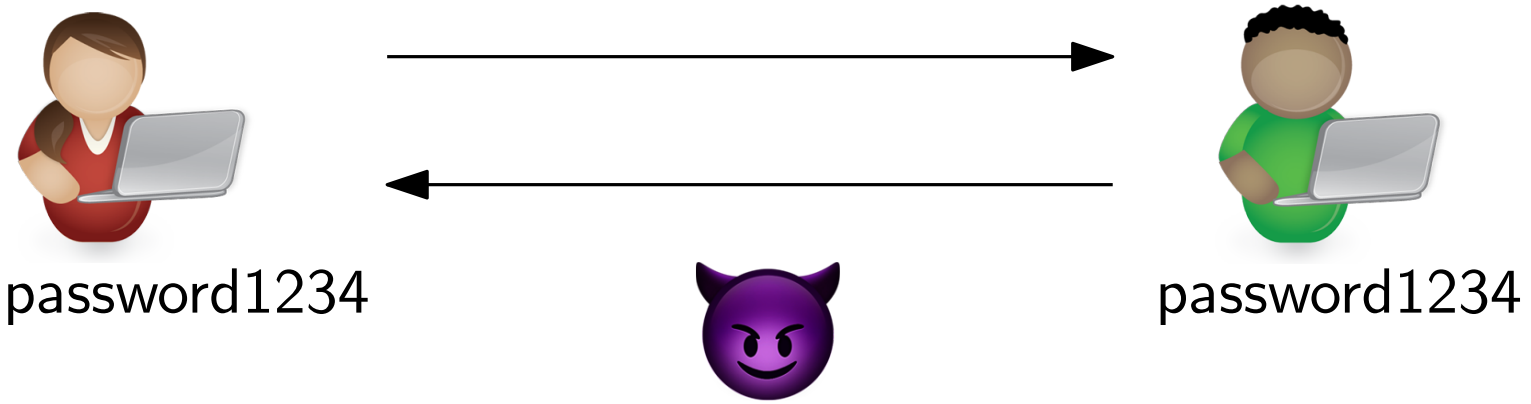
Generalized Fuzzy Password-Authenticated Key Exchange from Error Correcting Codes

Jonathan Bootle, Sebastian Faller, Julia Hesse, Kristina Hostáková, Johannes Ottenhues

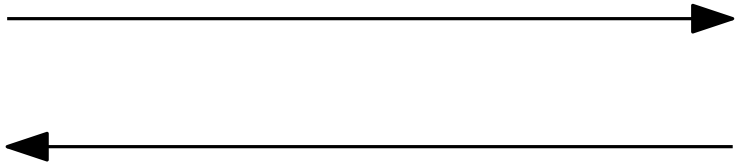
December 05, 2023

Password Authenticated Key Exchange (PAKE)



Password Authenticated Key Exchange (PAKE)

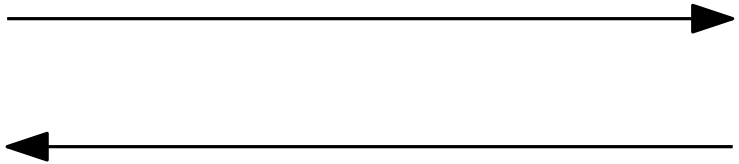
password1234



password1234

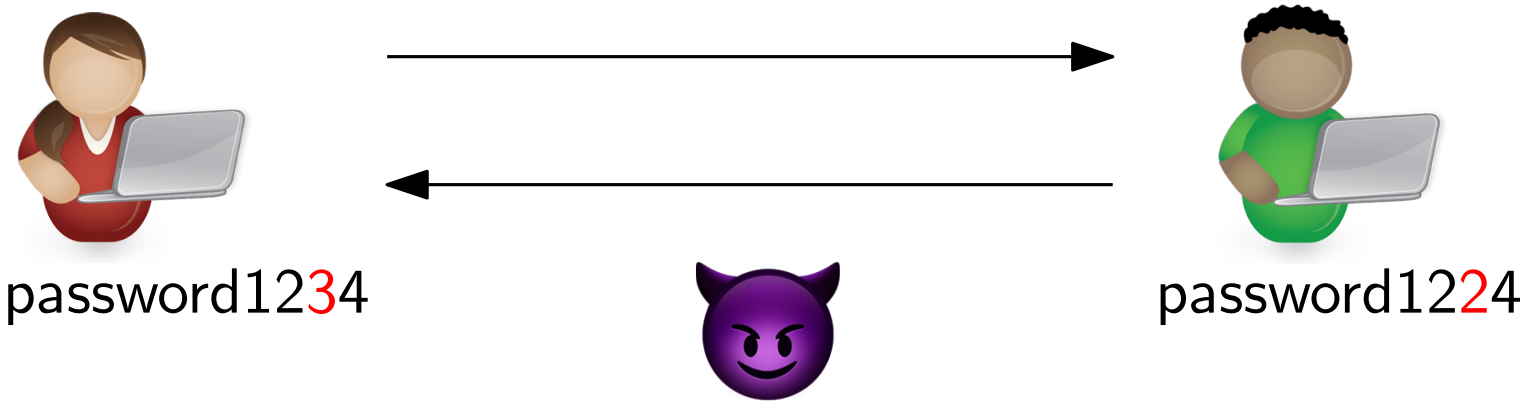
Password Authenticated Key Exchange (PAKE)

password1234



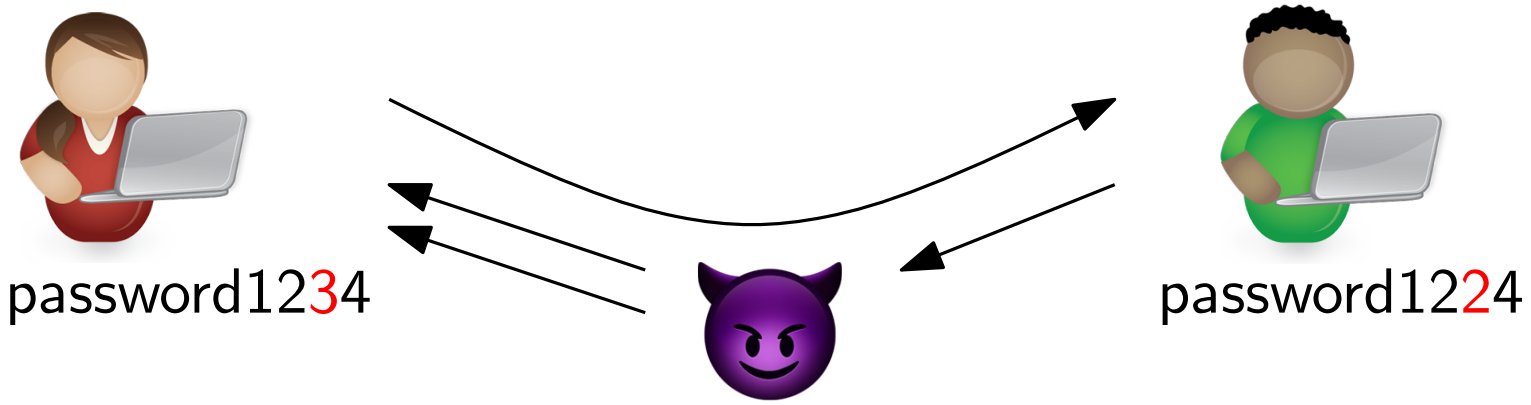
password1234

Fuzzy PAKE



- Typo tolerance
- Biometric readings as passwords
- Pairing of nearby IoT devices with sensor data as passwords

Fuzzy PAKE - Attack Model



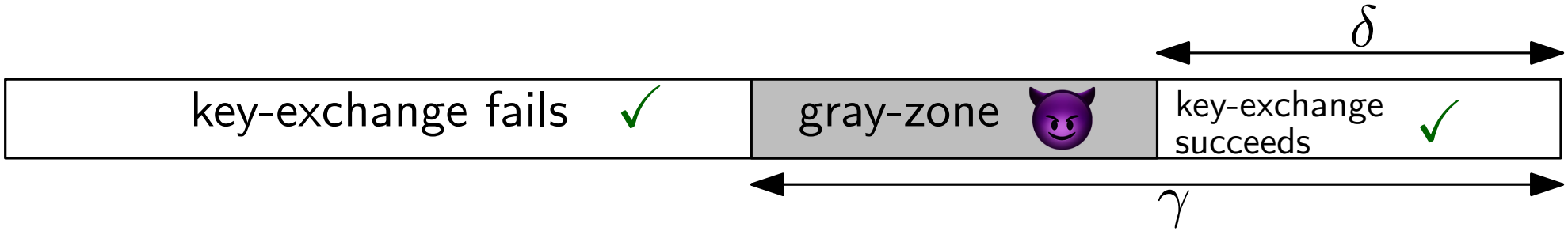
- Same session-key, if and only if the passwords are close
- $\mathcal{A}$ should not learn anything about the passwords
- No offline attacks
- $\mathcal{A}$ should only have one password guess per session

Existing Approaches from [DHP+18]

- Garbled circuit based protocol for arbitrary distances
- Robust secret sharing based, for Hamming distance

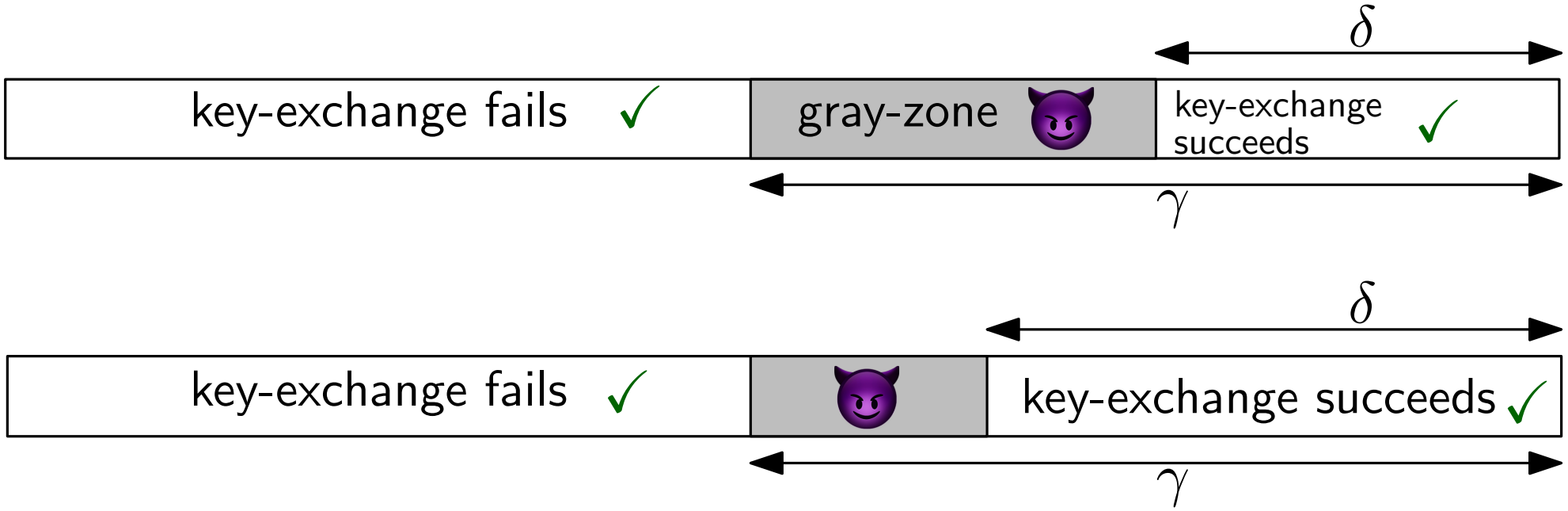
Existing Approaches from [DHP+18]

- Garbled circuit based protocol for arbitrary distances
- Robust secret sharing based, for Hamming distance



Existing Approaches from [DHP+18]

- Garbled circuit based protocol for arbitrary distances
- Robust secret sharing based, for Hamming distance



Intuition of the fPAKE-RSS protocol

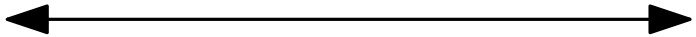
$\mathsf{pw} = 0110$

$\mathsf{pw}' = 0100$

Intuition of the fPAKE-RSS protocol

$\mathsf{pw} = 0110$

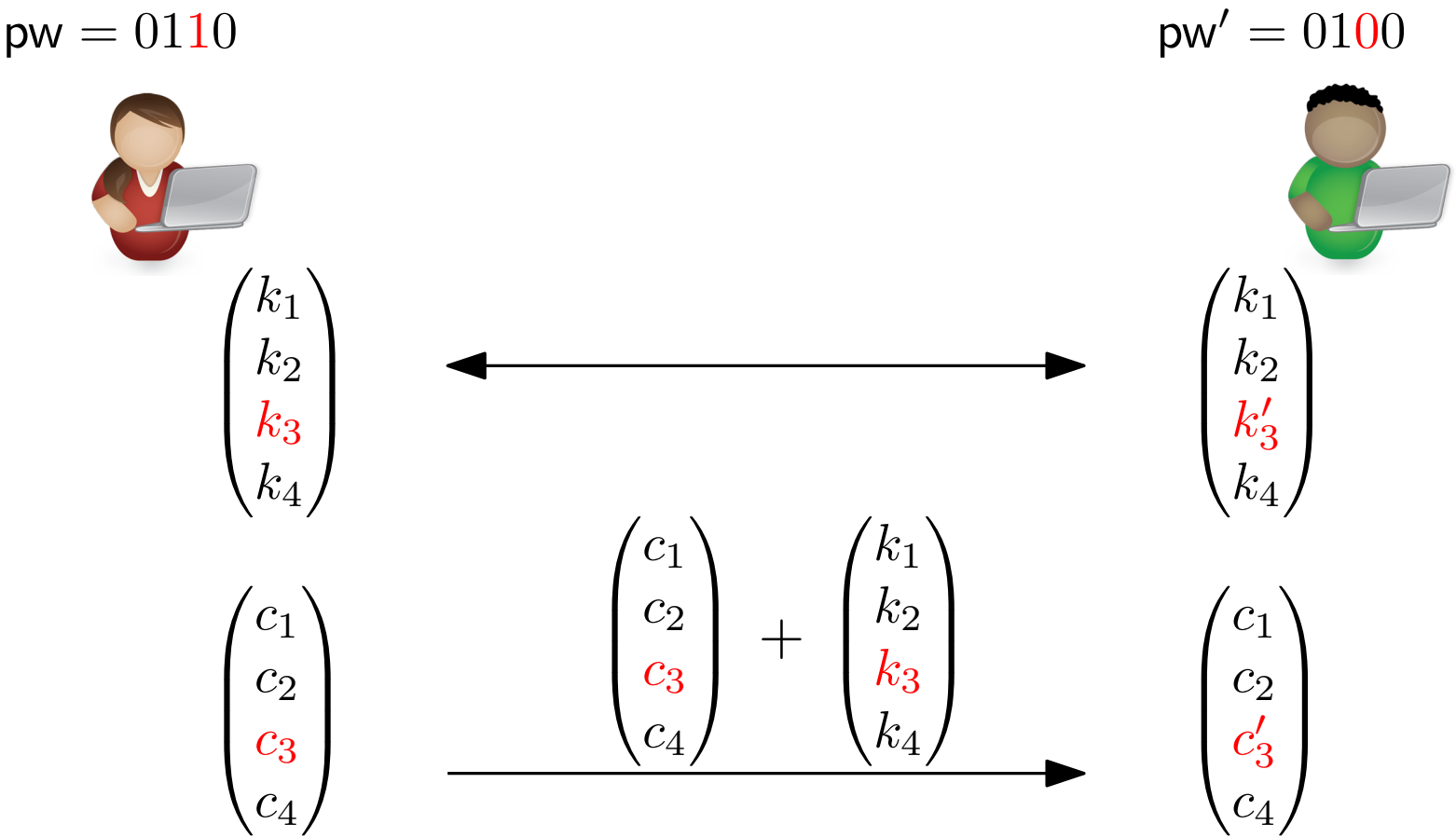
$$\begin{pmatrix} k_1 \\ k_2 \\ k_3 \\ k_4 \end{pmatrix}$$



$\mathsf{pw}' = 0100$

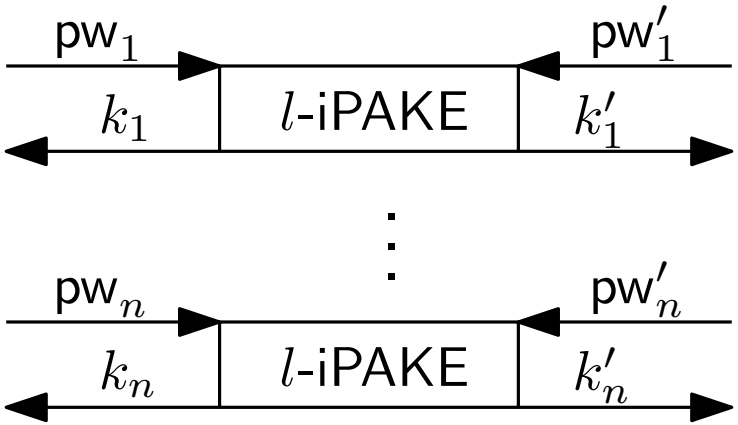
$$\begin{pmatrix} k_1 \\ k_2 \\ k'_3 \\ k_4 \end{pmatrix}$$

Intuition of the fPAKE-RSS protocol



Attack on the fPAKE-RSS protocol

$\mathsf{pw} = \mathsf{pw}_1, \ldots, \mathsf{pw}_n$



$\mathsf{pw}' = \mathsf{pw}'_1, \ldots, \mathsf{pw}'_n$

$\mathbf{K} := (k_1, \ldots, k_n)$
choose U at random
$\mathbf{C} \leftarrow \mathsf{Encode}(U)$
$\mathbf{E} := \mathbf{C} + \mathbf{K}$
$\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, \mathbf{E})$
session-key $:= U$

$\mathbf{E}, \sigma, \mathsf{vk}$

$\mathbf{K}' := (k_1, \ldots, k_n)$
verify signature
$\mathbf{C}' := \mathbf{E} - \mathbf{K}'$
$U' \leftarrow \mathsf{Decode}(\mathbf{C}')$
session-key $:= U'$

Attack on the fPAKE-RSS protocol

$\mathsf{pw} = \mathsf{pw}_1, \ldots, \mathsf{pw}_n$

pw_1 — k_1 — l-iPAKE — k'_1 — pw'_1

pw_n — k_n — l-iPAKE — k'_n — pw'_n

$\mathbf{E}, \sigma, \mathsf{vk}$

$\mathsf{pw}' = \mathsf{pw}'_1, \ldots, \mathsf{pw}'_n$

$\mathbf{K} := (k_1, \ldots, k_n)$
choose U at random
$\mathbf{C} \leftarrow \mathsf{Encode}(U)$
$\mathbf{E} := \mathbf{C} + \mathbf{K}$
$\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, \mathbf{E})$
session-key $:= U$

$\mathbf{K}' := (k_1, \ldots, k_n)$
verify signature
$\mathbf{C}' := \mathbf{E} - \mathbf{K}'$
$U' \leftarrow \mathsf{Decode}(\mathbf{C}')$
session-key $:= U'$

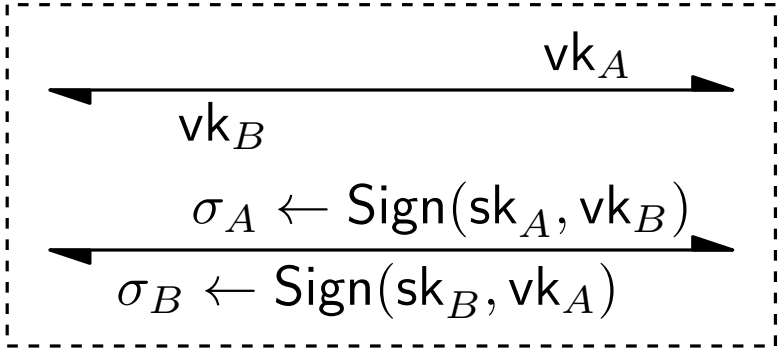
Summary of the Attack

- Requirements:
  - Both parties run the protocol
  - Both parties use the same password
  - The attacker actively interferes in the protocol
- Effect:
  - The attacker learns one bit of their choice of the password

Variations of the attack also work when the passwords are not identical

Overview of our fuzzy PAKE protocol

$\mathsf{pw} = \mathsf{pw}_1, \ldots, \mathsf{pw}_n$



$\mathsf{pw}' = \mathsf{pw}'_1, \ldots, \mathsf{pw}'_n$

Overview of our fuzzy PAKE protocol

$\mathsf{pw} = \mathsf{pw}_1, \ldots, \mathsf{pw}_n$ $\qquad$ $\mathsf{pw}' = \mathsf{pw}'_1, \ldots, \mathsf{pw}'_n$

vk_A

vk_B

$\sigma_A \leftarrow \mathsf{Sign}(\mathsf{sk}_A, \mathsf{vk}_B)$

$\sigma_B \leftarrow \mathsf{Sign}(\mathsf{sk}_B, \mathsf{vk}_A)$

$\mathbf{C} \leftarrow \mathsf{Encode}(\mathsf{secret})$
$\mathbf{E} := \mathsf{blind}(\mathbf{C})$
$h := H(\mathbf{C})$

$\mathbf{E}, h$

$\mathbf{C}' := \mathsf{unblind}(\mathbf{E})$
$L \leftarrow \mathsf{ListDecode}(\mathbf{C}')$
identify correct $\mathbf{C}$ via h
$\mathsf{secret} := \mathsf{Decode}(\mathbf{C})$

Our fuzzy PAKE protocol

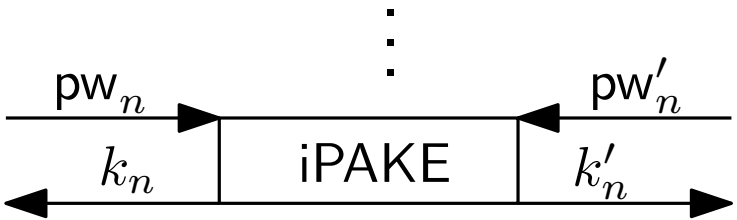
$\mathsf{pw} = \mathsf{pw}_1, \ldots, \mathsf{pw}_n$ $\mathsf{pw}' = \mathsf{pw}'_1, \ldots, \mathsf{pw}'_n$

set up split authenticated channel

Our fuzzy PAKE protocol

$\mathsf{pw} = \mathsf{pw}_1, \ldots, \mathsf{pw}_n$

$\mathsf{pw}' = \mathsf{pw}'_1, \ldots, \mathsf{pw}'_n$



$\mathbf{K} := (k_1, \ldots, k_n)$

$\mathbf{K}' := (k_1, \ldots, k_n)$

Our fuzzy PAKE protocol

$\mathsf{pw} = \mathsf{pw}_1, \ldots, \mathsf{pw}_n$

set up split authenticated channel

$\mathsf{pw}' = \mathsf{pw}'_1, \ldots, \mathsf{pw}'_n$

pw_1 — k_1 — iPAKE — k'_1 — pw'_1

$\mathbf{K} := (k_1, \ldots, k_n)$

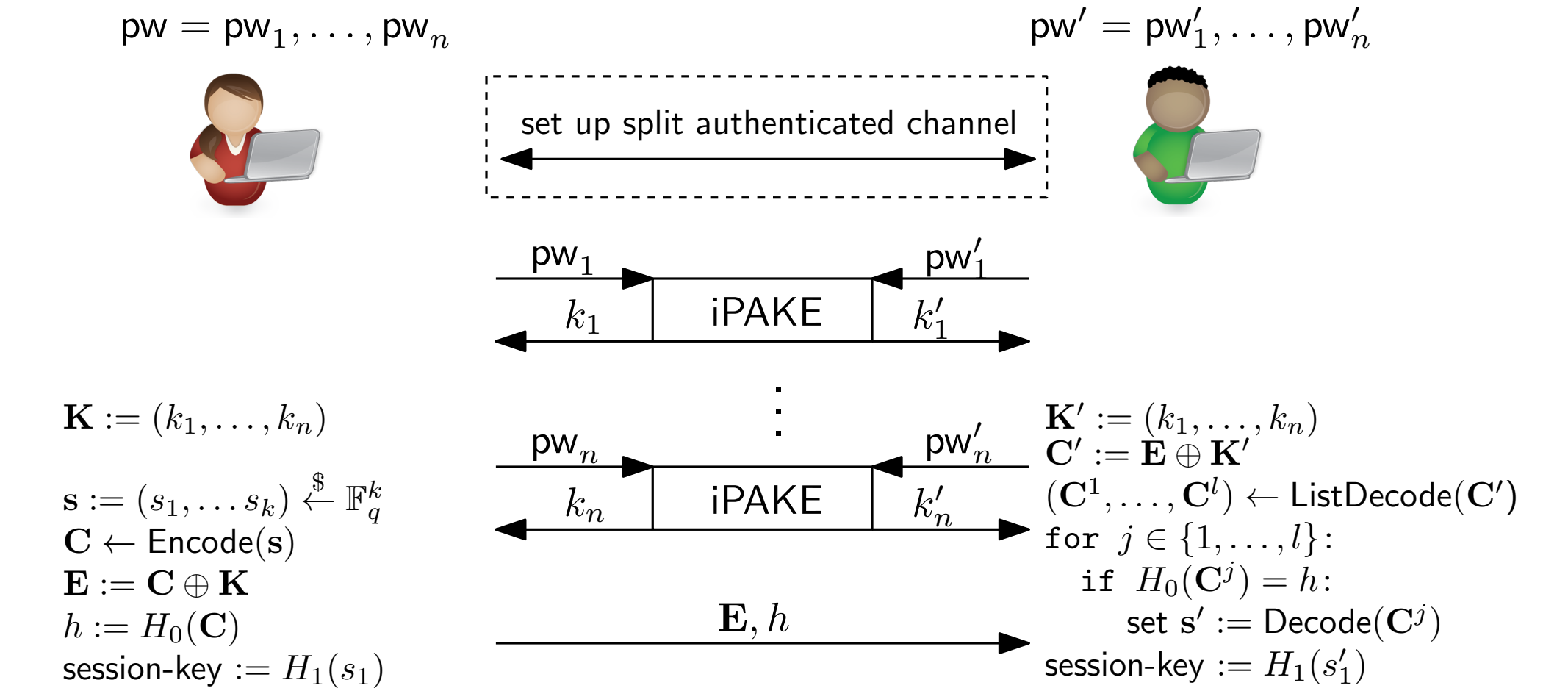
$\mathbf{s} := (s_1, \ldots s_k) \xleftarrow{\$} \mathbb{F}_q^k$
$\mathbf{C} \leftarrow \mathsf{Encode}(\mathbf{s})$
$\mathbf{E} := \mathbf{C} \oplus \mathbf{K}$
$h := H_0(\mathbf{C})$
$\mathsf{session\text{-}key} := H_1(s_1)$

pw_n — k_n — iPAKE — k'_n — pw'_n

$\mathbf{K}' := (k_1, \ldots, k_n)$

$\mathbf{E}, h$

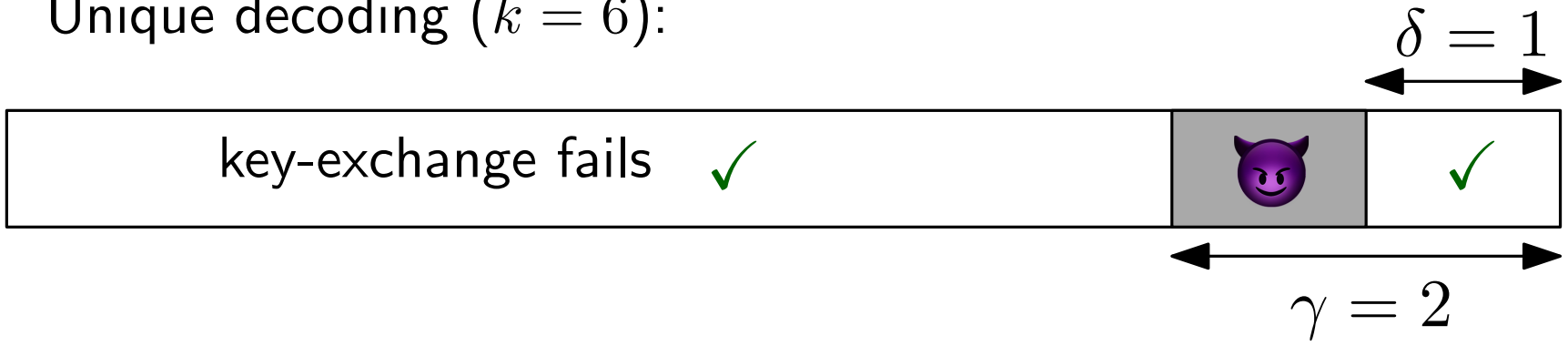
Our fuzzy PAKE protocol



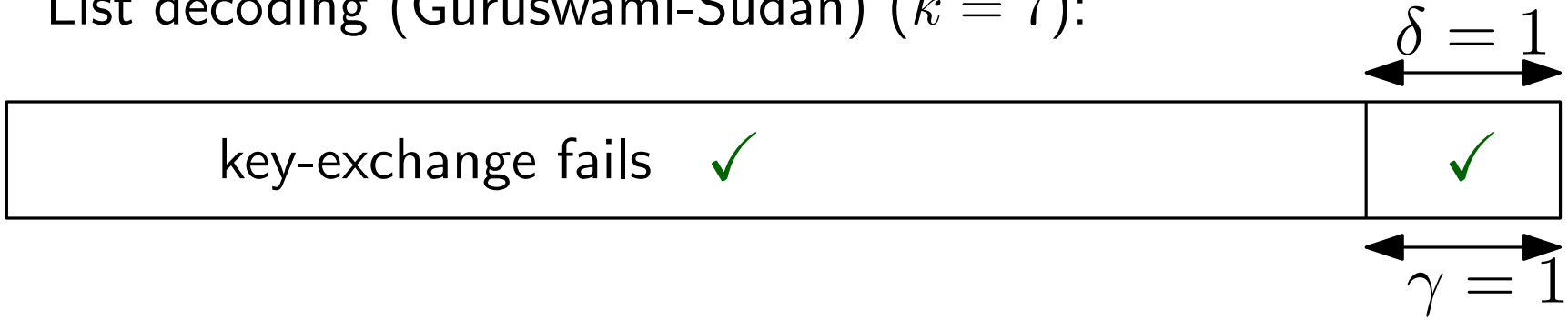
Improvements through list decoding

Correcting 1 error of an 8 character password (with an $[n, k]$ Code)

Unique decoding ($k = 6$):



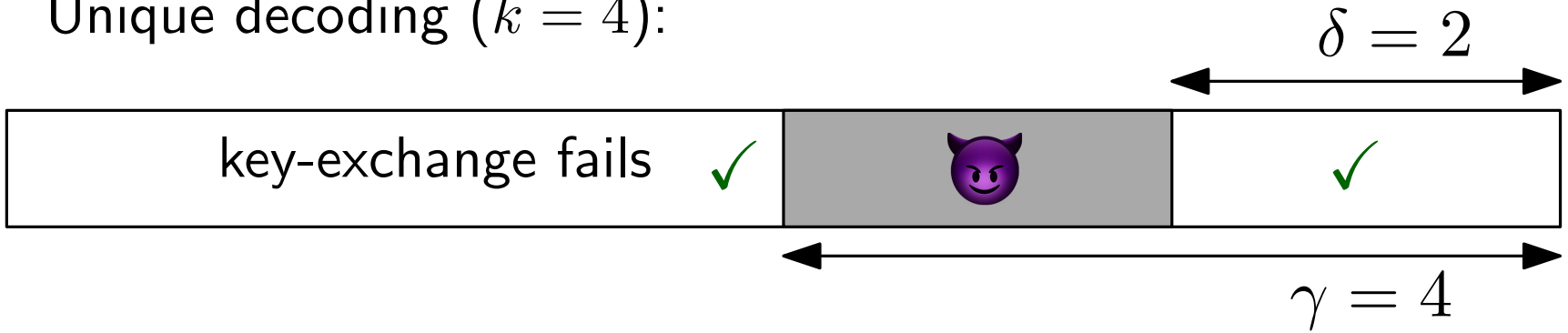
List decoding (Guruswami-Sudan) ($k = 7$):



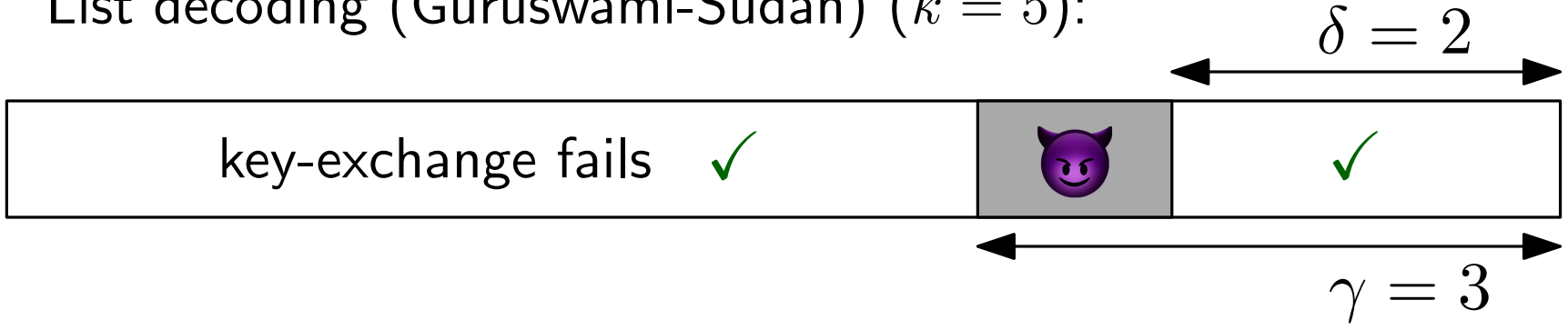
Improvements through list decoding

Correcting 2 error of an 8 character password (with an $[n, k]$ Code)

Unique decoding ($k = 4$):



List decoding (Guruswami-Sudan) ($k = 5$):



Questions

Paper at ia.cr/2023/1415