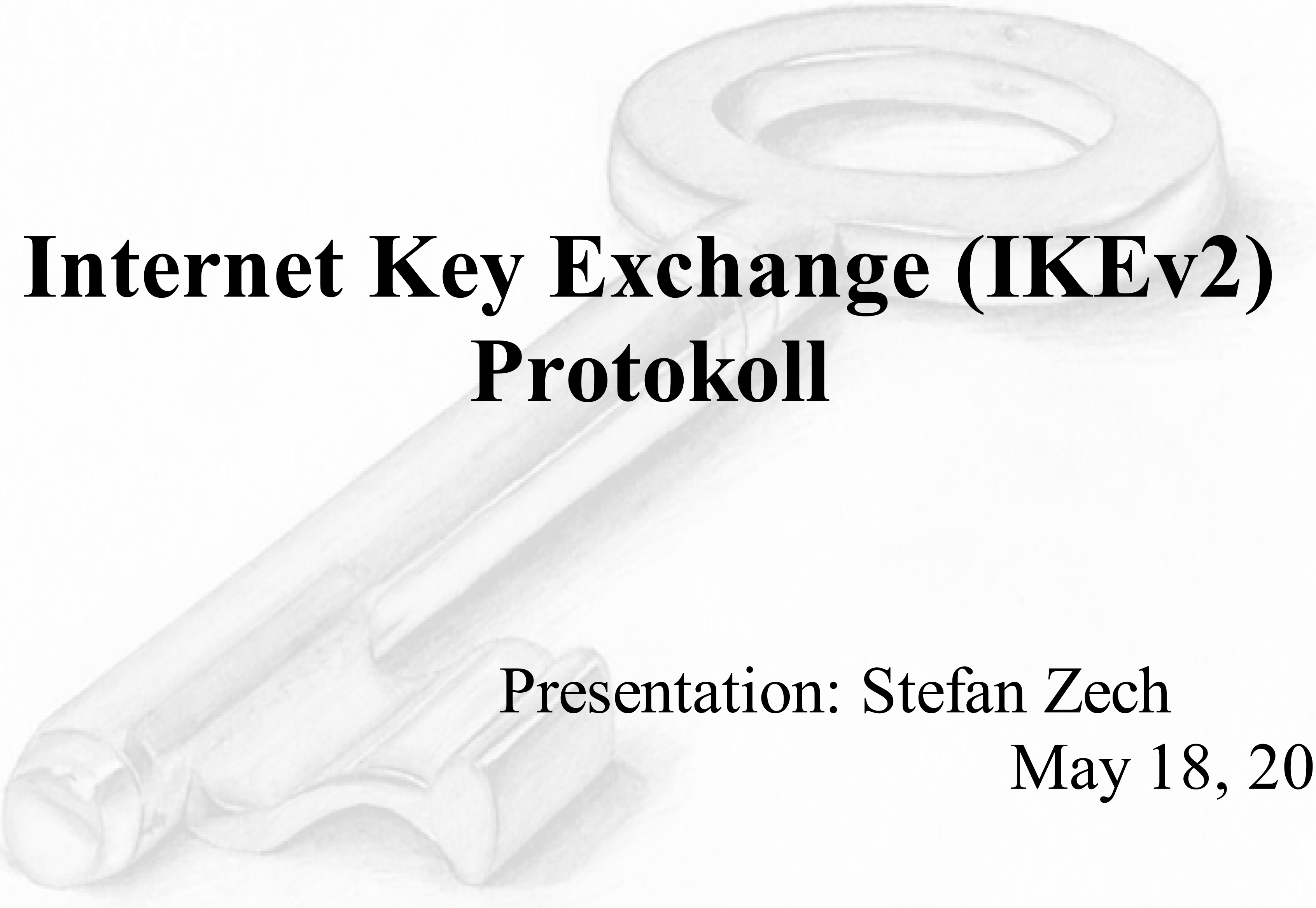
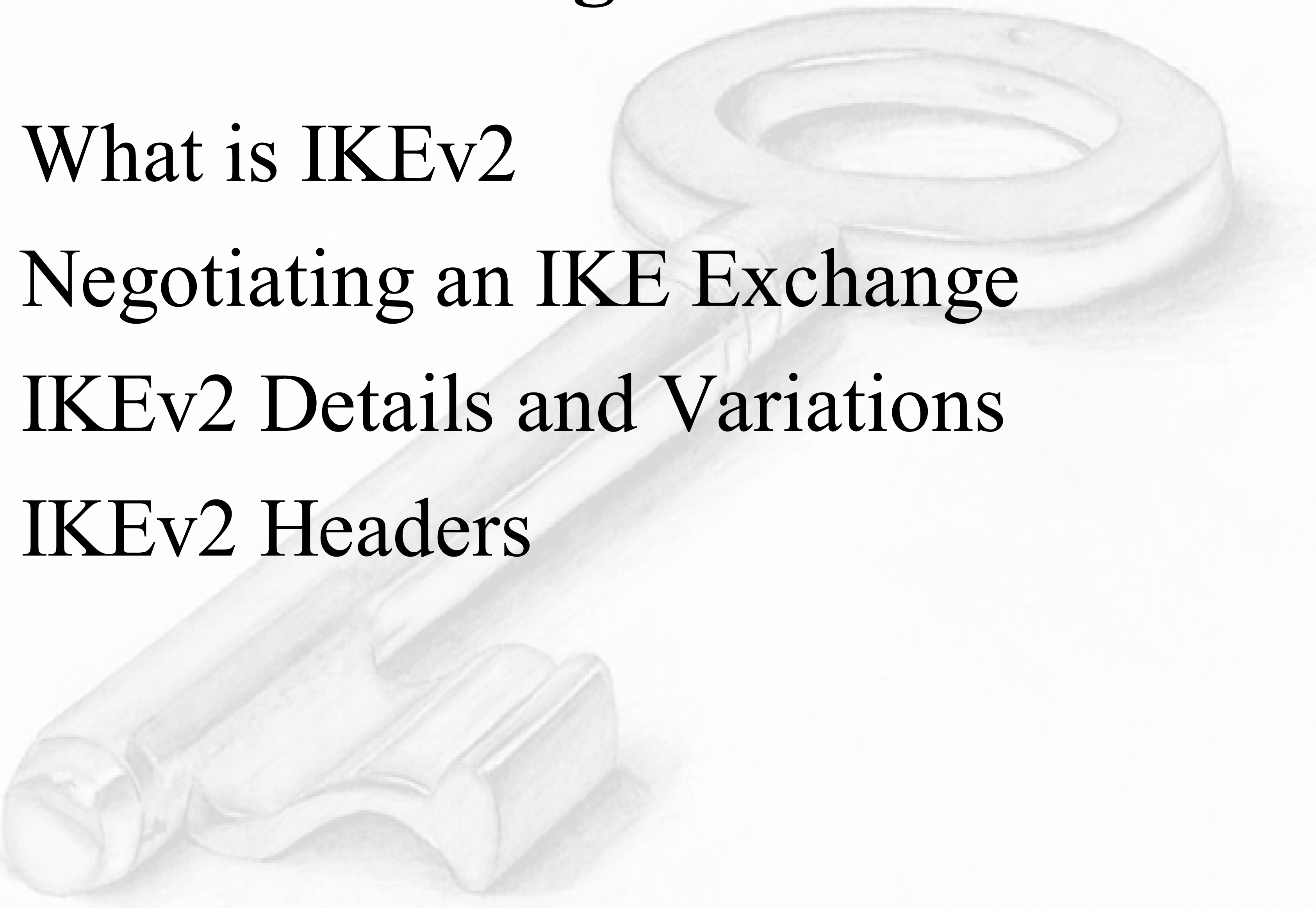
Internet Security SS 2004
Prof. Dr. P. Trommler



Internet Key Exchange (IKEv2) Protokoll

Presentation: Stefan Zech
May 18, 2004

Agenda



- What is IKEv2
- Negotiating an IKE Exchange
- IKEv2 Details and Variations
- IKEv2 Headers

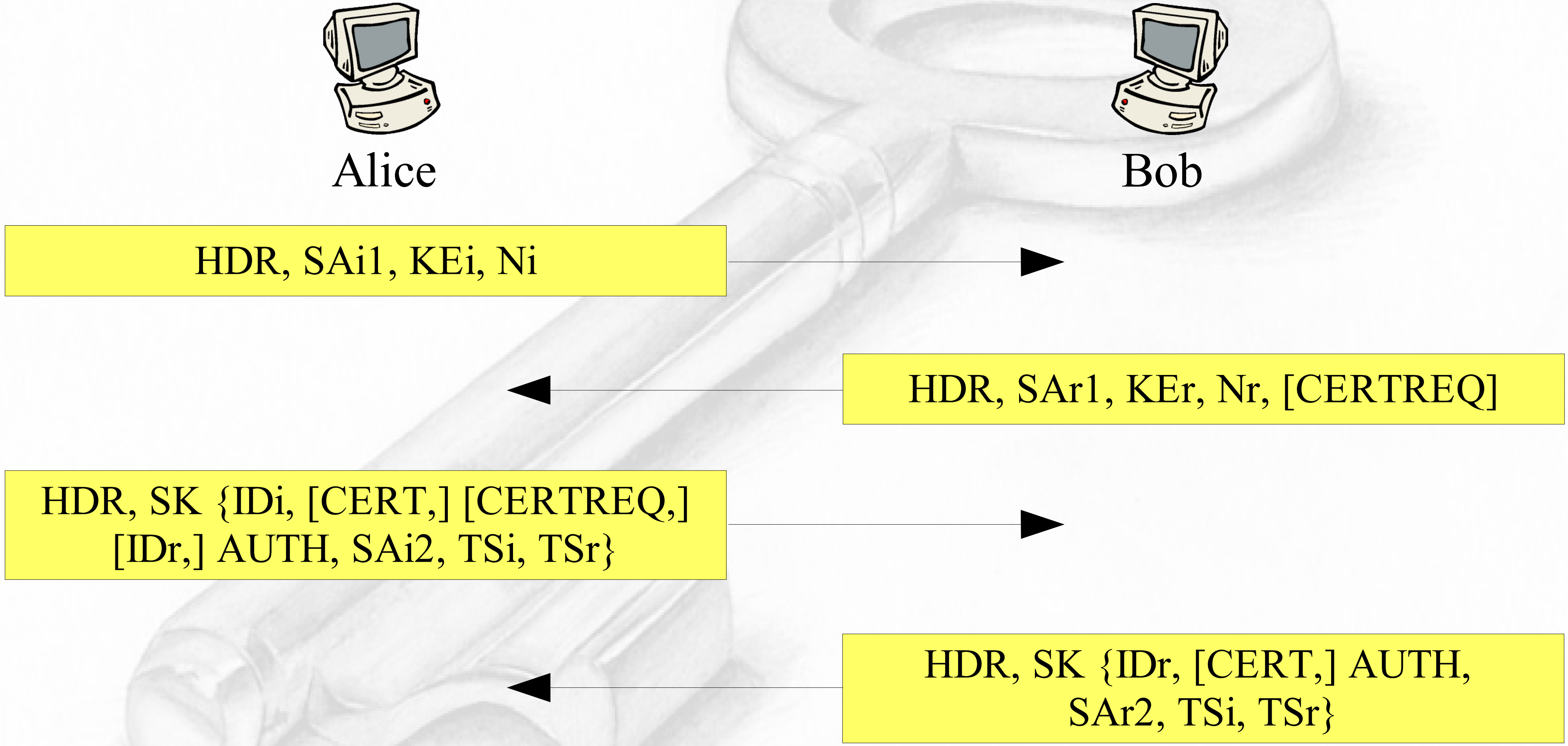
What is IKEv2

- For use with IPsec Protocol
- Establishing a secure connection with
  - Confidentiality
  - Data integrity
  - Access control
  - Data source authentication
- Uphold the secure connection
  - Rekeying
  - Errorhandling

Negotiating an IKE Exchange

- The initial exchanges
  - IKE_SA_INIT
  - IKE_AUTH
- CREATE_CHILD_SA exchange
- The INFORMATIONAL exchange

The initial exchanges



Alice

Bob

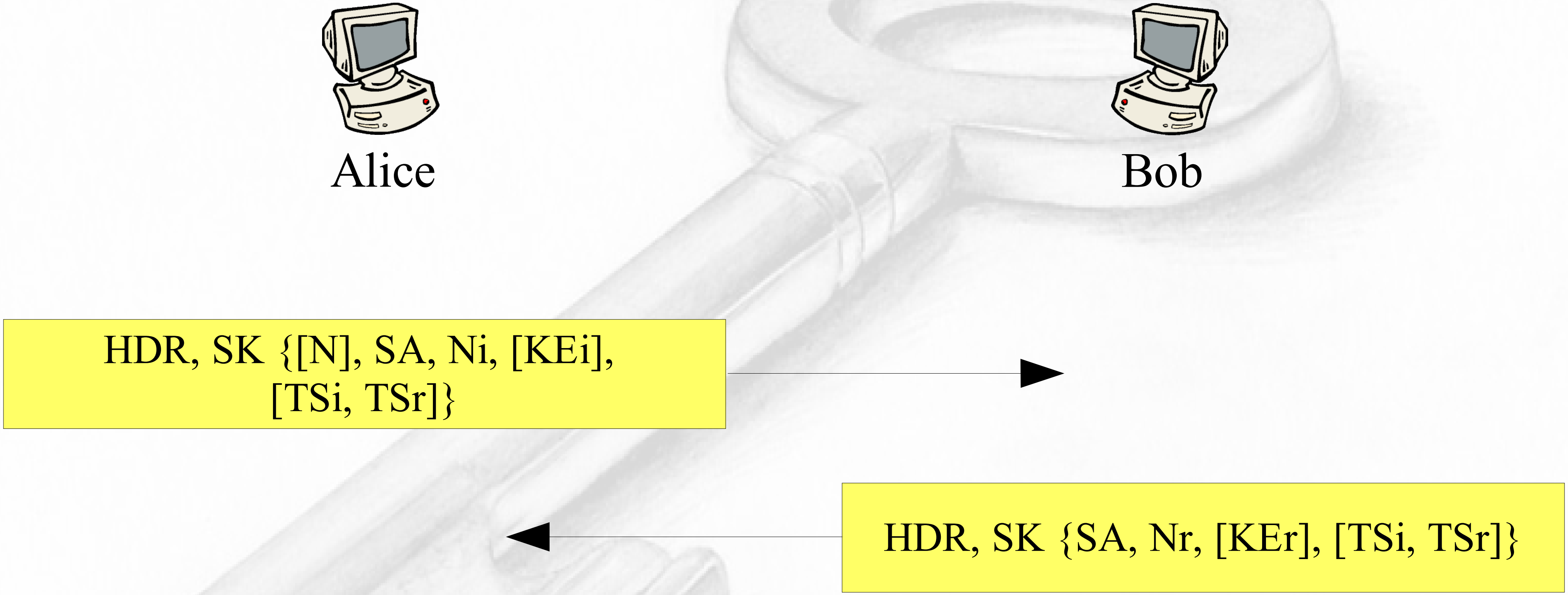
HDR, SAi1, KEi, Ni

HDR, SAr1, KEr, Nr, [CERTREQ]

HDR, SK {IDi, [CERT,] [CERTREQ,] [IDr,] AUTH, SAi2, TSi, TSr}

HDR, SK {IDr, [CERT,] AUTH, SAr2, TSi, TSr}

CREATE_CHILD_SA



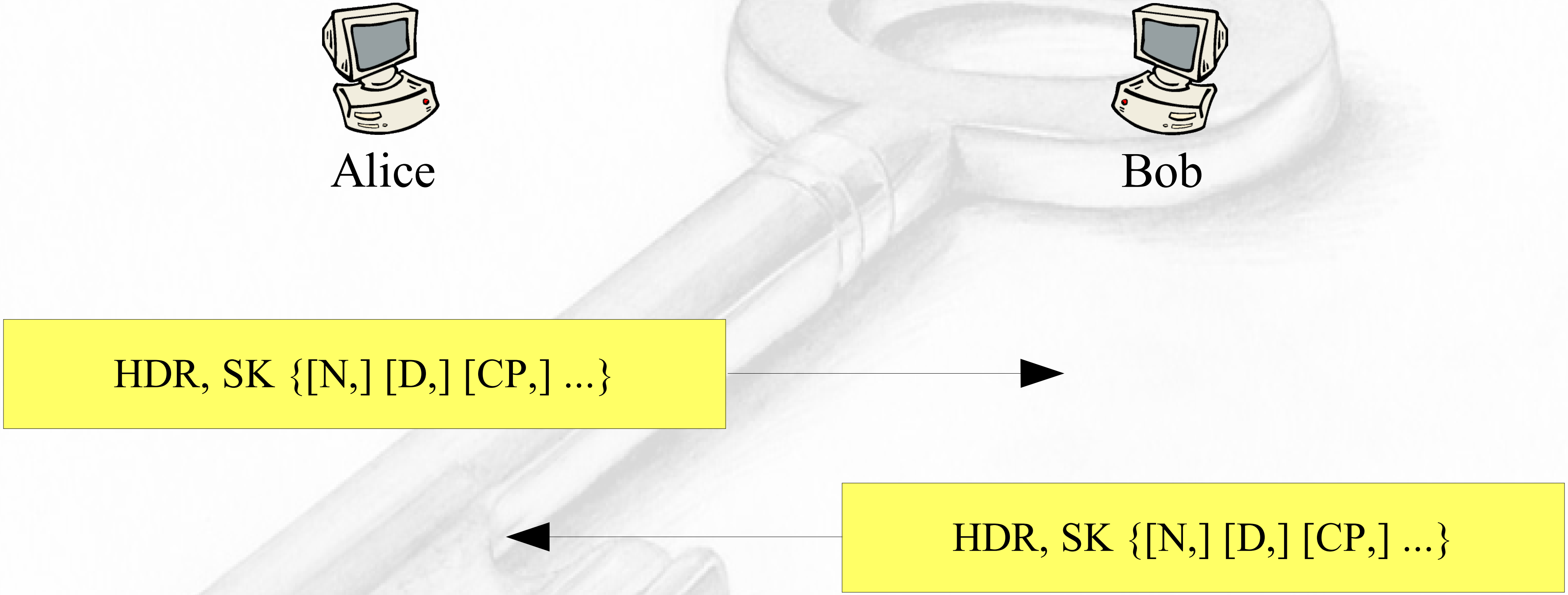
Alice

Bob

HDR, SK {[N], SA, Ni, [KEi], [TSi, TSr]}

HDR, SK {SA, Nr, [KEr], [TSi, TSr]}

The INFORMATIONAL exchange



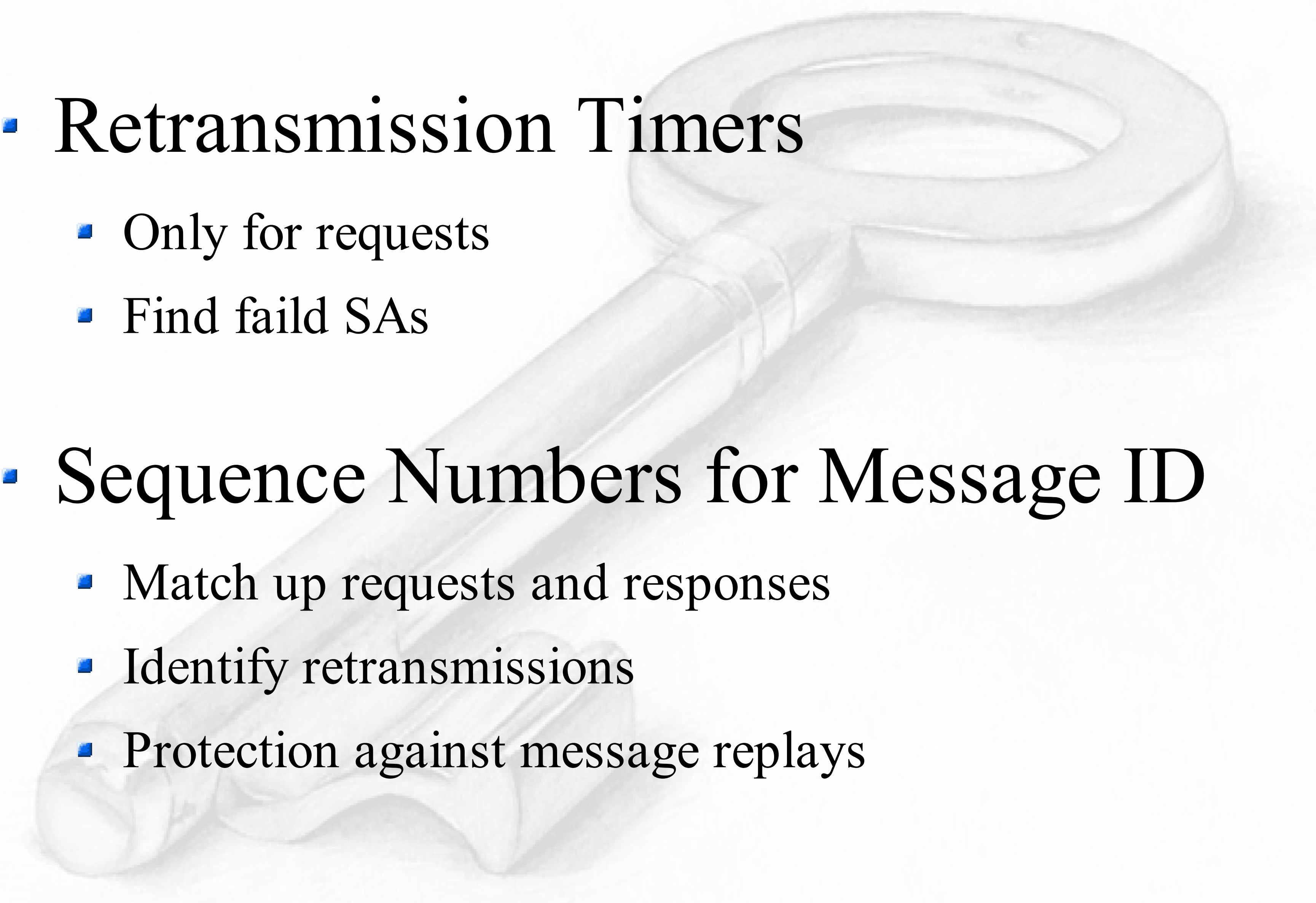
Alice

Bob

HDR, SK {[N,] [D,] [CP,] ...}

HDR, SK {[N,] [D,] [CP,] ...}

IKEv2 Details and Variations



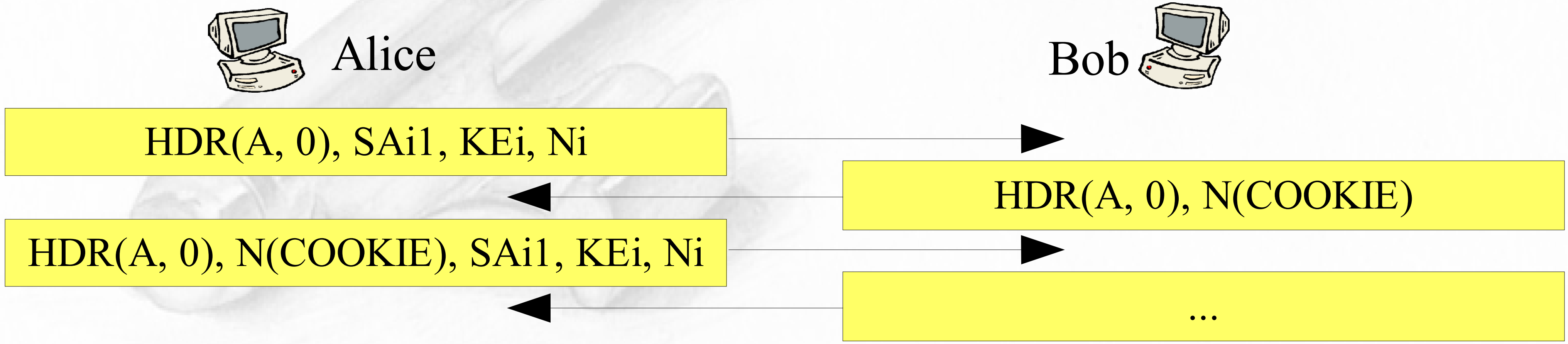
- Retransmission Timers
  - Only for requests
  - Find faild SAs
- Sequence Numbers for Message ID
  - Match up requests and responses
  - Identify retransmissions
  - Protection against message replays

IKEv2 Details and Variations

- Window size for overlapping requests
  - Multiple requests before getting a response
  - Maximizes throughput
- State Syncronization and Connection Timeouts
  - Check the other endpoint before concluding it failed
  - The rate of this checks MUST be limited
  - Reduces the risk of DoS-Attacs

IKEv2 Details and Variations

- Cookies
  - Used for limited DoS protection in case of forged source IP Adresses
  - Instead of respond a SA_INIT response send a notify Payload with the Cookie
  - The initiator must now retransmit the SA_INIT request with the Cookie



Alice

Bob

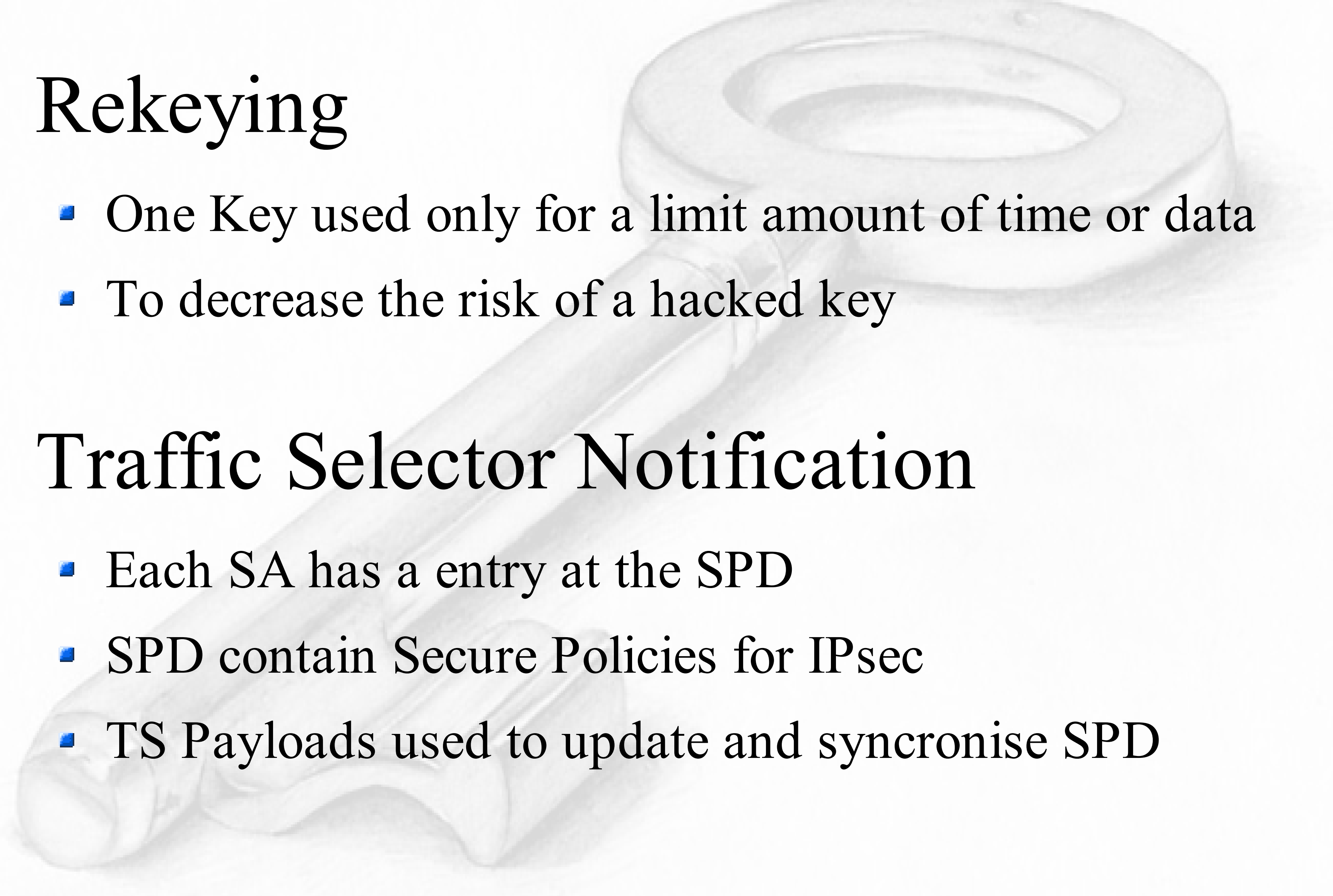
HDR(A, 0), SAi1, KEi, Ni

HDR(A, 0), N(COOKIE)

HDR(A, 0), N(COOKIE), SAi1, KEi, Ni

...

IKEv2 Details and Variations

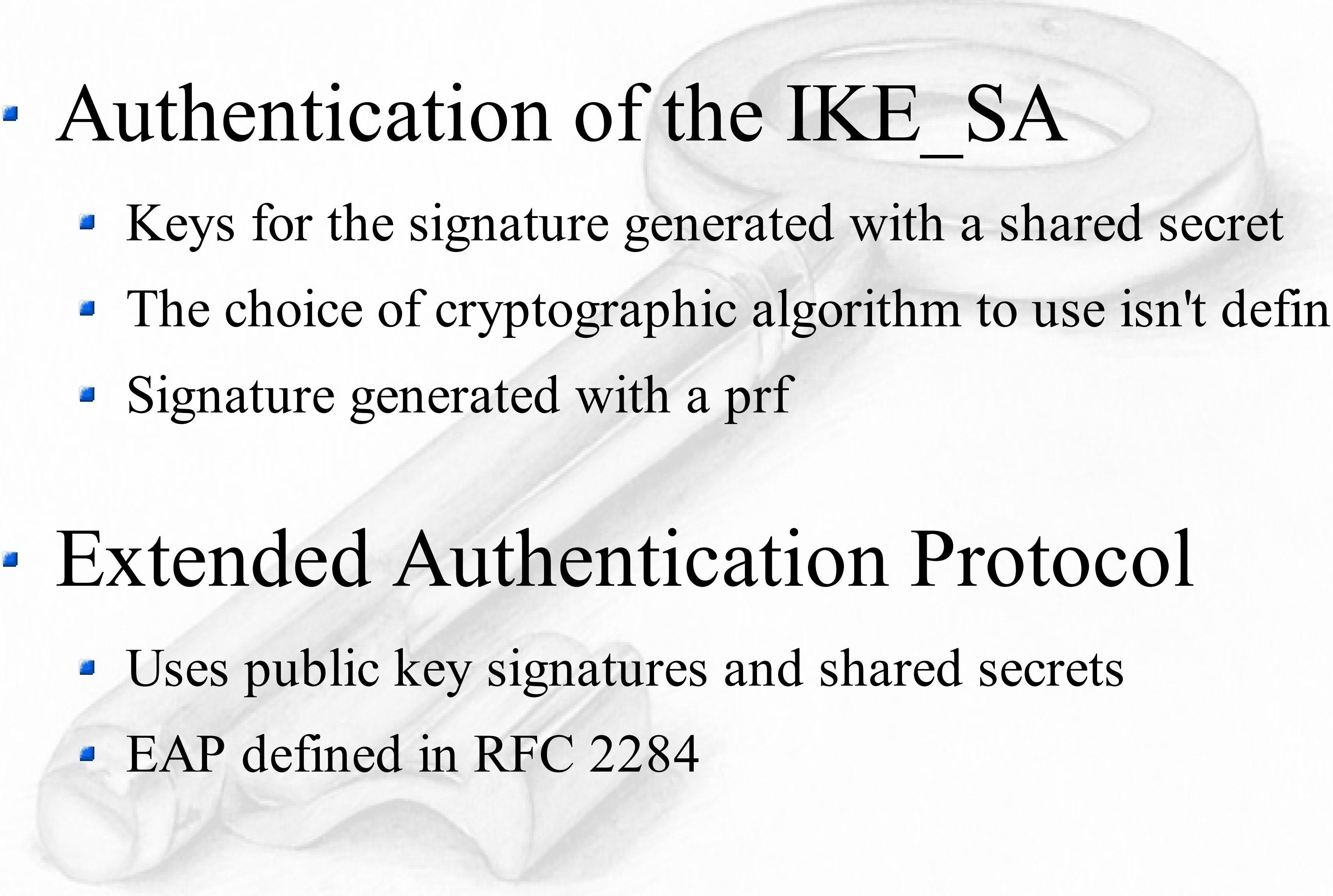


- Rekeying
  - One Key used only for a limit amount of time or data
  - To decrease the risk of a hacked key
- Traffic Selector Notification
  - Each SA has a entry at the SPD
  - SPD contain Secure Policies for IPsec
  - TS Payloads used to update and syncronise SPD

IKEv2 Details and Variations

- Nonces
  - Random value
  - Used as inputs to cryptographic functions
- Handling of Keys
  - Delete all Secrets after closing an SA
  - Don't reuse Diffie-Hellman Exponentials
  - Rules and hints for generating Key Material

IKEv2 Details and Variations



- Authentication of the IKE_SA
  - Keys for the signature generated with a shared secret
  - The choice of cryptographic algorithm to use isn't defined
  - Signature generated with a prf

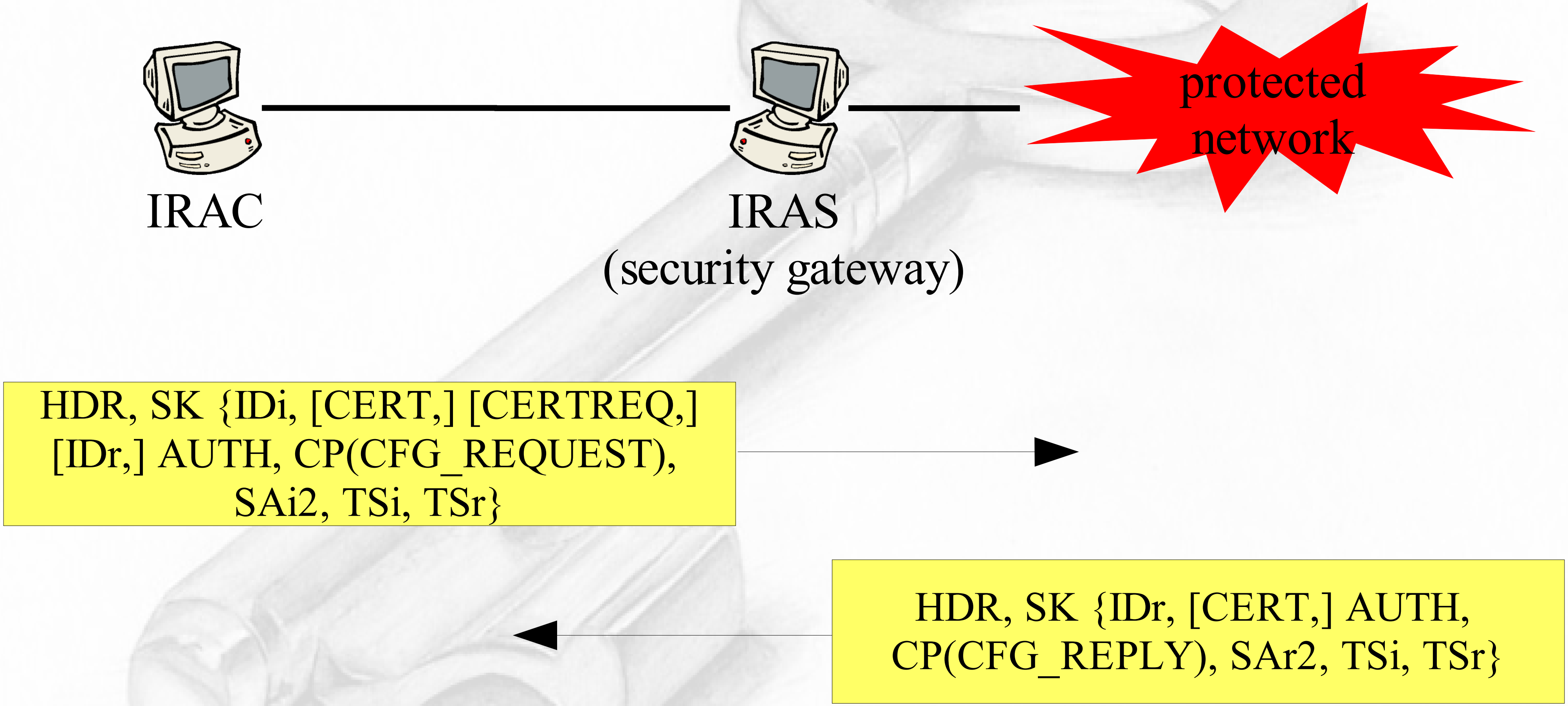
- Extended Authentication Protocol
  - Uses public key signatures and shared secrets
  - EAP defined in RFC 2284

IKEv2 Details and Variations

- Requesting an internal address on a Remote network
  - To provide an endpoint an IP address in a network protected by the security gateway
  - IP address of the IRAC getting changed
  - Result: Tunnel into the protected network

IKEv2 Details and Variations

- Example



IRAC

IRAS
(security gateway)

protected network

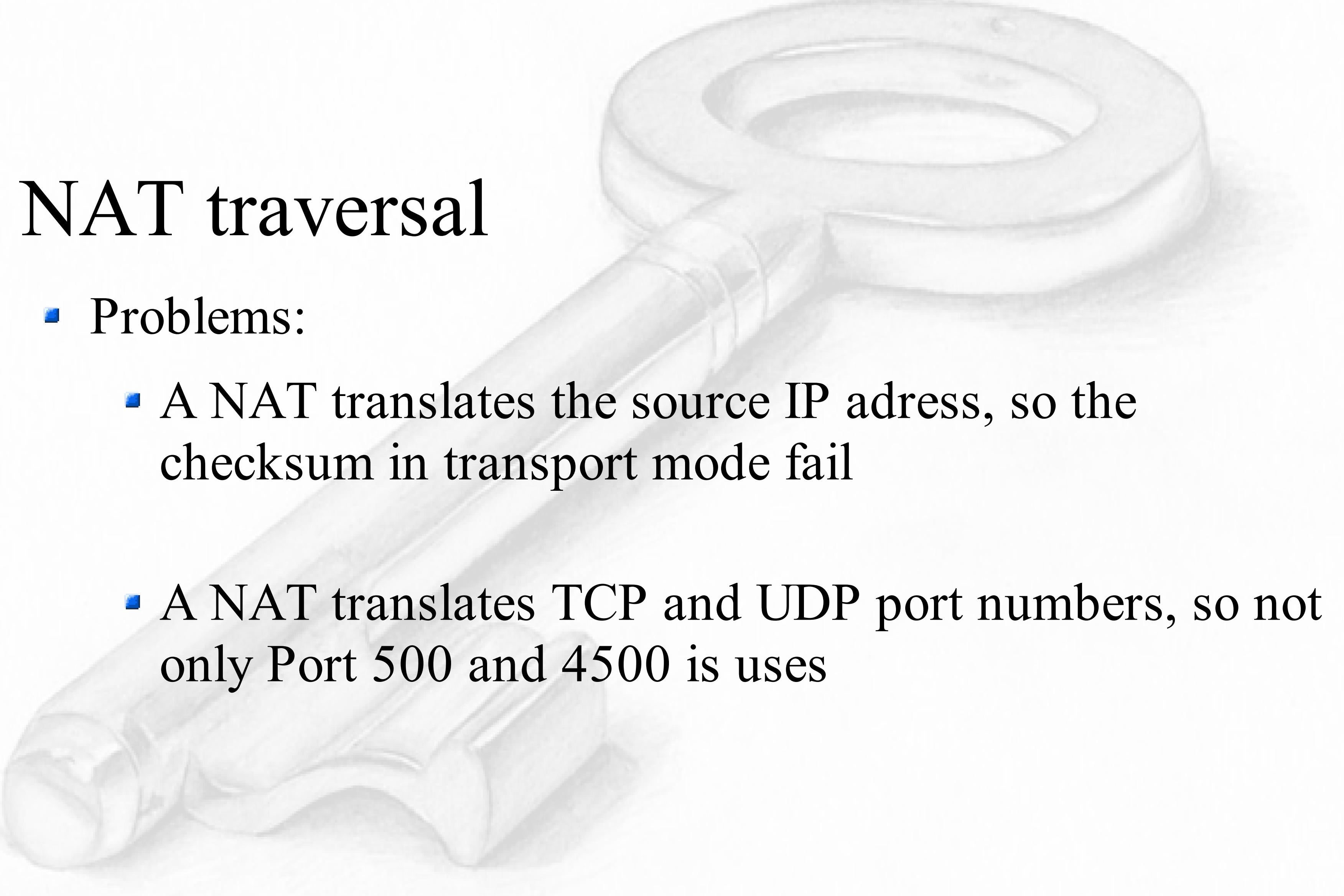
HDR, SK {IDi, [CERT,] [CERTREQ,] [IDr,] AUTH, CP(CFG_REQUEST), SAi2, TSi, TSr}

HDR, SK {IDr, [CERT,] AUTH, CP(CFG_REPLY), SAr2, TSi, TSr}

IKEv2 Details and Variations

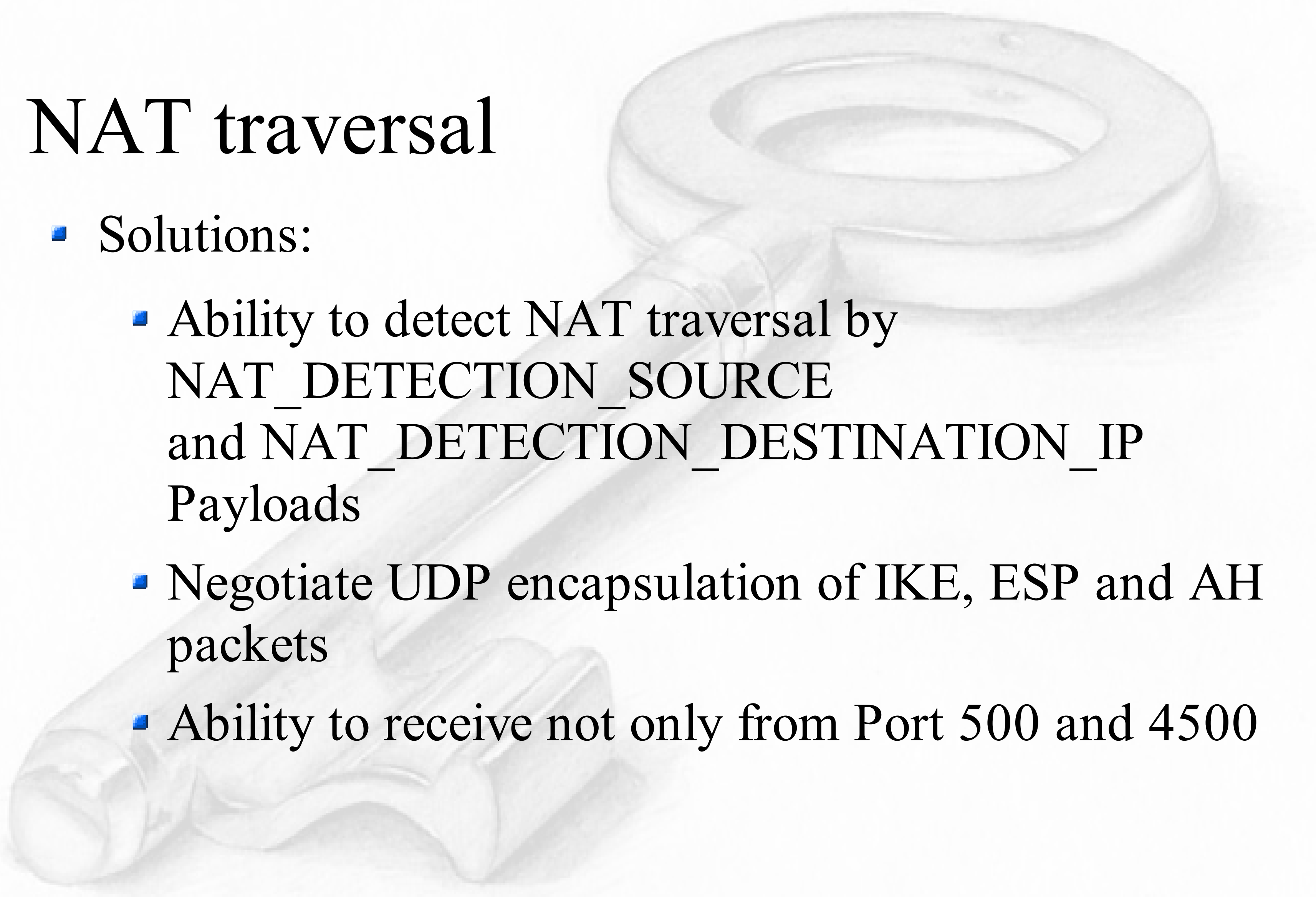
- Error handling
  - Errors without cryptographic protection are only hints that there might be problems
  - Such messages MUST be handled with care
  - A node MUST limit the rate of sending responses to unprotected messages

IKEv2 Details and Variations



- NAT traversal
  - Problems:
    - A NAT translates the source IP adress, so the checksum in transport mode fail
    - A NAT translates TCP and UDP port numbers, so not only Port 500 and 4500 is uses

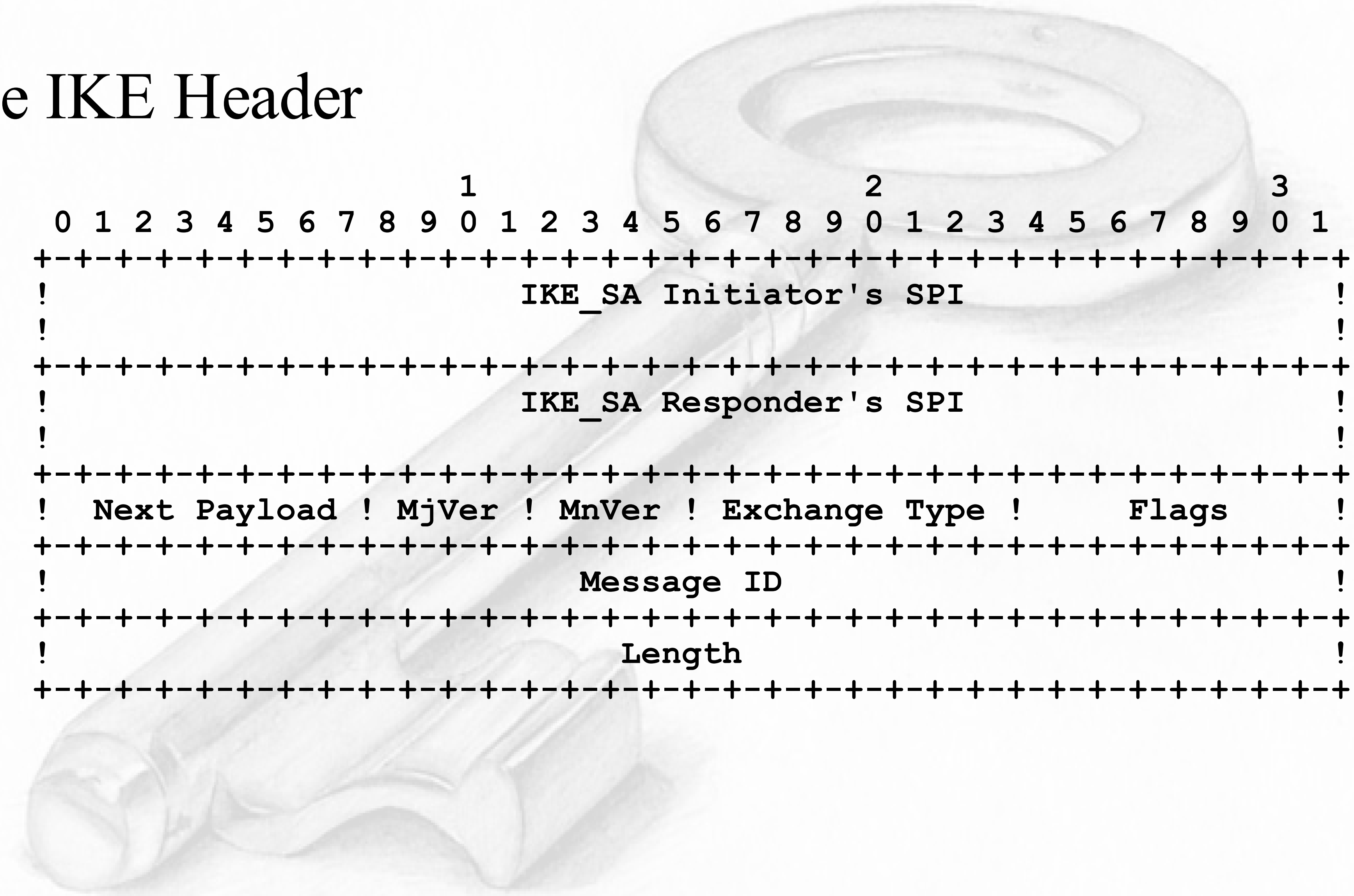
IKEv2 Details and Variations



- NAT traversal
  - Solutions:
    - Ability to detect NAT traversal by NAT_DETECTION_SOURCE and NAT_DETECTION_DESTINATION_IP Payloads
    - Negotiate UDP encapsulation of IKE, ESP and AH packets
    - Ability to receive not only from Port 500 and 4500

IKEv2 Headers

The IKE Header

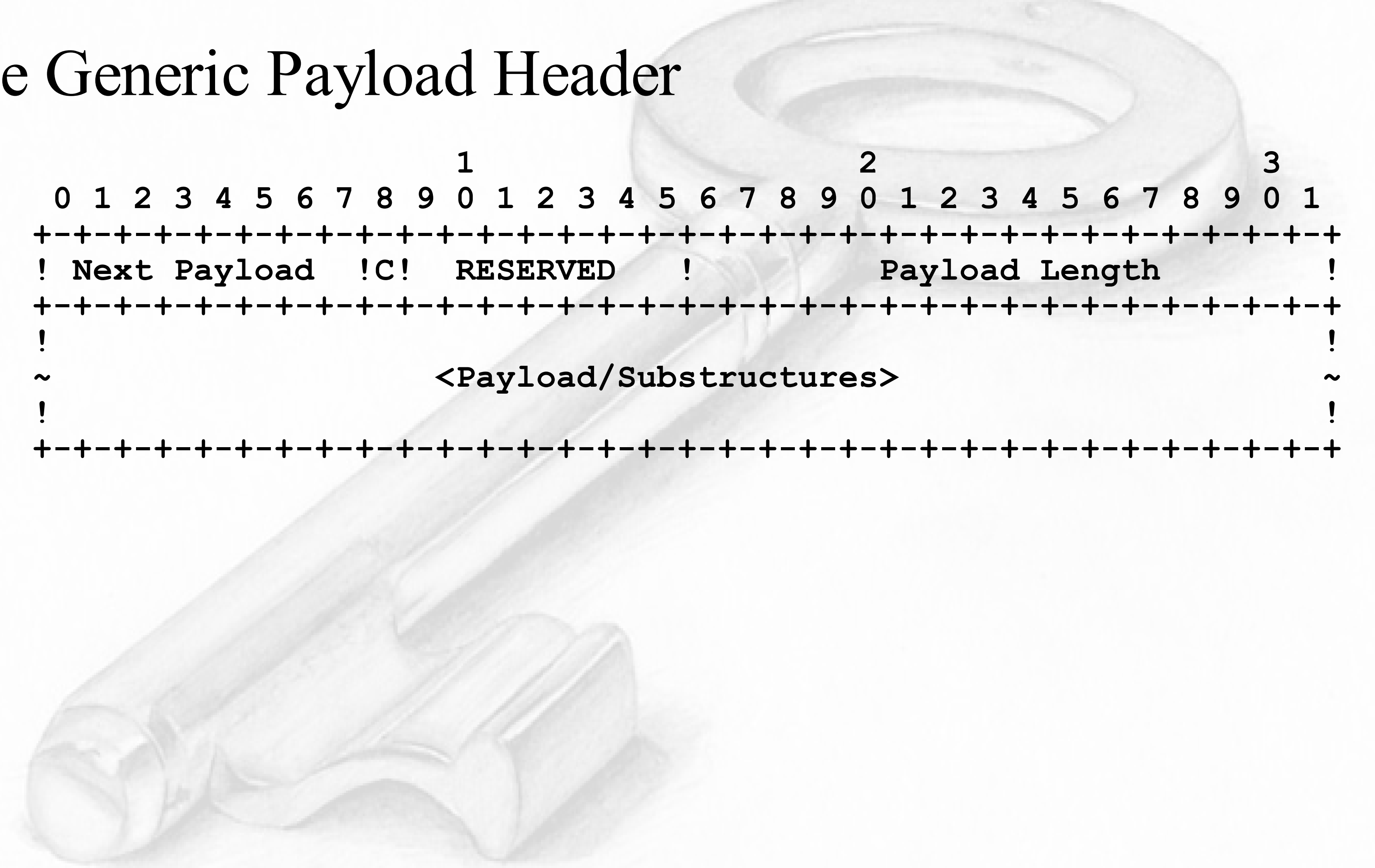


```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
!                       IKE_SA Initiator's SPI                  !
!                                                               !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
!                       IKE_SA Responder's SPI                  !
!                                                               !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
!  Next Payload ! MjVer ! MnVer ! Exchange Type !     Flags     !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
!                          Message ID                           !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
!                            Length                             !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

IKEv2 Headers

The Generic Payload Header

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
! Next Payload  !C!  RESERVED   !         Payload Length        !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
!                                                               !
~                   <Payload/Substructures>                     ~
!                                                               !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```



Thanks for listening!

Questions?