - Continuous Delivery
- navigate
 - Vorrausplanung
- communicate
 - Fordern
 - Fördern
 - Zusammenarbeiten