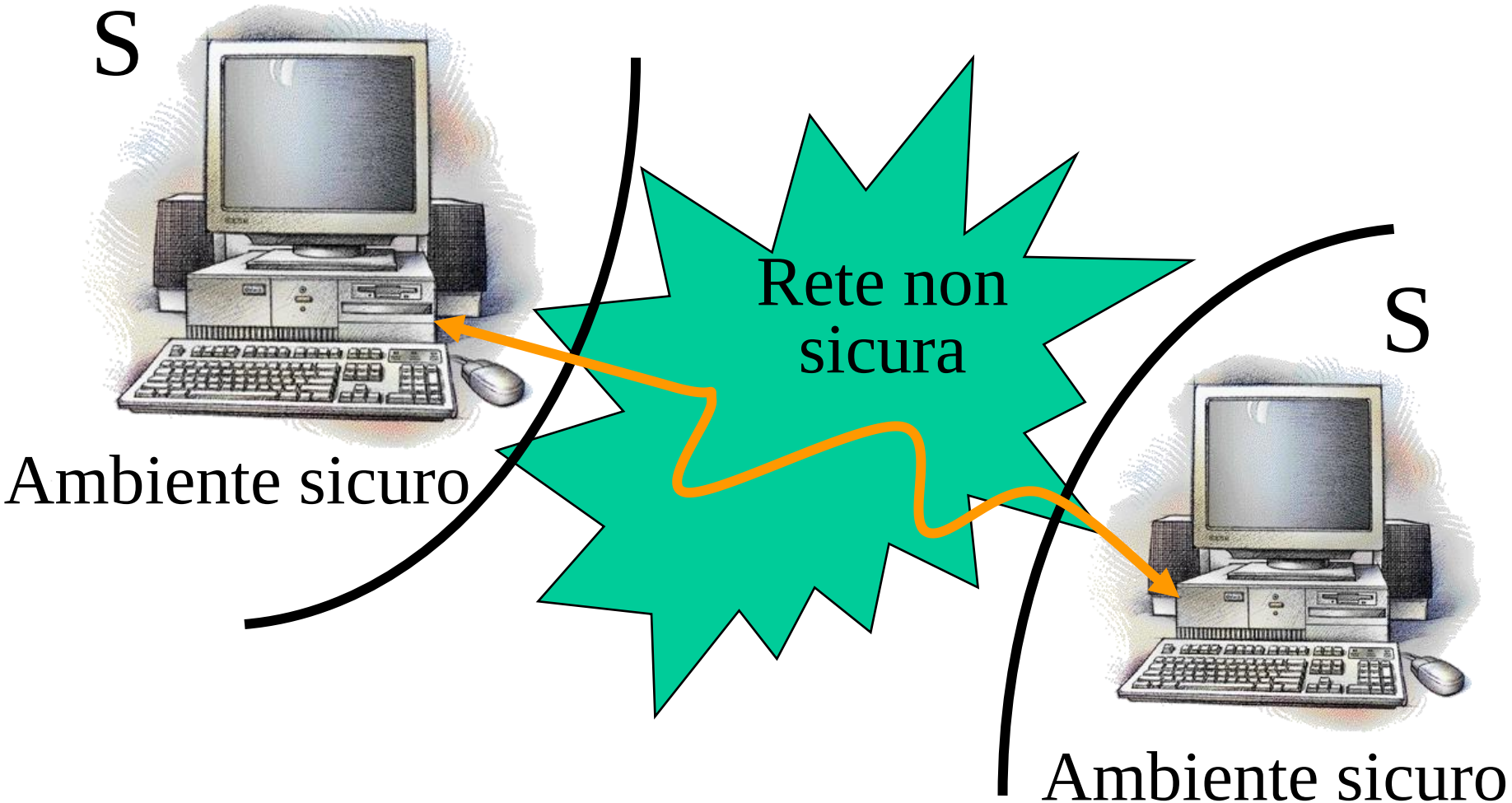
Autenticazione e Firma Elettronica

Prof. Francesco Bergadano

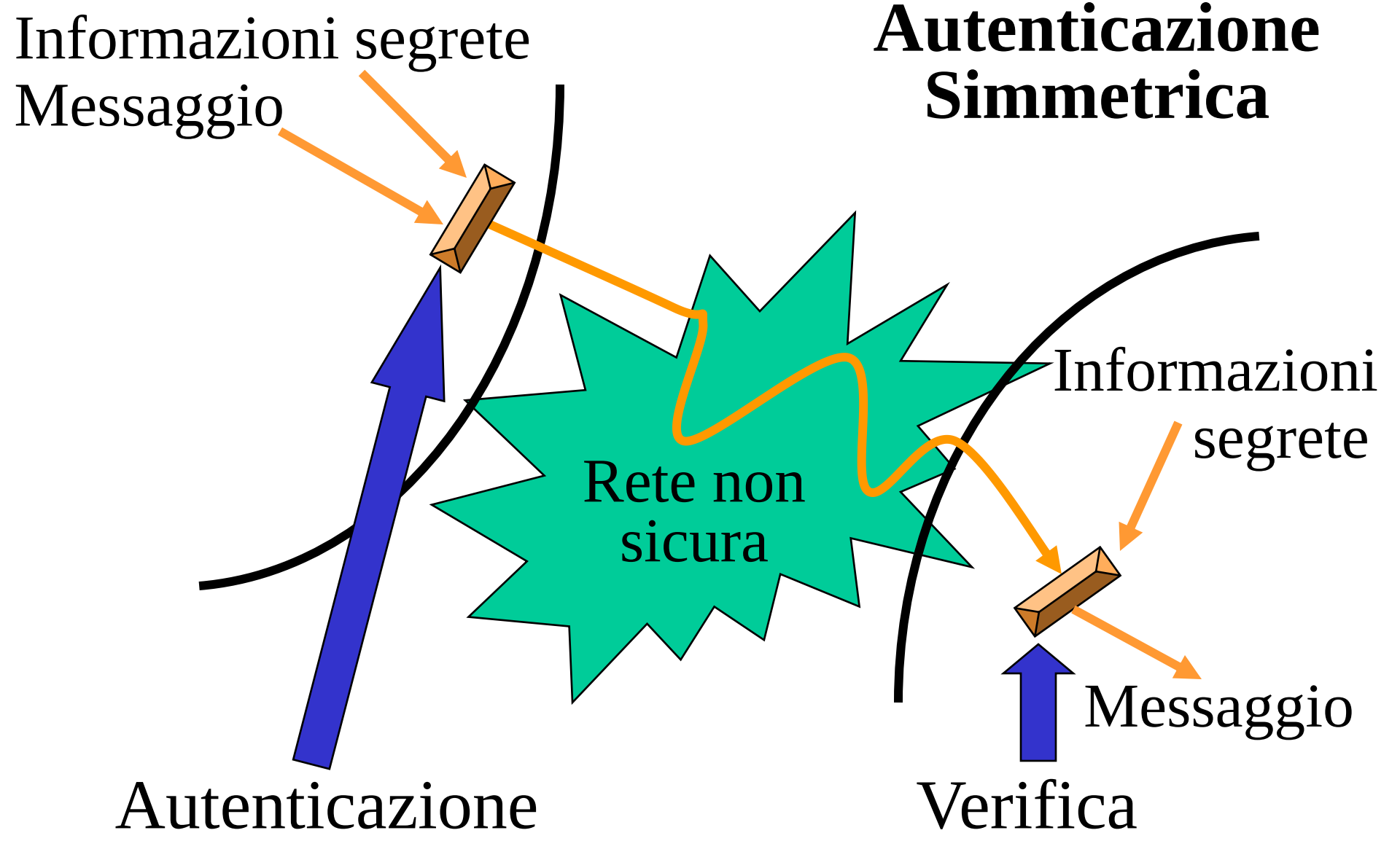
Dipartimento di Informatica

Università di Torino

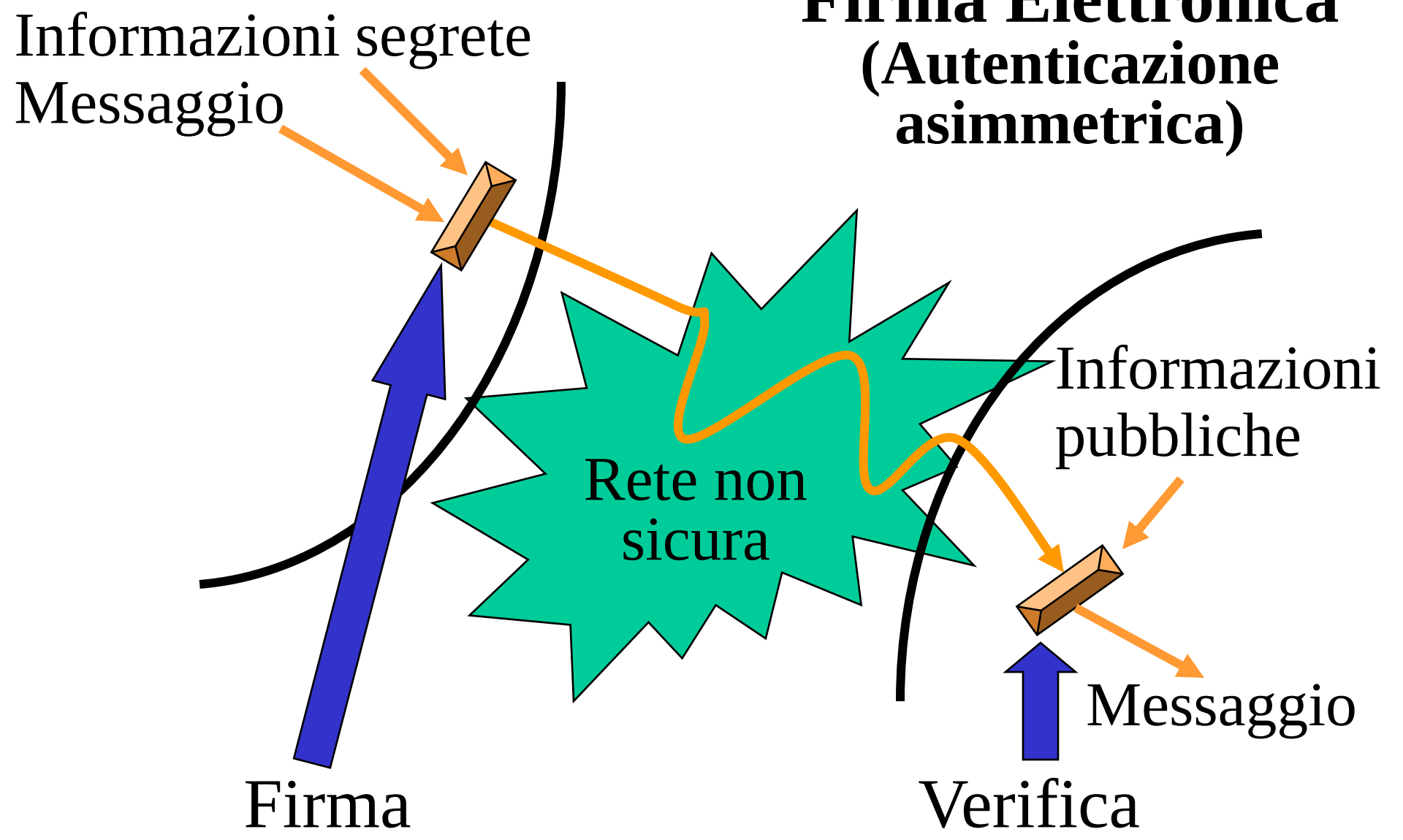
Contesto per autenticazione e firma



Autenticazione Simmetrica



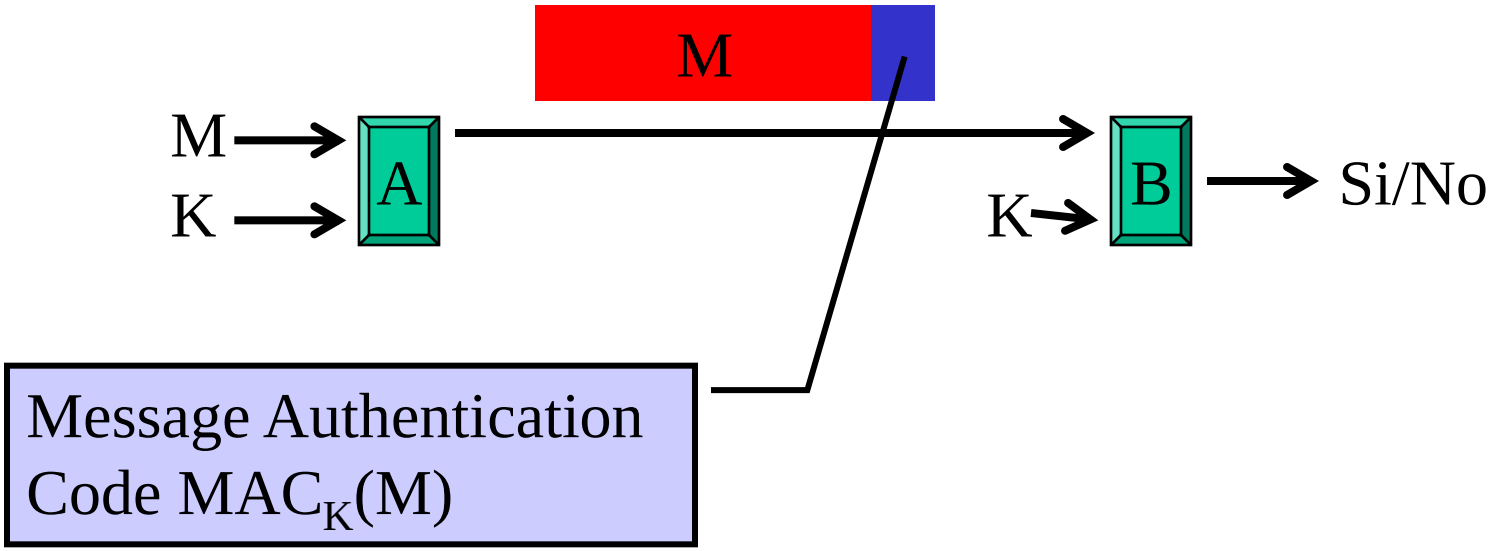
Firma Elettronica (Autenticazione asimmetrica)



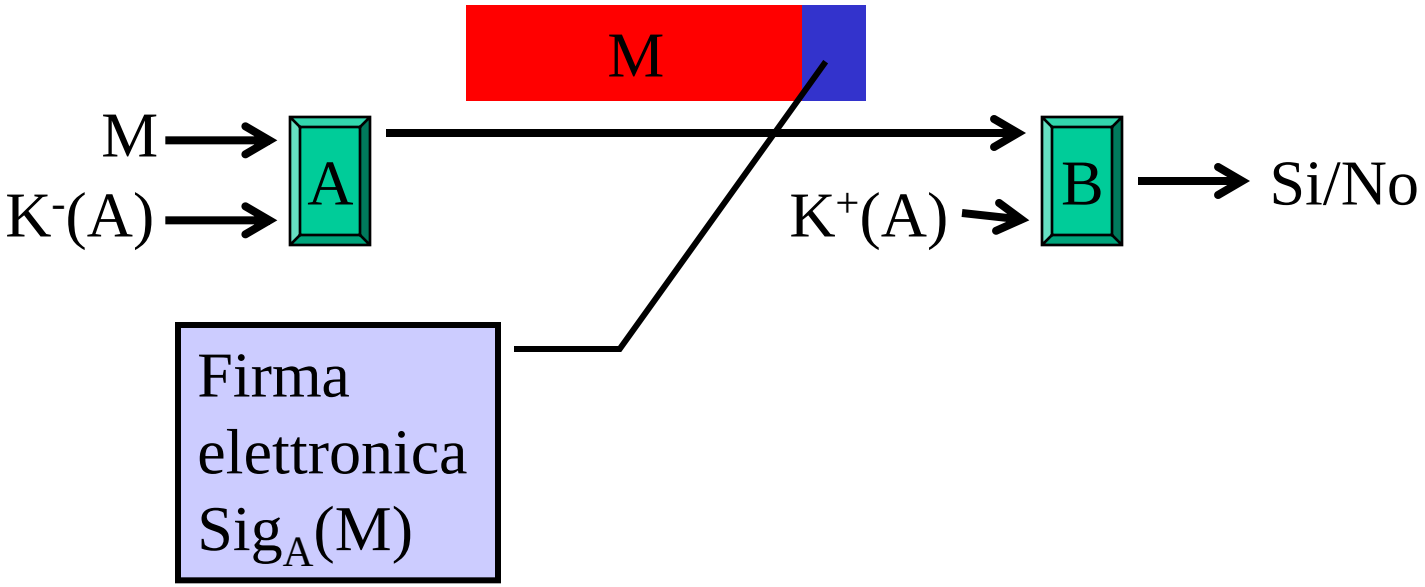
Autenticazione simmetrica vs firma elettronica

- L’autenticazione simmetrica si basa su cifrari simmetrici, utilizzando la chiave condivisa
- La firma elettronica si basa su cifrari asimmetrici, utilizzando in fase di firma la chiave privata di chi firma

Autenticazione simmetrica

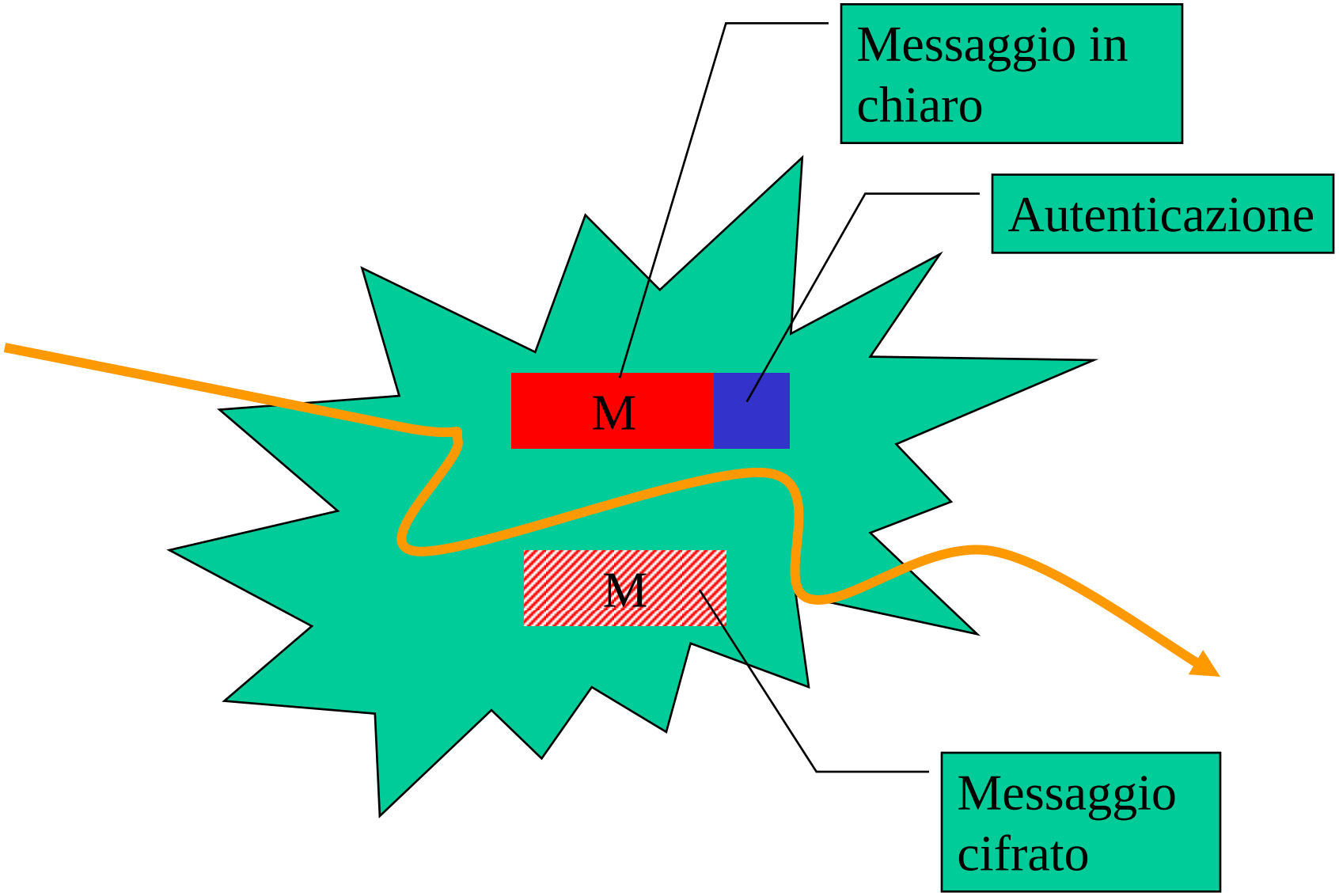


Firma Elettronica

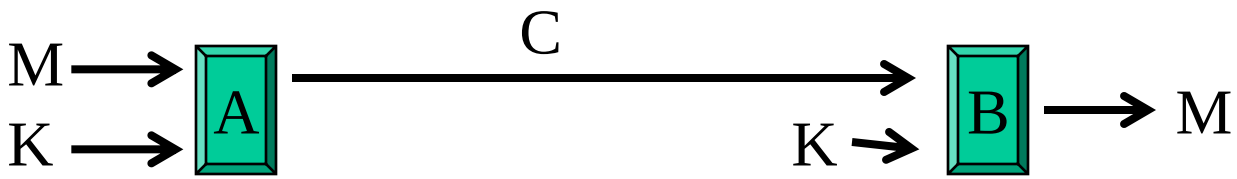


Autenticazione vs Encryption

- Un messaggio cifrato non è necessariamente autentico
- Un messaggio autenticato può essere leggibile e spesso non viene cifrato


Messaggio in chiaro
Autenticazione
M
M
Messaggio cifrato

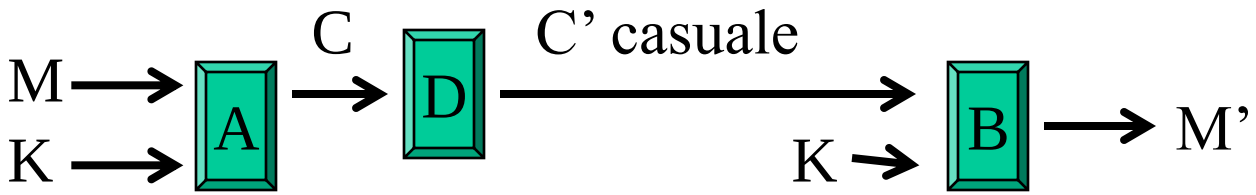
Perché un messaggio cifrato non è necessariamente autentico?



Questo è vero per certi cifrari e per certi messaggi, non in generale

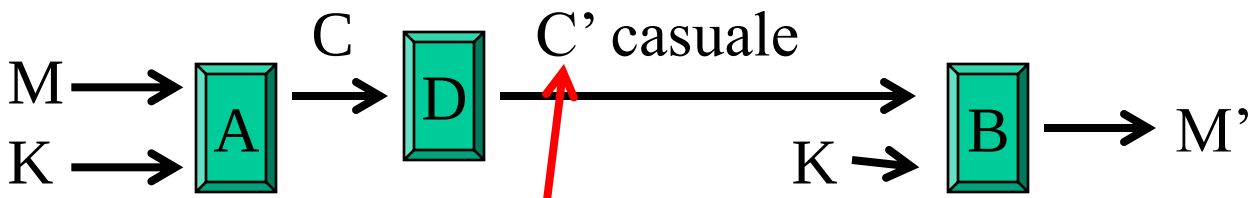
Sembrerebbe che, se solo A e B conoscono K,
il messaggio C possa essere prodotto solo da A
(e quindi il messaggio decifrato M dovrebbe essere autentico)

Perché un messaggio cifrato non è necessariamente autentico?



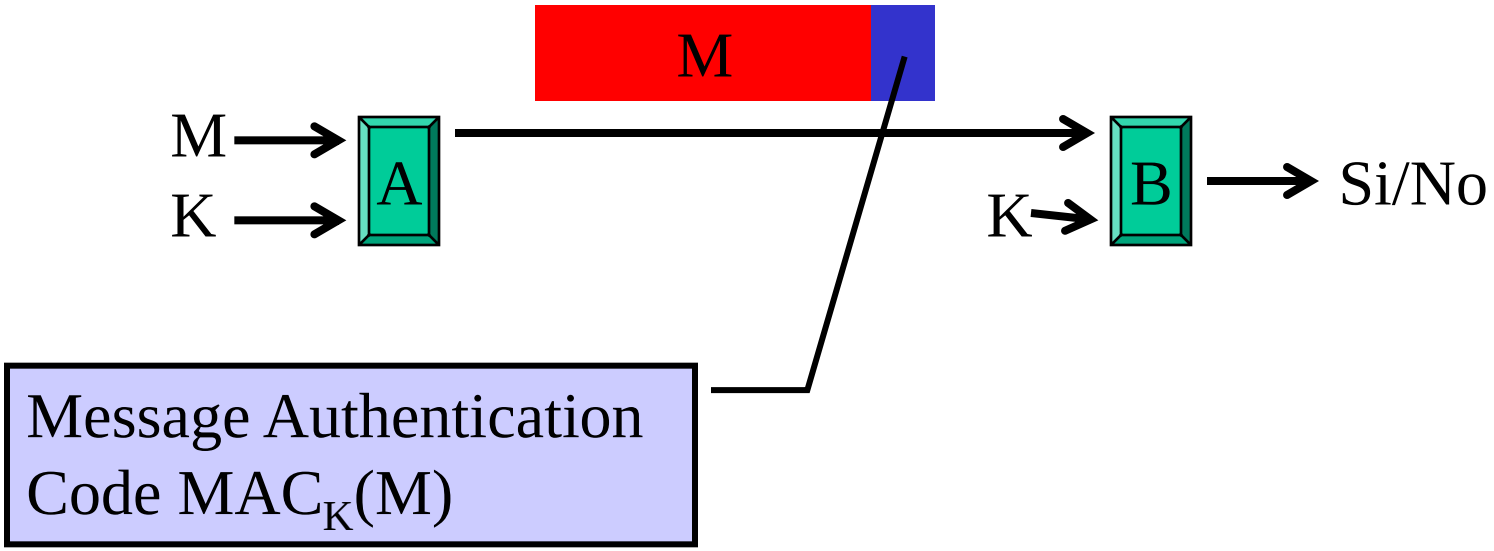
C' risulta cifrato, ma M' non autentico.
(Però M' molto probabilmente incomprensibile,
non così pero' se M ed M' sono numeri o codici)

Perché un messaggio cifrato non è necessariamente autentico? Esempio



Egregio signore, il suo PIN segreto è,
435945
cifrato con la chiave precedentemente inviatale. Qualora non dovesse funzionare, la preghiamo di telefonare allo 800666.

Autenticazione simmetrica



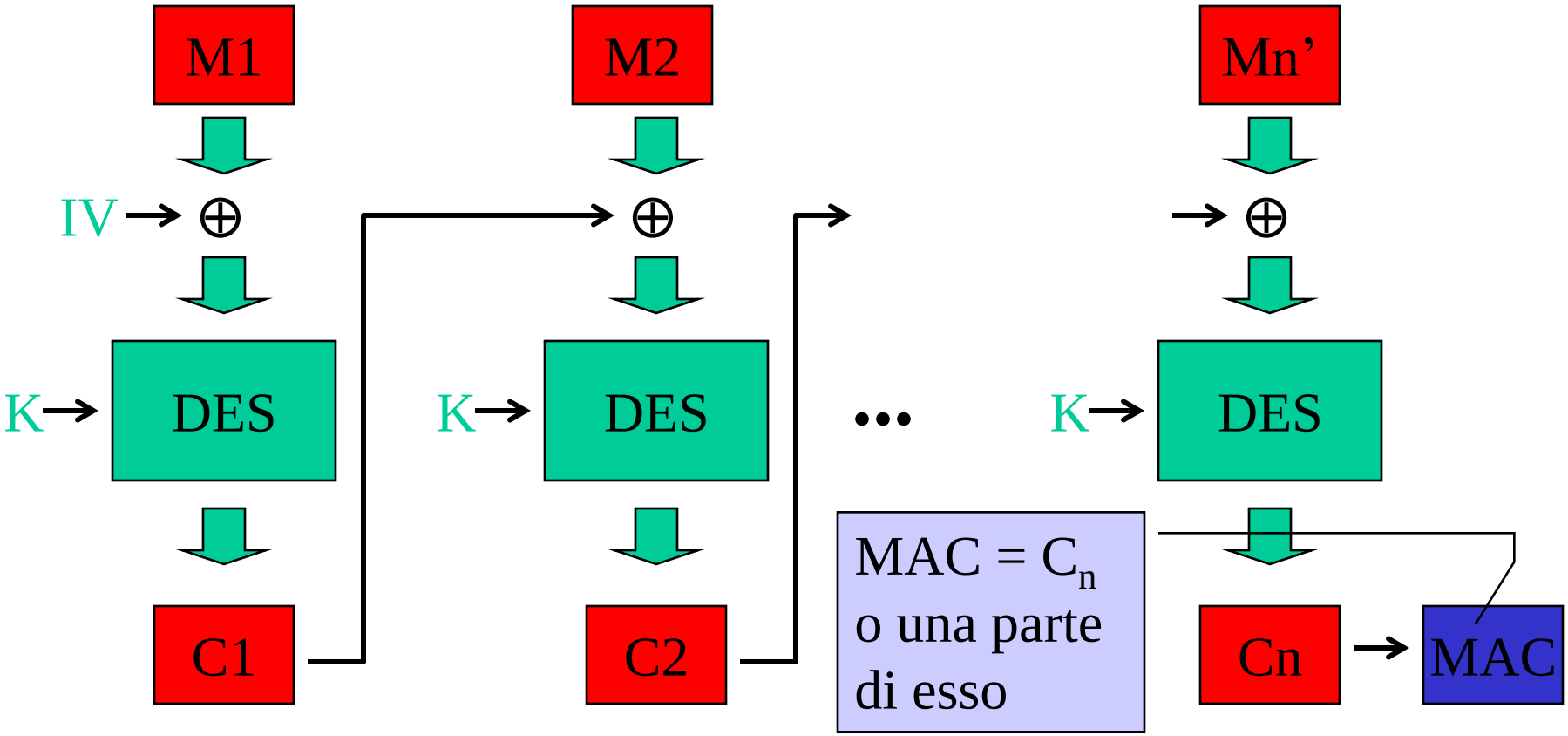
- **MAC con DES-CBC**
- **MAC con funzione di hash**

MAC con DES-CBC

- Si cifra il messaggio con DES-CBC
- Si usa l'ultimo blocco cifrato o parte di esso come MAC

$MAC_K(M)$ con DES-CBC
Padding a lunghezza multipla di 64 bit

$MAC_K(M)$ con DES-CBC



Sicurezza MAC con DES-CBC

- Il codice serve per autenticare, poiché se il messaggio venisse modificato, il ricevente otterrebbe un MAC diverso da quello ricevuto insieme al messaggio
- Non è possibile generare messaggi falsi, in quanto senza conoscere la chiave K non è praticamente possibile generare un MAC valido

Sicurezza MAC con DES-CBC

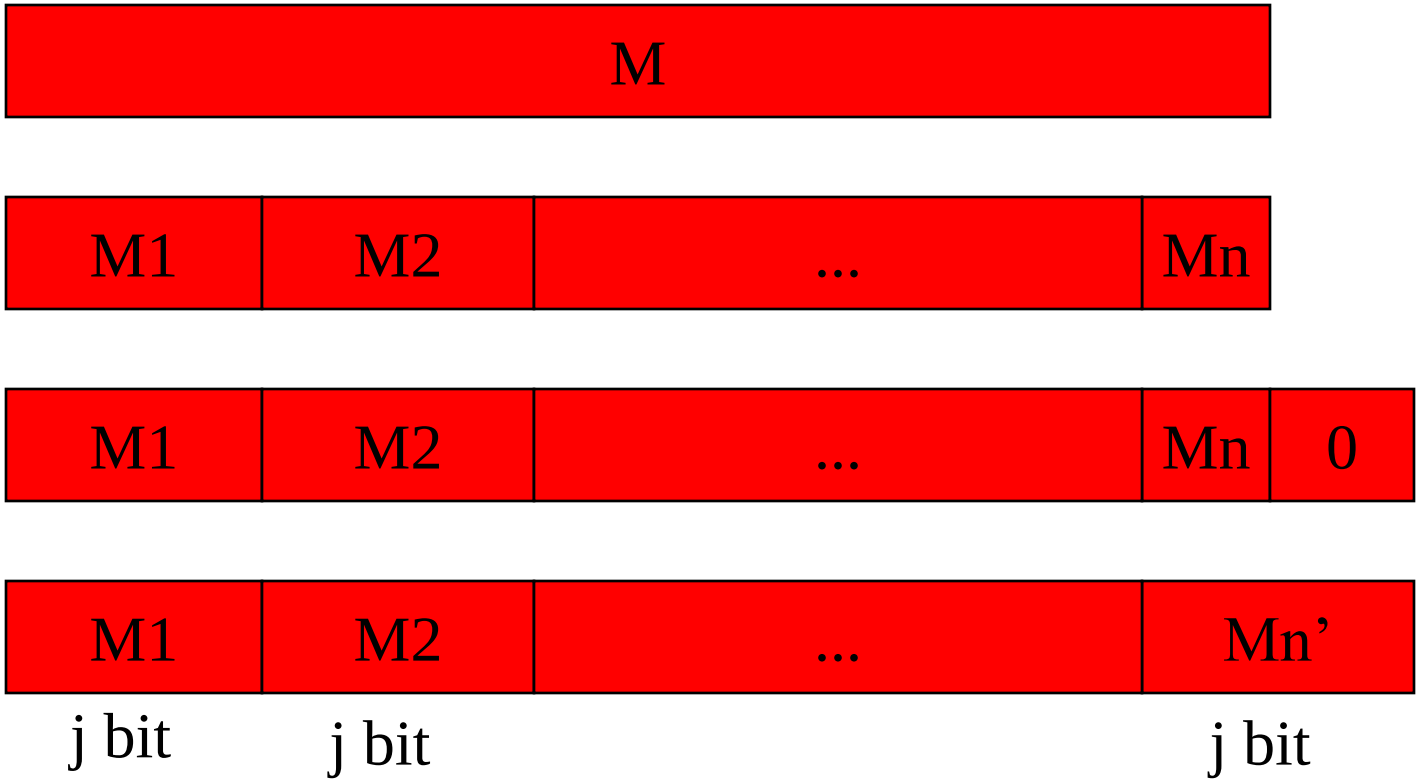
L'attacco del compleanno non funziona: anche se la probabilità di trovare una collisione in due insiemi $\{M_1,\ldots,M_n\}$ e $\{M'_1,\ldots,M'_n\}$ **è elevata**,

l'avversario non riesce a trovare la collisione, perché non sa calcolare $MAC\_CBC_k(M_i)$, non conoscendo k.

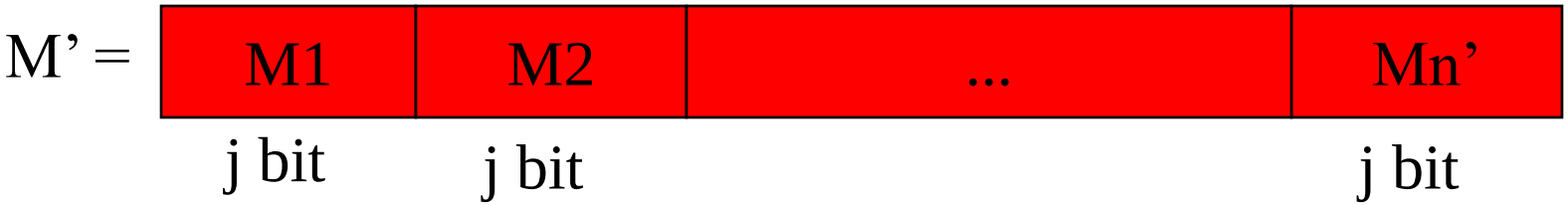
MAC con funzione di hash (keyed hash function)

Data una funzione di hash H resistente alle collisioni, si genera il MAC applicando H ad una combinazione del messaggio e di una chiave segreta

Esempio: HMAC

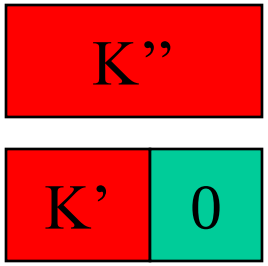


Esempio: HMAC

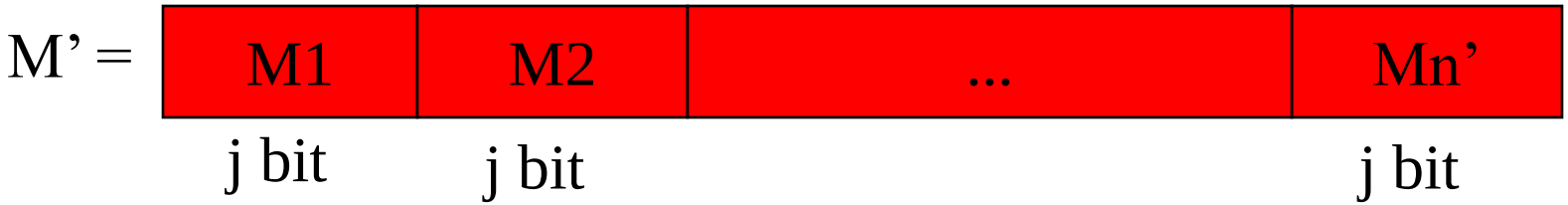


K' = chiave segreta K del MAC, oppure H(K) se K è più lunga di j bit

K'' = K' con padding di 0 fino a raggiungere j bit



Esempio: HMAC **(RFC 2104)**

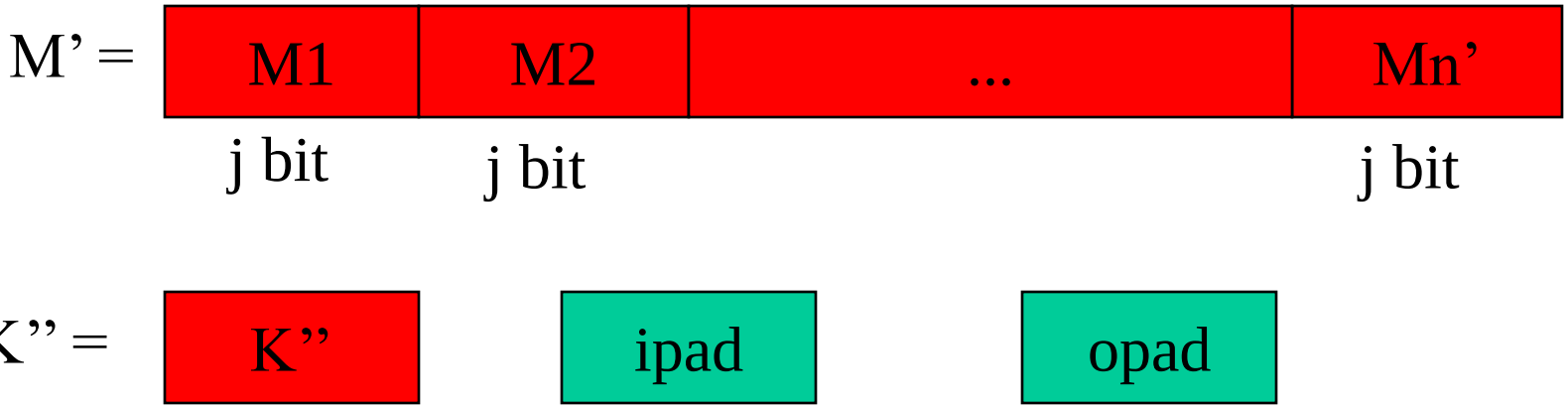


K’’ = K’’

ipad = 00110110 ripetuto j/8 volte

opad = 01011010 ripetuto j/8 volte

Esempio: HMAC



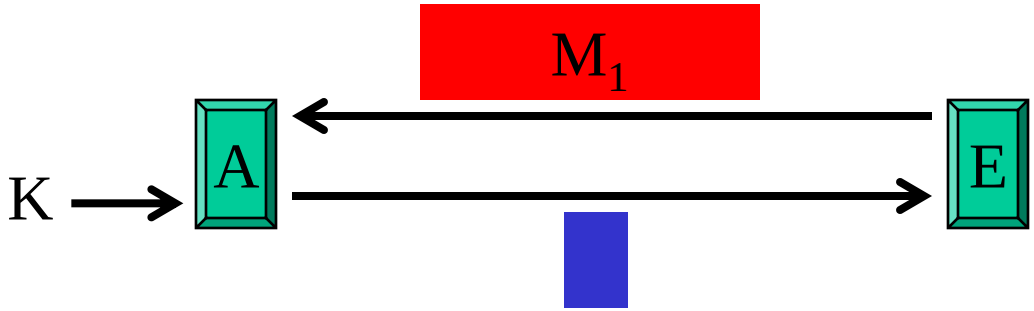
$$\mathbf{HMAC_K(M) = H(\underbrace{(K''\oplus opad)}_{K1}||\underbrace{H((K''\oplus ipad)}_{K2}||M'))}$$

Sicurezza di HMAC

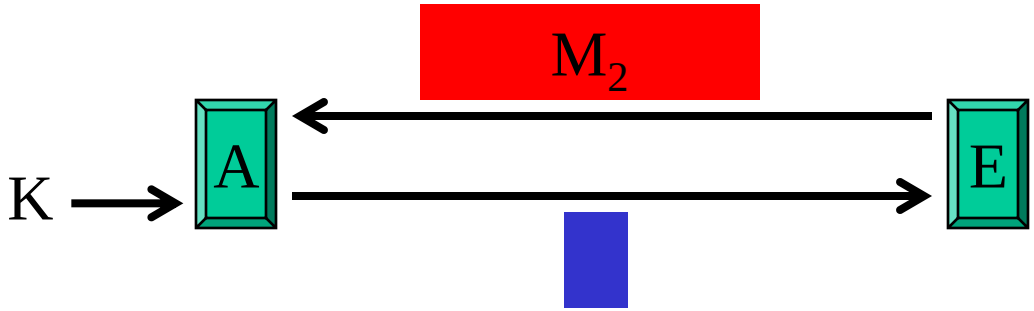
Per opportune scelte di H, HMAC è ritenuto sicuro contro attacchi con scelta dei messaggi autenticati ‘chosen message attacks’:

anche se l’avversario può scegliere molti messaggi e vederne il corrispondente valore di HMAC, non riesce a fornire un nuovo messaggio autenticato.

Sicurezza di HMAC

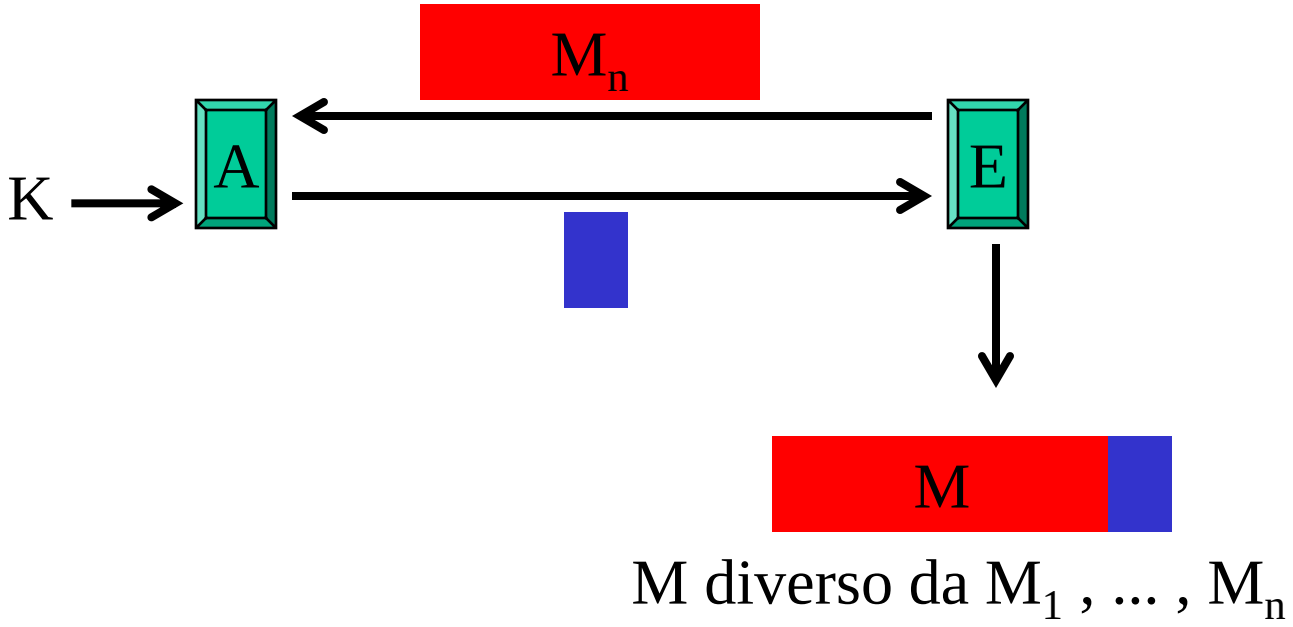


Sicurezza di HMAC



...

Sicurezza di HMAC



Si ritiene che con HMAC questo non sia possibile

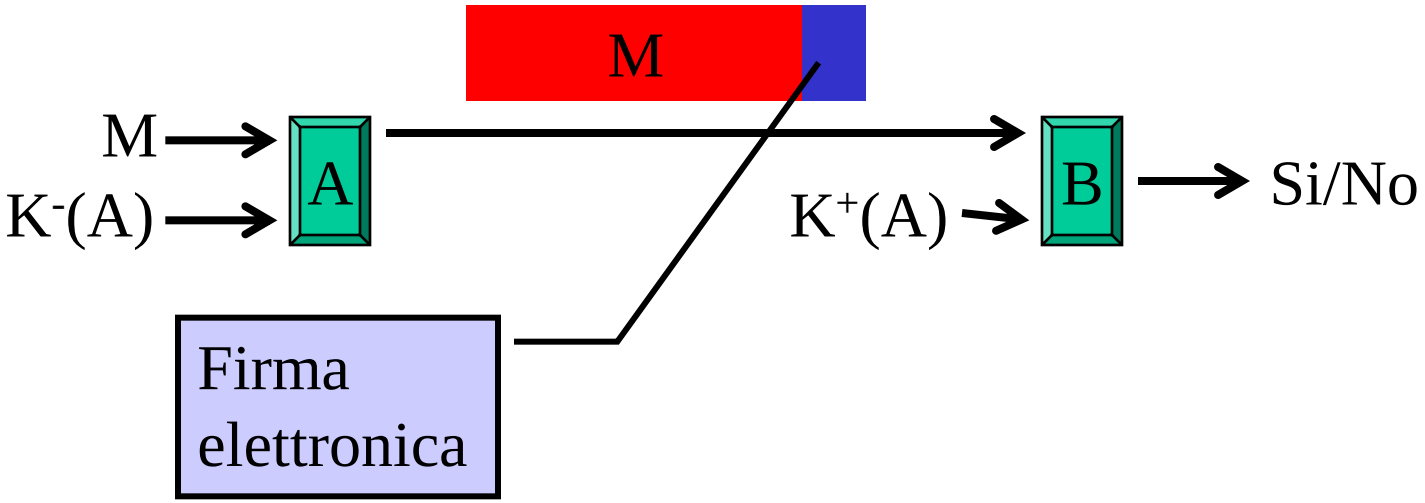
Sicurezza di HMAC

- Per una funzione di hash H, per trovare collisioni possiamo generare due insiemi S' e S'' di messaggi e verificare se esistono x in S' e y in S'' tali che H(x)=H(y)
- Per HMAC, questo non è possibile perché non sappiamo calcolare $HMAC_{\mathbf{K}}(z)$ per un messaggio arbitrario z, in quanto non conosciamo K

Efficienza di HMAC

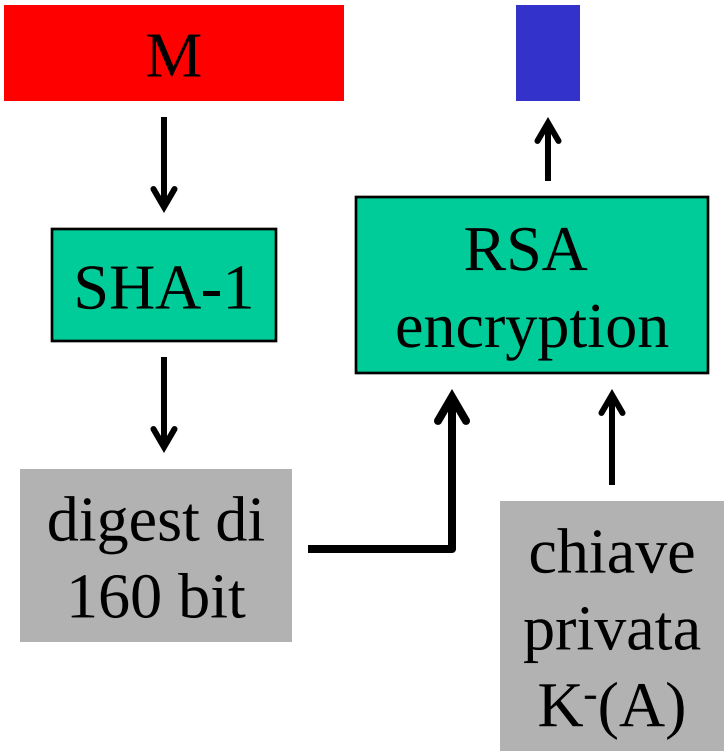
- Efficiente quanto la funzione di Hash H utilizzata (H viene chiamata due volte, ma la seconda volta con un argomento lungo solo j+N, dove N è la lunghezza del digest di H)
- Molto più efficiente di MAC-CBC

Firma Elettronica

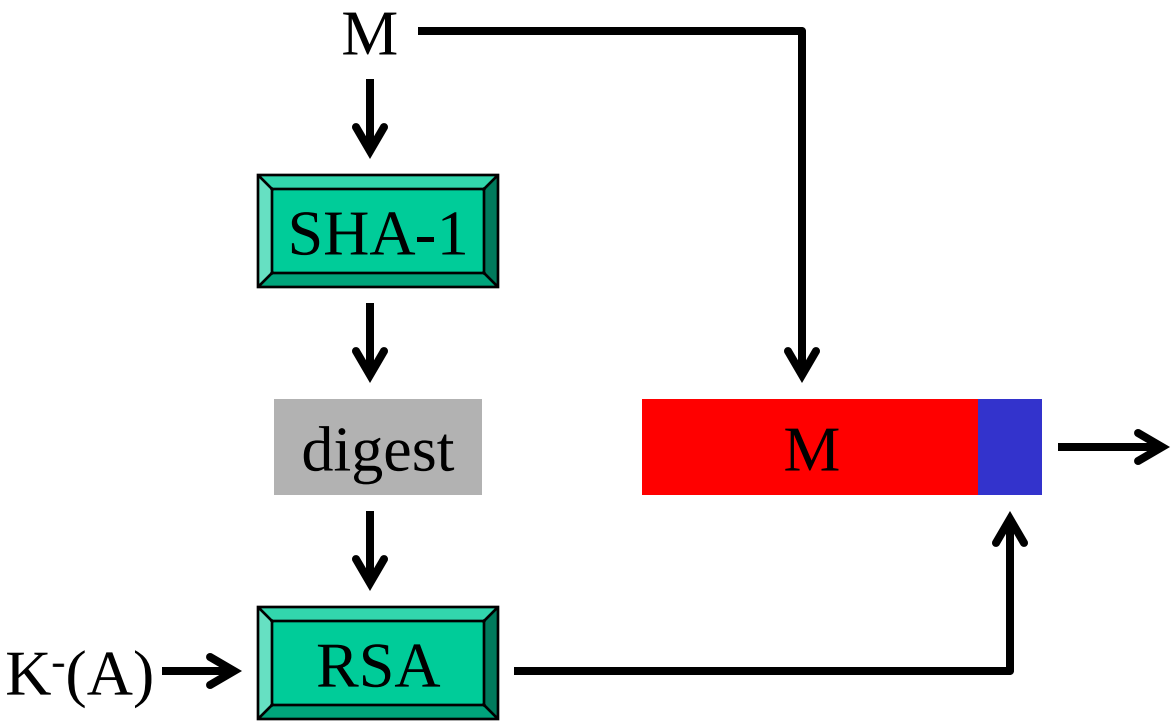


- **RSA con MD5/SHA-1**
- **DSA (con SHA-1)**

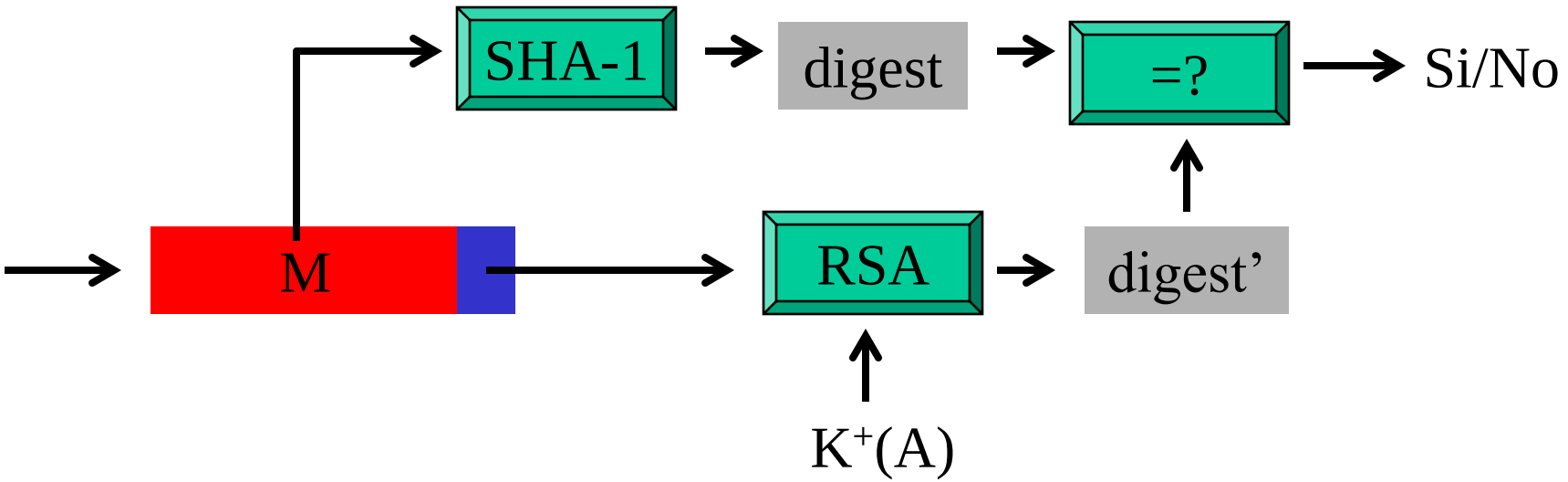
RSA con SHA-1



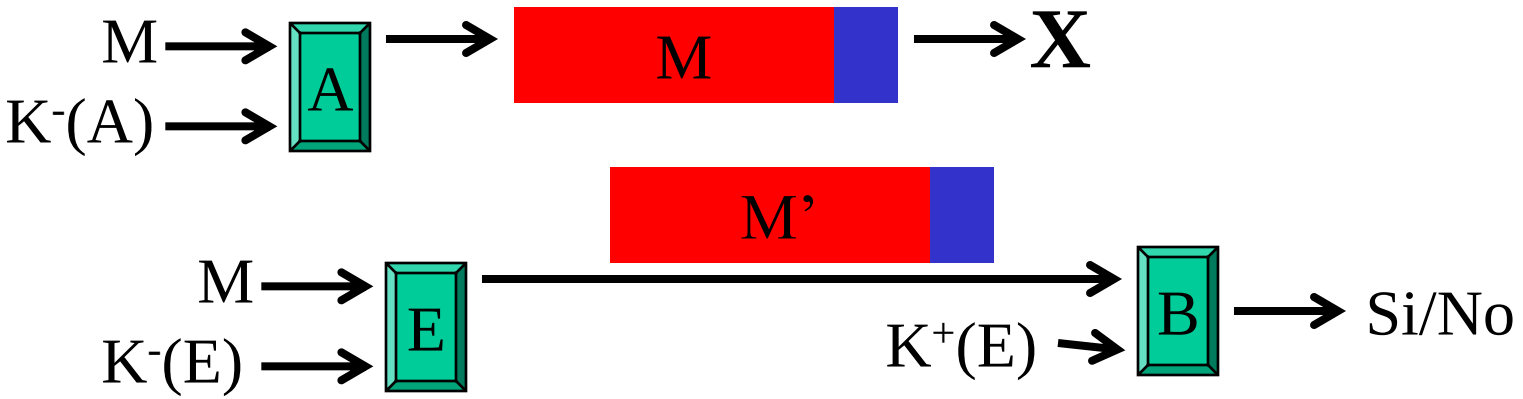
Firma Elettronica con RSA/SHA-1
lato mittente (A)



Firma Elettronica con RSA/SHA-1
lato ricevente (B)



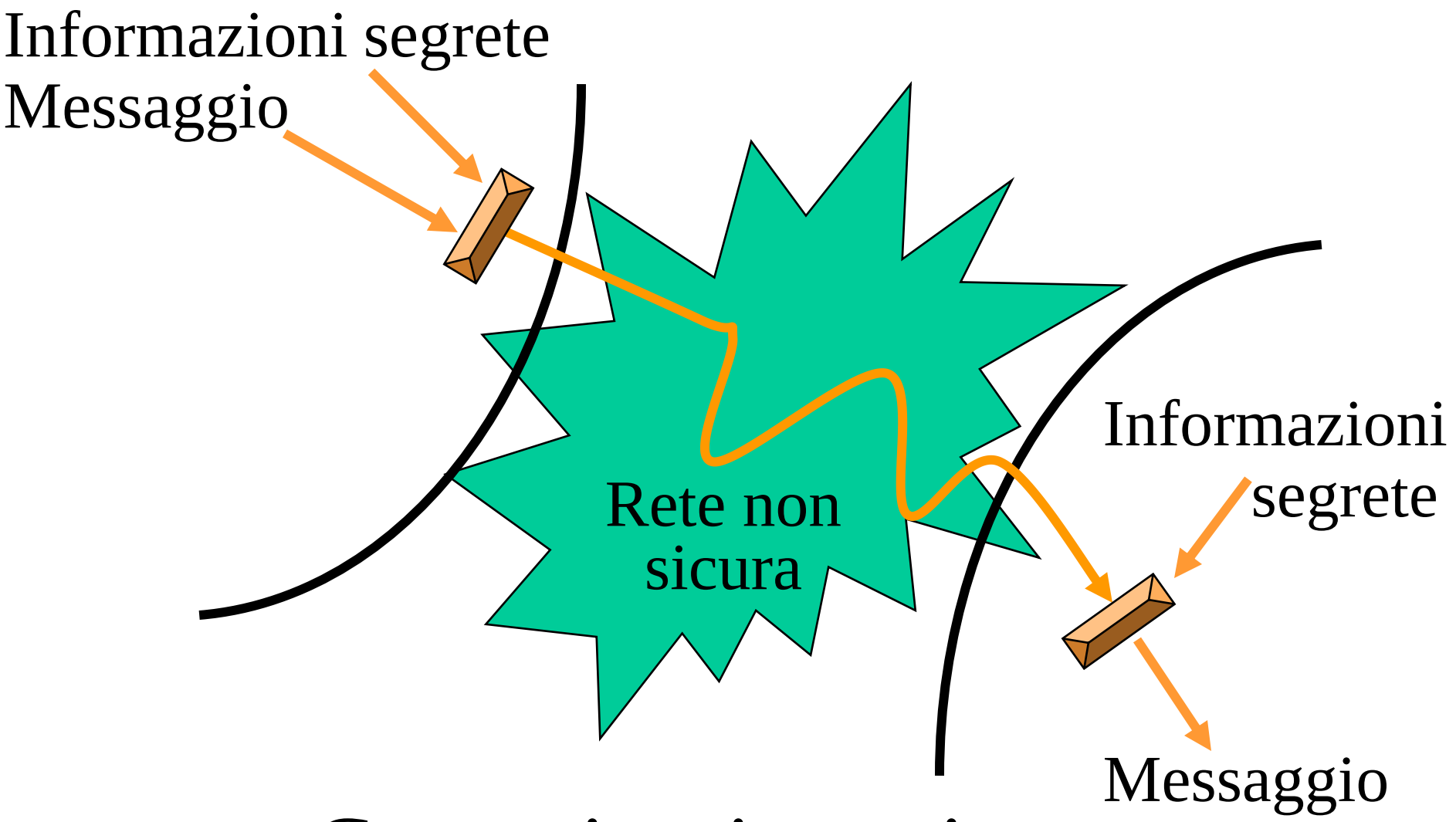
Firma Elettronica



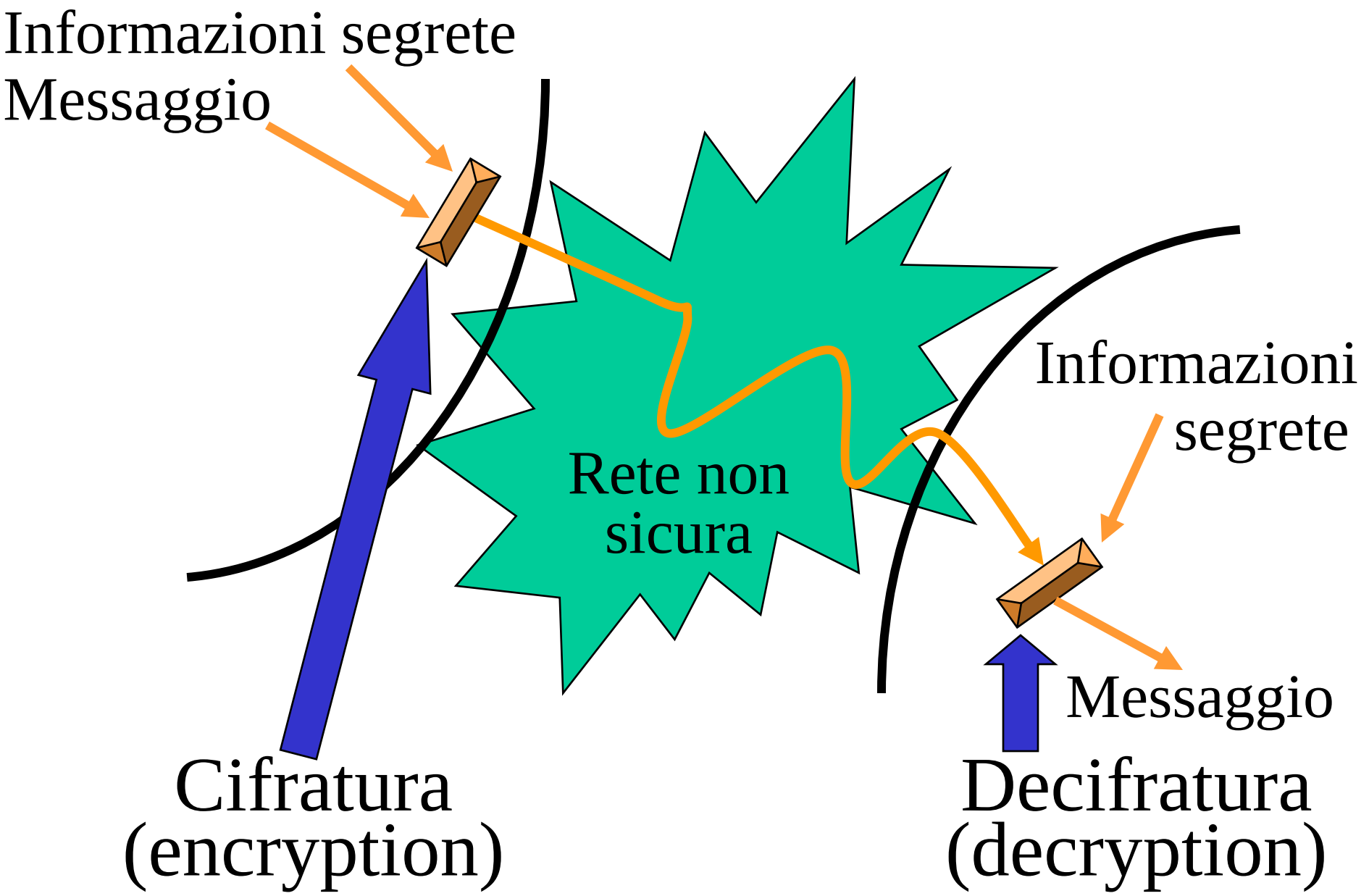
Per verificare la firma, B deve conoscere la chiave pubblica di A in modo certo, altrimenti è possibile fare accettare firme false

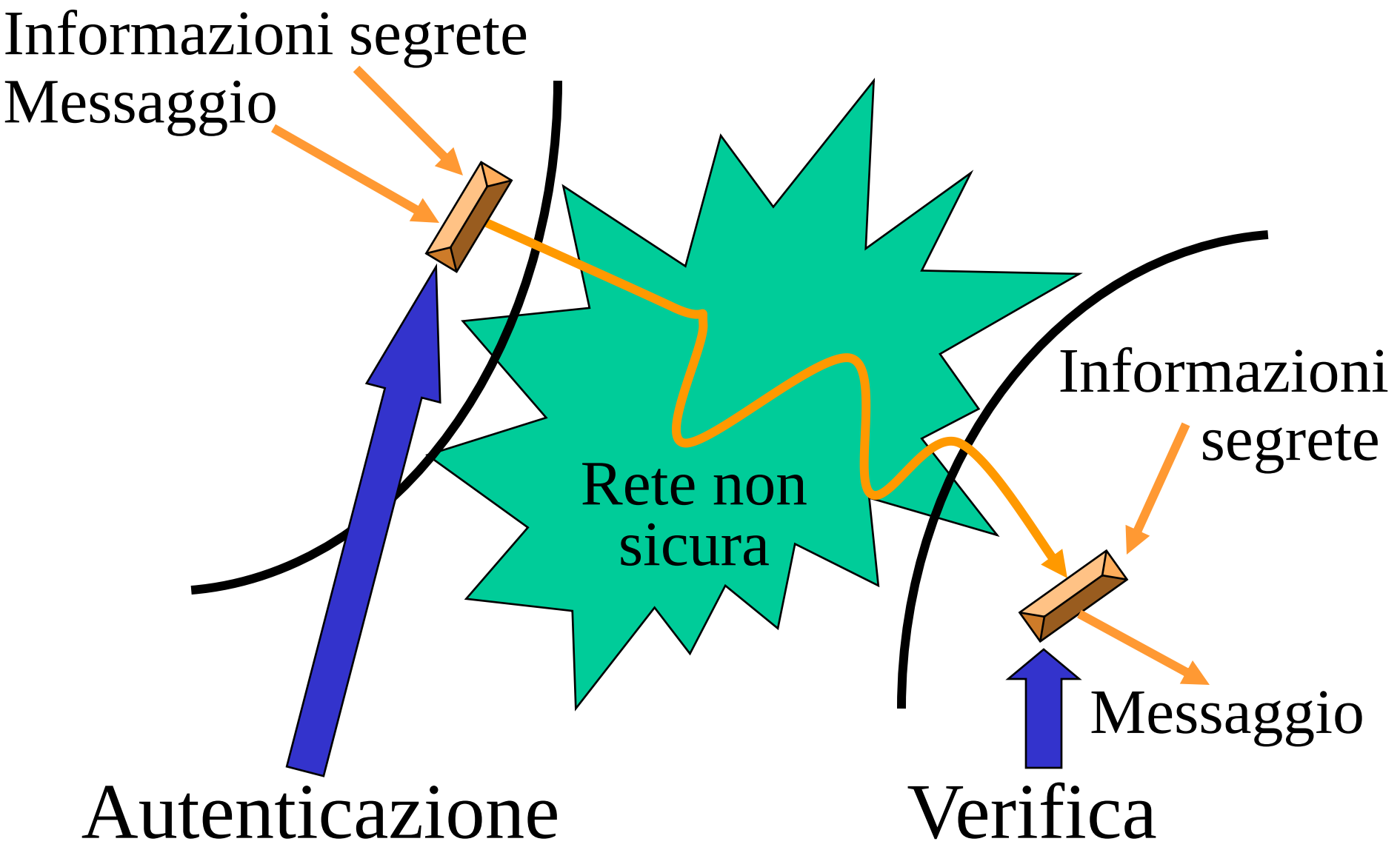
Comunicazioni Sicure (sintesi e distribuzione delle chiavi)

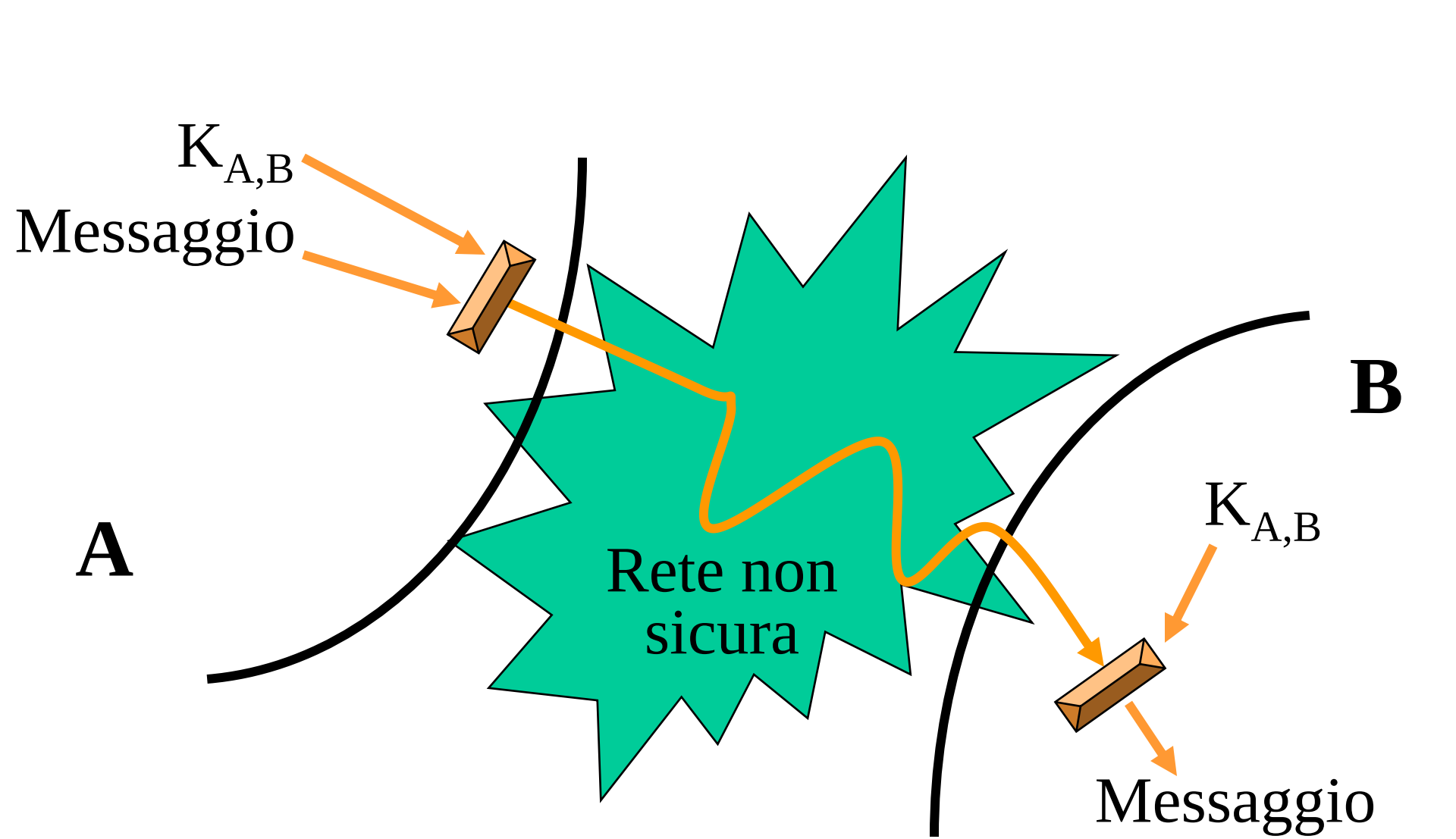
- Il messaggio viene modificato in modo da rendere impossibile l'intercettazione del contenuto originario (cifratura)
- Al messaggio vengono aggiunti codici in modo da rilevare la presenza di modifiche al momento della ricezione (autenticazione)



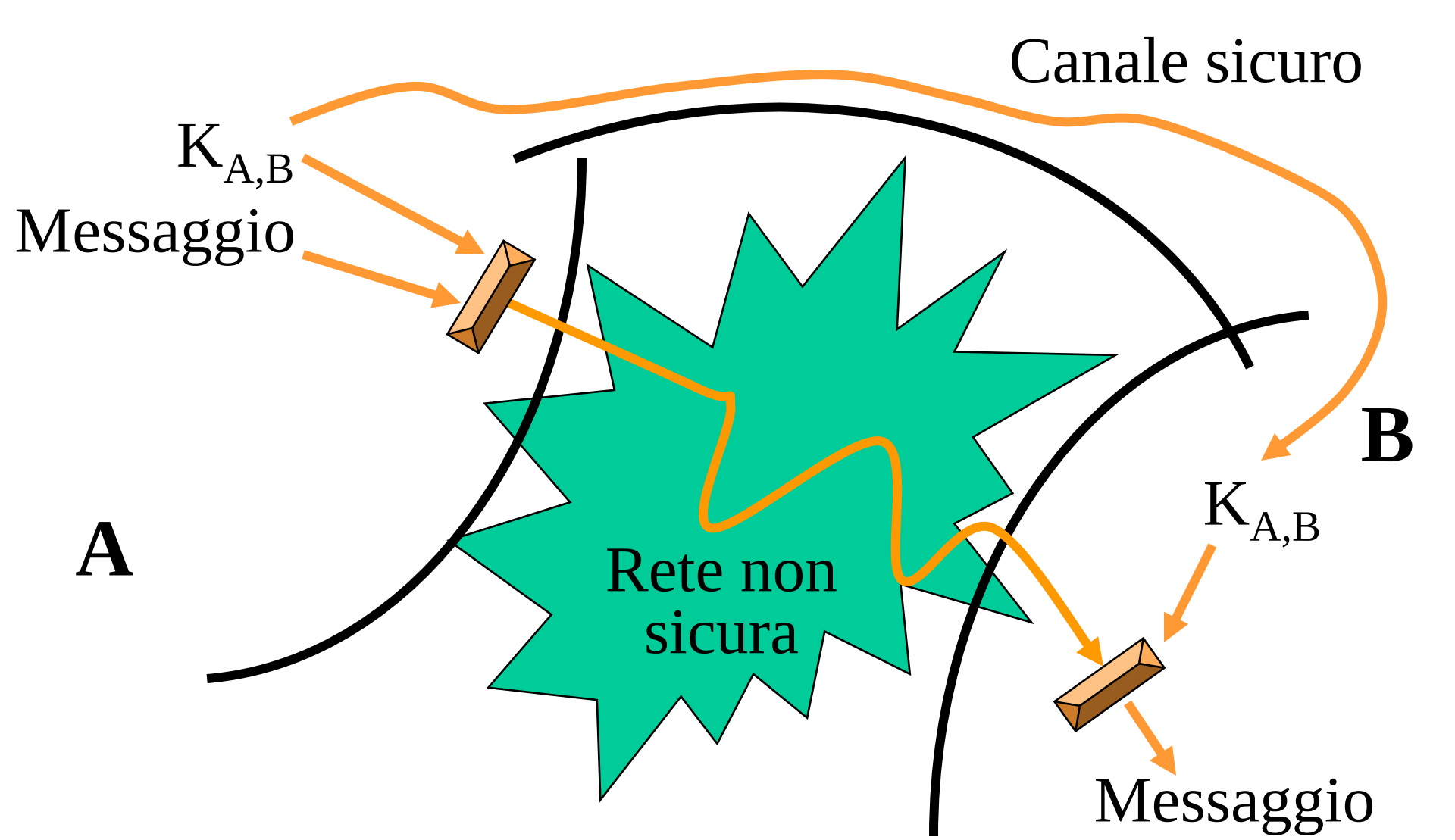
Comunicazione sicura


Informazioni segrete
Messaggio
Rete non sicura
Informazioni segrete
Messaggio
Cifratura (encryption)
Decifratura (decryption)

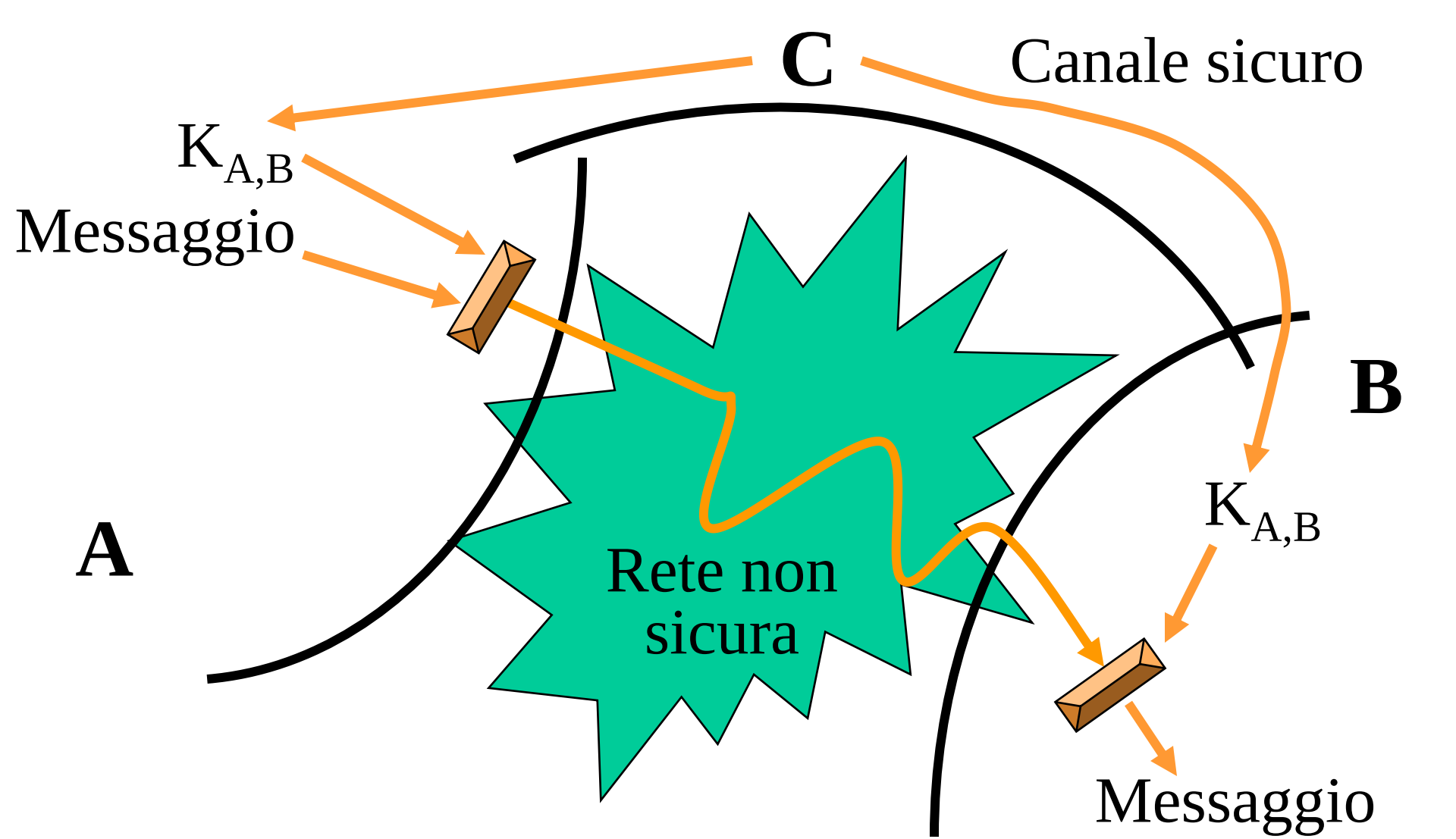

Informazioni segrete
Messaggio
Rete non sicura
Informazioni segrete
Messaggio
Autenticazione
Verifica



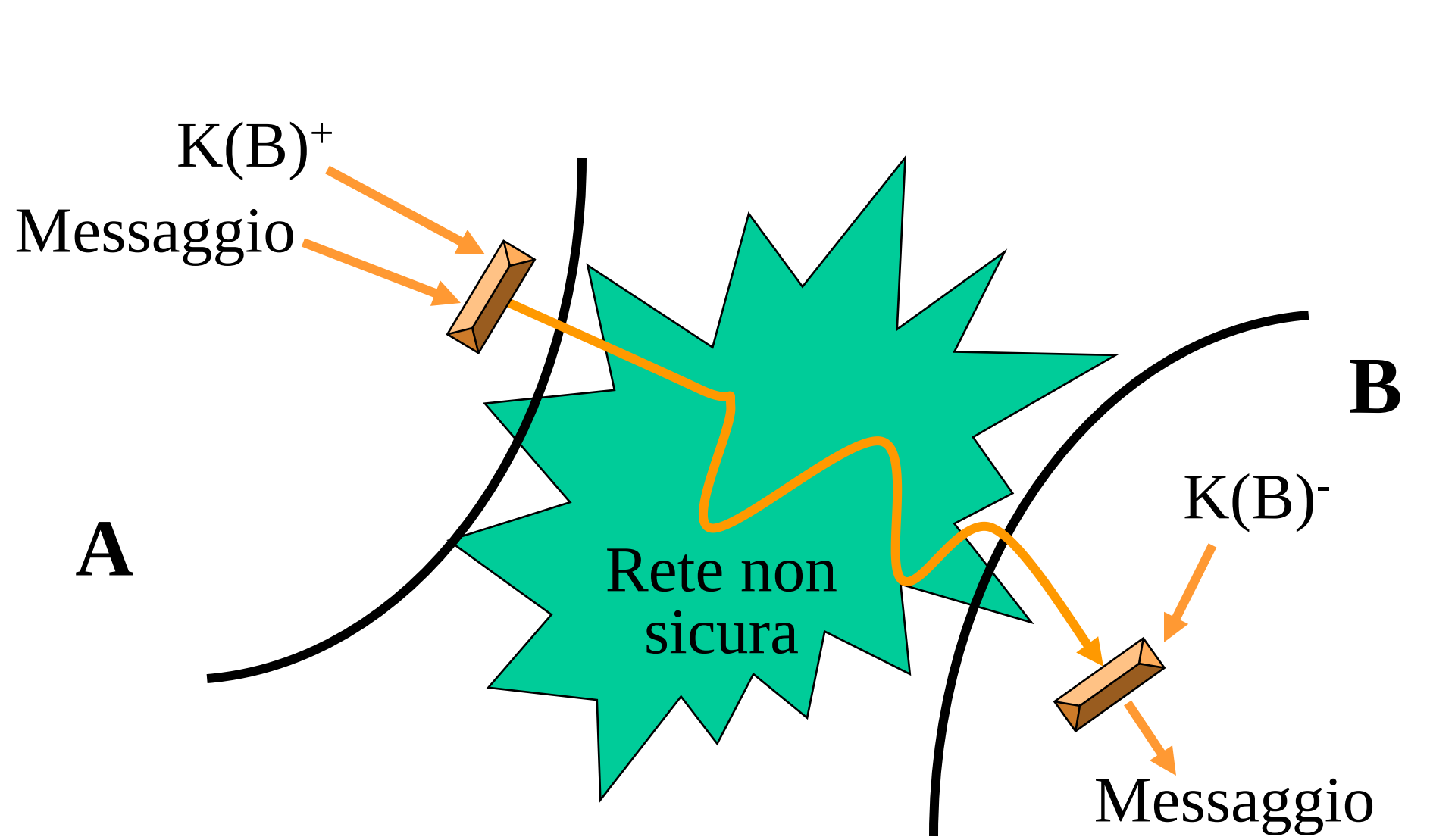
Modello a chiavi simmetriche o condivise



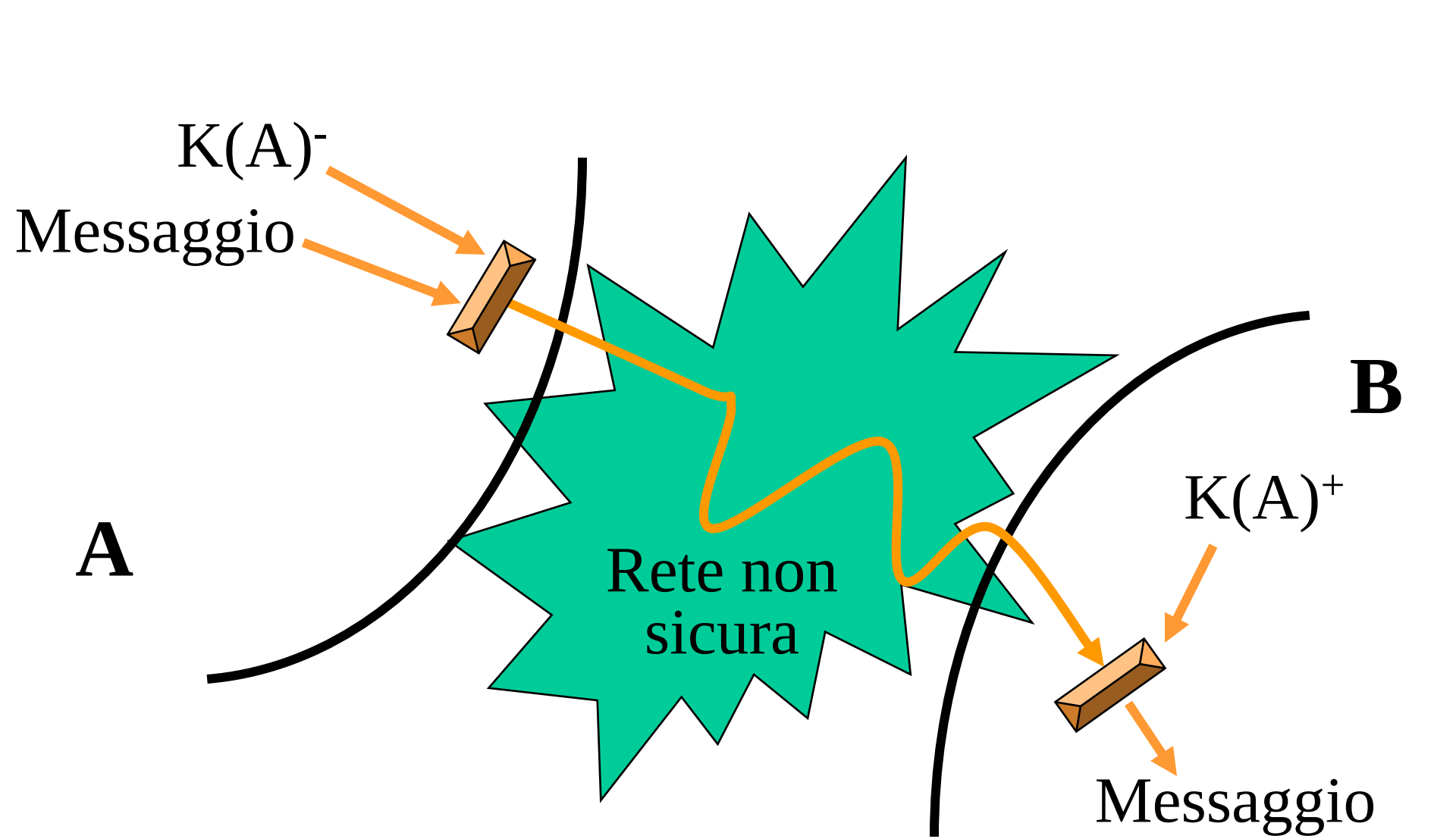
Distribuzione di chiavi simmetriche (diretta)



Distribuzione di chiavi simmetriche (con terza parte)



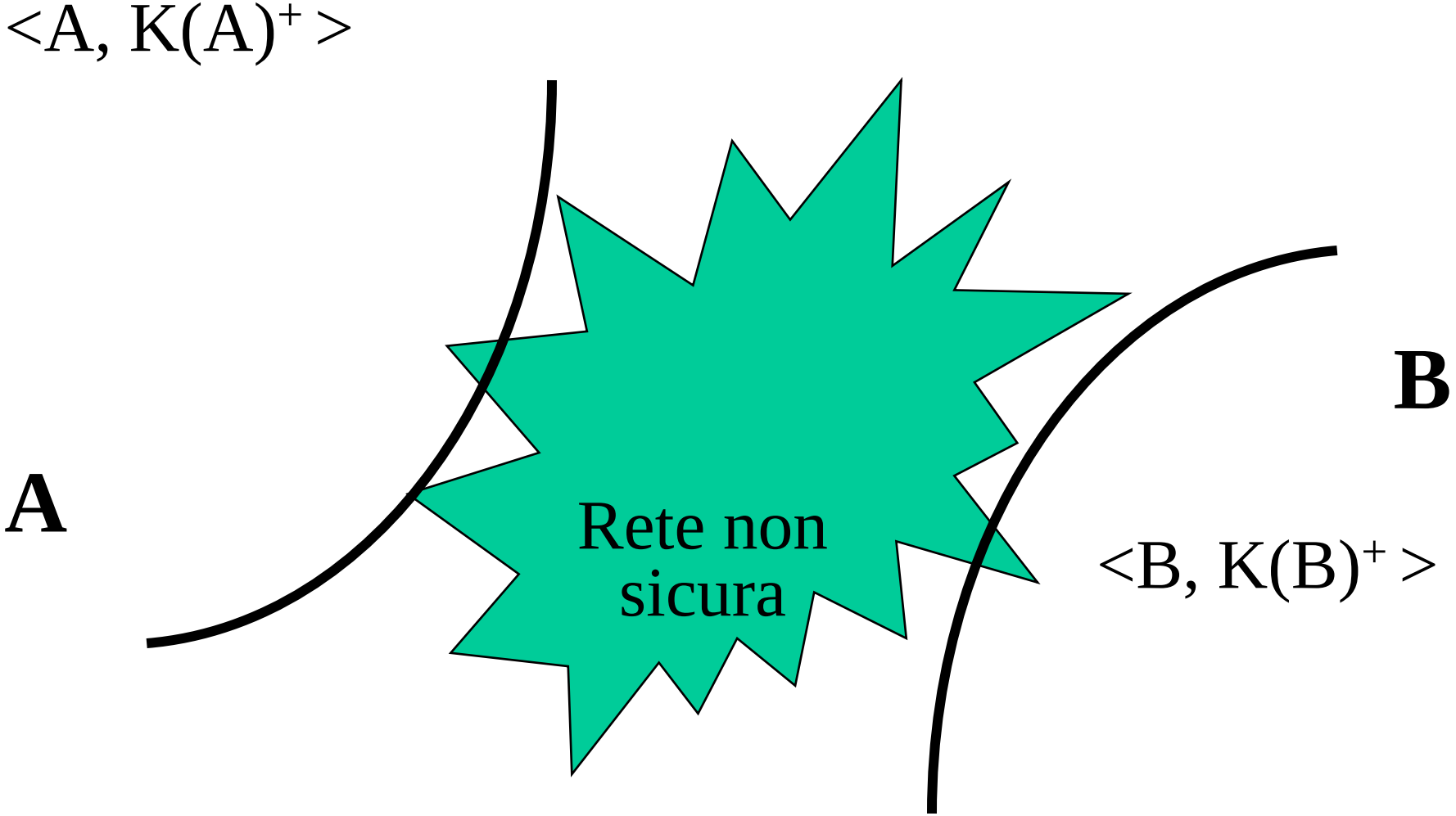
Modello a chiavi asimmetriche (cifratura)



Modello a chiavi asimmetriche (autenticazione/firma)

In questo caso si parla di firma perché abbiamo non-disconoscibilità:

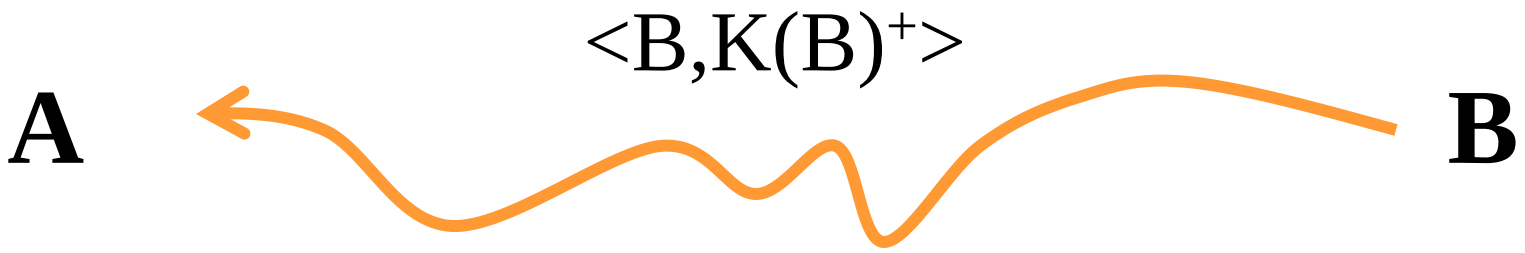
solo A conosce $K(A)^-$
quindi
solo A può autenticare

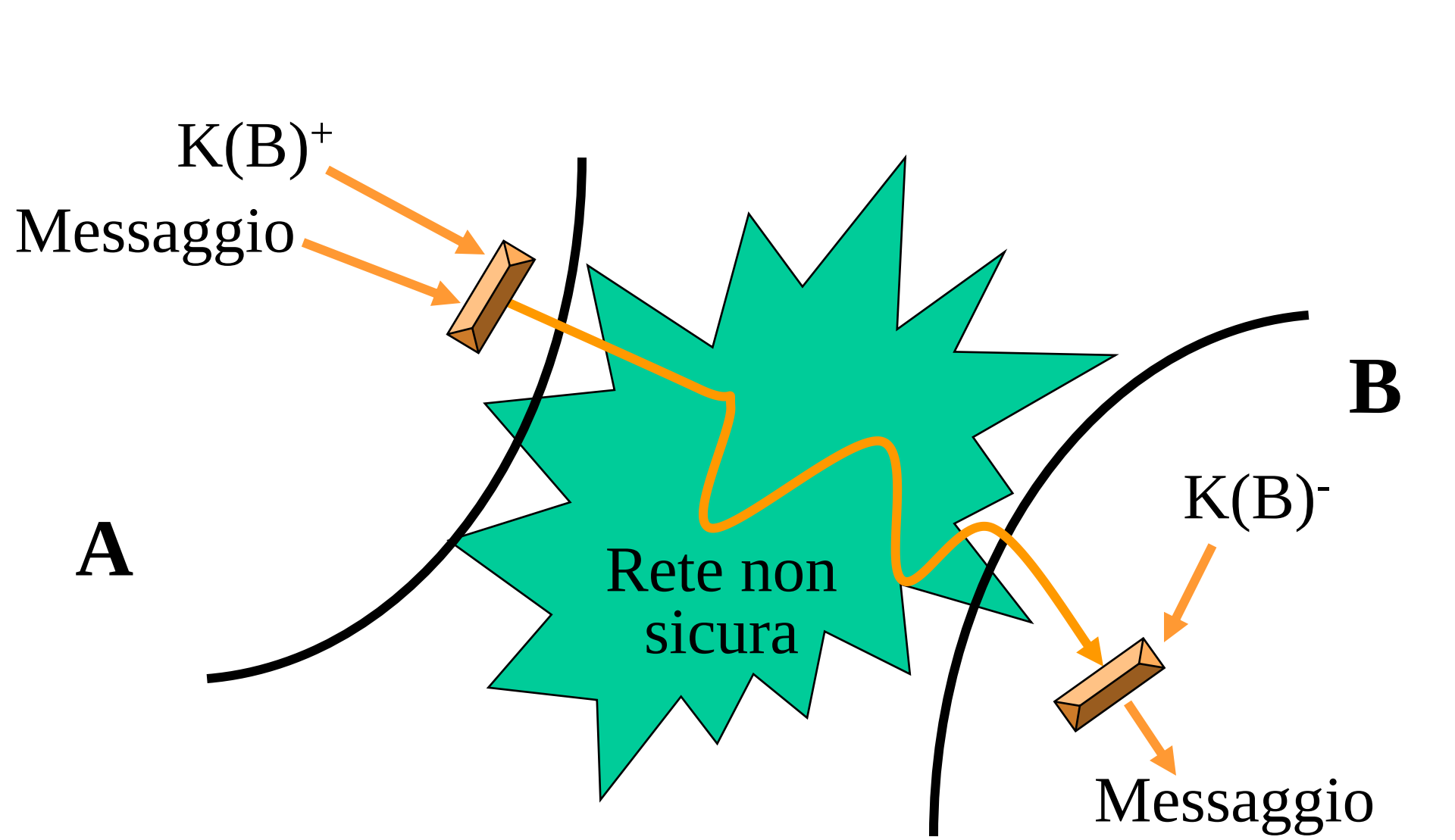


Problema della distribuzione di chiavi pubbliche

Cifratura asimmetrica

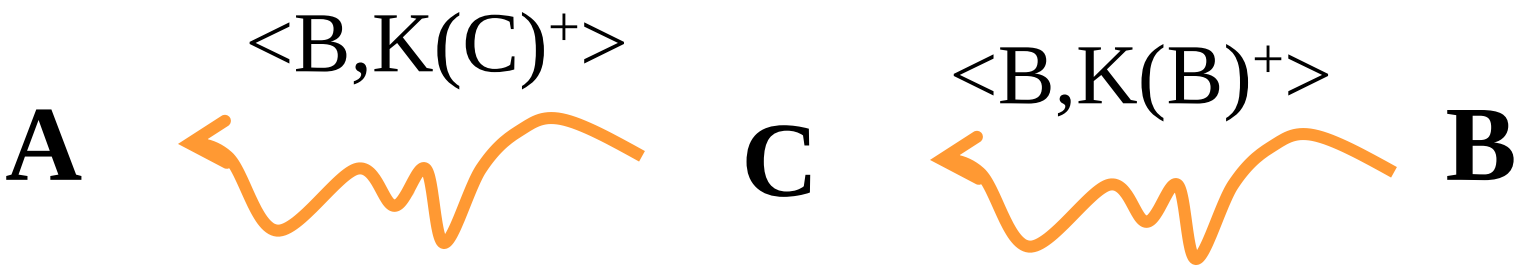
Il ricevente dovrà, in qualche modo, rendere nota la propria chiave pubblica, associando ad essa la propria identità

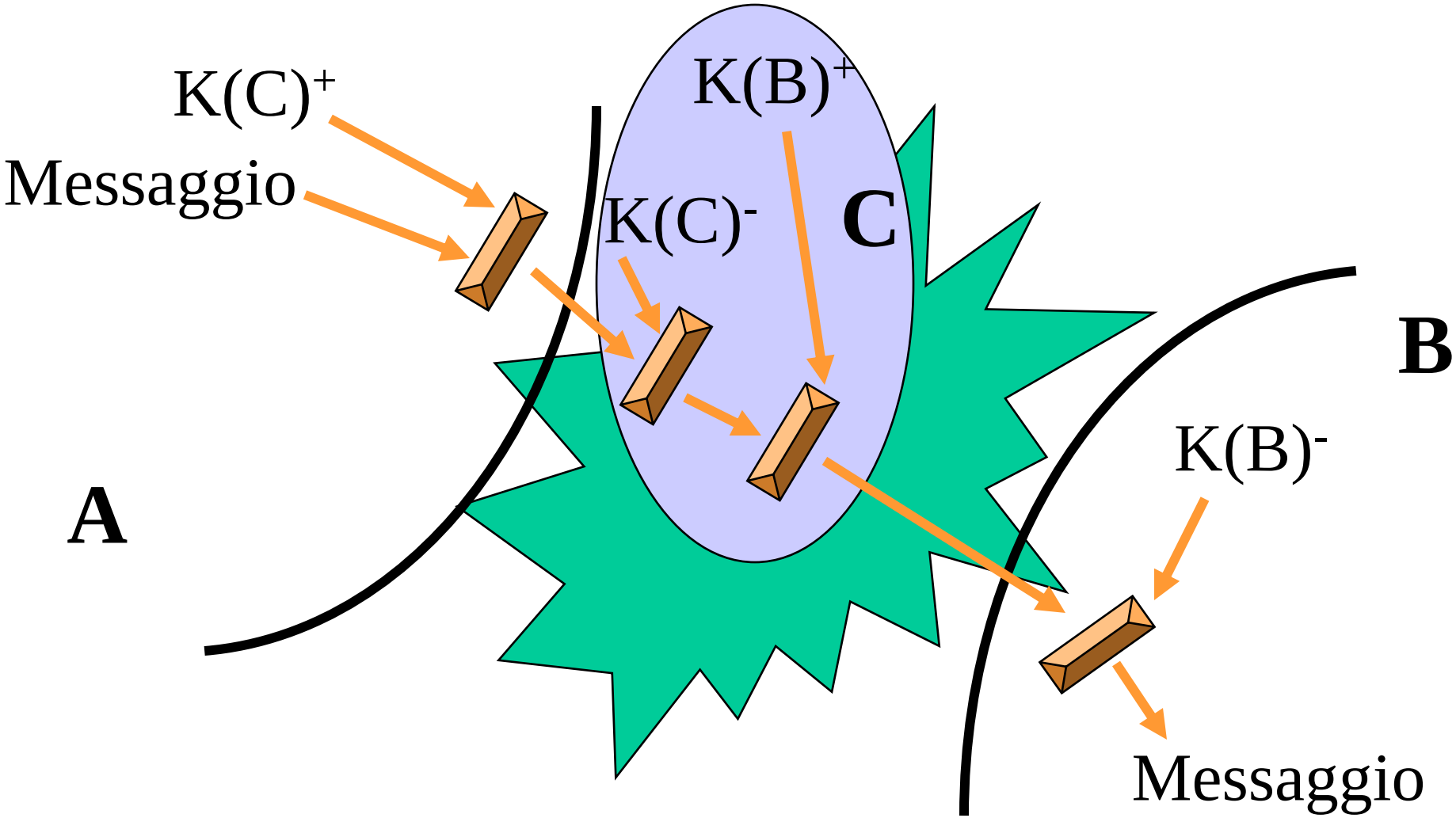




Cifratura asimmetrica

Principale problema (per cifratura)

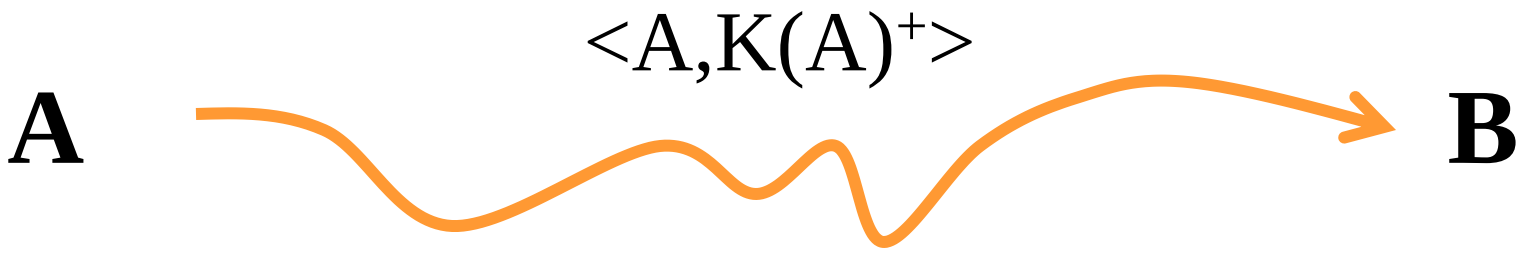


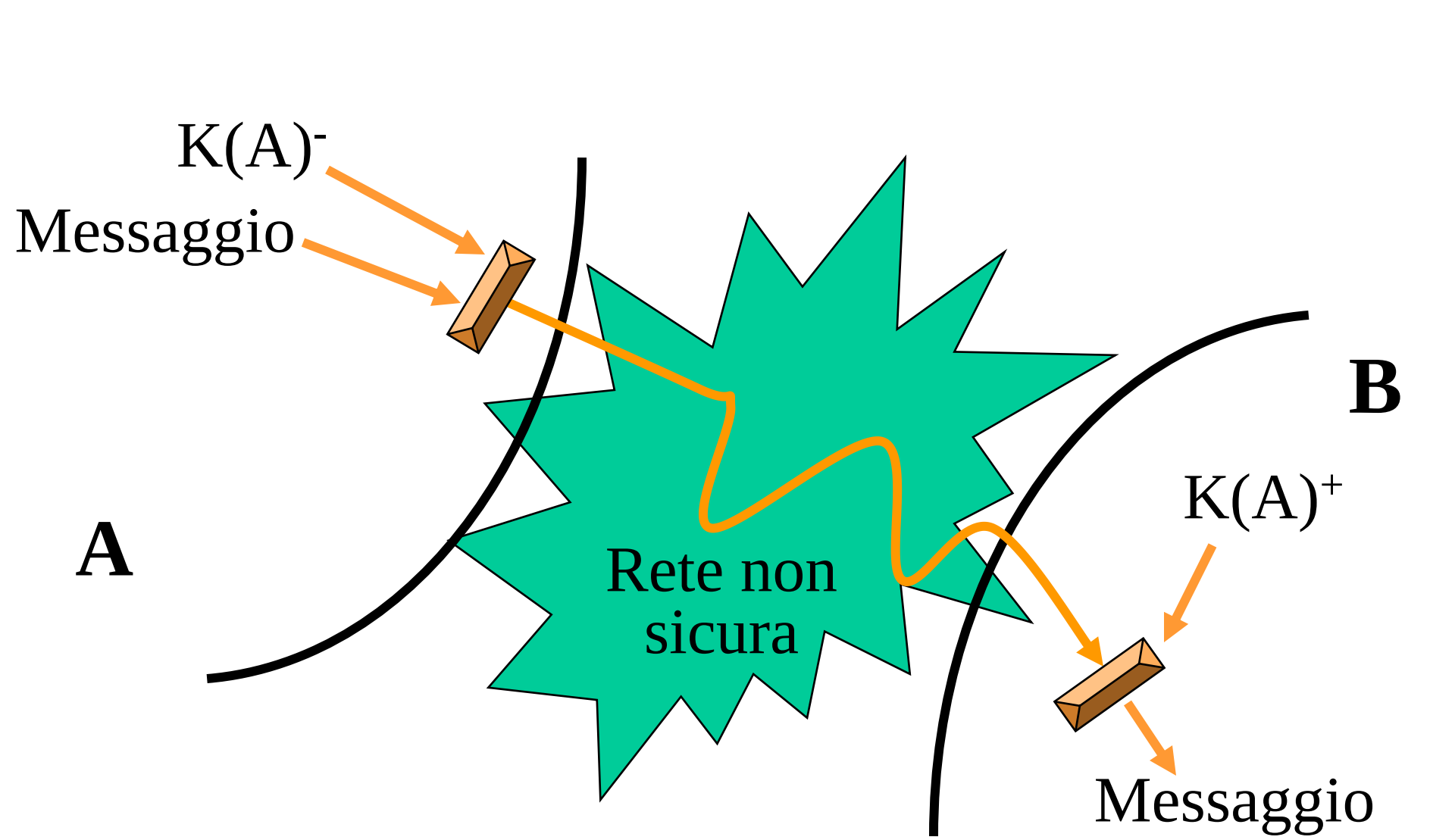


Problema utilizzo chiavi pubbliche

Autenticazione asimmetrica (firma)

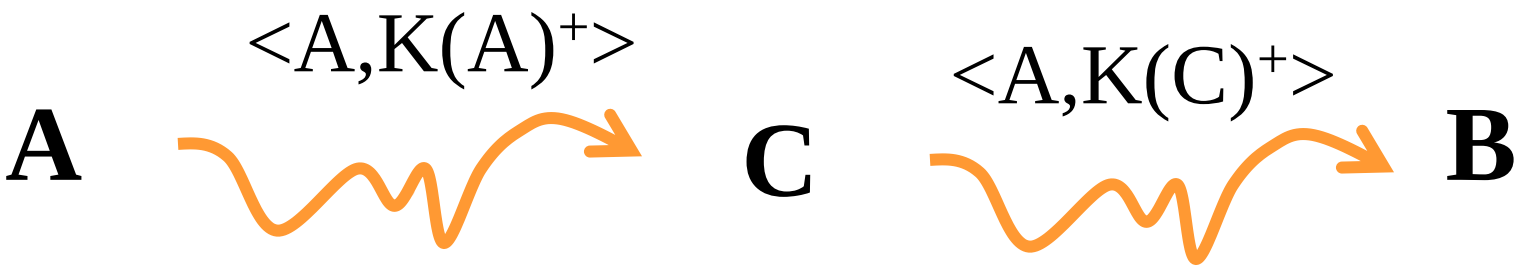
Il mittente dovrà, in qualche modo, rendere nota la propria chiave pubblica, associando ad essa la propria identità

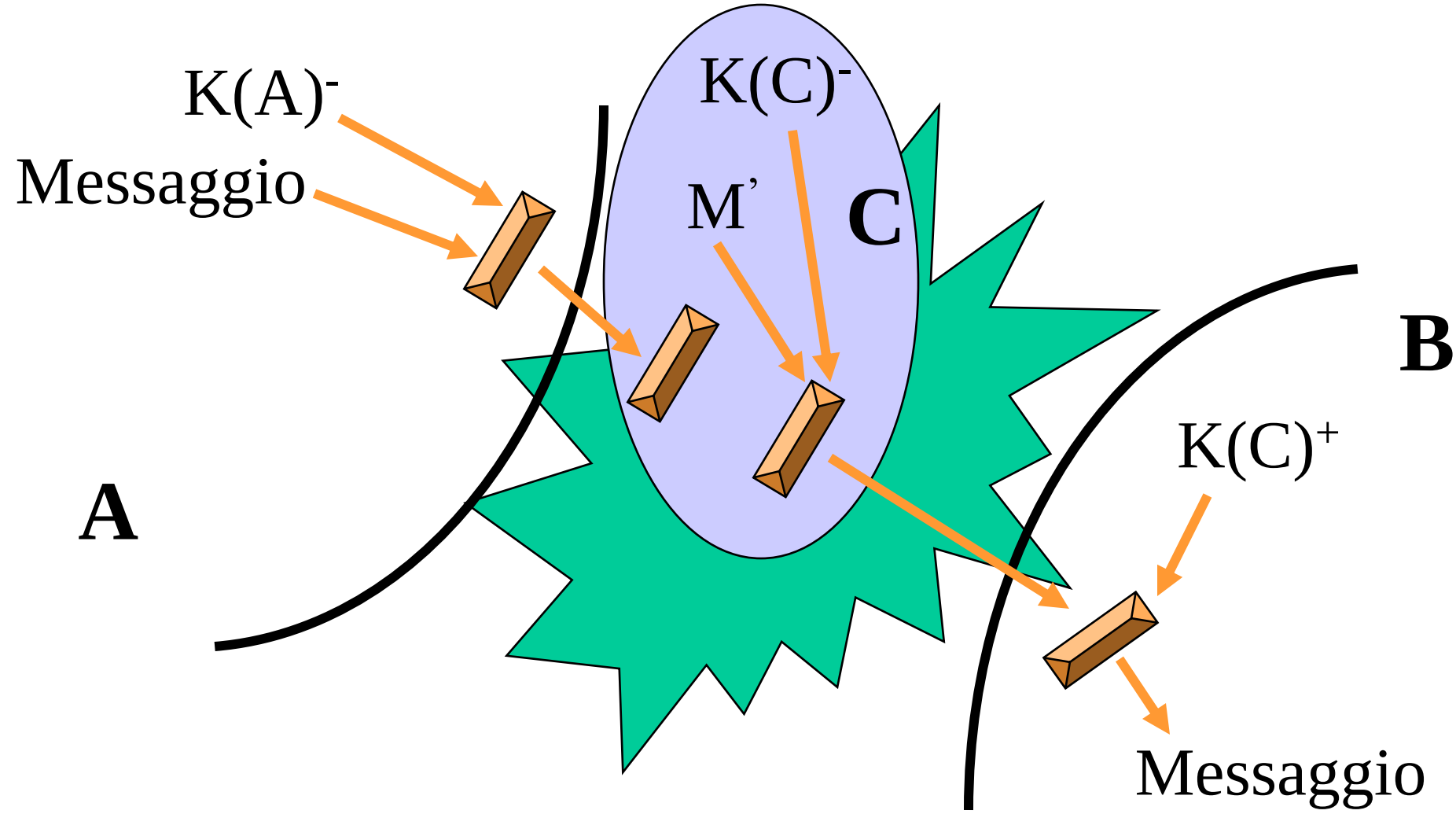




Autenticazione asimmetrica

Principale problema (per firma)



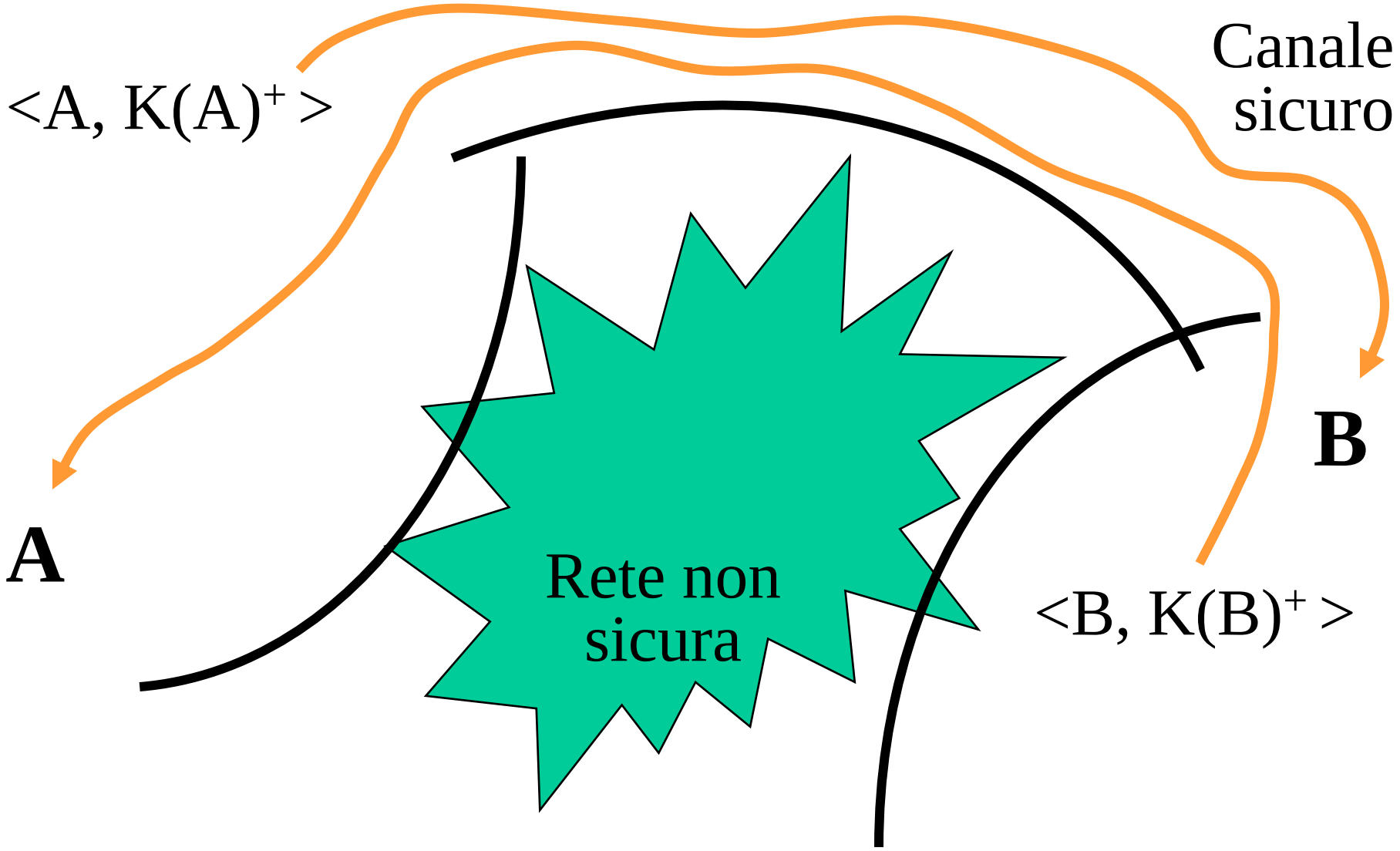


Problema utilizzo chiavi pubbliche

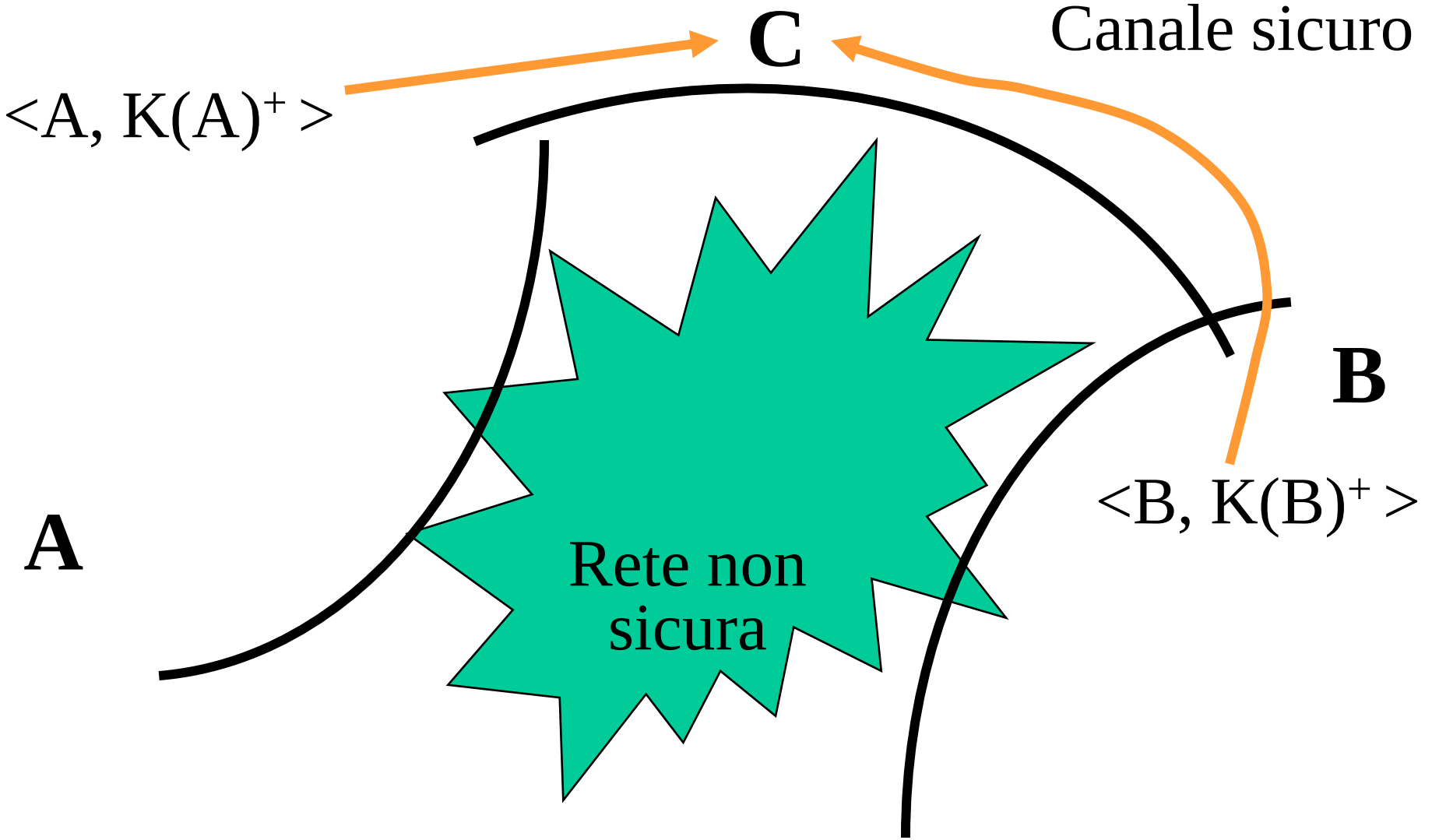
Quindi ...

… occorre una distribuzione sicura (autenticata) degli abbinamenti

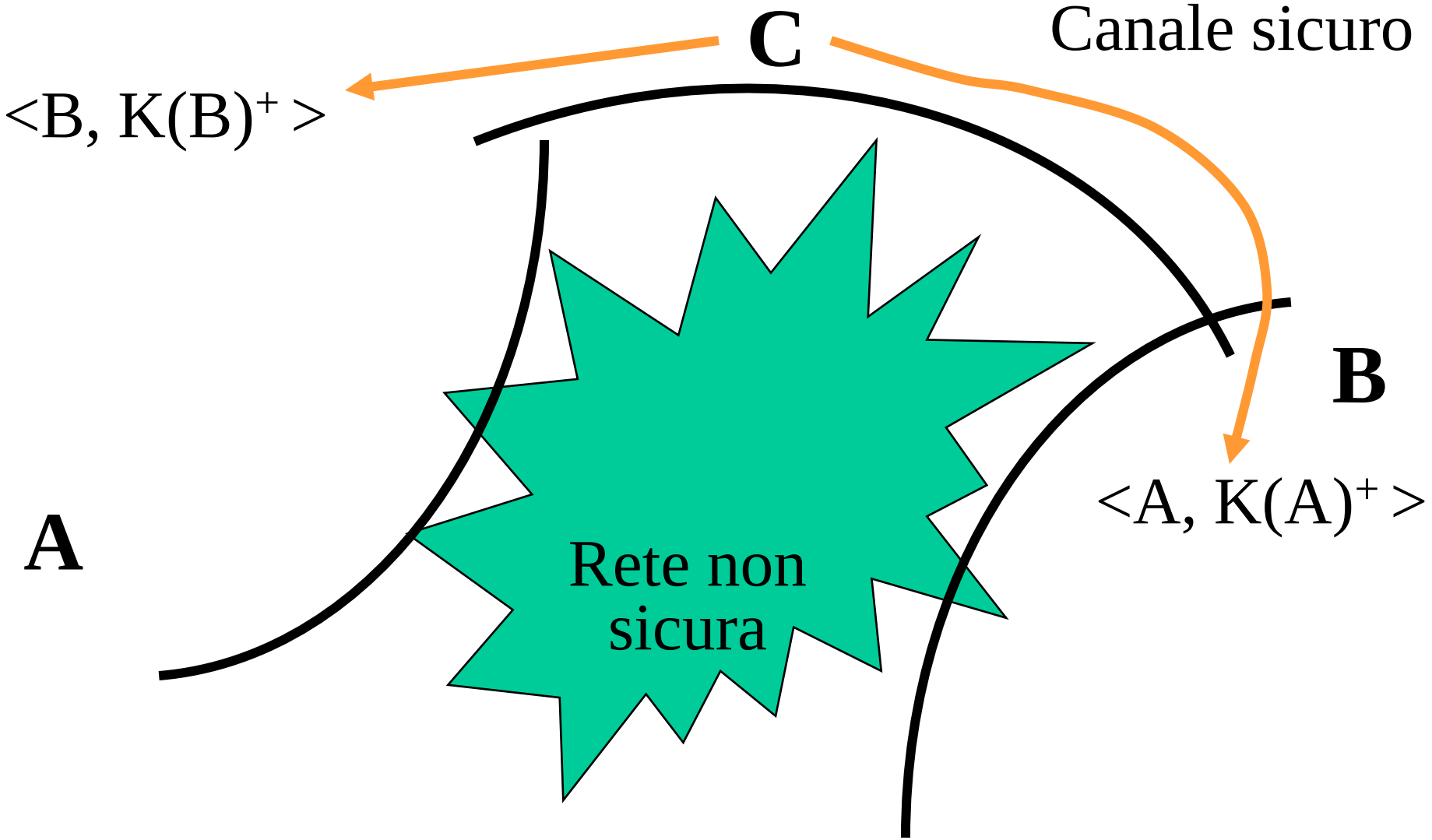
<utente,chiave pubblica>



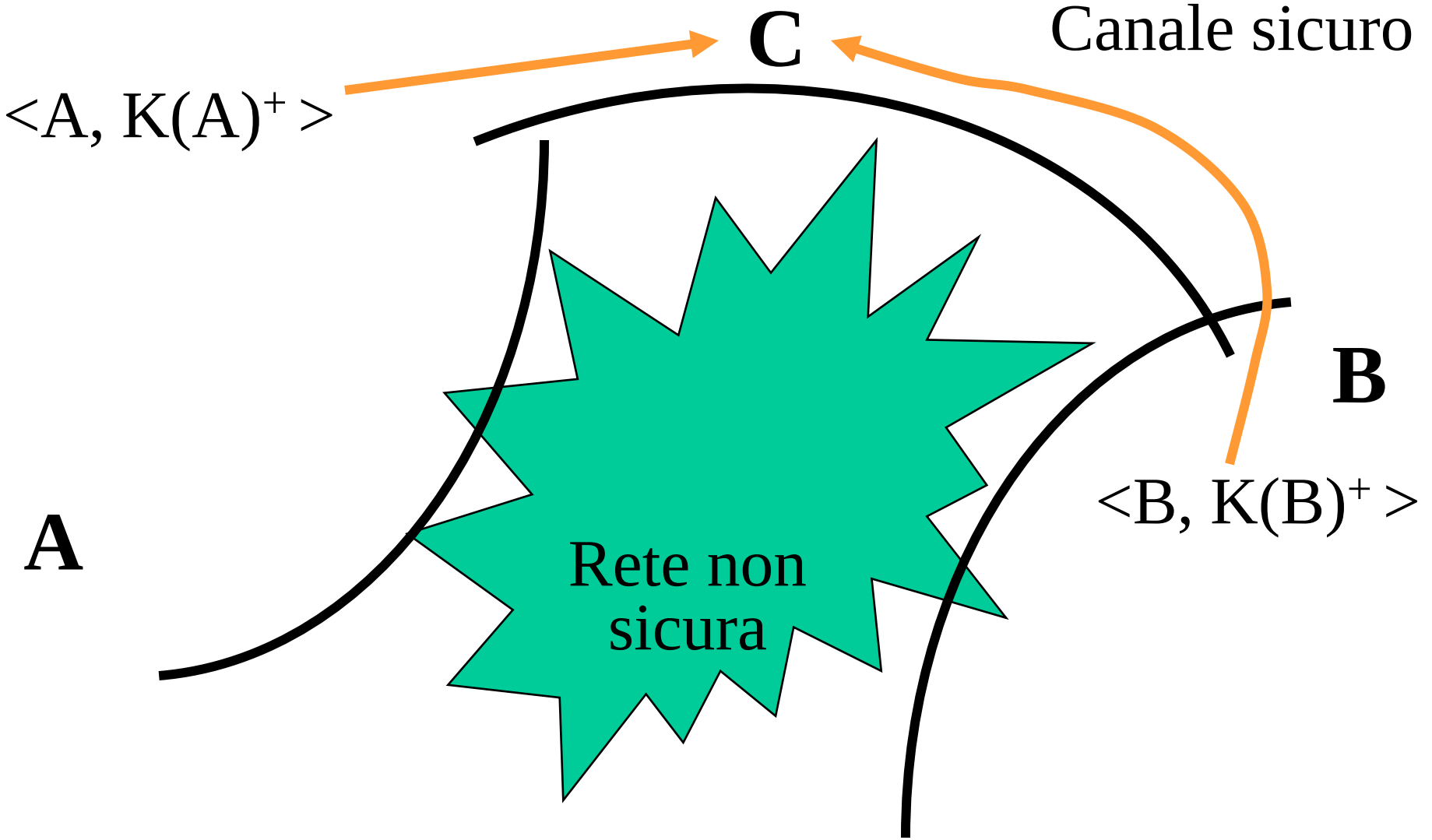
Distribuzione di chiavi pubbliche (diretta)



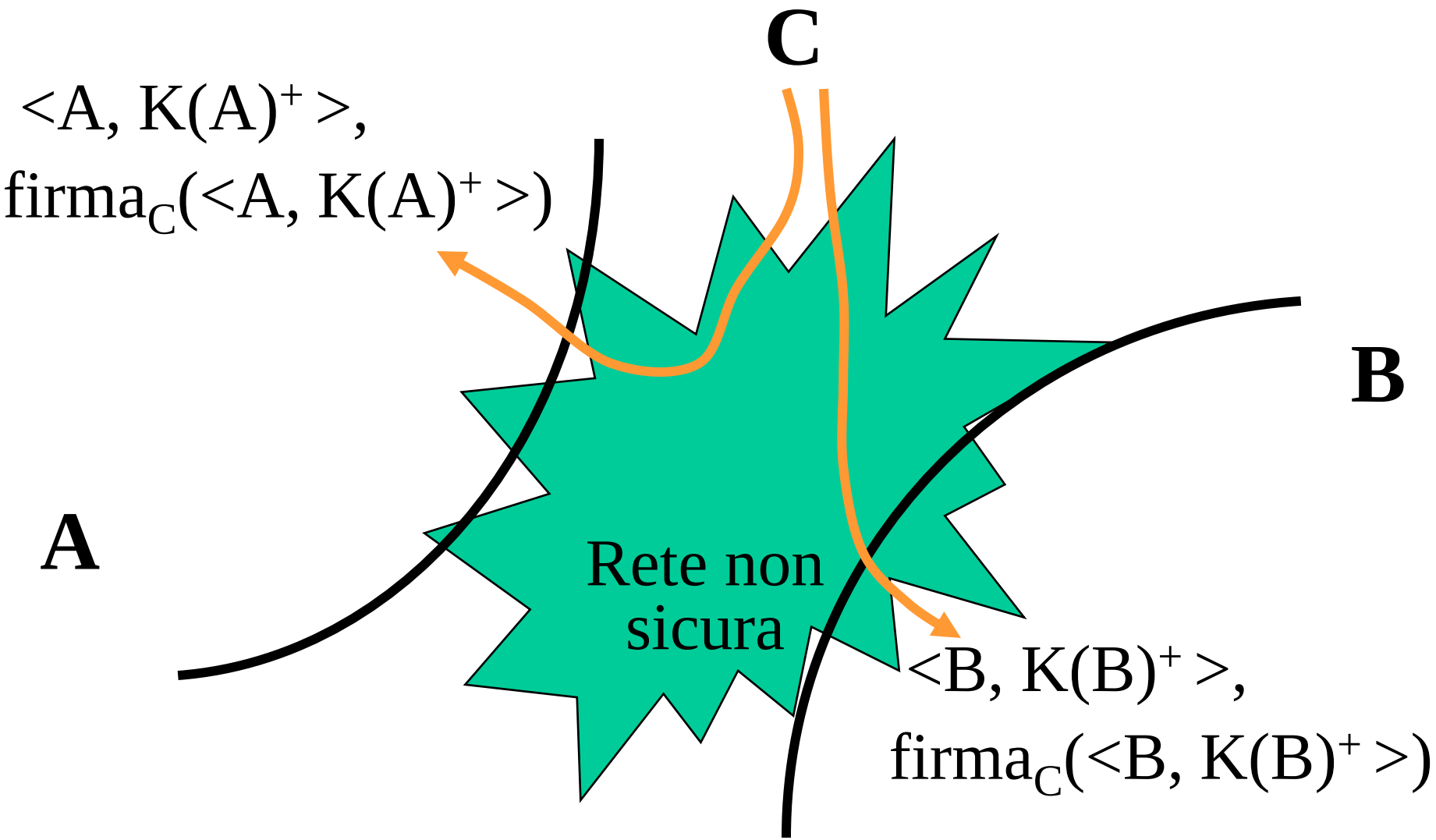
Distribuzione di chiavi pubbliche (con terza parte) - I



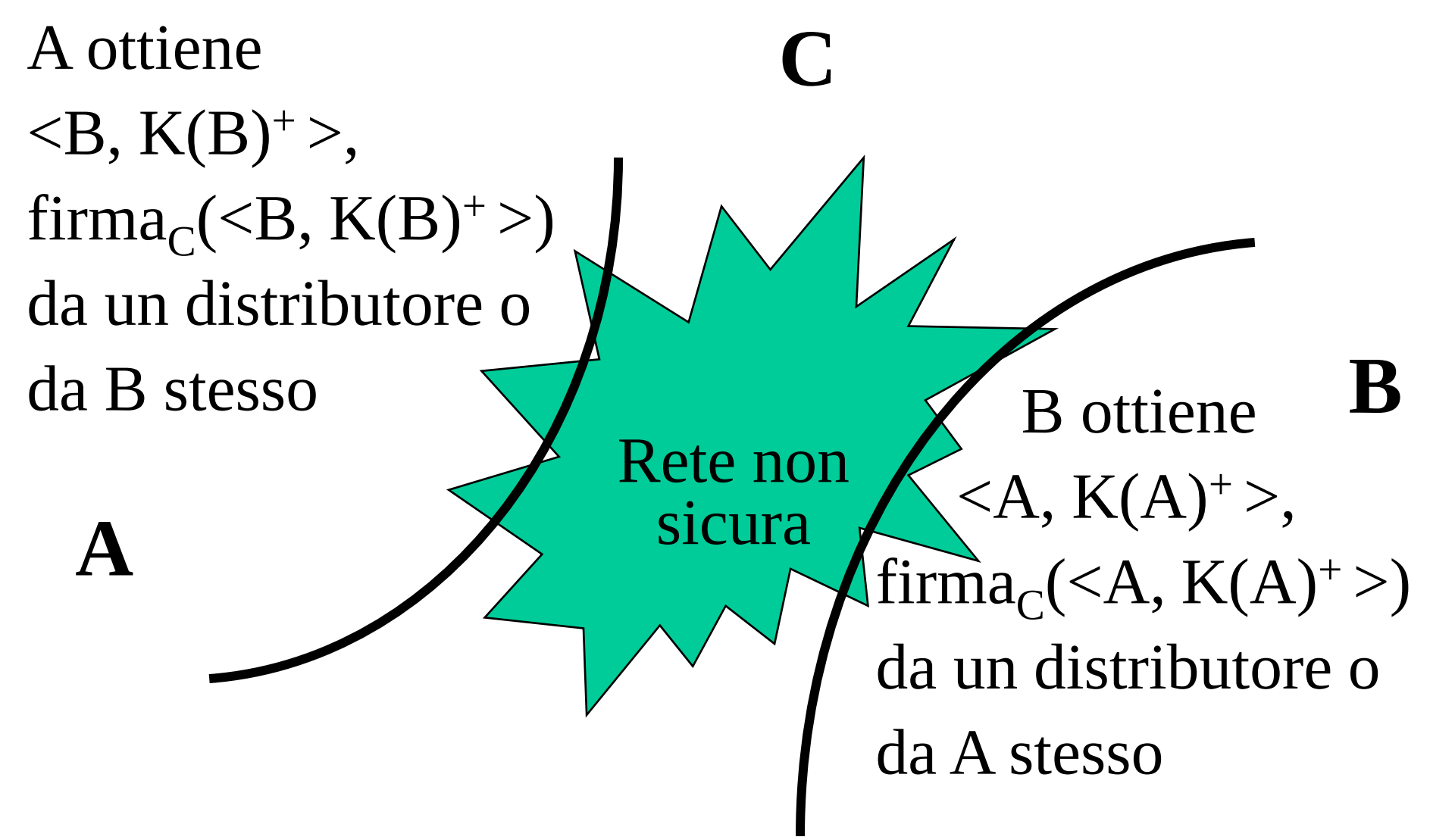
Distribuzione di chiavi pubbliche (con terza parte) - II



Distribuzione di chiavi pubbliche (con certificati) - I

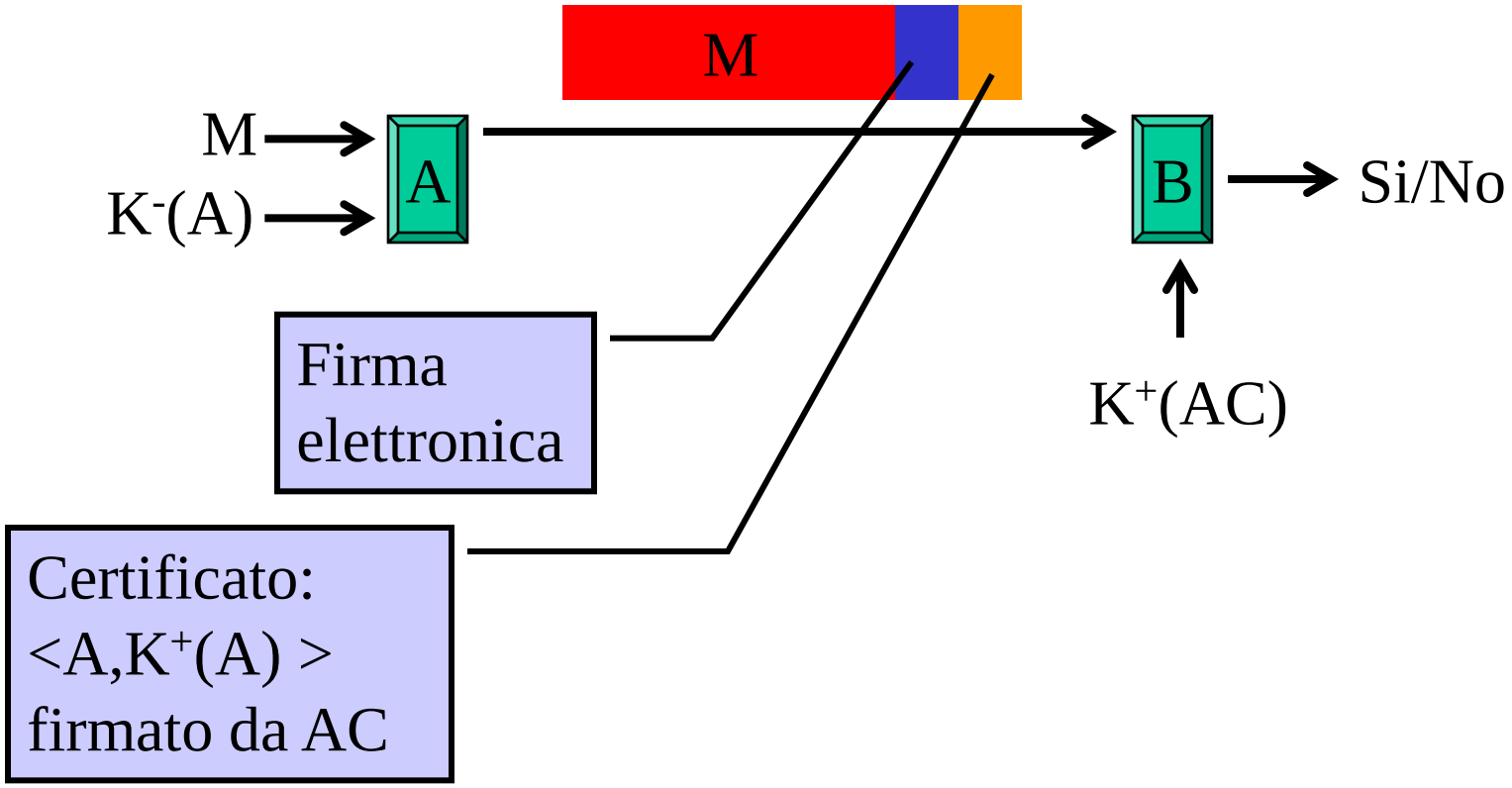


Distribuzione di chiavi pubbliche (con certificati) - II

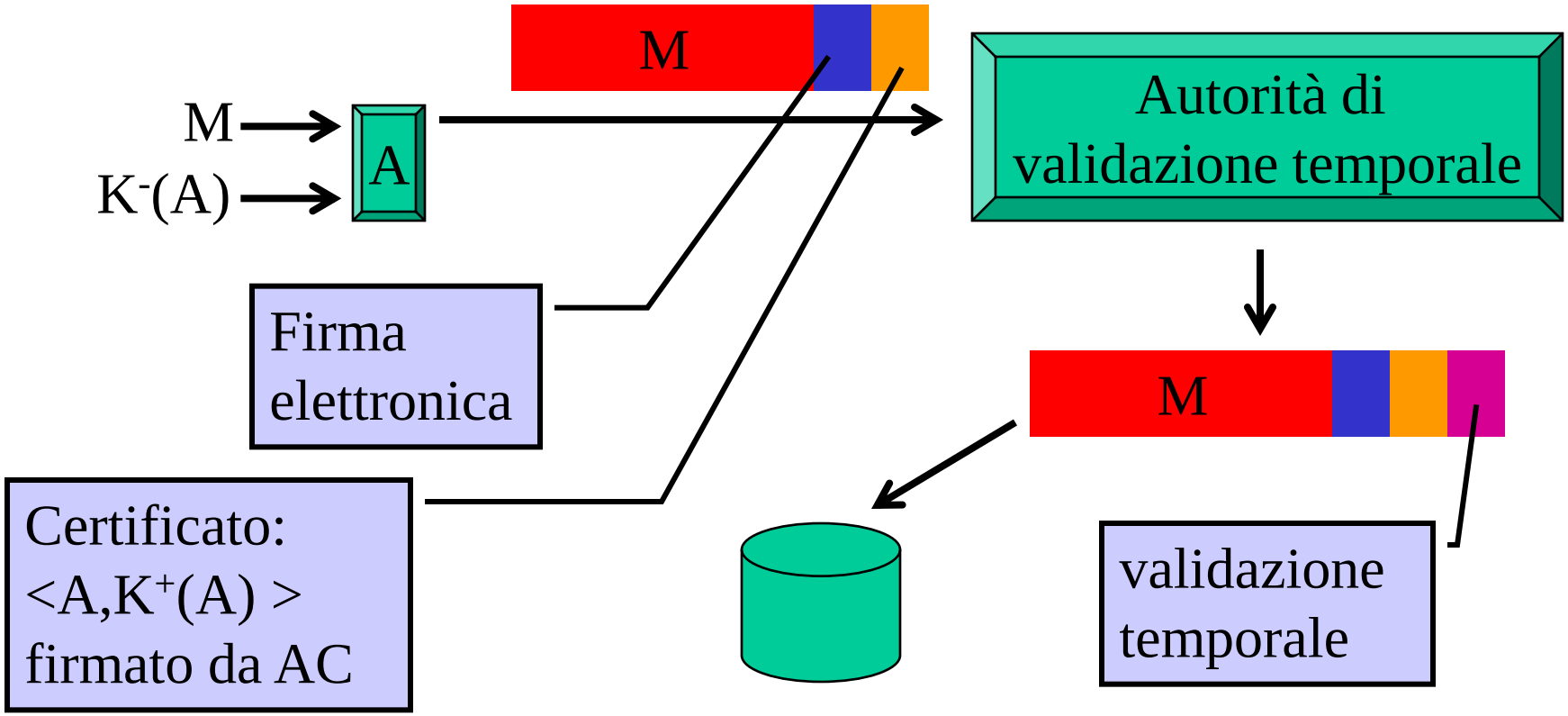


Distribuzione di chiavi pubbliche (con certificati) - III

Firma Elettronica con certificato



Validazione temporale



Firma Elettronica con certificato e timestamp