ZFONE

- Software di crittografia Voip,filtra i pacchetti in entrata e uscita da un softphone.
- Zimmermann 2006

- Win XP, Mac Os X, Linux.

- Integrabile come plug-in su diversi software Voip: SDK disponibile

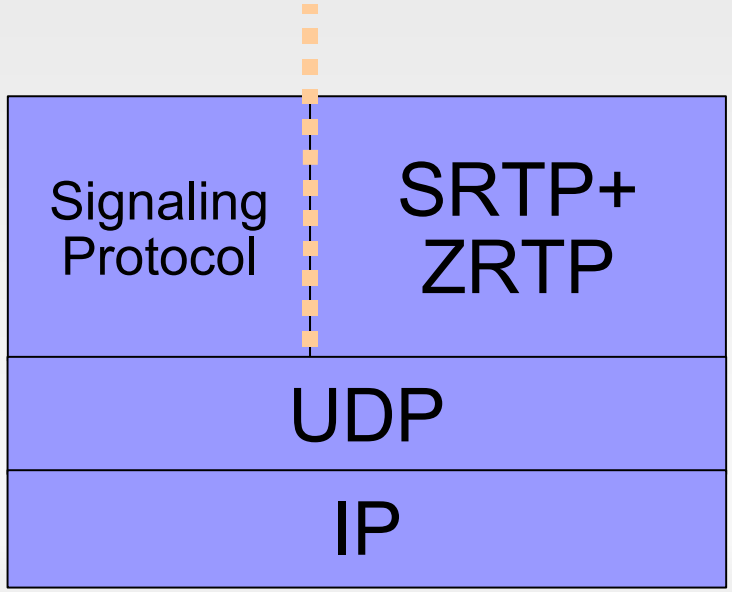
Protocol stack

- Signaling protocol (SIP o H.323) per inizializzare la sessione

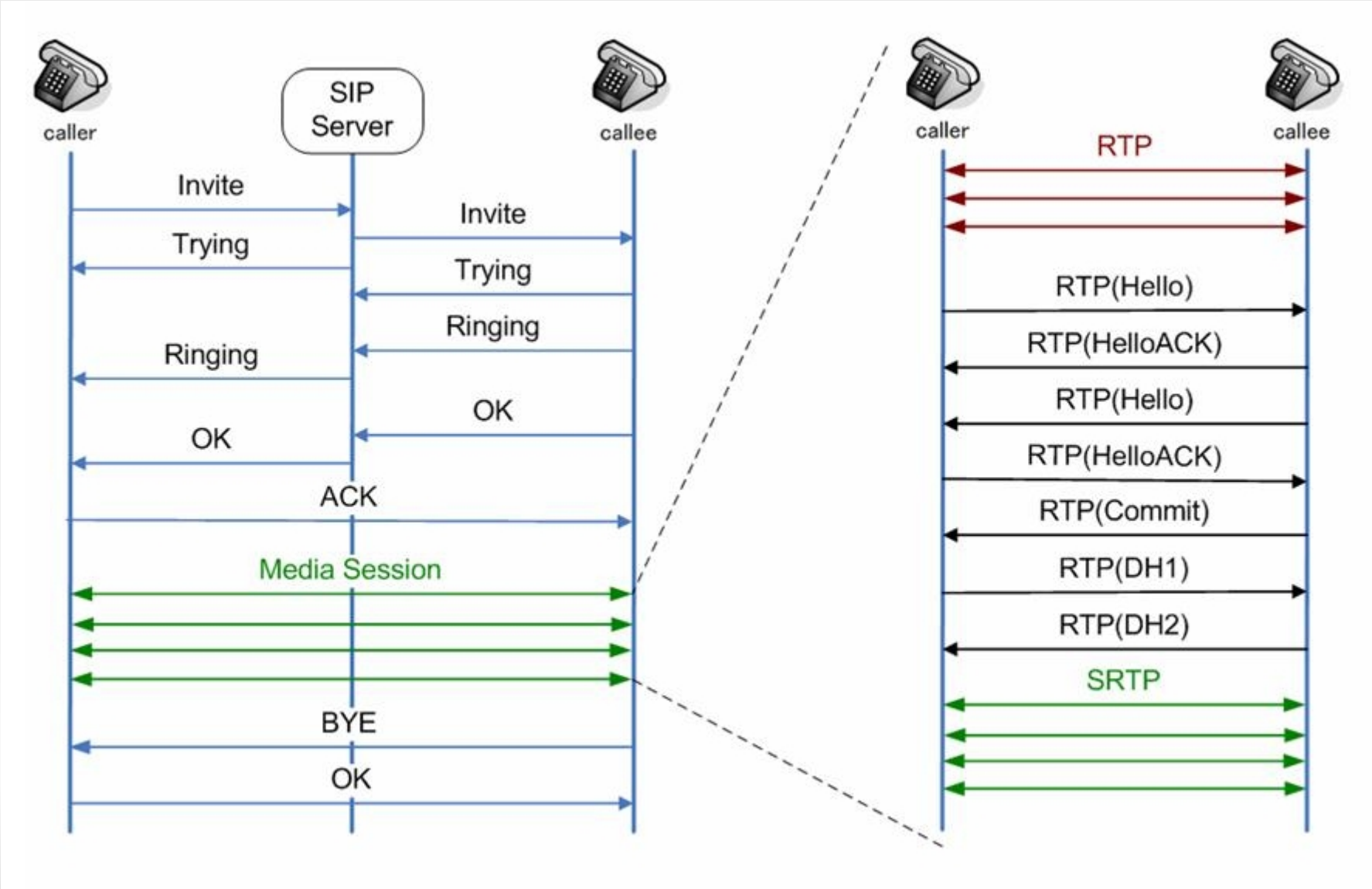
ad es. Session Initialization Protocol, livello 5 (Application) dello stack TCP/IP.Ha bisogno di proxy server intermedi per il routing delle richieste e la fornitura di altri servizi.È leggero e in formato testuale.

- Zfone opera in modo indipendente dal tipo di server Voip utilizzato.

- Realizza un accordo su chiavi in modalità *peer to peer* tra due client, *a livello di stream RTP.*



Come funziona una sessione Voip con Zfone



ZRTP

- ZRTP estensione di RTP (Realtime Transport Protocol) proposta come RFC da Zimmermann nel marzo 2006.

- Descrive l'implementazione di un'accordo su chiavi di tipo Diffie-Hellman per una sessione SRTP

- No PKI, no key-management, no trust models...

- *opportunistic encryption*: Zfone fa autosensing per determinare se il client destinatario supporta ZRTP; in caso positivo attiva la cifratura.

attacco Man in the middle

g,p scelti,
a,b = esponenti segreti

$A = g^a \bmod p$ →

← $B = g^b \bmod p$

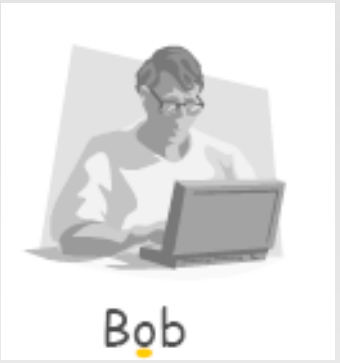
$S_{AB} = B^a \bmod p$ $S_{AB} = A^b \bmod p$

← $E(S_{AB})$ →

Attacco man in the middle

A

B



$E = g^e \bmod p$

$S_{AE} = E^a \bmod p$

$A^e \bmod p = S_{AE}$

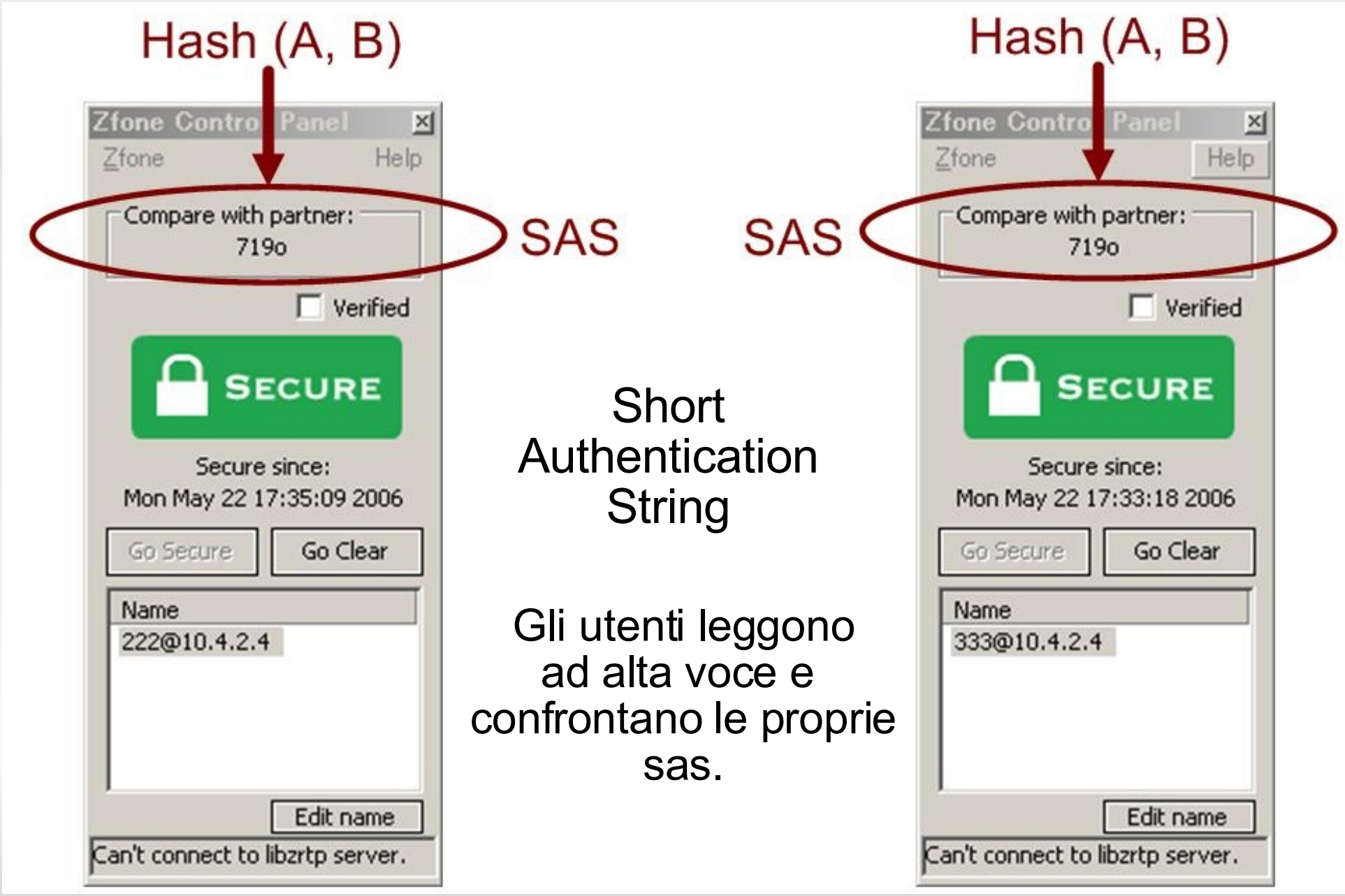
$B^e \bmod p = S_{BE}$

$SB_E = E^b \bmod p$

$E(S_{AE})$

$E(S_{BE})$

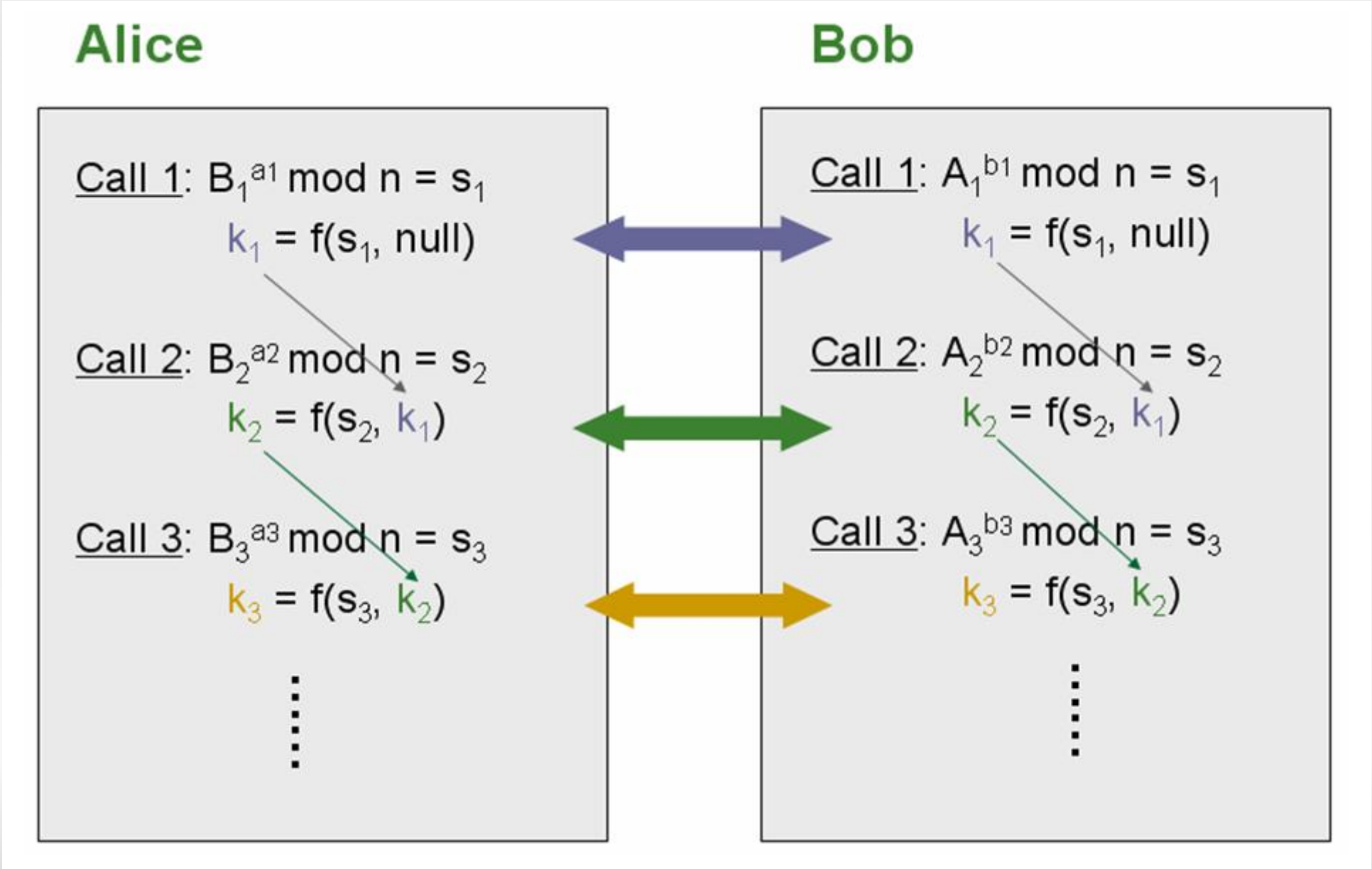
MITM: Soluzione



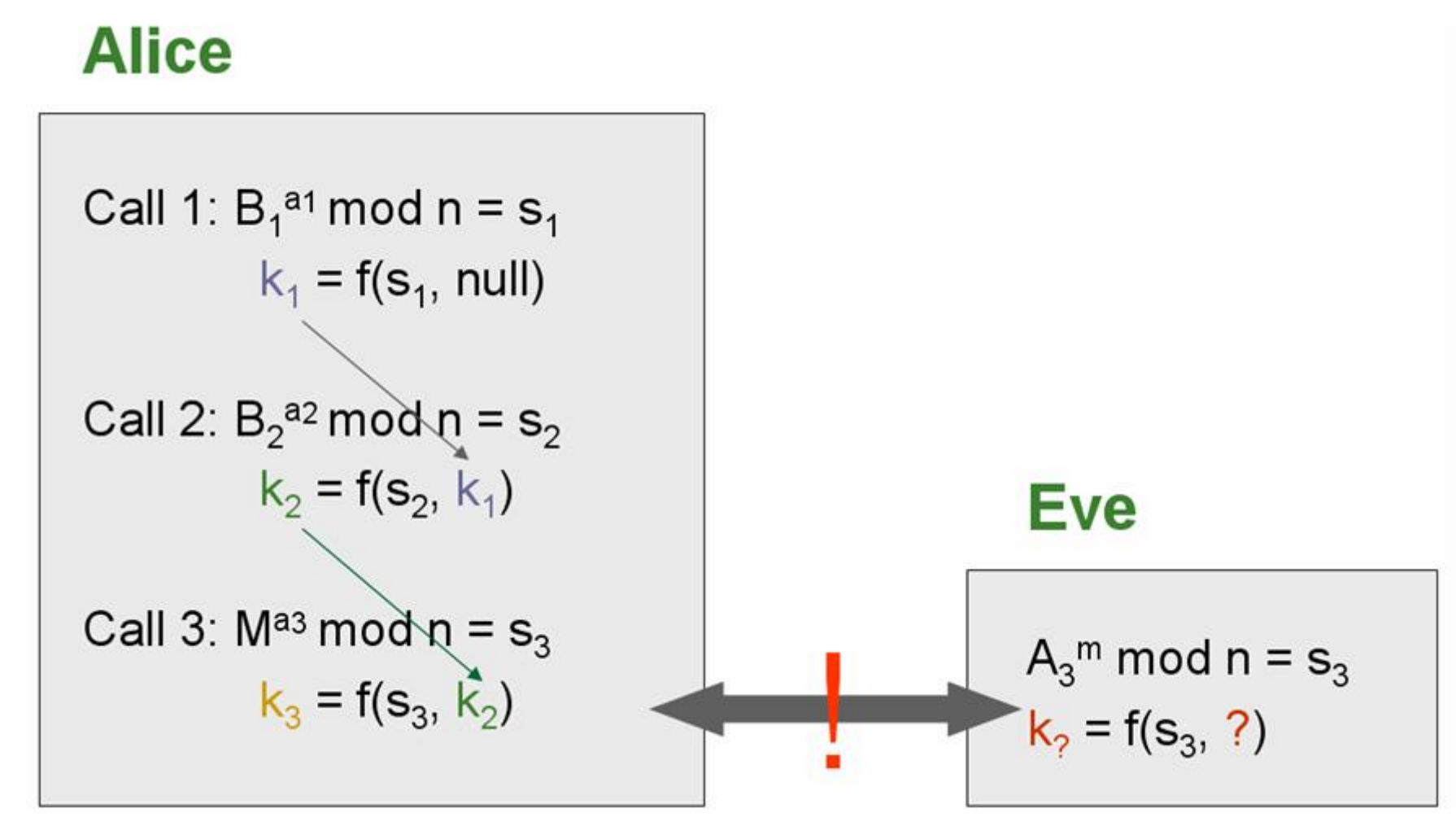
Key continuity

- Alice e Bob devono verificare la Sas almeno nella prima chiamata.
- Viene salvato un hash del segreto condiviso dal primo accordo su chiavi.
- Nella successiva chiamata tra Alice e Bob, la chiave di sessione sarà una combinazione tra il valore salvato e il nuovo segreto condiviso.

Key continuity



Key continuity



SRTP

- Secure Real-time Transport Protocol (RFC 3711), garantisce:

  1)Data-flow encryption
  2)Authentication
  3)Integrity
  4)Replay protection

- traffico RTP scorre su una rete unreliable con possibili perdite di pacchetti.

SRTP: proprietà

1) Lo standard prevede di utilizzare AES in 3 diverse modalità:

- AES 128 bit in una variante di Counter, con contatore intero
- f8 mode, variante di Output Feedback resa “seekable”
- null cipher, quando si vuole disabilitare la cifratura.

Le chiavi di cifratura vengono generate da una Master Key negoziata con un protocollo esterno (ZRTP...)

2) Autenticazione e integrità attraverso algoritmo HMAC-SHA1

Produce 160 bit usando il payload e parti dell'header del pacchetto,compreso il sequence number.

Conclusioni

- approccio alla security Voip è complesso,per il tipo di traffico e le infrastrutture coinvolte.

- implementare soluzioni compliant con i protocolli consente di 'stringere' il dominio e progettare soluzioni semplici ed eleganti.

link

- http://zfoneproject.com/
- http://www.schneier.com/blog/archives/2005/07/encrypted_voip.html
- http://voipsa.org/blog/2006/06/19/a-tour-through-zfone/
- http://zfoneproject.com/docs/ietf/draft-zimmermann-avt-zrtp-03.html
- PgpPhone,SRTP,IDEA... http://en.wikipedia.org/