

Secure Pairing with Biometrics: SAfE protocol

Ileana Buhan, Jeroen Doumen, Pieter Hartel, Raymond Veldhuis

DIES- Universiteit Twente

SAS – Universiteit Twente



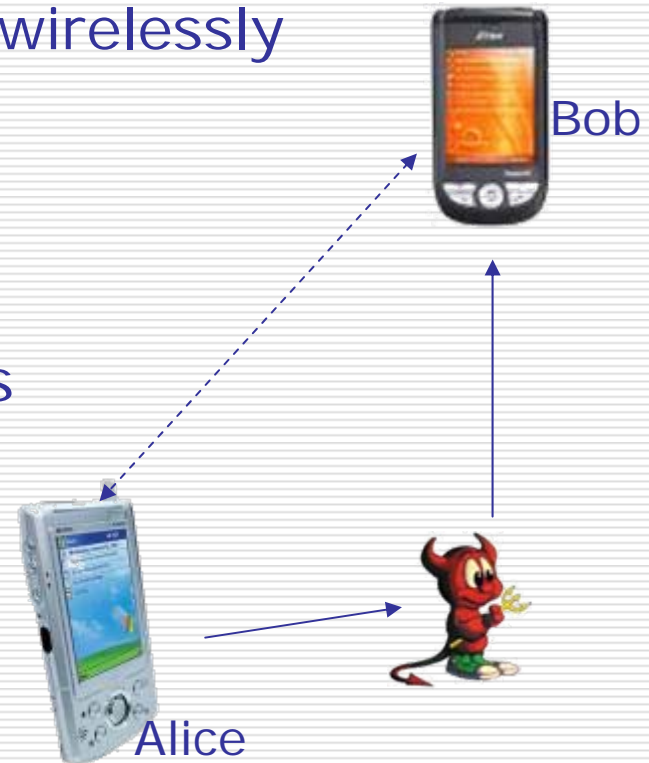
University of Twente
Enschede - The Netherlands

Problem: Secure Communication

- Alice and Bob communicate wirelessly
- Not prepared
- No shared secret
- No trusted authorities

- Alice and Bob are not experts

- Threat model:
 - Eavesdrop
 - Fabricate and modify



Our Idea

Construct the communication key between Alice and Bob using face recognition biometrics.

Why biometrics?

- Always available;
- Cannot be forgotten;
- User-friendly;
- Camera widely available;

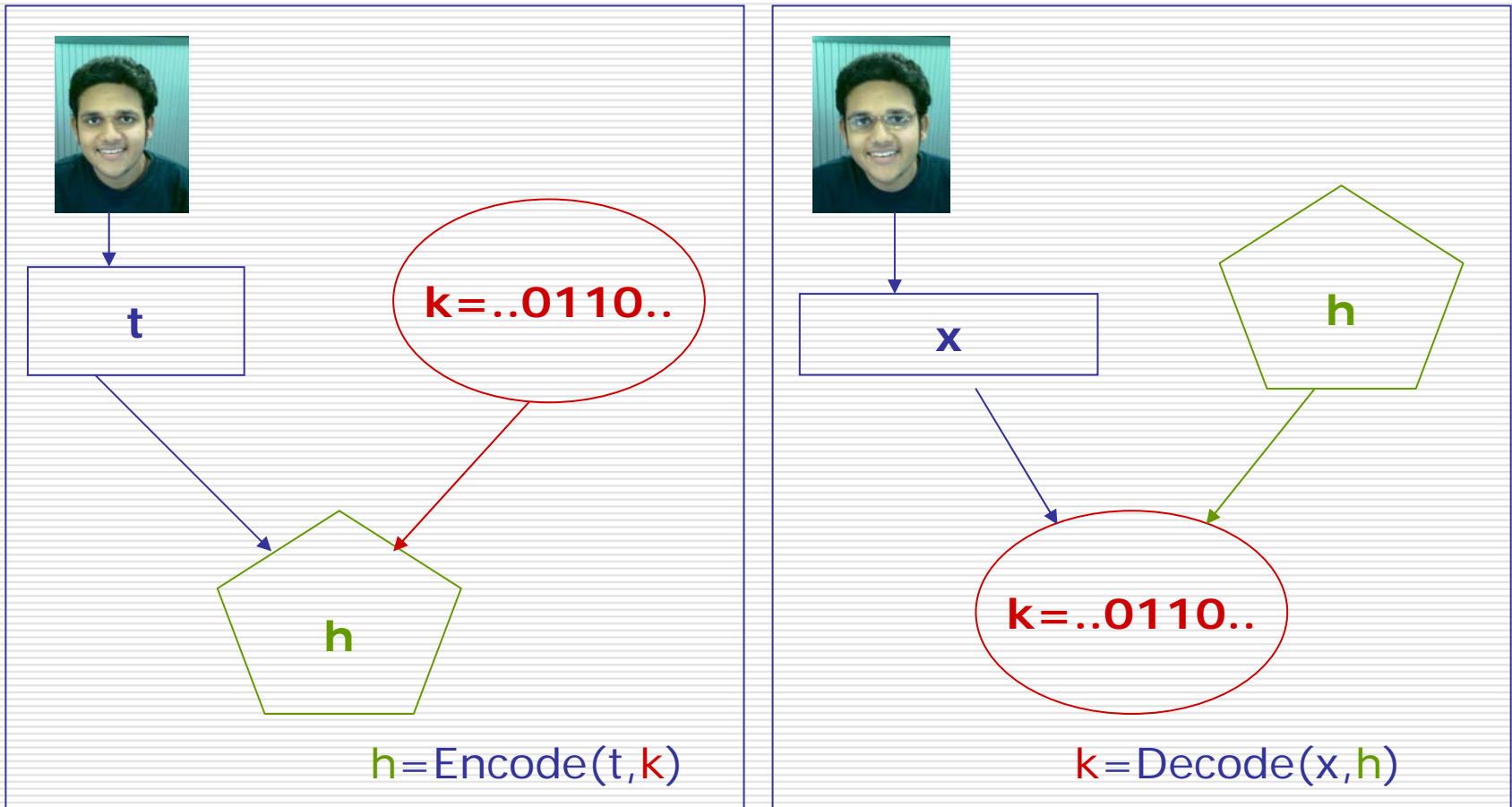
How? Stages in the SAfE protocol

1. Alice and Bob establish common source of randomness

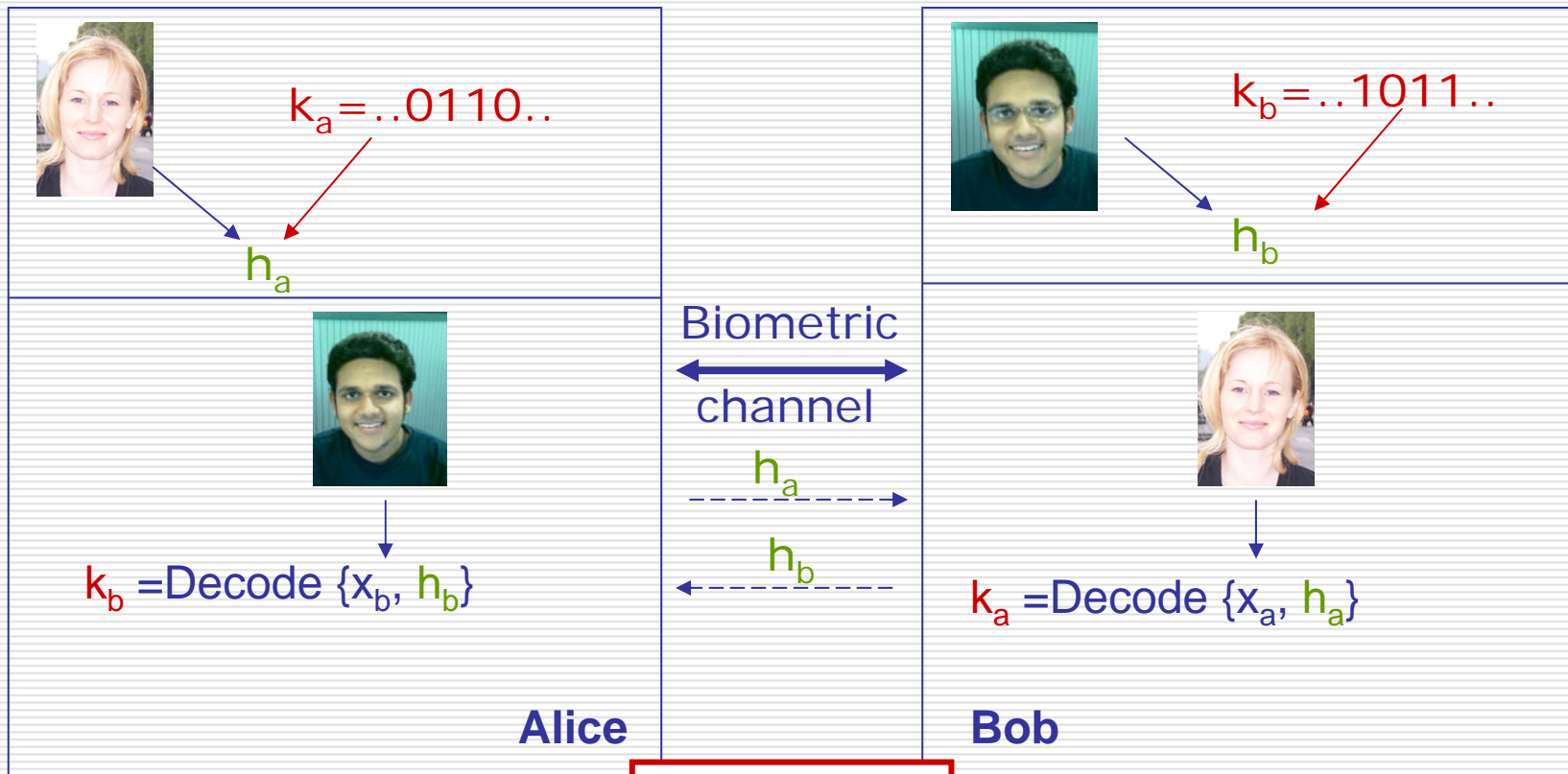


2. Devices construct communication keys
3. Communicate securely using the constructed keys

Face as keys? Hmm...

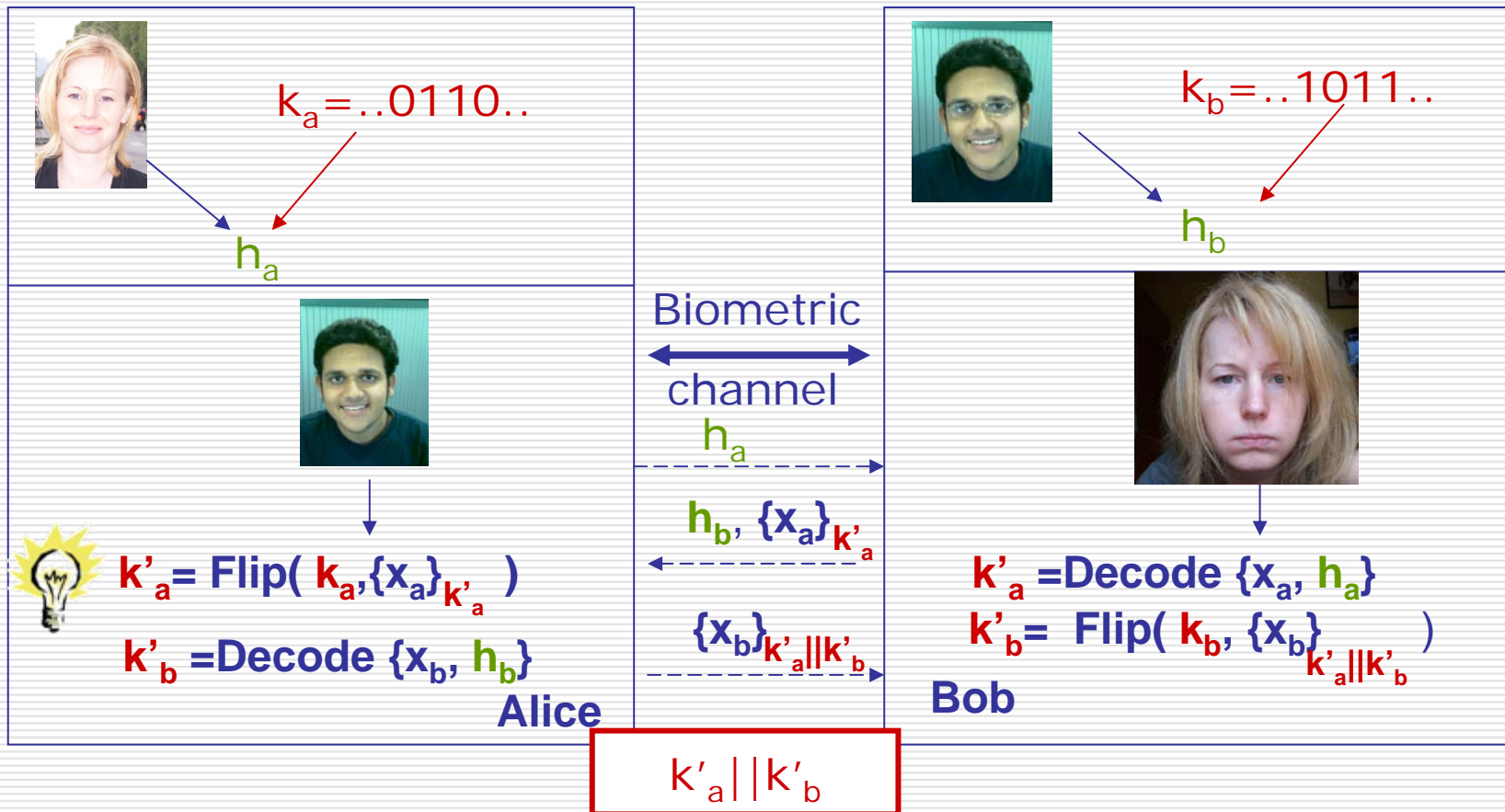


SAfE protocol (ideal case)



$$k_a || k_b$$

SAfE protocol (in a bad day...)






Computational Security Analysis

$|k'_a||k'_b|=112$ bits

Noise=6 bits

Alice (with error profile): 8 trials

Alice (without error profile): $\sim 10^4$ trials

	0	
0	$\sim 10^{66}$ trials	$\sim 10^{33}$ trials
	$\sim 10^{42}$ trials	$\sim 10^{16}$ trials

Usability study-Demographics

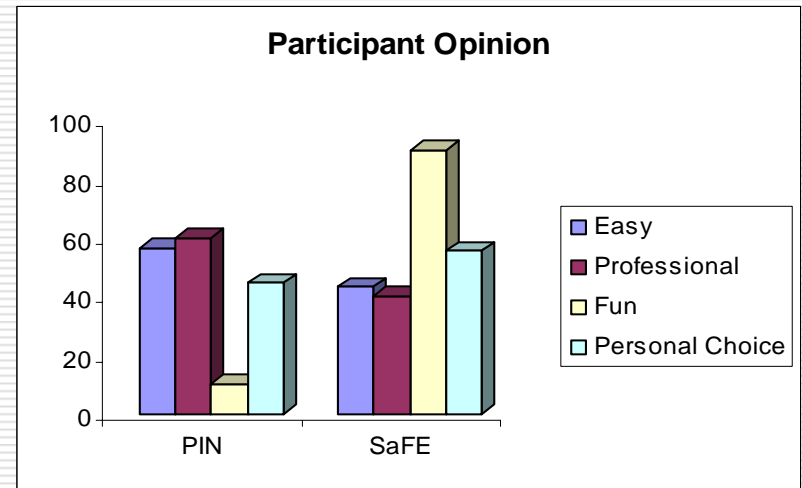
- ❑ 30 participants
- ❑ Computer science environment
- ❑ Average computer usage history ~ 15 years with 9h usage per day
- ❑ All possess a mobile device of which 85% of the devices had wireless capabilities

Usability study-Experiment

1. Brief introduction to secure spontaneous interaction
2. Subjects were asked to complete the background questionnaire
3. Try two types of pairing :
 - Bluetooth pairing (4 digit PIN code)
 - SAfE protocol
4. Fill-in the post test questionnaire

Usability Conclusions

- ❑ 85%: "I want security!"
- ❑ Easy:
 - more familiar
 - easier to type
 - but 80% same PIN
- ❑ 90% SaFE is more fun
- ❑ 73% would like to have both methods on their device
- ❑ 56% are not bothered to have their picture taken by a relative stranger



Conclusions

- Biometric pairing is promising
- Tests to be carried out on real face data
- It's fun!!