Authentication: Part 6

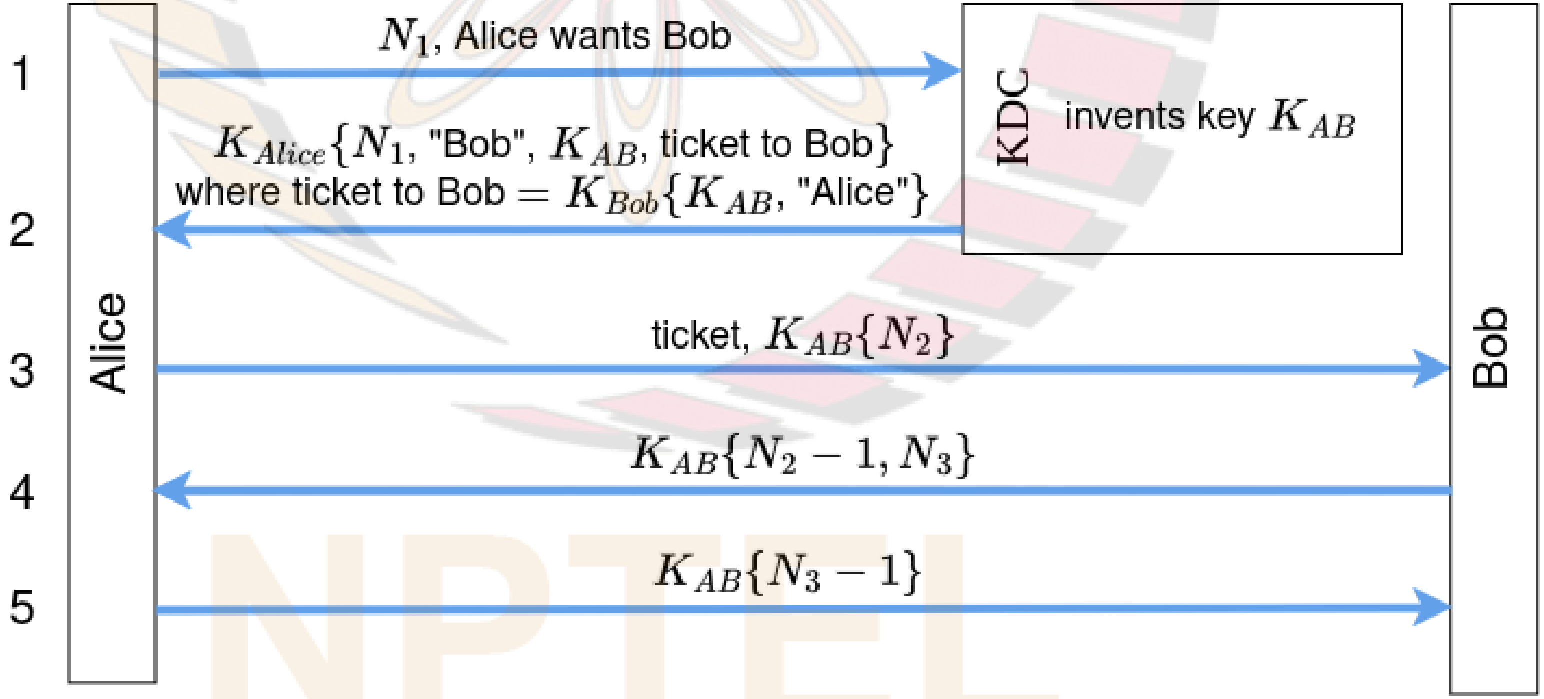
Gaurav S. Kasbekar
Dept. of Electrical Engineering
IIT Bombay

References

- J. Kurose, K. Ross, "*Computer Networking: A Top Down Approach*", Sixth Edition, Pearson Education, 2013
- C. Kaufman, R. Perlman, M. Speciner, "*Network Security: Private Communication in a Public World*", Pearson Education, 2nd edition, 2002

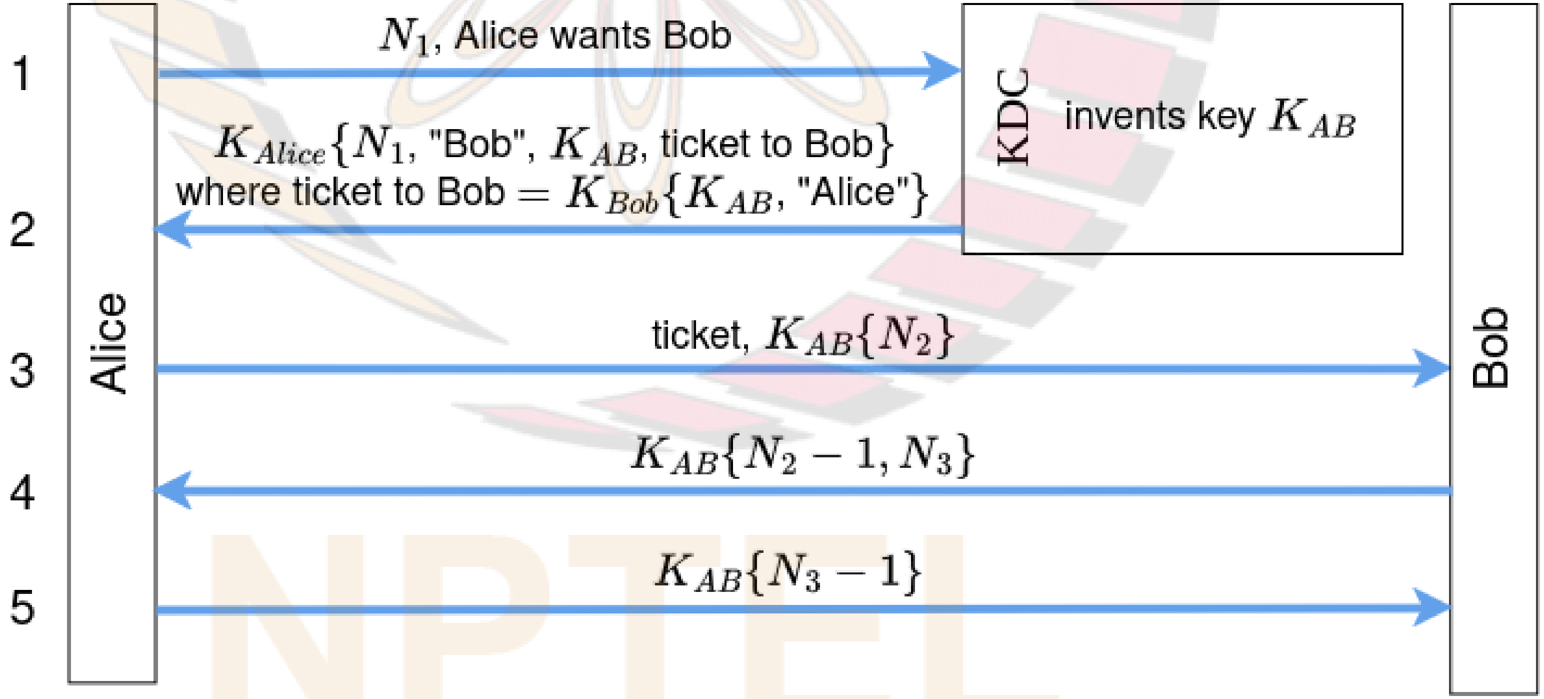
Needham-Schroeder Protocol

- Protocol shown in fig.
  - ❑ N_1, N_2 and N_3 are nonces
- Nonce N_1 is used to protect against foll. threat:
  - ❑ Trudy stole an old key ($K_{Bob,old}$) of Bob, after which Bob changed his key to K_{Bob}; also, she recorded msg. 2 when Alice earlier contacted KDC for getting shared key with Bob
  - ❑ Then Trudy waited for Alice to contact KDC; Trudy replayed recorded msg. 2 and then impersonated herself as Bob to Alice



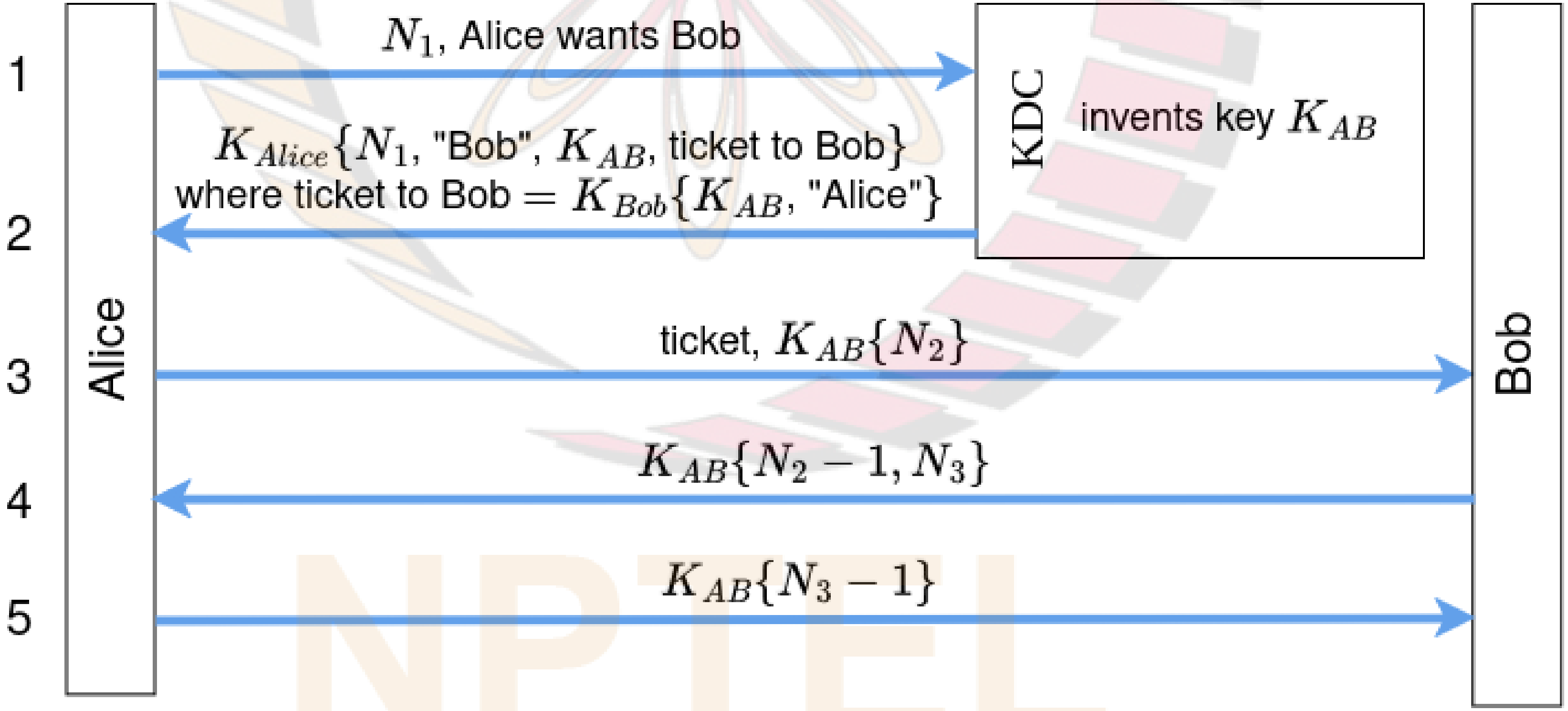
Needham-Schroeder Protocol (contd.)

- String “Bob” is included in msg. 2 to protect against following threat:
  - ❑ Trudy modifies “Bob” to “Trudy” in msg. 1
  - ❑ Then Trudy tricks Alice into talking to herself and thinking that she is talking to Bob
- **Note**:
  - ❑ Needham-Schroeder protocol has been criticized for unnecessarily doubly encrypting the ticket to Bob
  - ❑ no loss in security if ticket to Bob sent from KDC to Alice without encrypting with K_{Alice}



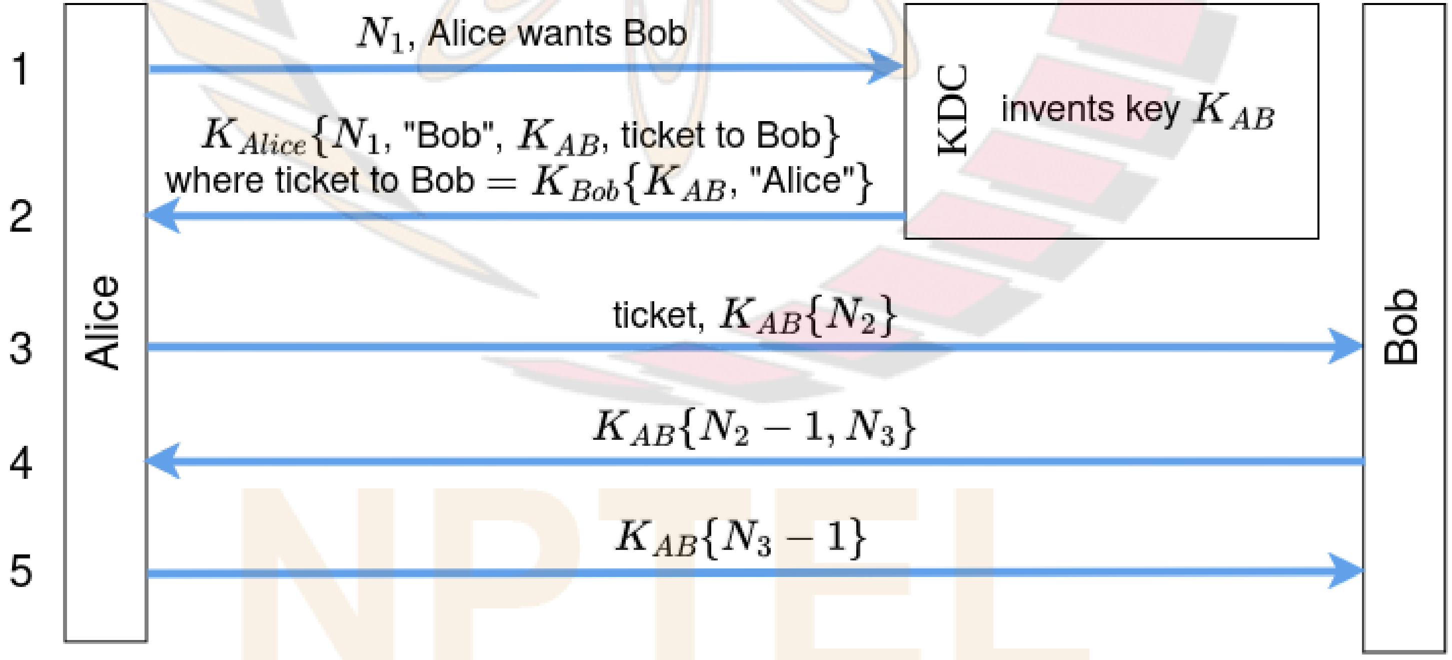
Needham-Schroeder Protocol (contd.)

- In msg. 3, Alice sends a challenge ($K_{AB}(N_2)$) to Bob
  - ❑ Bob responds to challenge by sending $K_{AB}(N_2 - 1)$ in msg. 4, which proves that he knows K_{AB}
- In msg. 4, Bob also sends a challenge ($K_{AB}(N_3)$) to Alice
  - ❑ Alice responds to challenge by sending $K_{AB}(N_3 - 1)$ in msg. 5 ,which proves that she knows K_{AB}
- Note: in above protocols, response to challenge $K_{AB}(N)$ is $K_{AB}(N - 1)$; alternatively, response could have been N



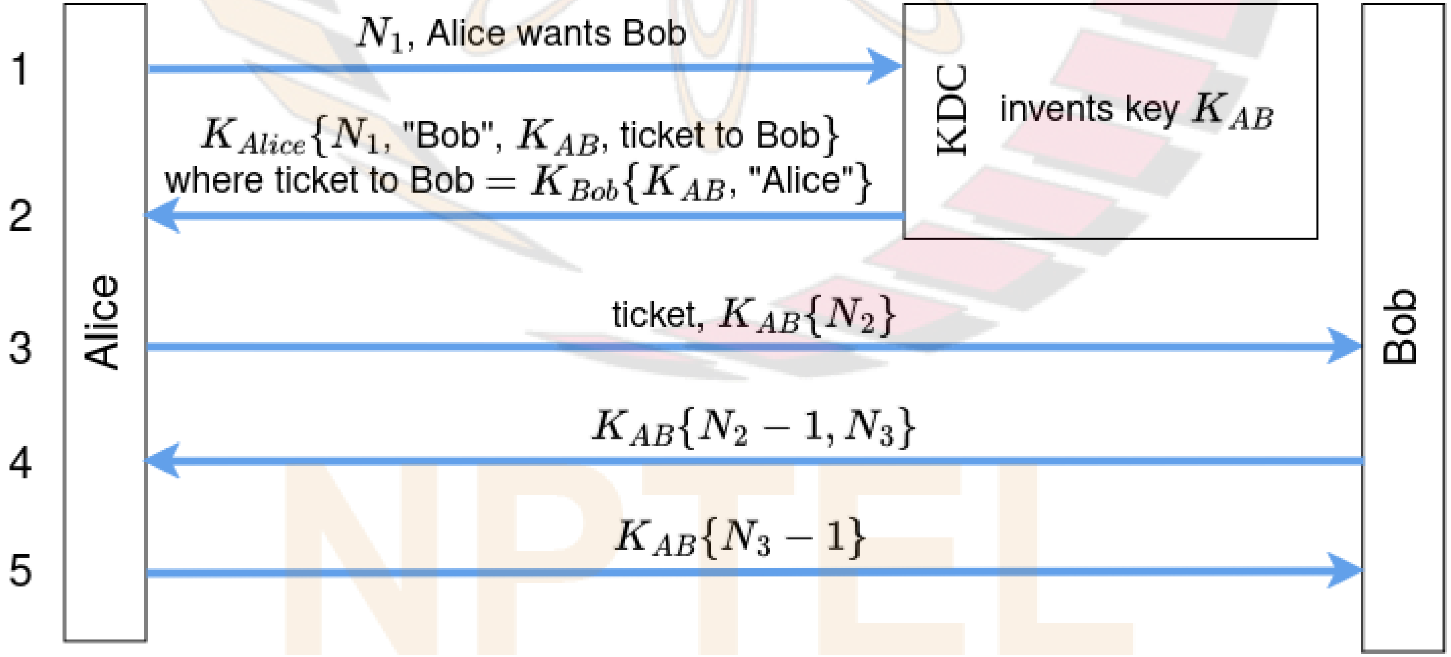
Needham-Schroeder Protocol (contd.)

- Suppose a block cipher with Electronic Code Book (ECB) is used to send msg. 4 such that it is of the following form: $K_{AB}(N_2 - 1), K_{AB}(N_3)$
- An intruder, Trudy, can launch following attack:
  - ❑ First, she eavesdrops on authentication exchange between Alice and Bob shown in fig., and records msg. 3
  - ❑ Later, she sends the recorded msg. 3 to Bob
  - ❑ Bob responds with $K_{AB}(N_2 - 1), K_{AB}(N_4)$, where $N_4 \neq N_3$
  - ❑ Trudy cannot compute $K_{AB}(N_4 - 1)$; instead, she opens a new connection to Bob and sends $K_{AB}(N_4)$
  - ❑ Bob responds with $K_{AB}(N_4 - 1), K_{AB}(N_5)$
  - ❑ Trudy then uses $K_{AB}(N_4 - 1)$ to complete the first authentication exchange
  - ❑ Note that the above attack is an instance of the "*reflection attack*"
- Defence against above attack:
  - ❑ In msg. 4, encryption should be done in such a way that $K_{AB}(N_2 - 1)$ cannot be deduced from $K_{AB}(N_2 - 1, N_3)$ if K_{AB} unknown



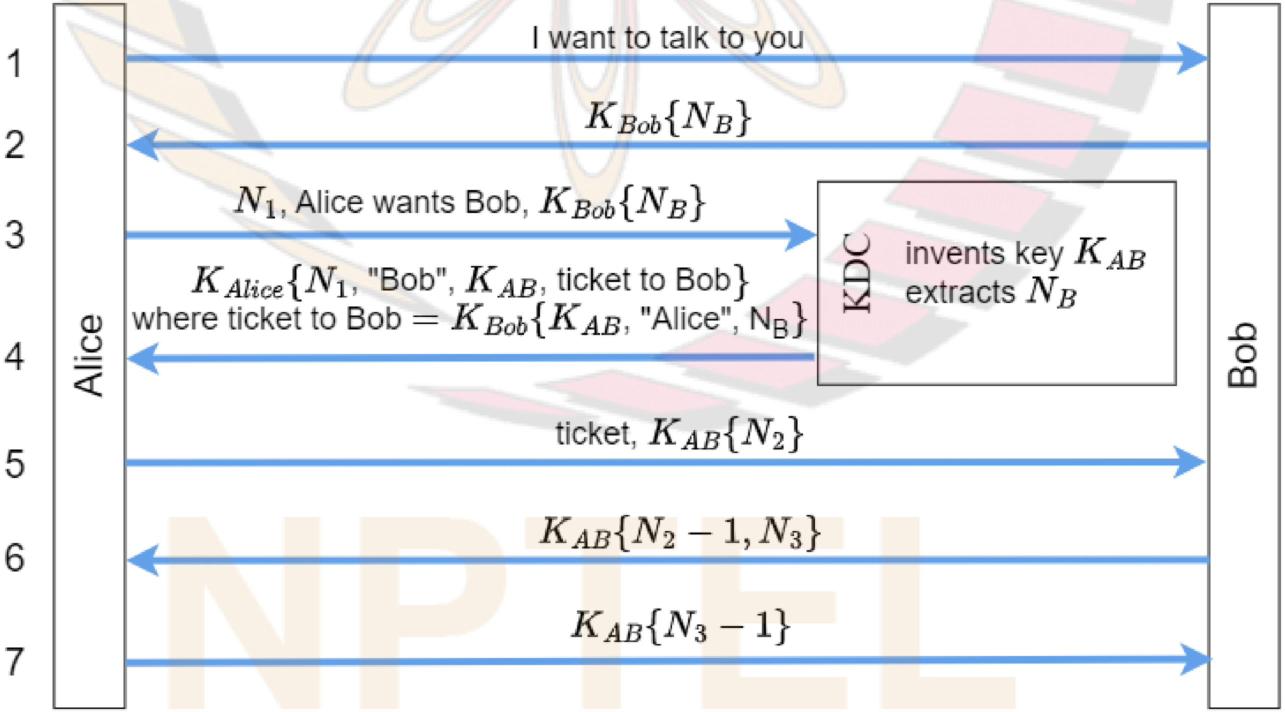
Needham-Schroeder Protocol (contd.)

- There is the foll. vulnerability in the Needham-Schroeder protocol shown in fig.
- Suppose initially, Alice's key is J_{Alice}; also, when Alice contacts KDC for a ticket to talk to Bob, an intruder, Trudy, records msgs. 1 and 2 of the exchange; also, in msg. 2, J_{AB} was the shared key generated by KDC
- Later, Trudy finds out J_{Alice} and uses it to find J_{AB}; Alice suspects that her key has been stolen and changes her key to K_{Alice}
- However, even after Alice changes her key, Trudy can still use J_{AB} and the old ticket $K_{Bob}(J_{AB}, \text{"Alice"})$ to impersonate herself as Alice to Bob
- To defend against this vulnerability:
  - ❑ two additional messages used at the beginning of the protocol, in which Alice asks for a nonce from Bob and Bob sends a nonce to Alice
  - ❑ resulting protocol called "*Expanded Needham-Schroeder Protocol*"



Expanded Needham-Schroeder Protocol

- In msg. 2, Bob sends $K_{Bob}(N_B)$, where N_B is nonce generated by Bob
- KDC includes N_B in the ticket to Bob
- Vulnerability described on previous slide is fixed because:
  - ❑ old recorded exchanges of Alice with KDC will not enable Trudy to authenticate as Alice to Bob since nonce in old ticket will not match new nonce sent by Bob
  - ❑ also, after Alice changes her key to K_{Alice}, KDC knows that her key is now K_{Alice}; so Trudy will not be able to talk to KDC using old key J_{Alice}


Alice
Bob
KDC
1
I want to talk to you
2
$K_{Bob}\{N_B\}$
3
N_1, Alice wants Bob, $K_{Bob}\{N_B\}$
invents key K_{AB}
extracts N_B
4
$K_{Alice}\{N_1$, "Bob", K_{AB}, ticket to Bob$\}$
where ticket to Bob = $K_{Bob}\{K_{AB}$, "Alice", $N_B\}$
5
ticket, $K_{AB}\{N_2\}$
6
$K_{AB}\{N_2 - 1, N_3\}$
7
$K_{AB}\{N_3 - 1\}$