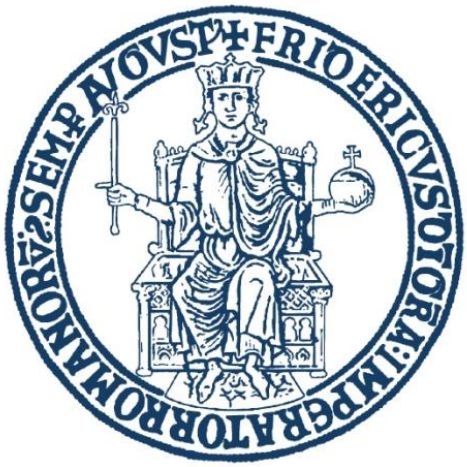

UNIVERSITÀ DEGLI STUDI
DI NAPOLI FEDERICO II

Corso di Laurea Magistrale in Ingegneria Informatica

Risk Assessment

CARAF: Crypto Agility Risk Assessment Framework

Professoressa Alessandra De Benedictis

Conte Pietro

Anno Accademico 2025–2026

Contents

Introduzione

Cosa tratteremo?

Negli ultimi anni la sicurezza informatica ha assunto un ruolo sempre più centrale, poiché la crescente digitalizzazione di servizi e comunicazioni ha reso i sistemi informativi un bersaglio privilegiato per attacchi e minacce. In questo contesto, la crittografia rappresenta uno degli strumenti fondamentali per garantire riservatezza, integrità e autenticità dei dati.
Tuttavia, l'evoluzione delle tecniche di attacco ha iniziato a mettere in discussione anche l'affidabilità degli attuali meccanismi crittografici. Per questo motivo, questo lavoro analizza i rischi connessi alla crittografia in assenza di un'adeguata gestione e di strategie di crypto-agility.

Con crypto agility faremo riferimento alla capacità di un'entità di sostituire rapidamente e a basso costo algoritmi o protocolli crittografici esistenti con nuove alternative più sicure. Il problema principale riguarda la transizione da una soluzione crittografica a un'altra: questa operazione può richiedere molto tempo ed esporre le organizzazioni a rischi non necessari.

In definitiva, questo paper propone un framework per analizzare e valutare i rischi derivanti dalla mancanza di crypto-agility, offrendo un approccio strutturato per supportare le organizzazioni nella gestione di questa criticità. Questo framework è *Crypto Agility Risk Assessment Framework (CARAF)*, un framework operativo in cinque fasi progettato per aiutare organizzazioni nelle varie analisi che verranno illustrate.

1 Capitolo 1

1.1 Origine del problema

La storia di Enigma rappresenta un primo esempio di come la mancanza di crypto-agility possa generare rischi significativi. Enigma, uno dei primi sistemi di crittografia più noti al mondo, era considerato estremamente sicuro alla sua creazione. Tuttavia, grazie allo studio di scienziati provenienti dai vari paesi del mondo, si riuscirono a decifrarne i codici. Nonostante la scoperta, i Nazisti non abbandonarono Enigma per passare a un sistema più sicuro. Questa scelta è dovuta ai vincoli operativi e organizzativi in quel periodo storico, perchè, sostituire un algoritmo crittografico comportava notevoli sfide.
Questo esempio storico mette in luce il concetto di crypto-agility: la capacità di sostituire algoritmi o protocolli crittografici con un impatto minimo sulle operazioni e sui costi. Nel caso di Enigma, la mancanza di crypto-agility limitò la capacità dei Nazisti di reagire a una vulnerabilità critica.
Anche le organizzazioni moderne si trovano oggi ad affrontare rischi analoghi, anche se il contesto è ben diverso.

Figure 1: Crypto-Agility

2 Capitolo 2

2.1 Tecnologia sotto minaccia

Le nuove tecnologie possono creare enormi problemi alle organizzazioni. Nel dettaglio, i computer quantistici possono rompere gli algoritmi crittografici tradizionali. Per citarne qualcuno, abbiamo:

1. algoritmo di Shor: in grado di violare quasi tutti i sistemi a chiave pubblica, come RSA:

2. algoritmo di Grover: in grado di aumentare il rischio anche per gli algoritmi simmetrici (come AES) e le funzioni hash (come SHA).

Per questo motivo, alcuni algoritmi non sono più sicuri senza una versione quantum-safe, mentre altri possono diventare sicuri con delle piccole accortenze, come l'aumento della lunghezza delle chiavi.

Algoritmi	**Tipo**	**Impatto Quantum**
AES	Simmetrica	Usare chiavi più lunghe
SHA	Hash	Output maggiore
RSA/ECC	Pubblica	Non più sicure

Table 1: Impatto dei computer quantistici su diversi algoritmi crittografici.

Tra le vulnerabilita' reali recenti, spicca particolarmente la vulnerabilità **ROCA (2017)**. Essa non è altro che un difetto nella libreria RSA che porto milioni di dispositivi a rischio. Questo dimostra che, **senza crypto-agility, le aziende non riescono a reagire rapidamente.**

2.2 Come valutare il rischio

La mancanza di crypto-agility non rappresenta soltanto una sfida tecnica, ma costituisce un vero e proprio **rischio aziendale**. Le organizzazioni, infatti, si trovano a dover rispondere a una domanda cruciale: **come valutare in maniera strutturata il rischio derivante dalla crypto-agility o dalla sua assenza?**
I metodi tradizionali di valutazione del rischio, come quelli proposti da NIST SP 800-30 o ISO/IEC 27005, risultano fondamentali per la sicurezza informatica in generale, ma sono meno efficaci quando si tratta di minacce incerte o difficilmente quantificabili, come nel caso della transizione crittografica.
Per affrontare questa lacuna, in questo capitolo viene presentato il **Crypto Agility Risk**

Assessment Framework (CARAF), un modello a cinque fasi (5D) che consente di valutare il rischio associato alla mancanza di crypto-agility. Troviamo:

- identificazione del vettore di minaccia;
- identificazione degli asset impattati;
- valutazione del valore atteso degli asset compromessi;
- scelta della strategia di mitigazione;
- definizione di una roadmap di implementazione.

NOTA: Il contributo di questo lavoro è un framework per affrontare la sicurezza e la gestione del rischio in modo proattivo: cerca di anticipare i problemi invece di reagire solo quando si verificano incidenti.

2.3 Threat modeling operativo

Il *threat modeling* è il processo sistematico volto a identificare gli attori ostili, le loro capacità e motivazioni, i vettori d'attacco e gli asset esposti, con l'obiettivo di produrre scenari di minaccia direttamente utilizzabili nella valutazione del rischio secondo CARAF. Per rendere operativo questo processo si normalizzano i seguenti elementi:

Attori (Threat Actors): categorie di attaccanti rilevanti per l'organizzazione;

Risorse e abilità: per ciascuna categoria indicare risorse tipiche (potenza di calcolo, accesso fisico), skill (capability di eseguire attacchi crittografici o di compromissione);

Vettori di attacco (Attack Vectors): superfici d'attacco concrete; per esempio:

- Compromissione di chiavi private;
- Debolezze nelle librerie di generazione chiavi (es. ROCA).

3 Capitolo 3

Introduciamo le cinque fasi.

3.1 Fase 1: Identificazione della minaccia

In questa fase si individua il vettore di minaccia che giustifica la valutazione del rischio. CARAF mira ad affrontare una probabile futura minaccia alla sicurezza, consentendo all'organizzazione di prepararsi in anticipo. Tuttavia, poiché la minaccia è futura, un problema di questa fase potrebbe essere quello di non avere informazioni sufficienti per identificare accuratamente il danno. Bisogna però ricordare che uno dei punti di forza del framework in esame è quello di essere proattivo.

3.2 Fase 2: Inventario degli asset

Una volta identificata la minaccia, il passo successivo consiste nel creare un inventario dettagliato degli asset crittografici impattati. Gli aspetti principali da considerare sono:

- **Ambito (Scope):** quali asset rientrano nell'analisi;
- **Sensibilità (Sensitivity):** valutare l'importanza degli asset;
- **Crittografia (Cryptography):** elencare gli algoritmi utilizzati;
- **Gestione del ciclo di vita (Lifecycle Management):** backup, sostituzione e condivisione dati con terze parti.

3.3 Fase 3: Stima del rischio

La formula generica per la stima del rischio è: **"Rischio = Probabilità * Impatto"**. Invece, nella crypto-agility il rischio viene valutato diversamente. Si valuta considerando **Tempistica** e **Costo di mitigazione**:

$$\text{Rischio} = \text{Tempistica} \times \text{Costo}$$

Tempistica si basa sul modello XYZ di Mosca:

- X – durata residua dell'asset;
- Y – tempo necessario per aggiornare l'asset;
- Z – tempo stimato prima che la minaccia diventi concreta. Ad esempio il numero di anni prima che si verifichi.

Se X + Y > Z, il rischio è alto o critico; se X + Y < Z, il rischio è basso o medio.

Costo di mitigazione dipende da complessità tecnica, infrastruttura e dalla flessibilità degli asset.

3.4 Fase 4: Strategie di mitigazione

In questa fase si definiscono le azioni in base al rischio e al costo:

- **Mettere in sicurezza l'asset:** aggiornare algoritmi o implementare controlli compensativi;
- **Accettare il rischio:** se il rischio è tollerabile.
- **Eliminare gradualmente gli asset impattati:** se il costo di mitigazione supera il valore dell'asset.

3.5 Fase 5: Roadmap organizzativa

Infine, si definisce una roadmap operativa per implementare la strategia scelta. Gli elementi principali includono:

- Aggiornamento delle politiche crittografiche, rimuovendo algoritmi obsoleti;
- Pianificazione del change management per aggiornamento o sostituzione;
- Implementazione di automazioni per la gestione di chiavi e algoritmi;
- Revisione dei contratti con fornitori di terze parti.

Questa fase assicura che le decisioni siano integrate nella governance aziendale e nei processi di sicurezza.

Figure 2: Grafico a torta

4 Capitolo 4

In questo capitolo tratteremo un caso di studio.

4.1 Caso di studio

L'obiettivo del caso di studio è usare il framework CARAF per valutare il rischio e decidere come mitigarlo, in modo strutturato e proattivo.
La prima cosa da fare è **indiviuare la minaccia**. Nei capitoli precedenti, abbiamo capito che il quantum computing può compromettere molte organizzazioni e algoritmi, in particolare quelli a chiave pubblica. I nuovi algoritmi **quantum safe (PQC)** si basano su principi matematici diversi, ma introducono nuovi vincoli per le organizzazioni:

- Chiavi più grandi → più memoria richiesta;
- Output più grandi → più dati da trasmettere, quindi maggiore larghezza di banda.

Il secondo passo è **l'inventario degli asset**. L'inventario è il passaggio in cui si identificano tutti gli asset crittografici impattati. Qui ci concentriamo su TLS, ossia la crittografia usata per le comunicazioni sicure, in particolare nei dispositivi IoT. In questa fase, ricordiamo che ci sono 4 aspetti principali da considerare:

- Ambito: TLS;
- Sensibilità: dispositivi IoT e dati critici;
- Crittografia: principalmente a chiave pubblica;
- Gestione del ciclo di vita: i dispositivi devono rispettare le politiche di aggioramento e sostituzione.

Il terzo step è la **stima del rischio**. Il rischio dipende da quanto presto la minaccia diventa reale (Z), quanto tempo serve per mitigare (Y) e quanto è lunga la vita utile dell'asset (X).
Iniziamo presentando la minaccia (Z), ossia il tempo prima che i computer quantistici diventino una reale minaccia:

Durata in anni	Livello
0-5	Critico
5-10	Alto
10-20	Medio
20+	Basso

Table 2: Tabella durata anni.

Passiamo adesso a (Y), ossia al tempo necessario per mitigare quell'asset. Si dividono in due tipi:

- Asset con supporto quantum: 5-10 anni;
- Asset senza supporto quantum: 11-20+ anni.

L'ultimo fattore è (X), ossia la durata di vita. I dispositivi IoT hanno una durata che va da 2 a 20+ anni.
Di seguito è riportata la tabella che fornisce la stima del rischio:

Tempistica	1–Rischio Basso	2–Rischio Medio	3–Rischio Alto	4–Critico
X (Durata/Vita utile)	5	10	20	20+
Y (Mitigazione)	0–5	6–10	11–20	20+
Z (Minaccia)	20+	10–20	5–10	0–5

Table 3: Stima del rischio di tempistica in anni.

Come viene interpretato tutto ciò? Se X+Y>Z, il rischio è alto o critico perché la minaccia arriva prima che l'asset possa essere aggiornato.

Rischio	Significato
1	Basso
2	Medio
3	Alto
4	Critico

Table 4: Tabella di rischio.

Invece, il costo della mitigazione varia in base al tipo di asset e se supportano già PQC, ad esempio:

- Asset già compatibili PQC → costo basso;
- Asset non compatibili PQC → costo alto.

Adesso inizia la fase 4, ossia **la strategia di mitigazione**. In questa fase si decide cosa fare in base al rischio e al costo. Si può:

1. Accettare il rischio → se basso o se la gestione costosa;
2. Mettere in sicurezza → aggiornare a PQC o a soluzioni ibride;
3. Eliminare gradualmente → sostituire gli asset obsoleti o non aggiornabili.

L'ultimo step è la **Roadmap organizzativa**. La roadmap specifica come implementare le azioni:

- Rischio basso → continuare con i piani attuali;
- Rischio medio → processo di eccezione, aggiornamenti pianificati;
- Rischio alto/critico su terze parti → eliminare gradualmente, sostituire fornitori se necessario;
- Aggiornamento a algoritmi quantum-safe → valutare trade-off, investire in test personalizzati.

5 Conclusioni

Il framework CARAF consente alle organizzazioni di affrontare i rischi derivanti dalla mancanza di crypto-agility in modo strutturato e proattivo. Il caso di studio sul quantum computing mostra come identificare minacce, inventariare asset, stimare rischi, scegliere strategie di mitigazione e definire una roadmap concreta.