



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:

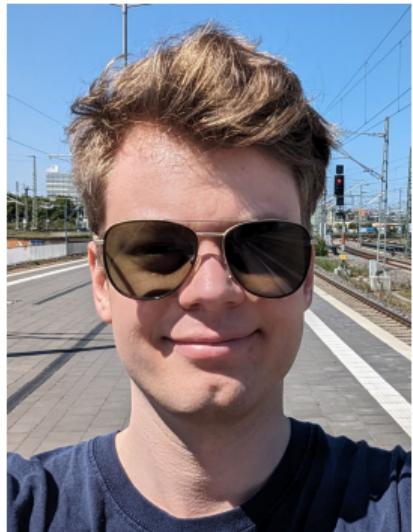
[github.com/rosenpass/slides/blob/main/ 2025-05-15-cast/slides.pdf](https://github.com/rosenpass/slides/blob/main/2025-05-15-cast/slides.pdf)

Karolin Varner

- Softwareentwicklerin & 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

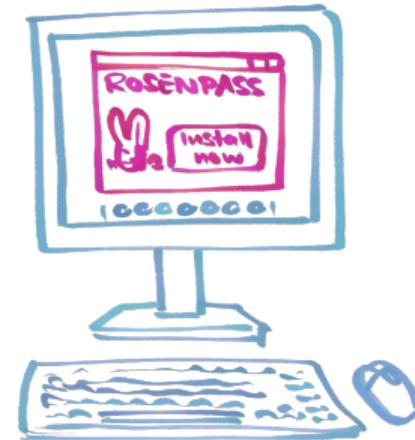


- Researcher & Softwareentwickler
- 4 Jahre Forschung im Deutsches Zentrum für Luft- und Raumfahrt (DLR)
- Schwerpunkte: Moderne Softwaretechnologien in die Avionik bringen
- Rosenpass Mitgründer



Rosenpass e.V.

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



rosenpass.eu

Safety & Security

Kulturelle Aspekte



Safety & Security: Definition

Safety

- Schutz von Lebewesen
 - Maschine, die Computer enthält

Security

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

Problemstellungen & Rahmenbedingungen

Safety

- Zufällige Fehler
- Im Fehlerfall: Weiterbetrieb ermöglichen!
- Stabile Zieldefinition:
Physik bleibt gleich
- Abgehängene Software → Stabil!
- Normierte Validierungsprozesse

Security

- Gezielte Fehler durch Angreifer
- Im Fehlerfall: Lieber das System stoppen
- Zieldefinition ist in Bewegung:
Angreifer lernen auch dazu
- Abgehängene Software → Unsicher?
- Dynamische Validierungsprozesse

Akzeptanzkriterien

Kriterium	Safety		Security	
	Konfidenz	Verbreitung	Konfidenz	Verbreitung
Praktische Tests	+++	+++	+	++
Proven-in-use	++	+	-	+
Mathematische Beweise	+++	-	+++	++
Externe Audits	++	+++	+++	+++

Table: Übersicht der Akzeptanzkriterien in Safety und Security

Verbreitung Häufigkeit als tragendes Argument im Assurance-Case

Konfidenz Vertrauen in das Kriterium

Kulturen

- Safety
 - Menschen Sterben bei Versagen
 - Probleme sind Verstanden und Stabil
 - ⇒ Konservative Ingenieurskultur
- Security
 - Versagen erzeugt eher Finanziellen Schaden
 - Problemtypen sind dynamisch und ändern sich dauernd
 - ⇒ Progressive Ingenieurskultur
- Security und Safety Kombiniert:
 - Menschen sterben bei Versagen
 - Aber die Probleme sind dynamisch, die Zielsetzung in Bewegung
 - ⇒ Konservativ ↳ Progressiv



Safety + Security Benötigt

- Hohe Zuverlässigkeit
 - Klarheit über Systemziele
 - Rigorose Validierungsprozesse (Unabhängiges Review)
 - Analyse von Softwaresystemen in reeller Hardware
 - Redundante Systeme
- ⇒ **Kryptoagilität**

Die Vier Domänen der Sicherheit sind...

Luftfahrt

Automobile

Medizintechnik

Automatisierung

Kryptografie in der Avionik

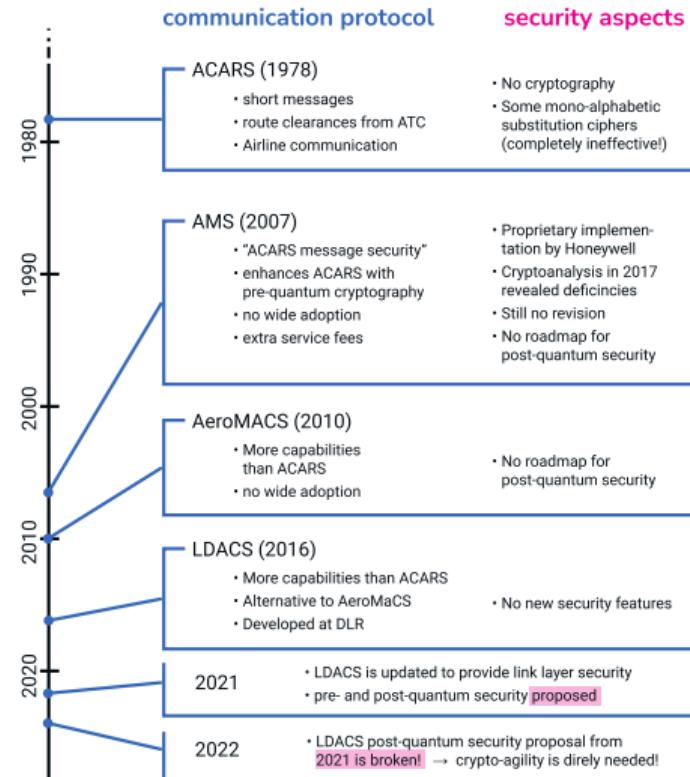


Sichere Kryptografie in der Avionik

(Gähnende Leere)

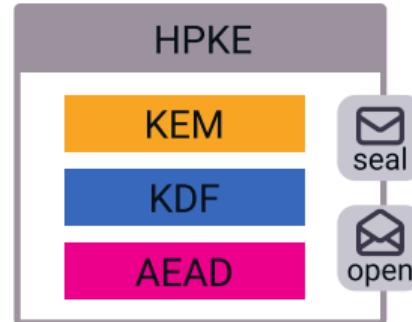
Zum erschrecken aller...

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



Kryptographie in der Avionik: Ansatz

- HPKE-Standard als Basis
- Schnittstelle aus HPKE
 - Seal: Nachricht verschlüsseln (und signieren)
 - Open: Nachricht entschlüsseln (und prüfen)
- Interne Umsetzung Modular basiert auf Modulen (KEM, KDF & AEAD^a)



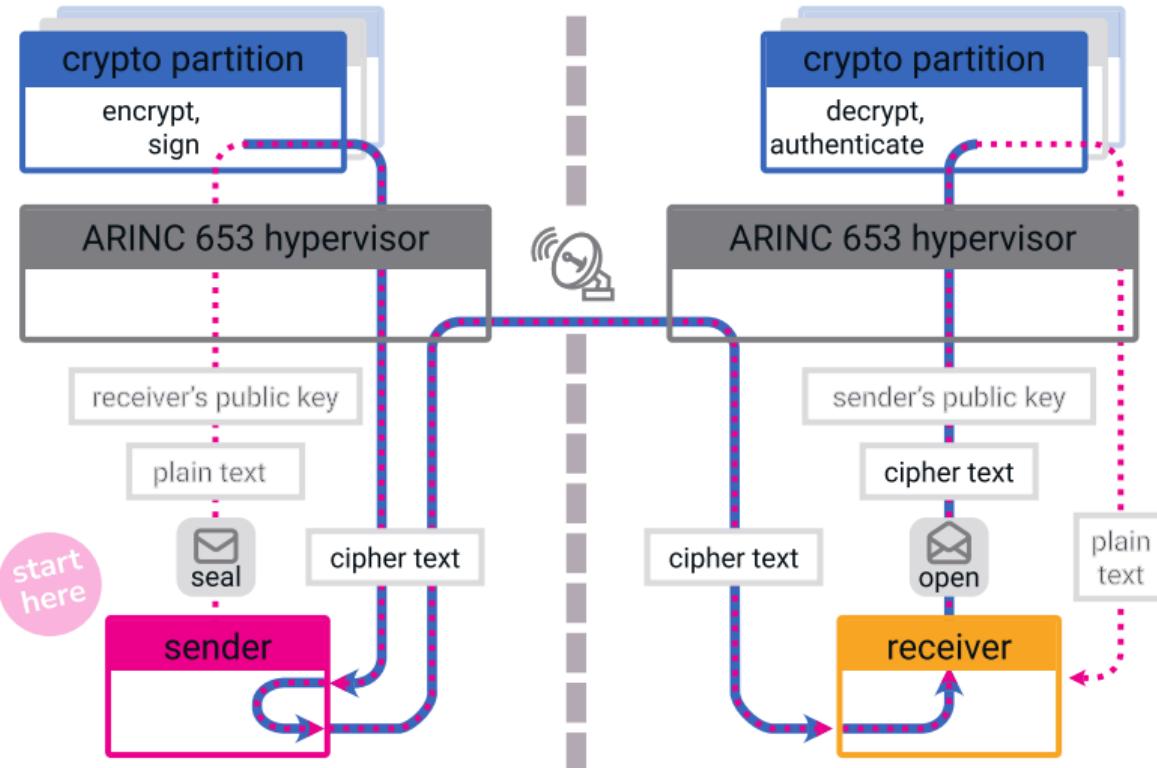
^a Avioniker und auch Kryptographen lieben Akronyme

Flexible Einsatzszenarien, gleiche Schnittstelle

- Pre oder Post-Quantum?
- Mehr oder weniger Speicherbedarf?
- Schenelle or langsame Berechnung?
- Post-quantum Authentisierung?

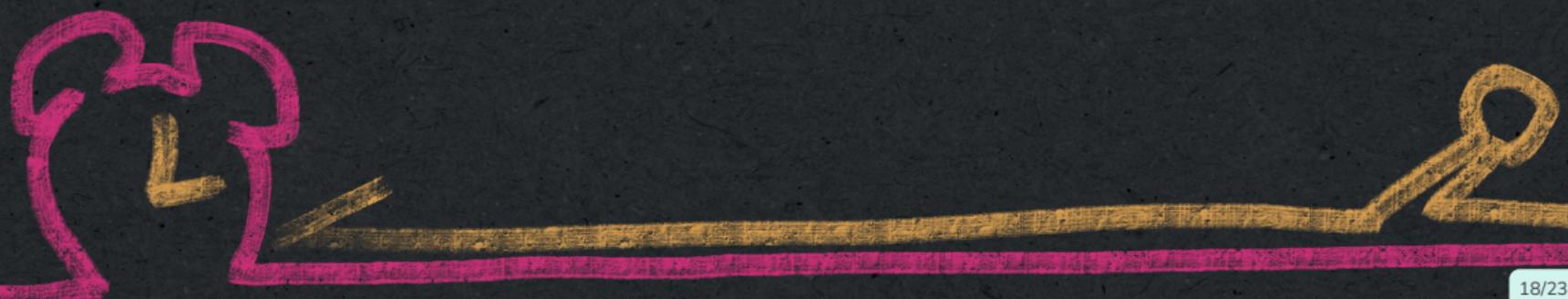
		confidentiality		authenticity	
		classic	post-quantum	classic	post-quantum
HPKE Diffie-Hellman based AKEM (Authenticated Key Encapsulation Method) x25519HkdfSha256		DHKEM		✓	✗
KEM (Key Encapsulation Method) Kyber768		Kyber	DHKEM	✓	✓
signature scheme Dilithium3		Dilithium	Kyber	✓	✓
		DHKEM		✓	✓

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
 - Zweischniedige Klinge; "Verpflichtung zur Mittelmäßigkeit"
 - Peer Review
 - Forderungen ⇔ Förderungensonst Wettbewerbsnachteil
 - Compliance-Tools
 - Methoden-Forschung
 - Chiffren-Wettbewerbe



Kryptoagilität

Leitmotiv



Fortschritt benötigt fortschrittliche Prozesse

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