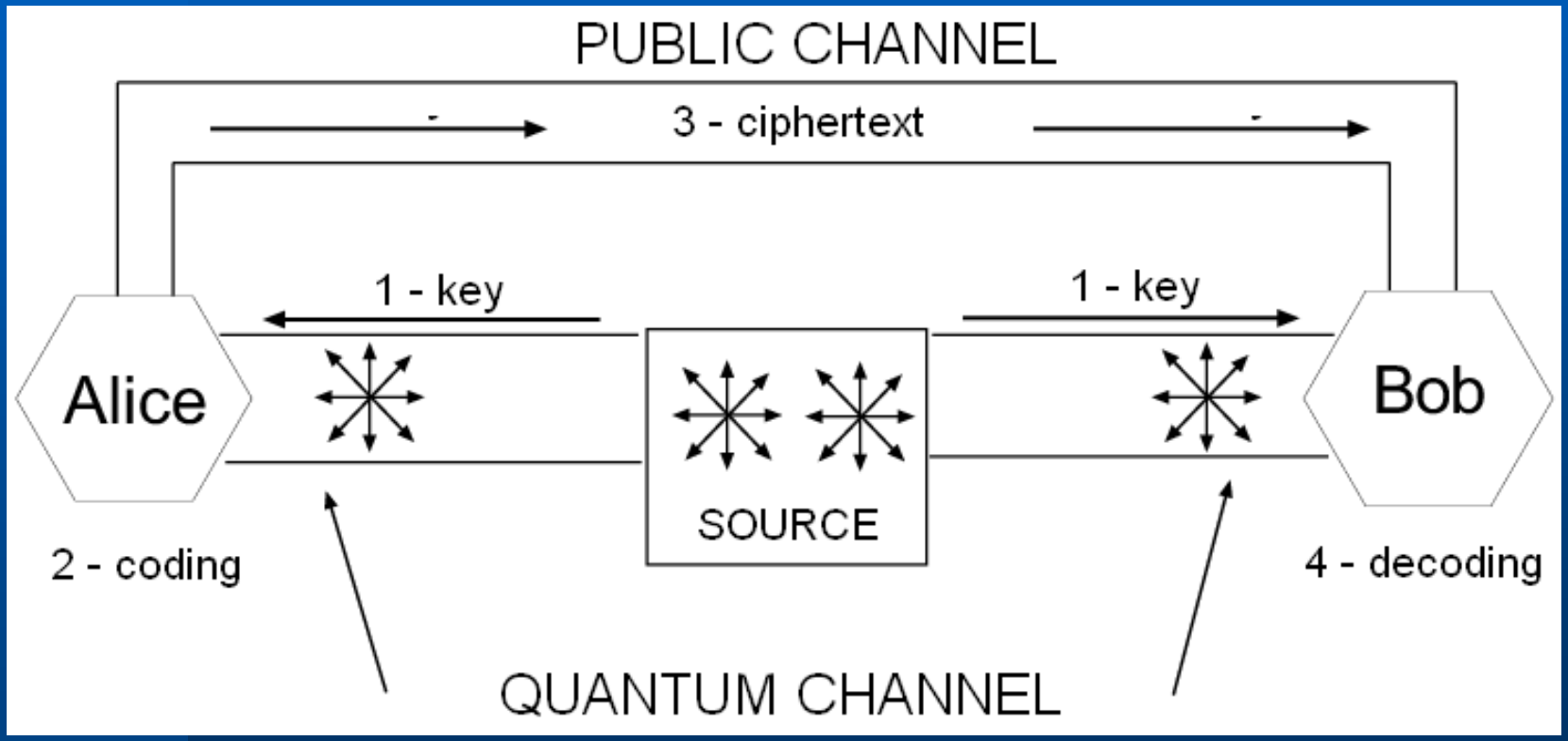
# Unconditional security of a quantum-key storage

Alessio Merlo

# Agenda

- **Introduzione al problema**
  - **Crittografia Quantistica e OTP**
  - **Problema del key-storage**
- **Difesa dello storage**
  - **Architetture ATHOS, PORTOS e ARAMIS**
- **Conclusioni e future works**

# Crittografia Quantistica



# Problema e obiettivi

- **Implementazioni attuali non garantiscono la produzione di chiave “on-demand”. Chiave creata, salvata su storage e usata in fasi successive.**

- **Obiettivi:**
  - **Sicurezza incondizionata dello storage in rete**
  - **Costo “ragionevole”**
  - **Il piu’ possibile general purpose**

# Lo scenario

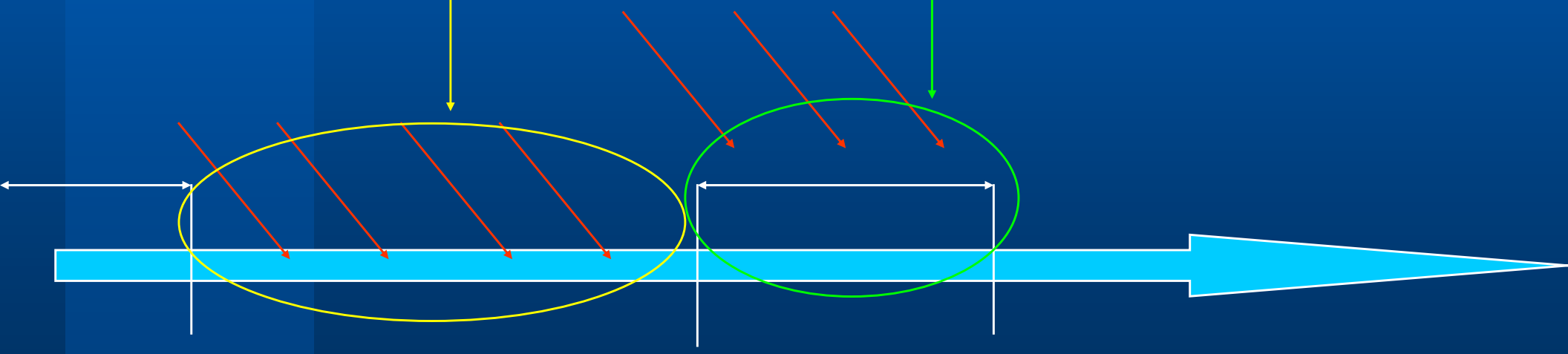

- **Lo storage DEVE essere collegato ad una macchina in rete**
- **MINACCE: attacchi dalla rete**
- **Sicurezza incondizionata = impossibilita' di attacchi esterni**

# L’idea

Suscettibile ad attacchi

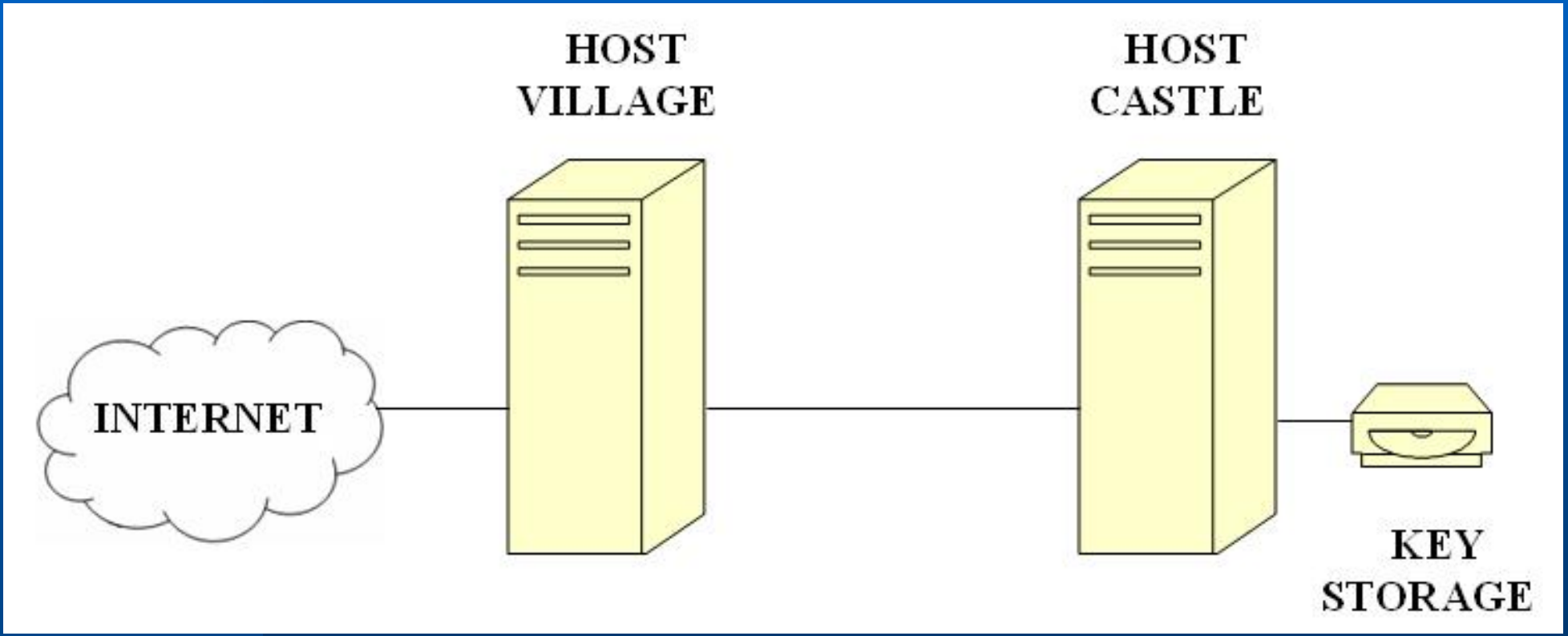
Eliminazione attacchi presenti prima della connessione = Impossibilità nuovi attacchi

**SICUREZZA INCONDIZIONATA**



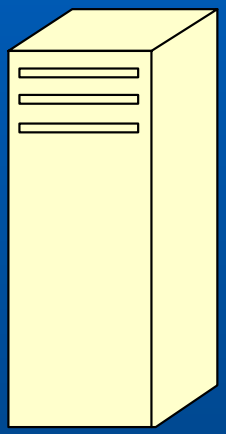
# ATHOS Defensive System

## (Asymmetric Two-HOsts Storage Defensive System)




Lo storage è un dispositivo specifico e monoutente.

# L’host CASTLE

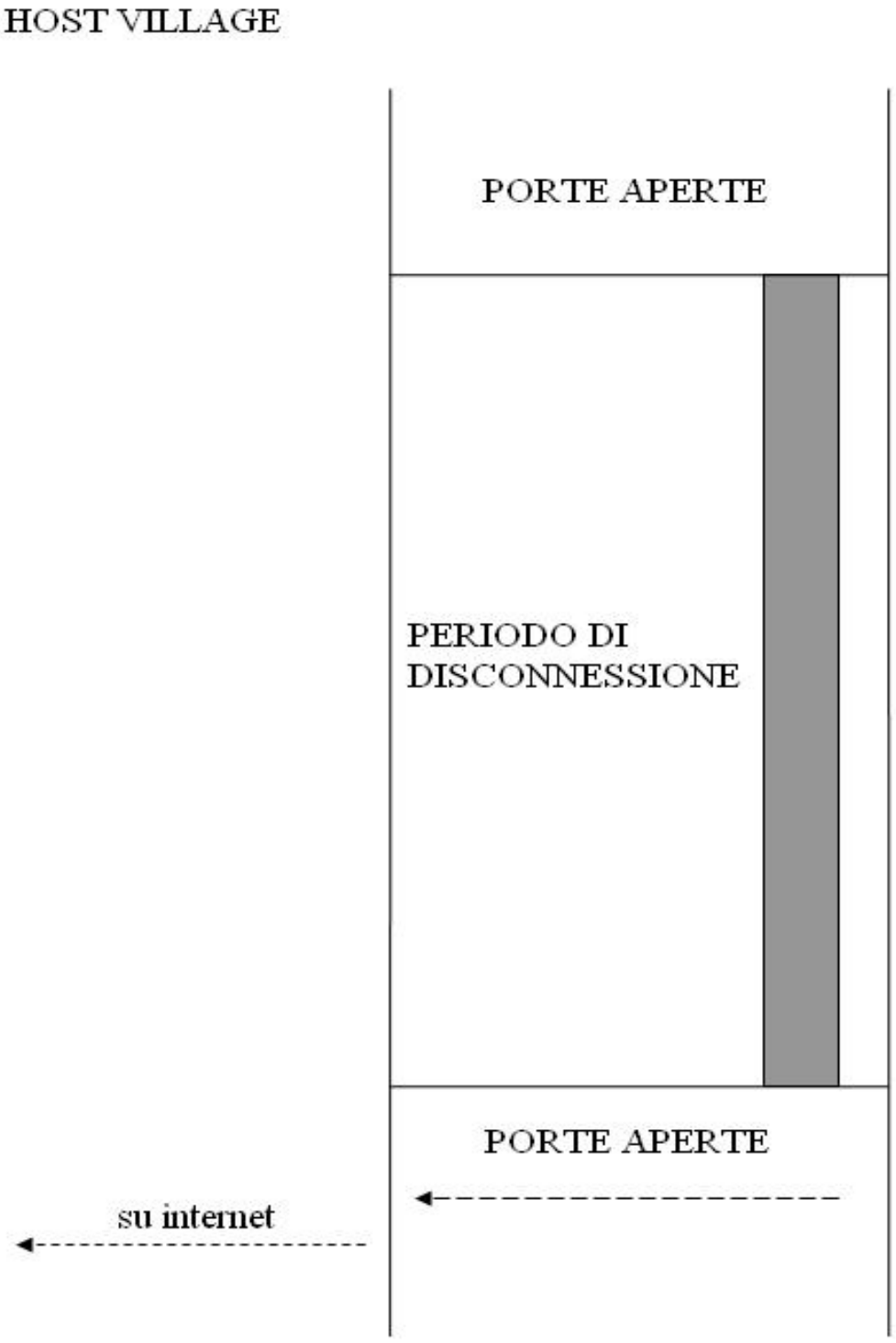


- un dispositivo di output video, dispositivi standard di input (tastiera, mouse) per l’utente
- un dispositivo di input e output dati (lettore floppy, cd-rw, dvd-rw, porta usb per penna o hd esterno) NON ESEGUIBILE
- Un altro dispositivo di I/O ove montare il dispositivo di storage con le chiavi
- Memoria primaria
- NESSUN DISPOSITIVO DI MEMORIA SECONDARIA
- Sistema operativo residente su ROM (MOSES) che sovrintende le operazioni di cifratura implementando due diversi protocolli per le fasi di invio e ricezione di ciphertext.

# MOSES
## (Minimal Operating System Enhancing Security)

- Minimale, fase di boot molto rapida e dedicato
- attivazione e disattivazione della porta di rete
- mount e dismount logico dell'unita' di storage, lettura ed eliminazione della chiave
- cifratura/decifratura OTP
- Protocolli di comunicazione con l'host VILLAGE
- Avvio dell'host CASTLE in due modalità (TRANSMITTER e RECEIVER)

# INVIO




1) Log-on dell'utente
2) Riavvio dell'host CASTLE in modalita' TRANSMITTER

SISTEMA "PULITO"

3) Connessione del dispositivo contenente il messaggio da cifrare
4) Collegamento dello storage sull'Host CASTLE
5) Calcolo del messaggio cifrato
6) Smontamento del dispositivo di storage
7) Smontamento del supporto di input
8) Collegamento dell'host CASTLE all'host VILLAGE
9) Invio del messaggio
10) Log-off dell'utente

# FASE DI RICEZIONE

HOST VILLAGE

HOST CASTLE

da internet

1) Segnalazione all'host CASTLE dell'arrivo di un messaggio

2) Invio del messaggio cifrato al'Host CASTLE

porte aperte

PERIODO DI DISCONNESSIONE

porte aperte

3) Chiusura delle porte di rete

4) Collegamento dispositivo di storage

5) Collegamento del dispositivo di output

6) Decifratura e salvataggio del messaggio

7) Eliminazione della chiave usata dal supporto di storage e smontamento

8) Smontamento del dispositivo di output

9) Riavvio del sistema sull'host CASTLE in modalità RECEIVER (porte aperte).

- SISTEMA PULITO -

RICEZIONE

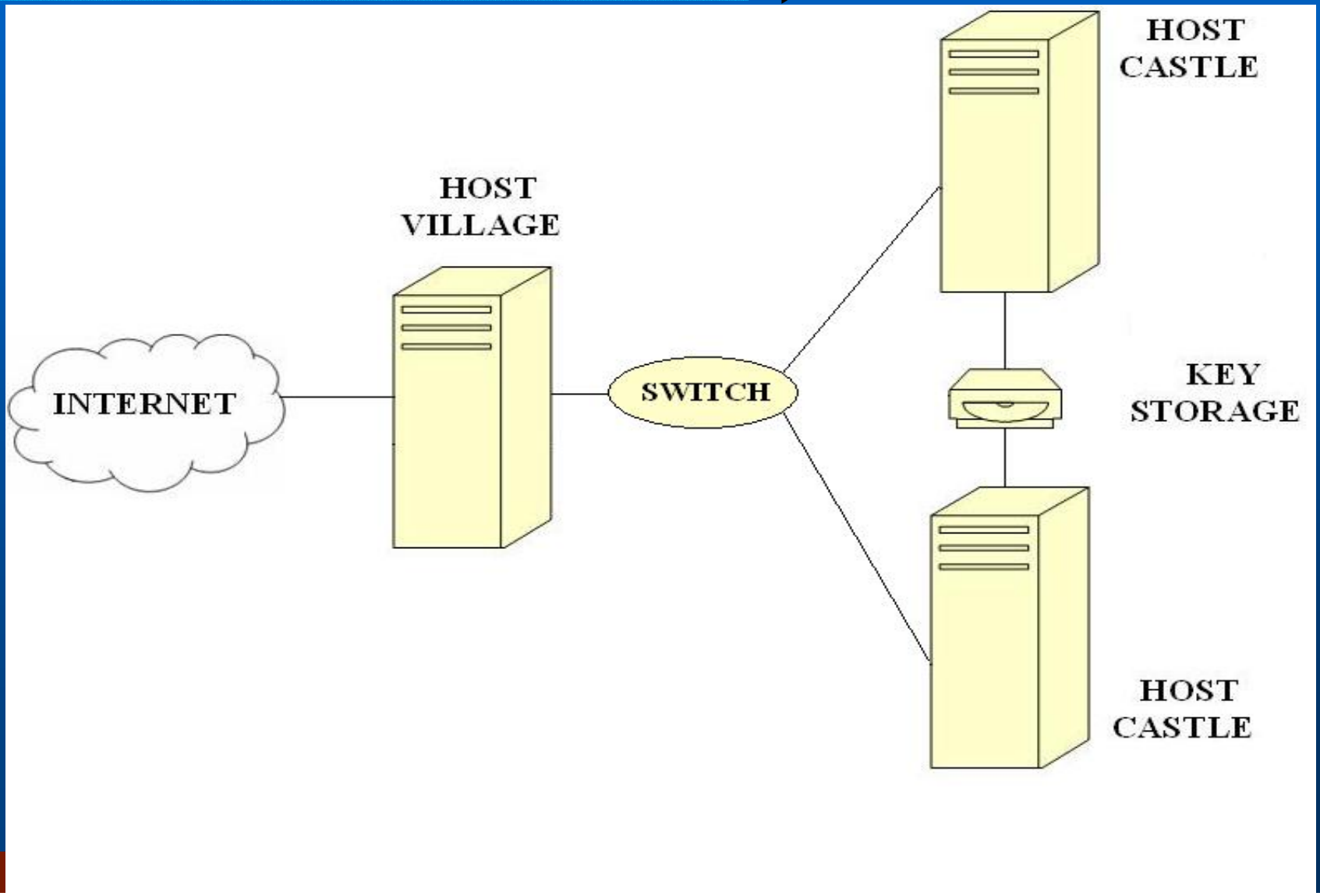
# Considerazioni su ATHOS

**+ Attacchi impossibili sotto le ipotesi fatte**

**- Alto OVERHEAD a causa dei riavvii**

**- Ogni operazione comporta un riavvio**

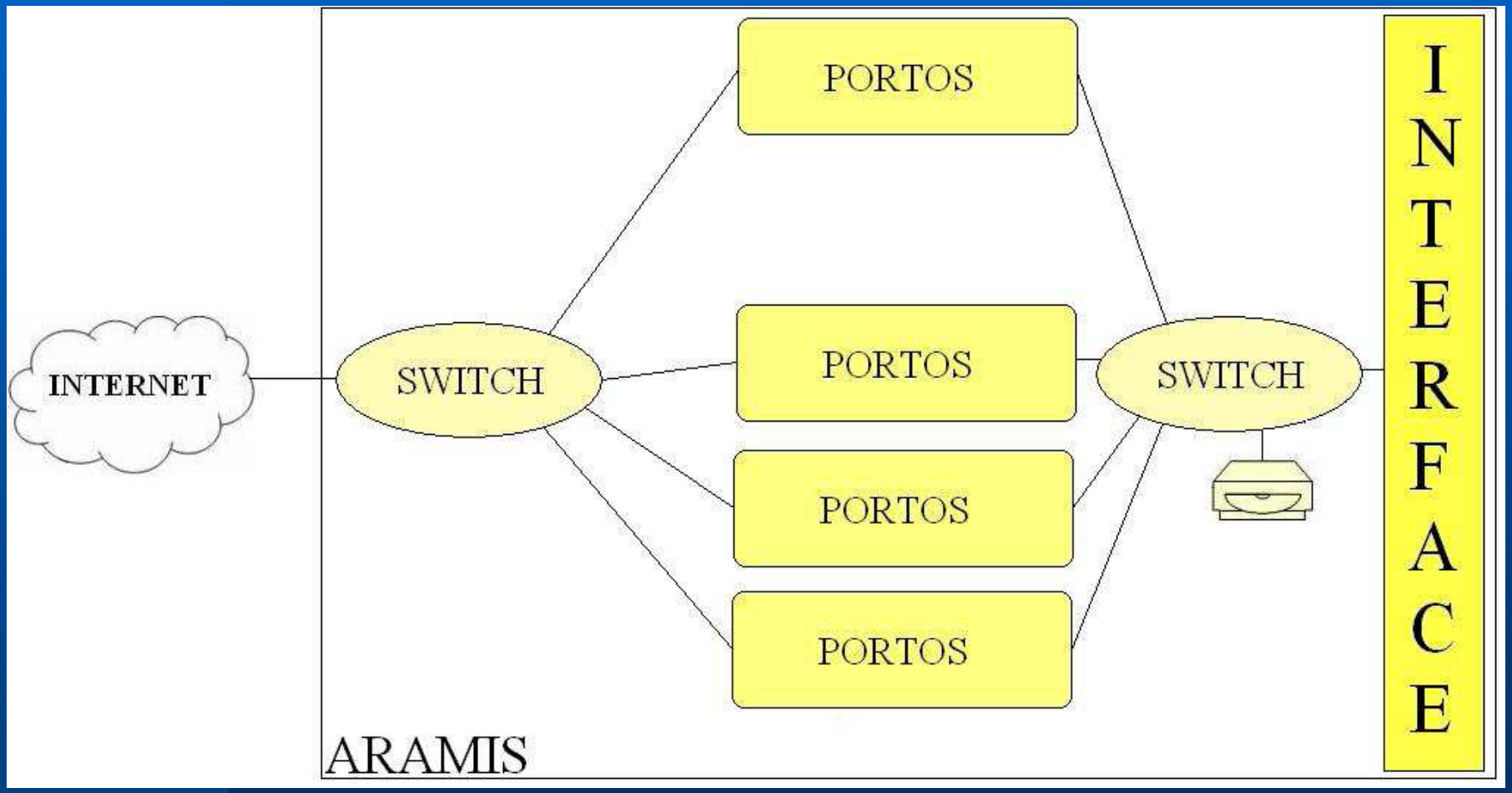
# PORTOS Defensive System (Pair-Organized Recovering Time On Stall)



# Peculiarita’ di PORTOS

+ Maggiore efficienza di ATHOS
+ Costi contenuti
+ Struttura poco piu’ complicata
+ Strategie di sicurezza aumentate
- Impossibilita’ di un utilizzo parallelo degli host CASTLE
- Efficienza dipendente dalla lunghezza media delle operazioni di ricezione (T(boot)>T(op) )

# ARAMIS Defensive System (Advanced Redundant Asymmetric Multipoint-Installation Storage)



# Conclusioni e future works

- **ARAMIS è *scalabile* e garantisce una potenziale disponibilità totale (al costo di spreco di risorse). Al momento è un work in progress.**
- **Autenticazione dell'utente: SCANNER (Smart Card Authentication with New Number at Every Reading)**
- **Lavoro eseguito in collaborazione con Elsag S.p.A.**