Ad-Hoc Security Associations for Groups

Jukka Valkonen[1], **N. Asokan**[1,2], **Kaisa Nyberg**[1,2]

[1]**Helsinki University of Technology and** [2]**Nokia Research Center**

jukka.valkonen@tkk.fi, n.asokan@tkk.fi, kaisa.nyberg@tkk.fi

21.9.2006

Outline

1. Motivation for group associations
2. Two authentication protocols
   - Protocols to authenticate some data, for example a shared secret negotiated between the devices
3. User actions needed to form a group
4. Conclusions

Background

- Ad-Hoc authentication and key exchange between two devices
- Numeric comparison
  - Devices derive a short string of l digits from negotiated material
  - The short string is verified by the users
  - Security depends on the length l
  - Bluetooth, Wireless USB
- Passkey-based
  - Devices share a secret passkey P which is used in the authentication
  - Security depends on the length of P
  - Bluetooth, Microsoft Connect Now-NET

Motivation for Group Associations (1/2)

- Ad-hoc networks
  - Business scenarios
  - Home scenarios
- Goal: to share one authenticated key among a group of devices
  - The key is negotiated using, for example, Diffie-Hellman key exchange for groups
  - This key shall be authenticated
- The devices have no prior information of other devices
- One time passkeys or verification of a one-time string
  - No need to memorize passkeys

Motivation for Group Associations (2/2)

- Straightforward solution: Each device pairs with a master device selected by the users. This master then transmits the shared key to other devices.
  - $n-1$ authentications
  - Cumbersome and insecure as the size of the group grows
- If pairwise associations are used, the probability of a successful attack increases as the size n of the group grows:

$l \backslash n$	5	10	15	20
2	3.9	8.6	13.1	17.3
4	0.03	0.08	0.1	0.2
6	$3.9 \cdot 10^{-4}$	$8.9 \cdot 10^{-4}$	0.0014	0.0019

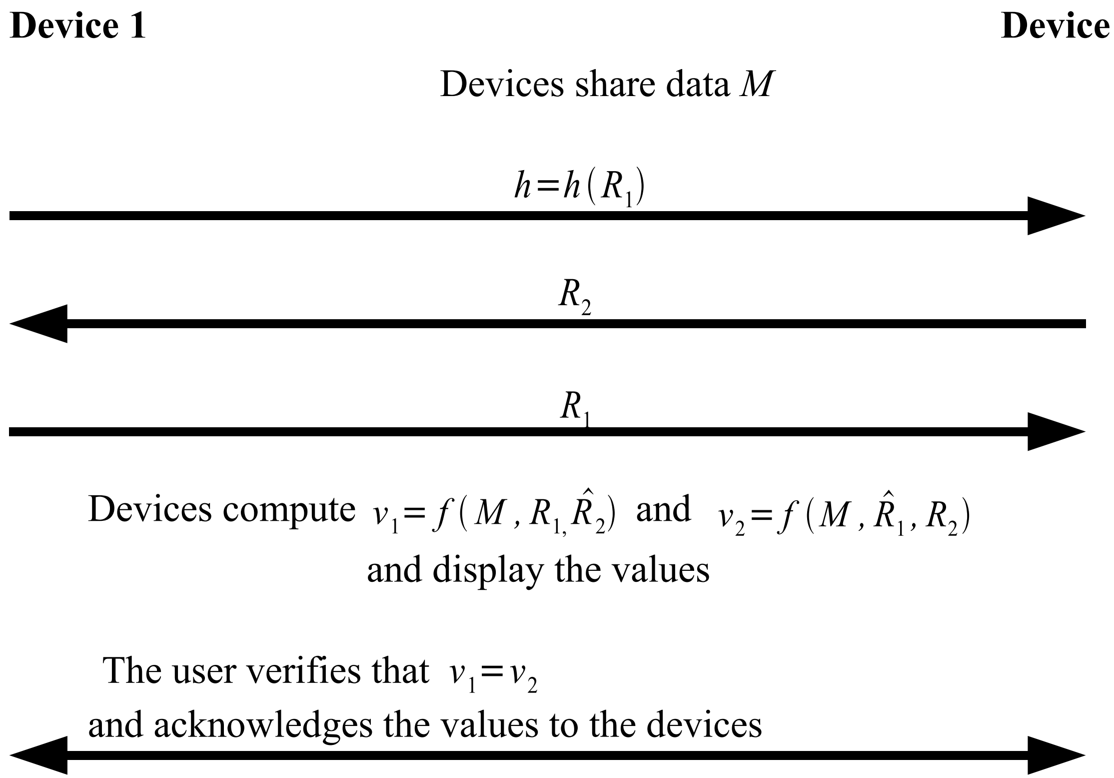
Table 1: Probability for a successful attack in percent

Related Work on Group Associations

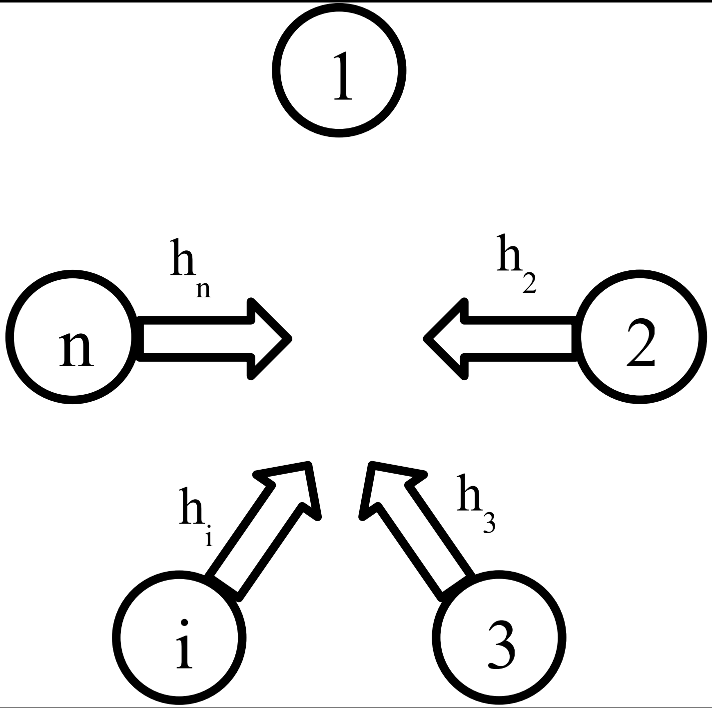
- N. Asokan and P. Ginzboorg, (2000)
- S.-M. Lee, J. Y. Hwang and D. H. Lee, (2004)
- R. Dutta and R. Barua, (2006)
- M. Abdalla et. al. (2006)
- Common with all these protocols: Authentication is based on a shared passkey

MANA IV

- Three-round mutual authentication protocol by Laur, Asokan and Nyberg (2005) using numeric comparison for two devices
  - Security proof given in standard model

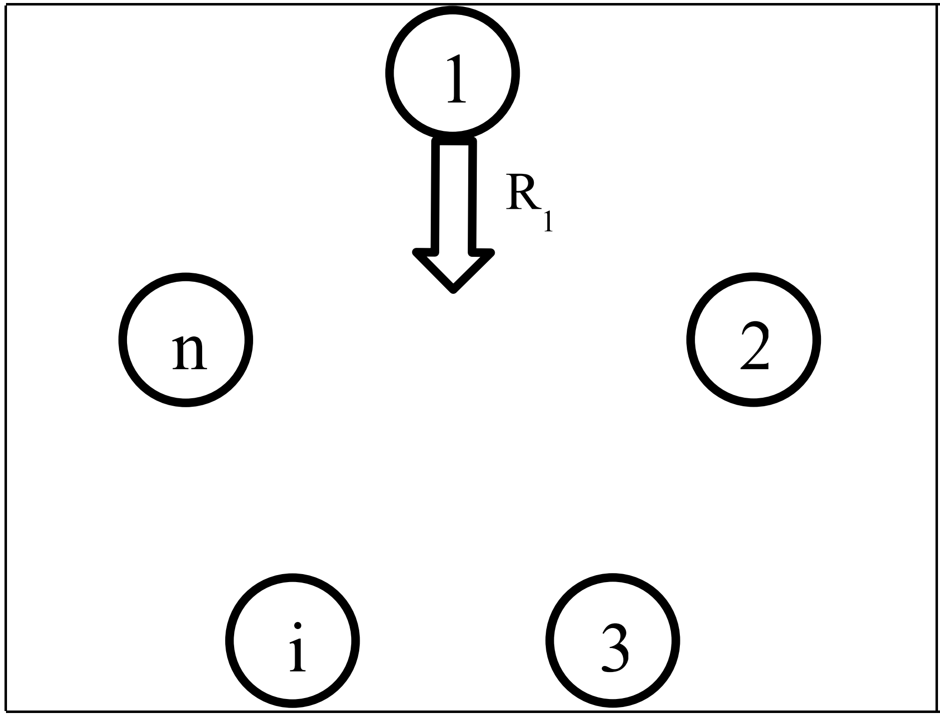


Group Numeric Comparison Protocol (1/5)



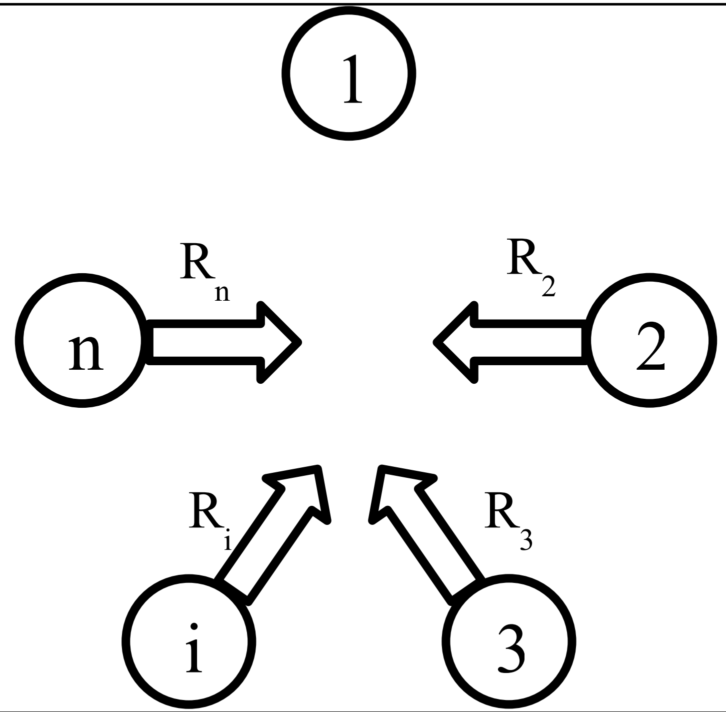
- The devices share data M
- D$_i$, $i = 2, \ldots, n$, generates a fresh long random number R_i, computes $h_i = h(i, R_i)$ and broadcasts the value
- $n - 1$ messages

Group Numeric Comparison Protocol (2/5)



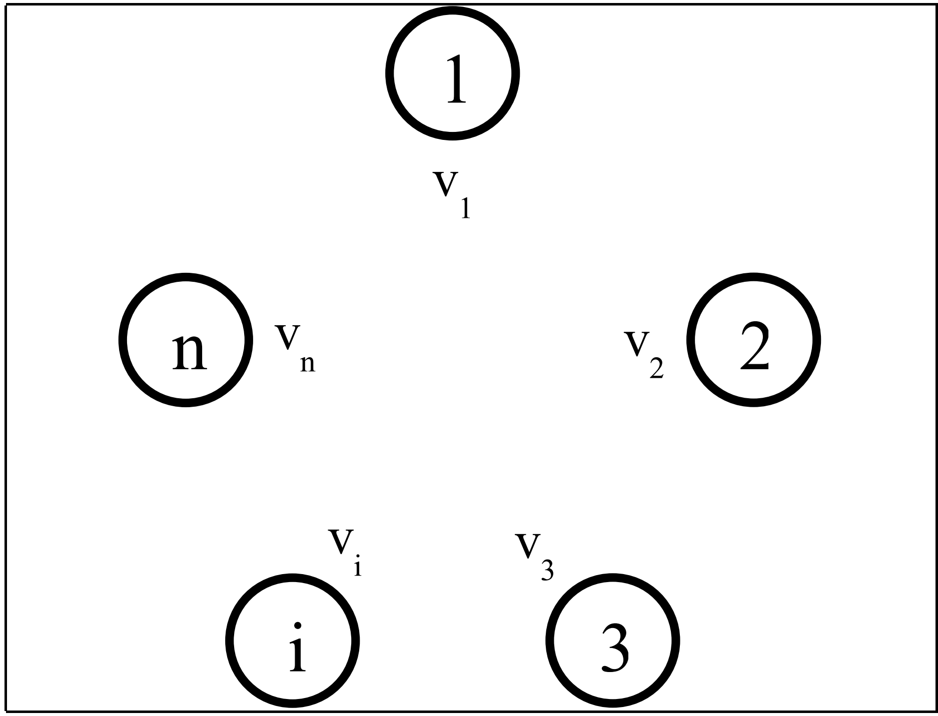
- D_1 waits until it has received $n-1$ hashes, picks a fresh random R_1 number and broadcasts it
- 1 message

Group Numeric Comparison Protocol (3/5)



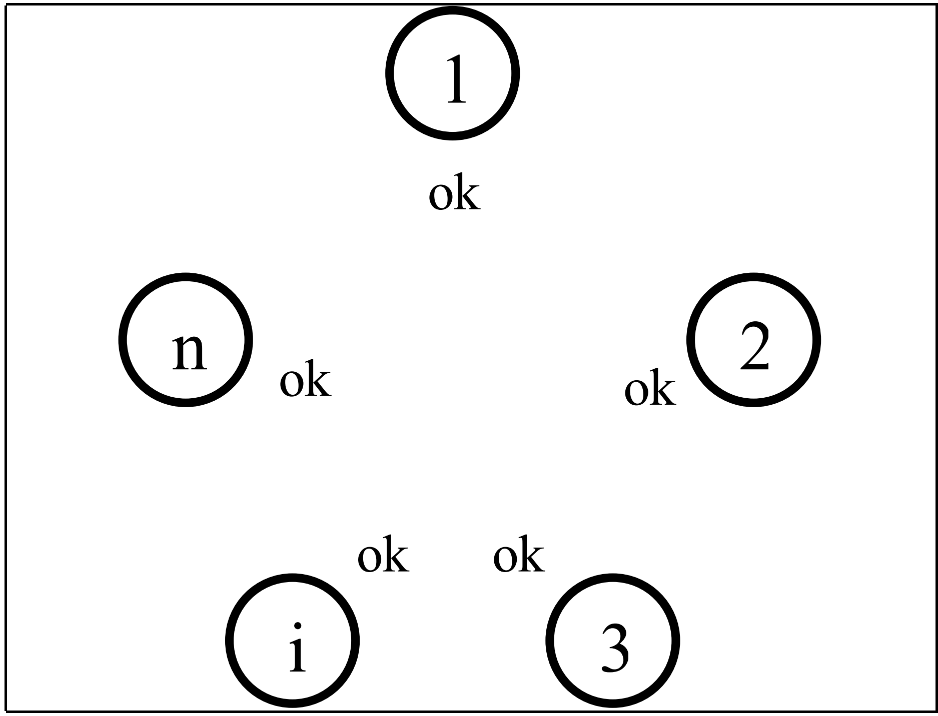
- D_i, $i = 2, \ldots, n$, waits until it receives $\hat{R}_1$ and $\hat{h}_j$ from other devices D_j, $j = 2, \ldots, n$, $i \neq j$. It then broadcasts R_i
- $n - 1$ messages

Group Numeric Comparison Protocol (4/5)



- D_i, $i = 1, \ldots, n$, waits until it receives $\hat{R}_j$ from other devices D_j, $j = 2, \ldots, n$, $i \neq j$. D_i computes $v_i = f(M, \hat{R}_1, \ldots, R_i, \ldots, \hat{R}_n)$

Group Numeric Comparison Protocol (5/5)



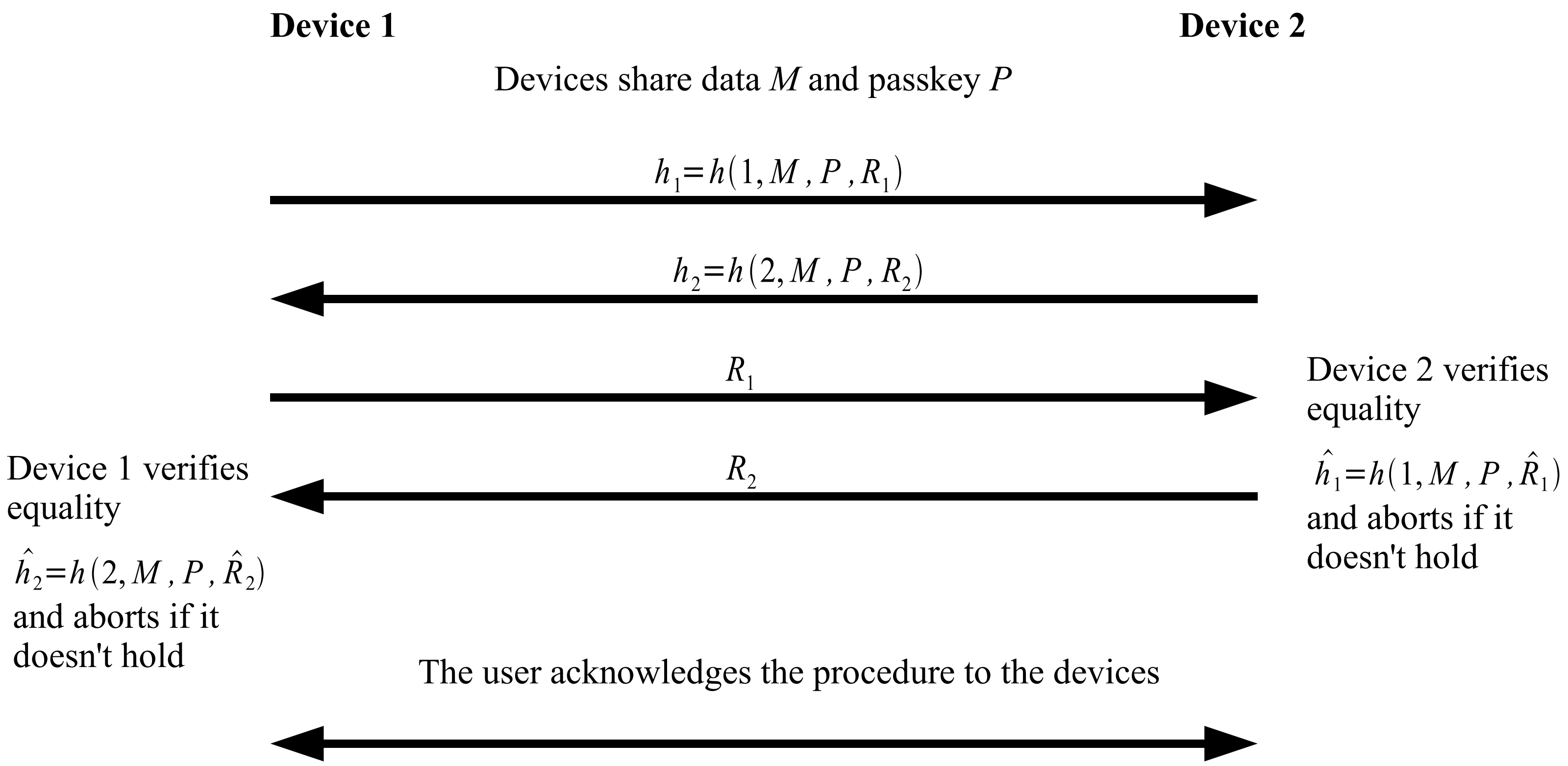
- The users acknowledge the values to the devices if and only if each device displays the same verification string
- Total $2n-1$ messages used

Group Numeric Comparison Protocol Analyzed

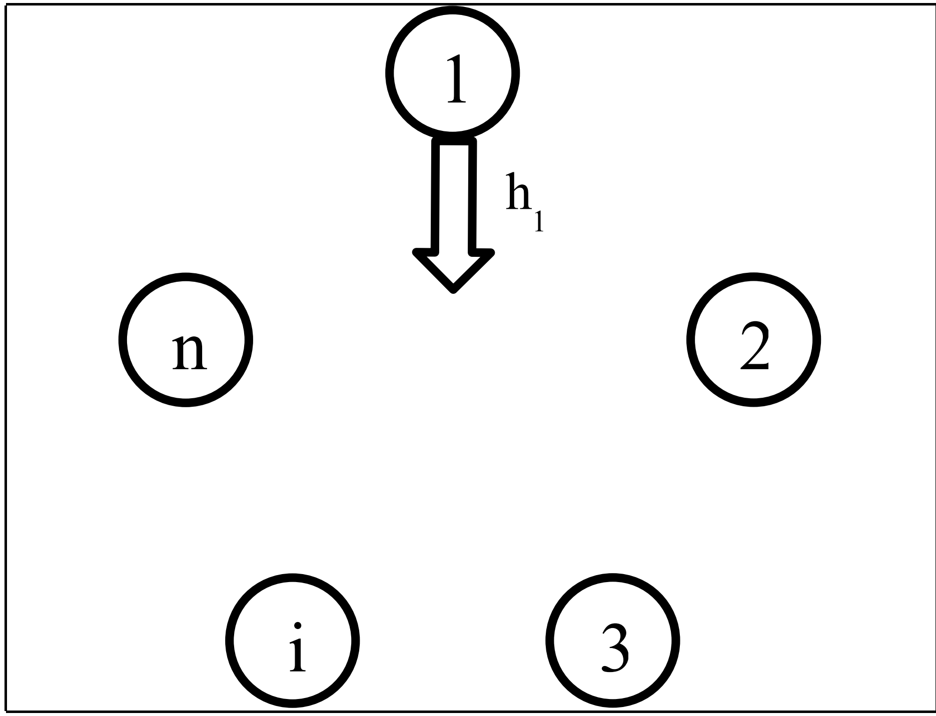
- Security properties inherited from MANA IV, which is proven secure by Laur and Nyberg (2006)
  - The probability for a successful attack is $\varepsilon = 10^{-l}$ where l is the length of the verification string in digits
  - Attacker forced to fix data before the data needed to compute the verification string becomes public.
- To achieve probability for a successful attack smaller than ε, the length of the verification string must be larger than $\log \frac{1}{\varepsilon}$, if the length is measured in digits
- NIST requires that $\varepsilon \leq \frac{1}{1000000}$, which means that $l \geq 6$

MANA III

- Passkey-based authentication method described by Gehrmann et al. (2004)

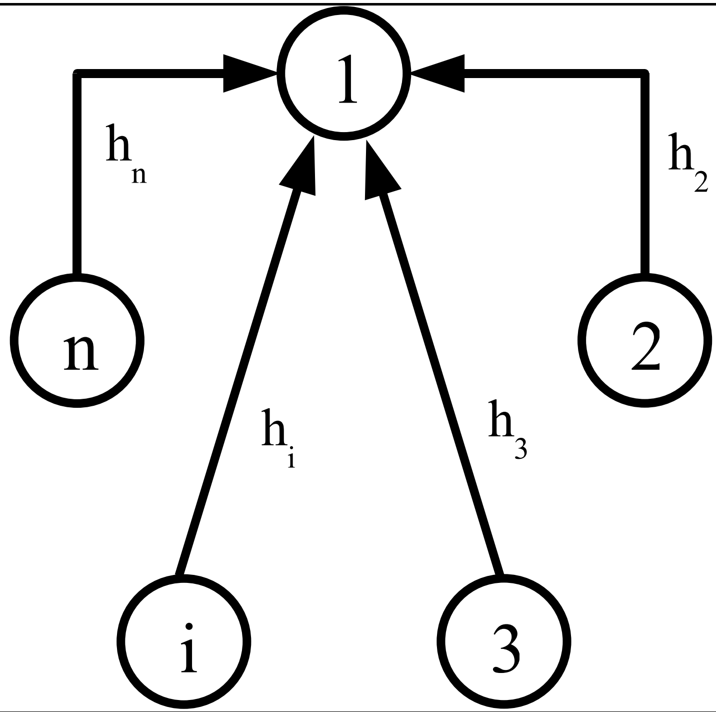


Passkey-based Verification in a Group (1/5)



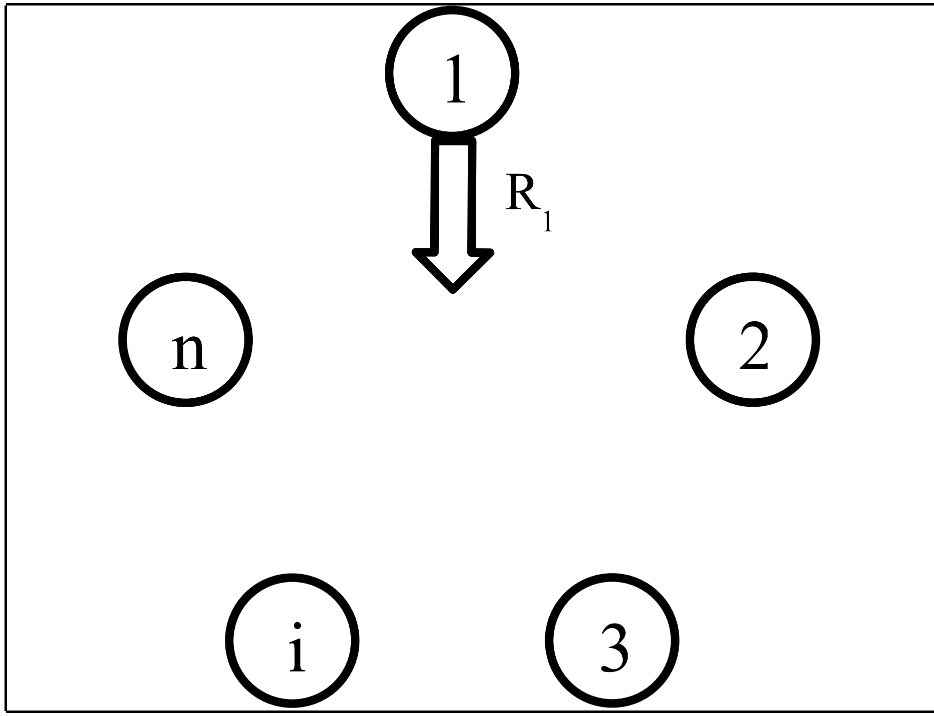
- The device share data M and passkey P
- D_1 generates random data string R_1, computes a commitment $h_1 = h(1, M, P, R_1)$ and broadcasts it
- 1 message

Passkey-based Verification in a Group (2/5)



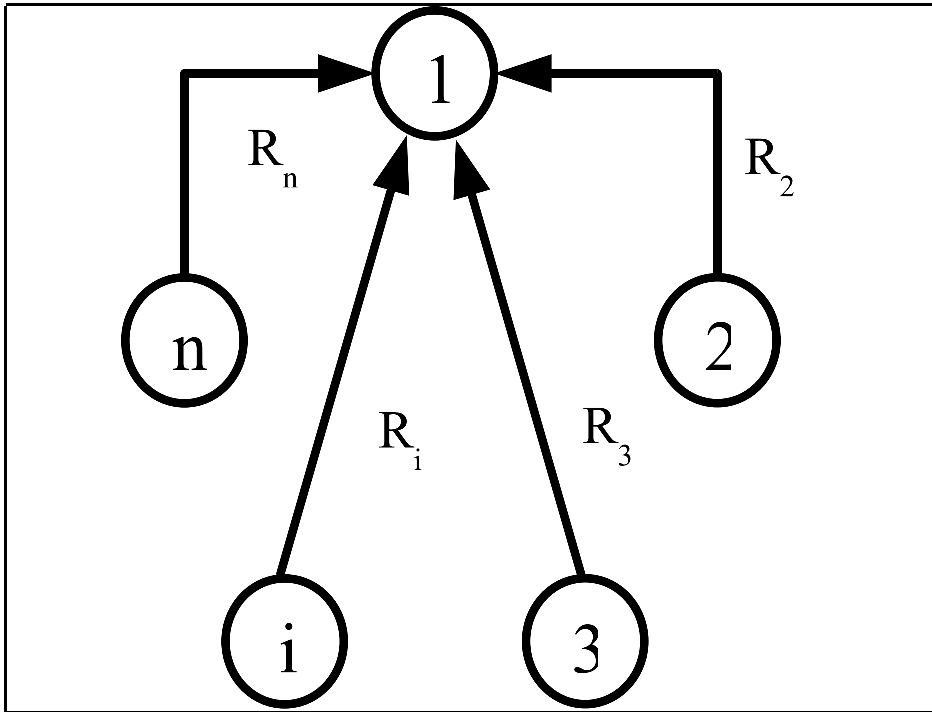
- D_i generates random data string R_i, computes a commitment $h_i = h(i, M, P, R_i)$ and sends it to D_1
- $n-1$ messages

Passkey-based Verification in a Group (3/5)



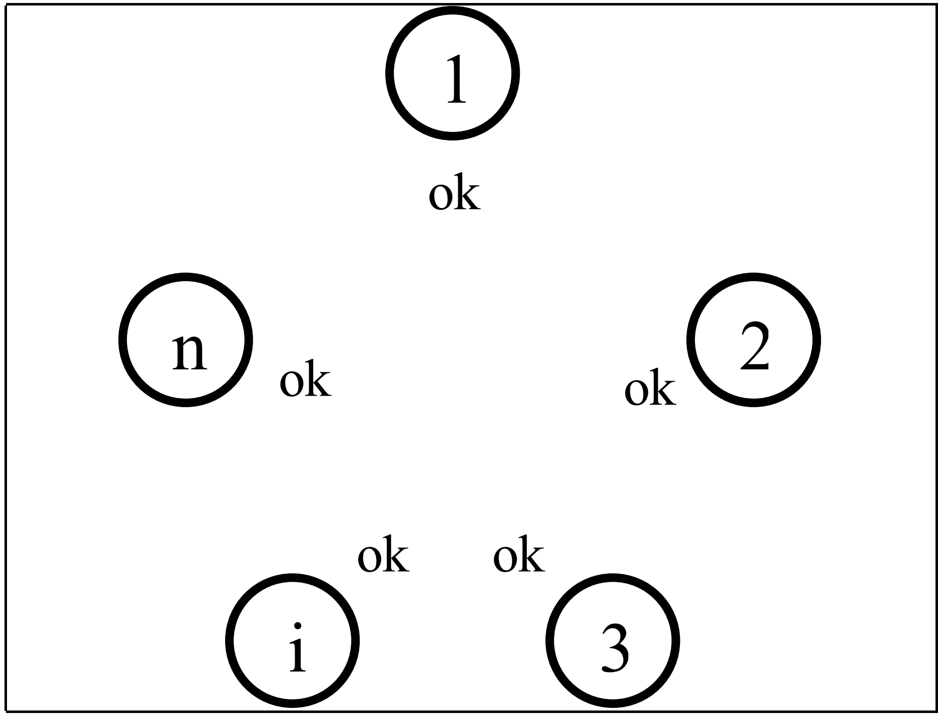
- After D_1 has received all commitments $\hat{h}_i$, it opens its commitment by broadcasting R_1.
- D_i verifies equality $\hat{h}_1 = h(1, M, P, \hat{R}_1)$ and aborts if it doesn't hold
- 1 message

Passkey-based Verification in a Group (4/5)



- D_i responds by opening its commitment by sending R_i to D_1
- D_1 verifies equality $\hat{h}_i = h(i, M, P, \hat{R}_i)$ for all $i = 2, \ldots, n$, and aborts if there is i for which it does not hold
- $n - 1$ messages

Passkey-based Verification in a Group (5/5)



- The users are prompted to acknowledge the procedure, if none of the devices aborted in the previous steps
- Total $2n$ messages used

Passkey-based Verification in a Group Analyzed

- Type in passkey and verify the process
  - Verifying can be avoided using twice as long passkey and a second run of the protocol
- Passkey is revealed to a passive attacker, and therefore cannot be used more than once
- Passkey must be held secret until the procedure is verified by the users

User Procedures

- One device must be selected as a leader
  - To act as device D_1 in the authentication protocol
- Count the number of joining devices and enter it into the devices
  - To prevent unauthorized devices from participating in the protocols
- Information about the success of the protocol must be collected by the leader and distributed to the other users

Conclusions

- Clear-cut modular security
  - (Non-authenticated) Group DH Key Agreement gives security against passive wiretapping.
  - The shared secret group DH-key is authenticated using a manual data authentication protocol.
- Implementations and user experiments currently planned

Thank You!

Questions?