Oblivious PAKE

Efficient Handling of Password Trials

Franziskus Kiefer, Mark Manulis

Surrey Centre for Cyber Security
Department of Computer Science
University of Surrey, UK

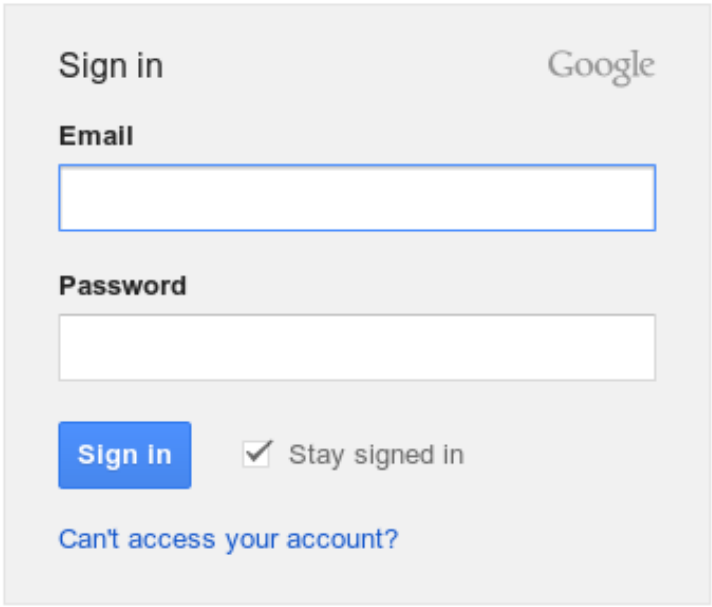
Information Security Conference (ISC 2015),
September 9-11, 2015
Trondheim, Norway

Outline

Password Based Authentication on the Web

TLS Channel

HTML Form




```
<h2>Sign in <strong></strong></h2>
<form novalidate id="gaia_loginform"
action="https://accounts.google.com/ServiceLoginAuth"
method="post">


<div class="email-div">
  <label for="Email"><strong class="email-label">
Username</strong></label>
  <input type="email" spellcheck="false"
name="Email" id="Email" value="">
</div>

<div class="passwd-div">
  <label for="Passwd"><strong class="passwd-label">
Password</strong></label>
  <input type="password" name="Passwd" id="Passwd">
</div>
<input type="submit" class="g-button
g-button-submit" name="signIn" id="signIn"
value="Sign in">
```

Password Based Authentication on the Web

Drawbacks

- Requires PKI
- Server receives passwords in clear
- User has to remember passwords & password-username-server mapping

...Not the best way to do it...

Better Solution

Password Authenticated Key Exchange

Password Based Authentication on the Web

Drawbacks

- Requires PKI
- Server receives passwords in clear
- User has to remember passwords & password-username-server mapping

...Not the best way to do it...

Better Solution

Password Authenticated Key Exchange

Password Based Authentication on the Web

Drawbacks

- Requires PKI
- Server receives passwords in clear
- User has to remember passwords & password-username-server mapping

...Not the best way to do it...

Better Solution

Password Authenticated Key Exchange

Password Authenticated Key Exchange (PAKE)

PAKE protocols known since over 20 years

- Security against Offline Dictionary attacks
- Established security models
  - Game Based Security Model [BPR00]
  - Universally Composable PAKE [CHK+05]
- Many secure protocols known
  - Simple password-based encrypted key exchange protocols [AP05]
  - Faster and shorter password-authenticated key exchange [Gen08]
  - Round-Optimal Password-Based Authenticated Key Exchange [KV11]
  - ...

PAKE Protocols

Example: SPAKE

SPAKE [AP05] uses DL-hard group G and public $M, N \in G$; hash function H as random oracle

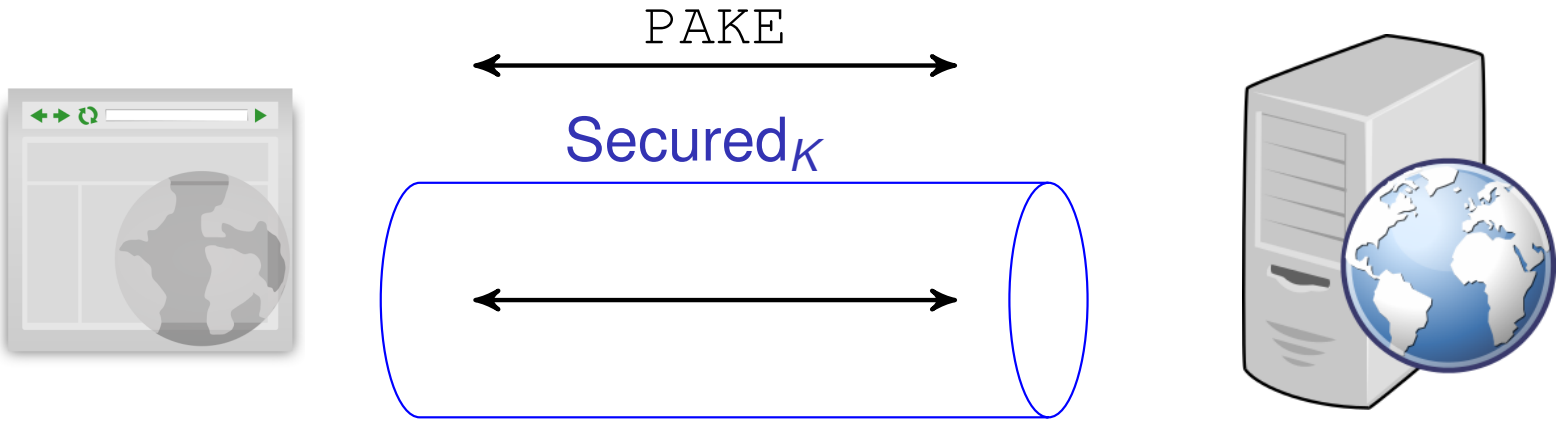
$$x \in_R \mathbb{Z}_p,\ X \leftarrow g^x \qquad \xrightarrow{\quad X' \quad} \qquad y \in_R \mathbb{Z}_p,\ Y \leftarrow g^y$$
$$X' \leftarrow X \cdot M^{\mathrm{pw}} \qquad\qquad Y \leftarrow Y \cdot N^{\mathrm{pw}}$$
$$K'_A \leftarrow (Y'/N^{\mathrm{pw}})^x \qquad \xleftarrow{\quad Y' \quad} \qquad K'_B \leftarrow (X'/M^{\mathrm{pw}})^y$$

Key derivation:

$K_A \leftarrow H(A, B, X', Y', K'_A, \mathrm{pw})$

$K_B \leftarrow H(A, B, X', Y', K'_B, \mathrm{pw})$

PAKE on the Web



- No server certificates (PKI) needed
- Passwords are not transmitted at all

However, PAKE protocols are hardly used in practice (missing standards / incompatibility may be a reason)

The Problem of Failed Logins

Users are still not good with passwords [FH07, GF06]:

- 2.4 failed login attempts on average
- 6.5 different passwords in use
  (on approx. 25 accounts)
- Password disclosure with current practice

PAKE

- Run n PAKE protocols
- Linear amount of work

TLS-based

- Establish 1 TLS channel
- Send n forms

SPAKE execution for 3 passwords: 3×4 Exponentiations

The Problem of Failed Logins

Users are still not good with passwords [FH07, GF06]:

- 2.4 failed login attempts on average
- 6.5 different passwords in use
  (on approx. 25 accounts)
- Password disclosure with current practice

PAKE

- Run *n* PAKE protocols
- Linear amount of work

TLS-based

- Establish 1 TLS channel
- Send *n* forms

SPAKE execution for 3 passwords: 3×4 Exponentiations

Oblivious PAKE

Efficient PAKE with multiple client input passwords

Goals

- Efficient handling of password trials
- No leakage of non-matching passwords to the server
- Ease user's password handling

Oblivious PAKE

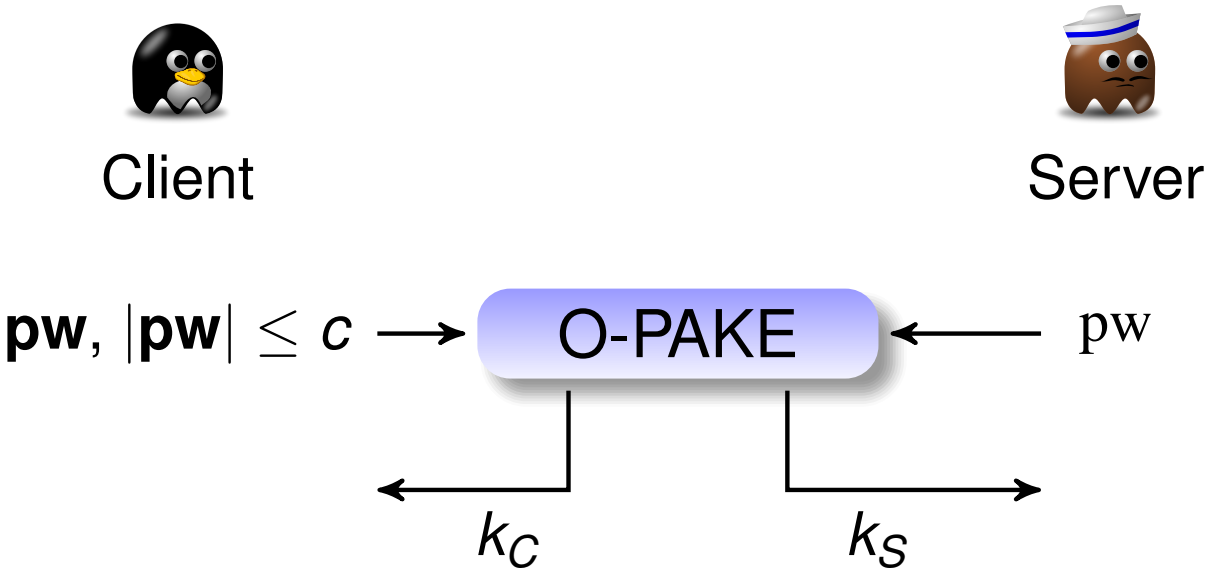
Efficient PAKE with multiple client input passwords

Goals

- Efficient handling of password trials
- No leakage of non-matching passwords to the server
- Ease user's password handling

Oblivious PAKE

Setting

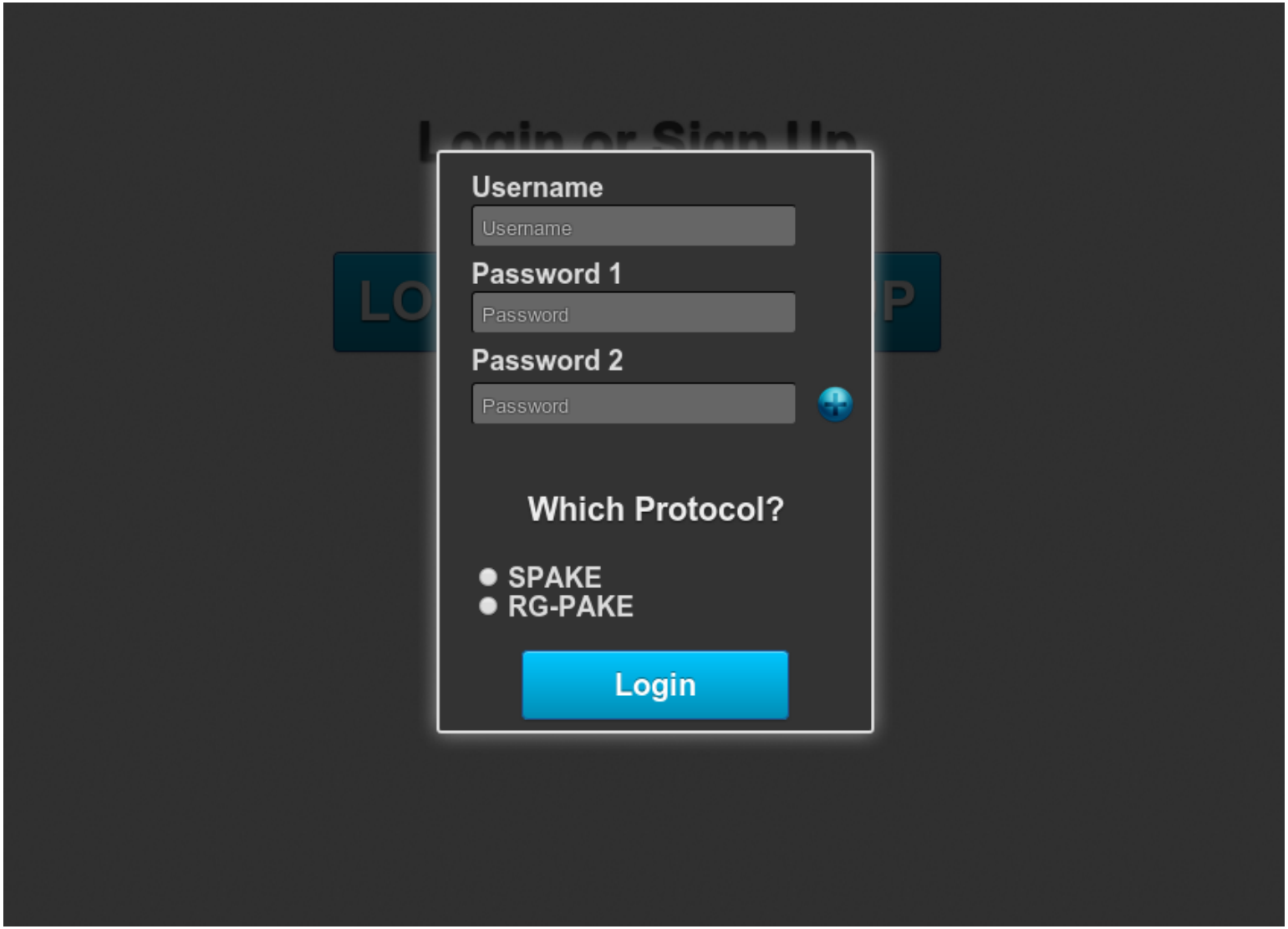


- Client and server share password pw
- Client inputs a list of up to c passwords **pw**
- Server can restrict c due to online dictionary attacks

Successful iff $\mathrm{pw} \in$ **pw**

Oblivious PAKE

Setting



Oblivious PAKE

Security Model

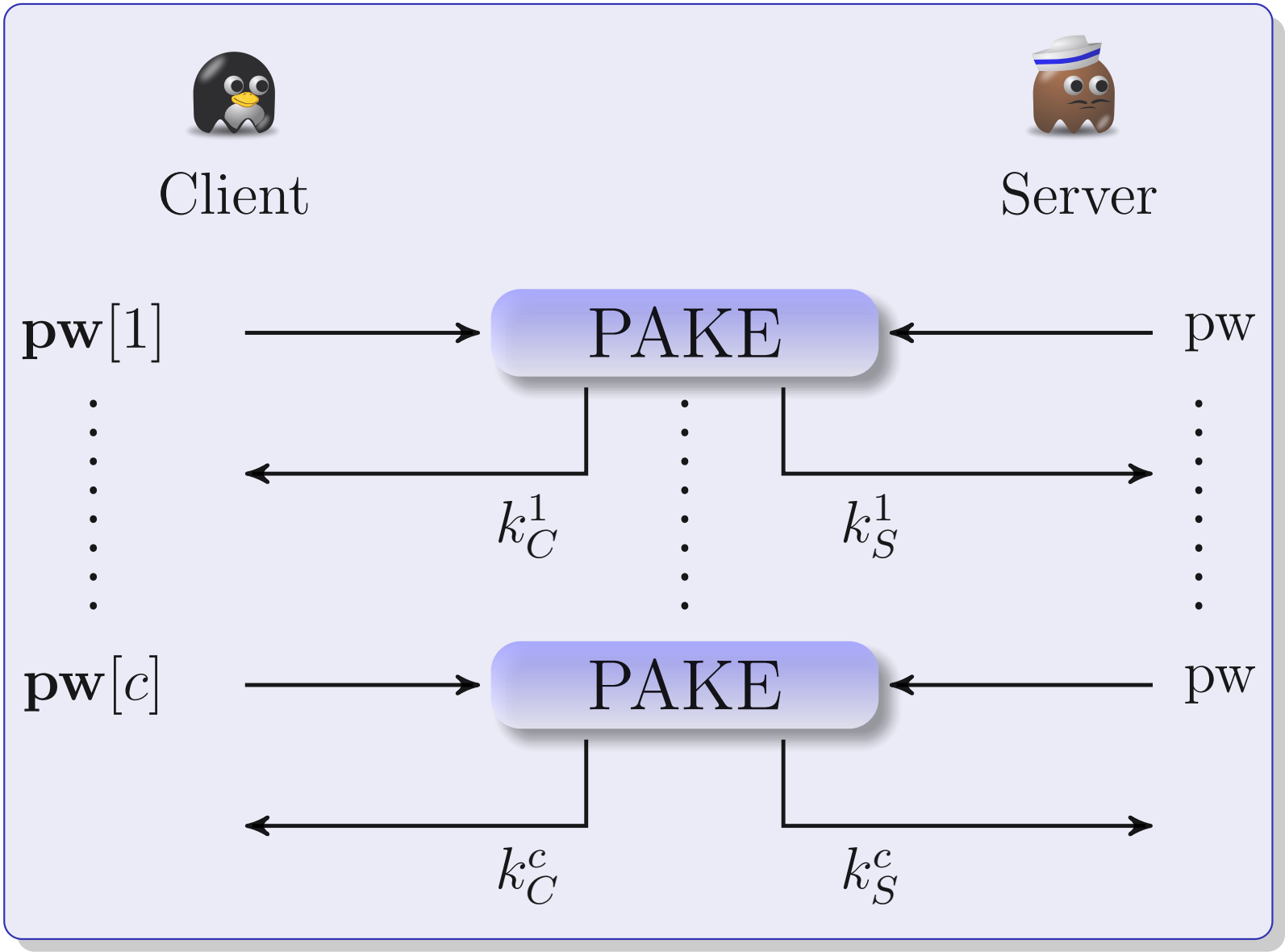
Game based security model from [BPR00, AFP05]:

- Real-or-Random (multiple Test queries)
- Forward Secrecy (Corrupt oracle)
- Extended to allow multiple input passwords

$$
\begin{array}{l}
c \in \mathbb{N}, b \in_R \{0,1\} \\
\forall (P, P') \in \mathcal{C} \times \mathcal{S}, \text{pick } \mathrm{pw}_{P,P'} \in_R \mathcal{D} \\
b' \leftarrow \mathcal{A}^{\text{Send,Execute,Corrupt,Test}}(\lambda, c) \\
\text{return } b = b'
\end{array}
$$

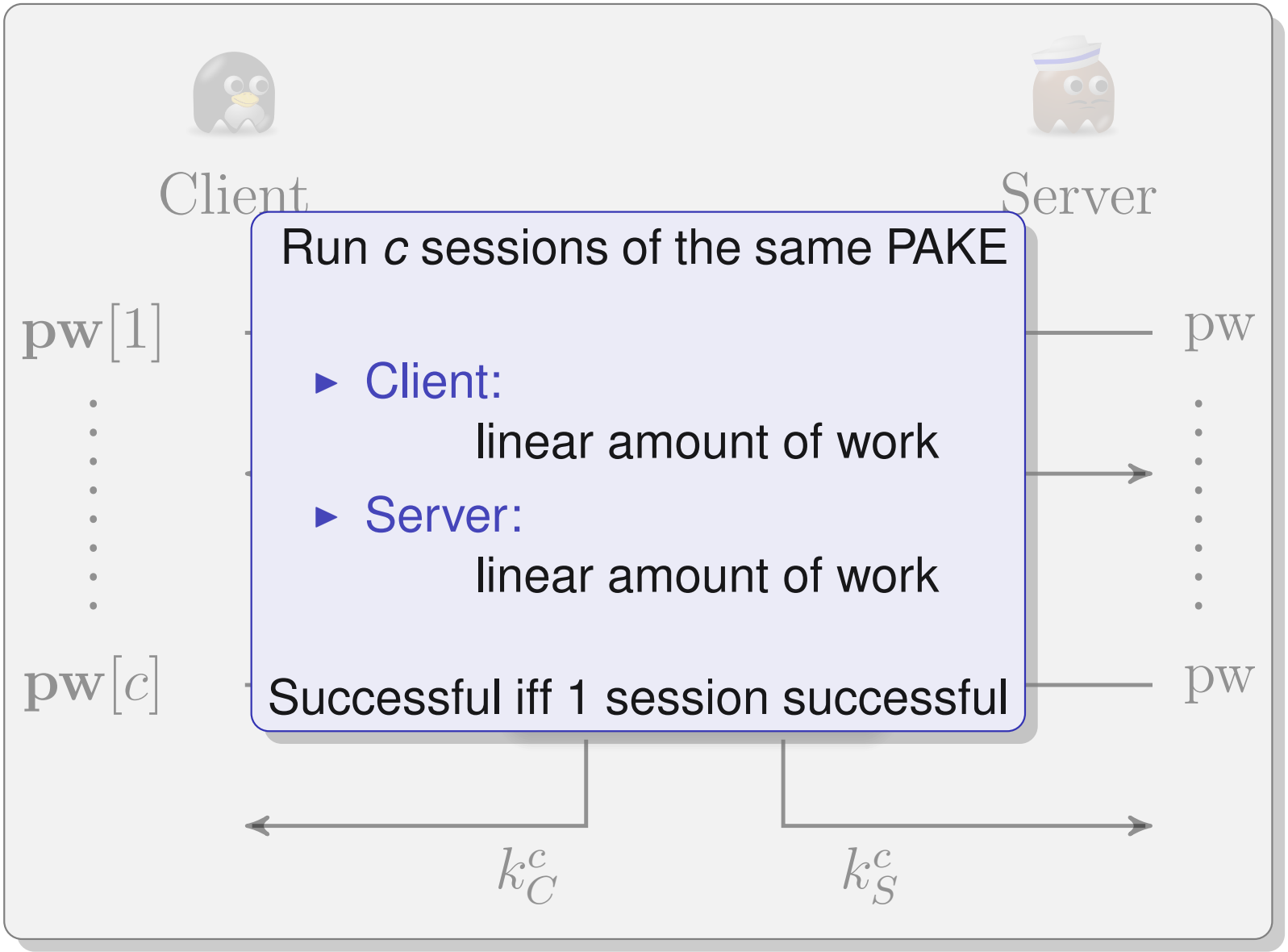
Oblivious PAKE

Naïve Solution



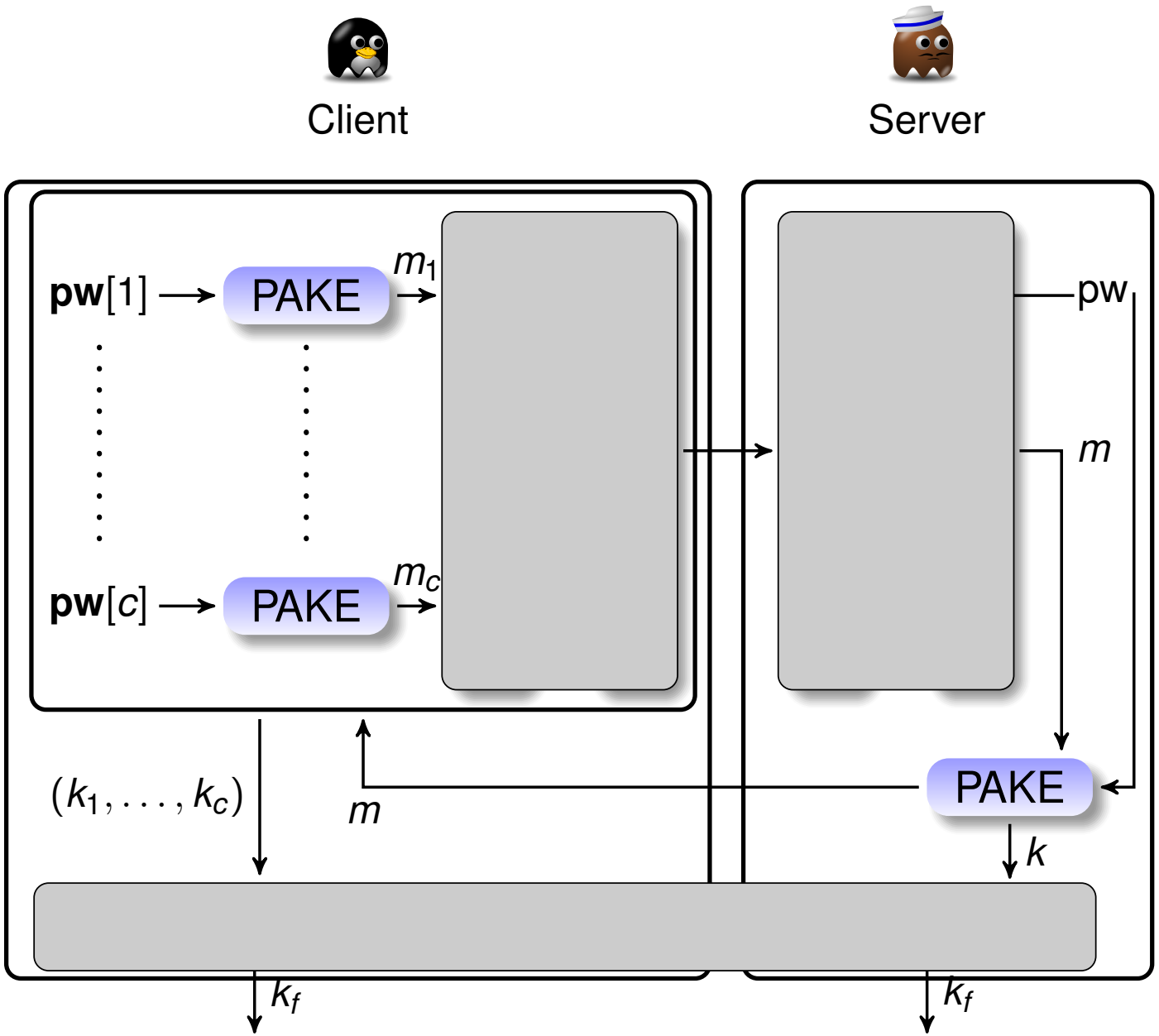
Oblivious PAKE

Naïve Solution



Oblivious PAKE

Idea



Building Blocks

Index-Hiding Message Encoding (IHME)

IHME, introduced in [MPP10], is a message encoding with following properties:

- Encodes set of index, message pairs (i, m)
- Ensures hiding of index i
- Length preserving

$S \leftarrow \texttt{iEncode}(P)$

$P = \{(\mathbf{pw}[1].\mathrm{ix}, m_1), \ldots, (\mathbf{pw}[c].\mathrm{ix}, m_c)\}$
$\rightarrow S = (a_{c-1}, \ldots, a_0)$

$f = \sum_{k=0}^{c-1} a_k x^k$ s.t. $f(\mathbf{pw}[i].\mathrm{ix}) = m_i \;\; \forall (\mathbf{pw}[i].\mathrm{ix}, m_i) \in P$

$m \leftarrow \texttt{iDecode}(S, \mathrm{pw.ix})$

$(S = (a_{c-1}, \ldots, a_0), \mathrm{pw.ix}) \rightarrow m$ with $m = f(\mathrm{pw.ix})$

Building Blocks

Index-Hiding Message Encoding (IHME)

IHME, introduced in [MPP10], is a message encoding with following properties:

- Encodes set of index, message pairs (i, m)
- Ensures hiding of index i
- Length preserving

$S \leftarrow \texttt{iEncode}(P)$

$P = \{(\mathbf{pw}[1].\mathrm{ix}, m_1), \ldots, (\mathbf{pw}[c].\mathrm{ix}, m_c)\}$
$\rightarrow S = (a_{c-1}, \ldots, a_0)$

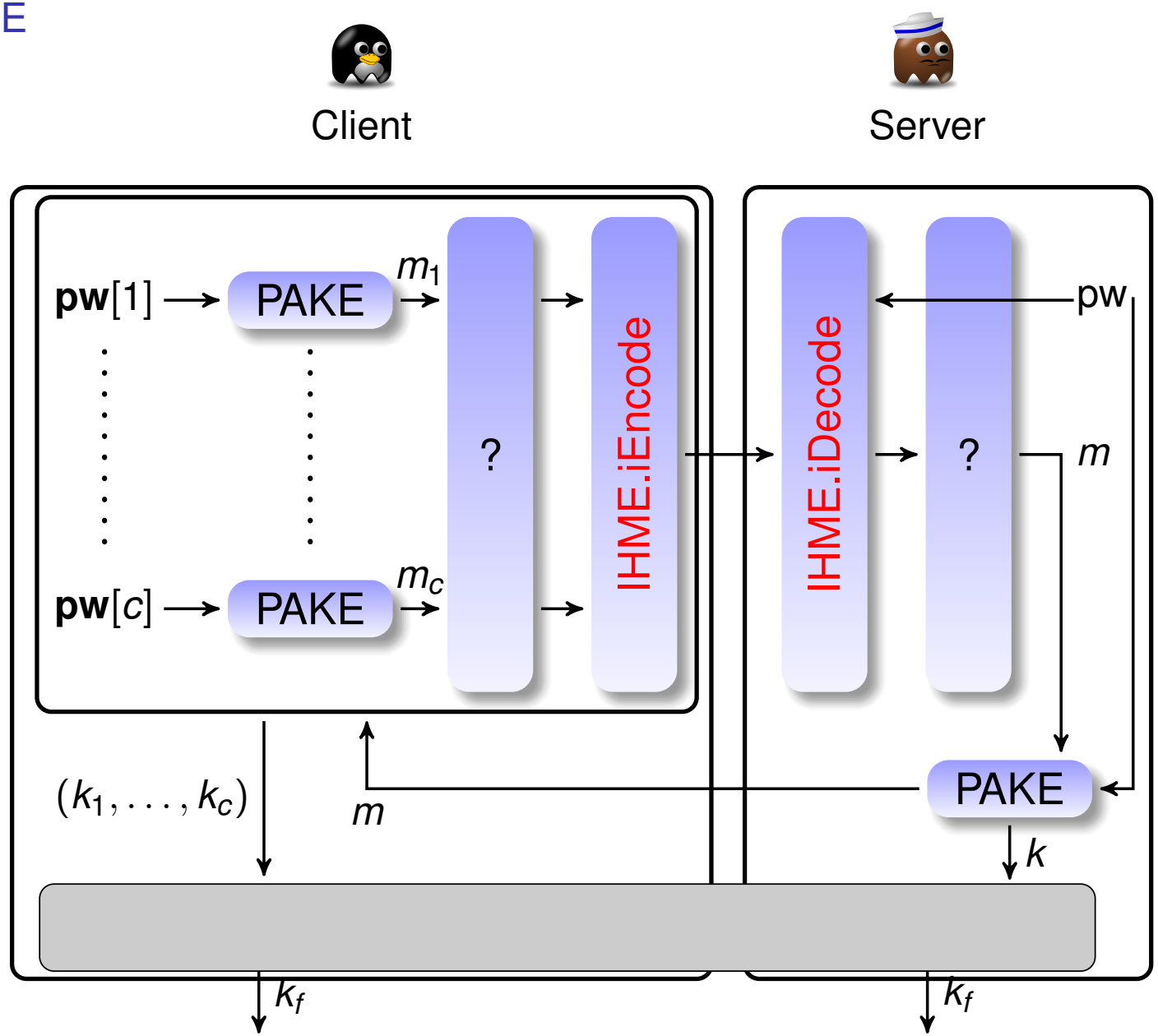
$f = \sum_{k=0}^{c-1} a_k x^k$ s.t. $f(\mathbf{pw}[i].\mathrm{ix}) = m_i \;\; \forall (\mathbf{pw}[i].\mathrm{ix}, m_i) \in P$

$m \leftarrow \texttt{iDecode}(S, \mathrm{pw.ix})$

$(S = (a_{c-1}, \ldots, a_0), \mathrm{pw.ix}) \rightarrow m$ with $m = f(\mathrm{pw.ix})$

Oblivious PAKE

IHME



Building Blocks

Admissible Encodings

Admissible Encodings $F : S \to R, \mathcal{I}_F : R \to S$, introduced in [BF01, BCI+10, FGK+11] encodes elements from set S to R such that:

- $\mathcal{I}_F(r)$ is statistically indistinguishable from uniform distribution over S
- Efficient computable

Building Blocks

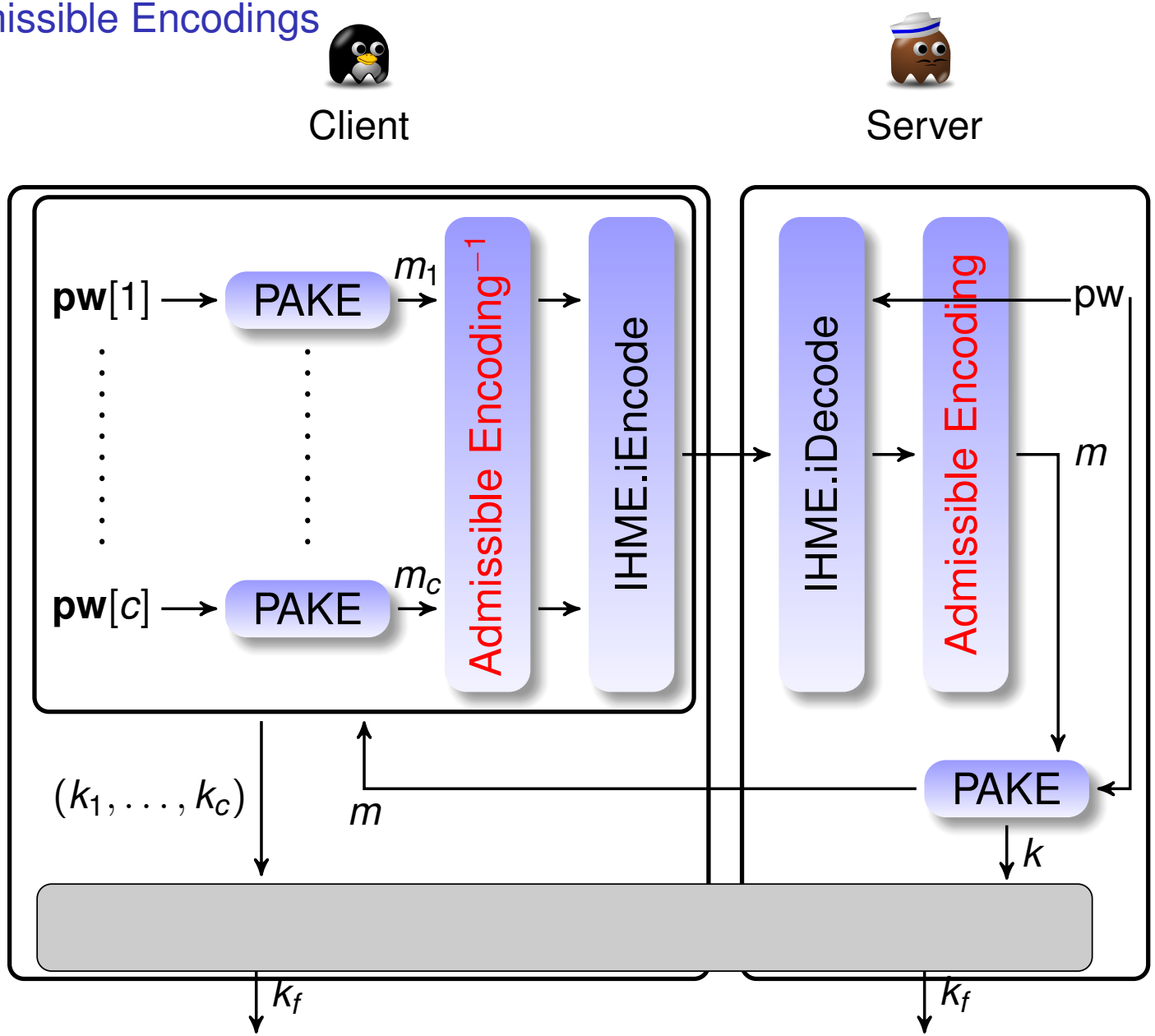
Admissible Encodings

Admissible Encodings $F : S \to R, \mathcal{I}_F : R \to S$, introduced in [BF01, BCI+10, FGK+11] encodes elements from set S to R such that:

- $\mathcal{I}_F(r)$ is statistically indistinguishable from uniform distribution over S
- Efficient computable

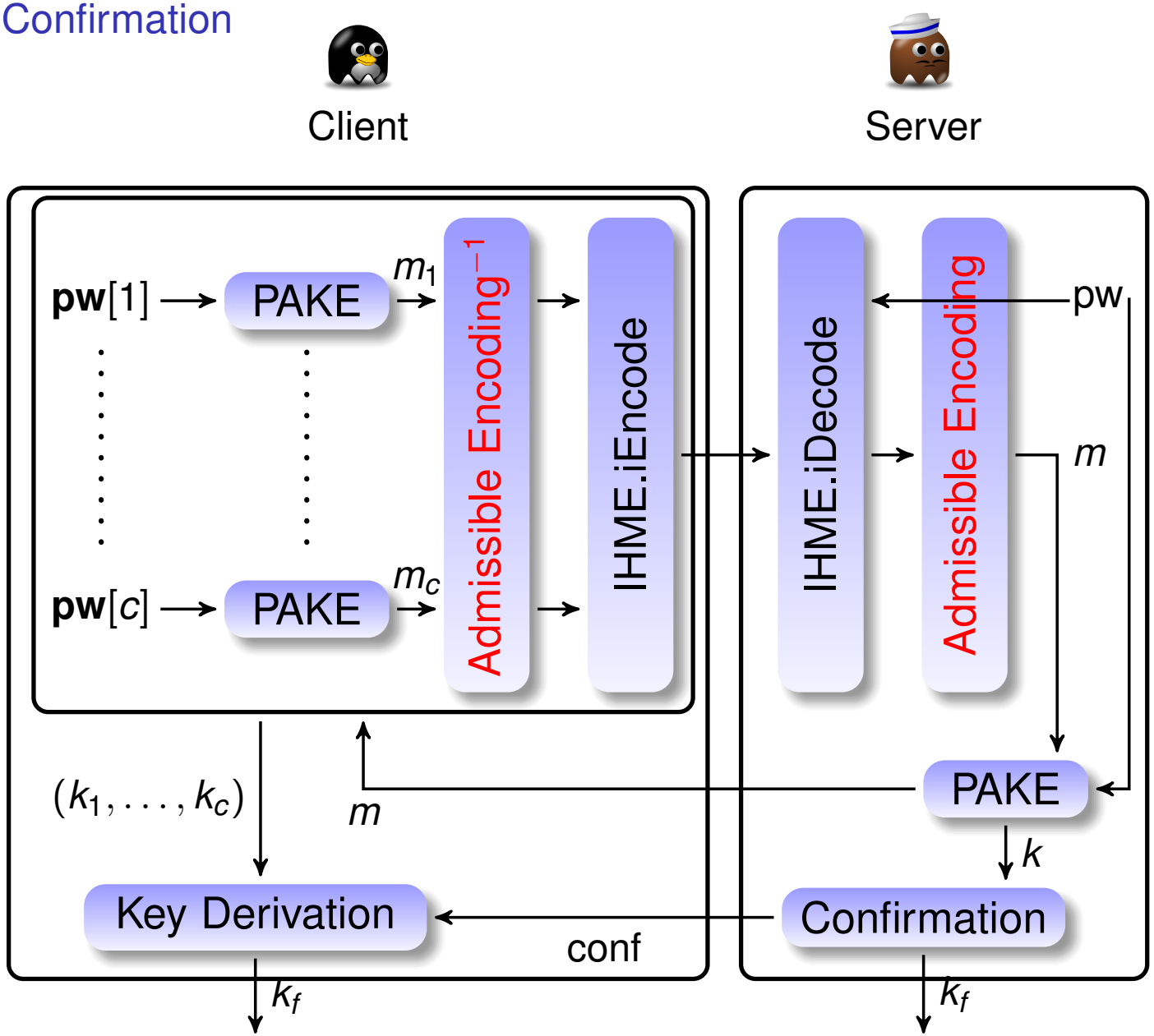
Oblivious PAKE

Admissible Encodings



Oblivious PAKE

Key Confirmation



O-PAKE Compiler

On the example of SPAKE

Client, **pw**

Server, pw

For $\mathrm{pw}_i \in$ **pw**

$x \in_R \mathbb{Z}_p, X \leftarrow g^x$

$X'_i \leftarrow X \cdot M^{\mathrm{pw}_i.\pi}$

$P = P \bigcup (\mathrm{pw}_i.\mathrm{ix}, \mathcal{I}_F(X'_i))$

$S \leftarrow$IHME.encode(P)

$\xrightarrow{S}$

$X^* \leftarrow$IHME.decode$(\mathrm{pw}.\mathrm{ix}, S)$

$X' \leftarrow F(X^*)$

$y \in_R \mathbb{Z}_p, Y \leftarrow g^y$

$Y \leftarrow Y \cdot N^{\mathrm{pw}.\pi}$

$\xleftarrow{Y'}$

$K'_B \leftarrow (X'/M^{\mathrm{pw}.\pi})^y$

$K_B \leftarrow H(A, B, X', Y', K'_B, \mathrm{pw})$

For $\mathrm{pw}_i \in$ **pw**

$K'_A \leftarrow (Y'/N^{\mathrm{pw}_i.\pi})^x$

$K^i_A \leftarrow H(A, B, X'_i, Y', K'_A, \mathrm{pw}_i)$

$\xleftarrow{C}$

$C \leftarrow \mathrm{PRF}_{K_B}(S, Y', 0)$

$K_{B_F} \leftarrow \mathrm{PRF}_{K_B}(S, Y', 1)$

$C' \leftarrow \mathrm{PRF}_{K^i_A}(S, Y', 0)$

IF $C = C'$

$K_{A_F} \leftarrow \mathrm{PRF}_{K_A}(S, Y', 1)$

break

OPAKE Implementation

Modular implementation

- Generic Oblivious PAKE Protocol, including
  - IHME
  - Admissible Encodings for $G_q \mapsto \mathbb{Z}_N$

Implementing an O-PAKE instance includes:

- Implementation of suitable PAKE protocols
- Poss. implementation of an admissible encoding

OPAKE Implementation

Modular implementation

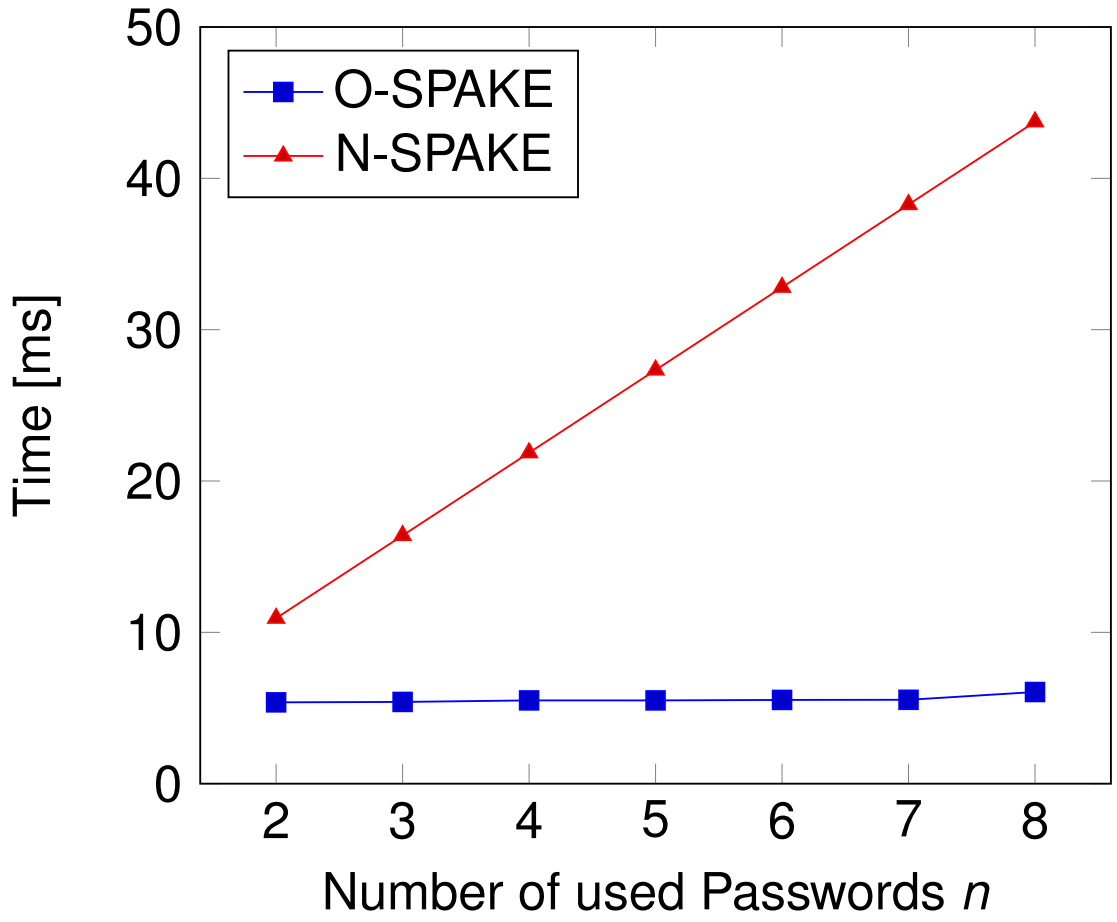
- Generic Oblivious PAKE Protocol, including
  - IHME
  - Admissible Encodings for $G_q \mapsto \mathbb{Z}_N$

Implementing an O-PAKE instance includes:

- Implementation of suitable PAKE protocols
- Poss. implementation of an admissible encoding

OPAKE Performance

Oblivious SPAKE Implementation



Summary

- We proposed Oblivious PAKE with multiple client passwords
- Security model and instantiation
- Implementation (Oblivious SPAKE)
- Constant server runtime even on failed login attempts

- Outlook
  - Real world application (e.g. browser integration)
  - Reduce Communication overhead

References I

Michel Abdalla, Pierre-Alain Fouque, and David Pointcheval.
Password-based authenticated key exchange in the three-party setting.
In *PKC'05*, pages 65–84, Berlin, Heidelberg, 2005. Springer-Verlag.

Michel Abdalla and David Pointcheval.
Simple password-based encrypted key exchange protocols.
In *CT-RSA'05*, pages 191–208, Berlin, Heidelberg, 2005. Springer-Verlag.

References II

Eric Brier, Jean-Sébastien Coron, Thomas Icart, David Madore, Hugues Randriam, and Mehdi Tibouchi.
Efficient indifferentiable hashing into ordinary elliptic curves.
In *CRYPTO'10*, pages 237–254, Berlin, Heidelberg, 2010. Springer-Verlag.

Dan Boneh and Matthew K. Franklin.
Identity-Based Encryption from the Weil Pairing.
In *CRYPTO'01*, volume 2139 of *LNCS*, pages 213–229. Springer, 2001.

References III

Mihir Bellare, David Pointcheval, and Phillip Rogaway.

Authenticated key exchange secure against dictionary attacks.
In *EUROCRYPT'00*, pages 139–155, Berlin, Heidelberg, 2000. Springer-Verlag.

Ran Canetti, Shai Halevi, Jonathan Katz, Yehuda Lindell, and Phil MacKenzie.
Universally Composable Password-Based Key Exchange.
In *EUROCRYPT'05*, pages 404–421, Berlin, Heidelberg, 2005. Springer-Verlag.

References IV


Nils Fleischhacker, Felix Günther, Franziskus Kiefer, Mark Manulis, and Bertram Poettering.
Pseudorandom Signatures.
IACR Cryptology ePrint Archive, 2011:673, 2011.


Dinei Florencio and Cormac Herley.
A Large-Scale Study of Web Password Habits.
In *16th international conference on World Wide Web*, WWW'07, pages 657–666, New York, NY, USA, 2007. ACM.


Rosario Gennaro.
Faster and Shorter Password-Authenticated Key Exchange.
In *TCC'08*, pages 589–606. Springer-Verlag, Berlin, Heidelberg, 2008.

References V


Shirley Gaw and Edward W. Felten.
Password Management Strategies for Online Accounts.
In *Symposium on Usable privacy and security*, SOUPS'06, pages 44–55, New York, New York, USA, 2006. ACM Press.


Jonathan Katz and Vinod Vaikuntanathan.
Round-optimal password-based authenticated key exchange.
In *TCC'11*, pages 293–310, Berlin, Heidelberg, 2011. Springer-Verlag.

References VI

Mark Manulis, Benny Pinkas, and Bertram Poettering.

Privacy-preserving group discovery with linear complexity.
In *ACNS'10*, pages 420–437, Berlin, Heidelberg, 2010. Springer-Verlag.