Karlsruhe Institute of Technology

KASTEL

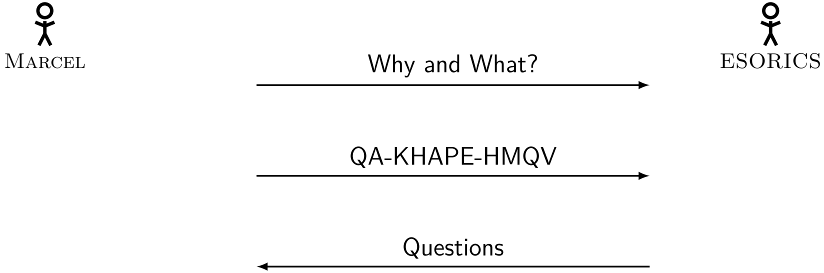
Making an Asymmetric PAKE Quantum-Annoying by Hiding Group Elements

ESORICS, The Hague, 2023

Marcel Tiepelt, Edward Eaton, Douglas Stebila

Making an **Asymmetric PAKE** **Quantum-Annoying** by Hiding Group Elements

Making an Asymmetric PAKE Quantum-Annoying by Hiding Group Elements



Marcel

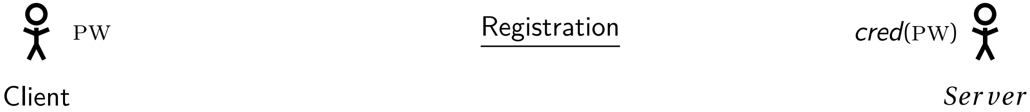
ESORICS

Why and What?

QA-KHAPE-HMQV

Questions

Typical Client-Server Authentication

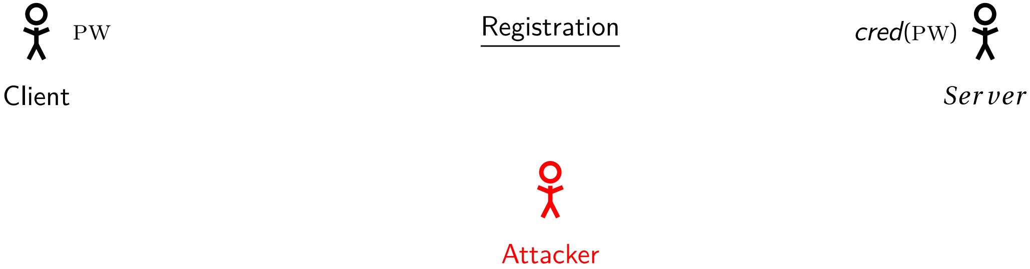


Client PW

Registration

$\mathit{cred}(\mathrm{PW})$ $Server$

Typical Client-Server Authentication



PW

Client

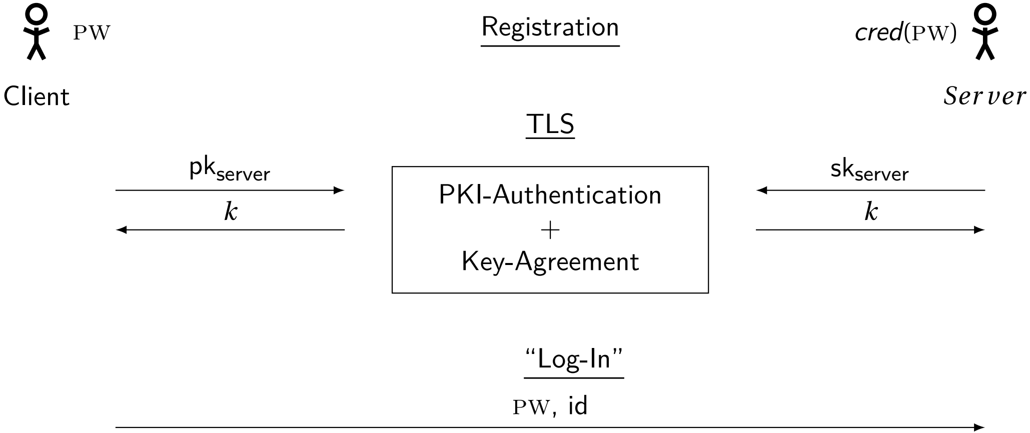
Registration

$\mathit{cred}(\mathrm{PW})$

$Server$

Attacker

Typical Client-Server Authentication



$\textsc{pw}$

Registration

$\mathit{cred}(\textsc{pw})$

Client

$Server$

TLS

$\mathsf{pk}_{\mathsf{server}}$

k

PKI-Authentication
+
Key-Agreement

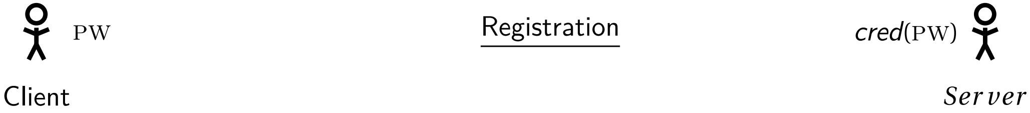
$\mathsf{sk}_{\mathsf{server}}$

k

“Log-In”

$\textsc{pw}$, id

Asymmetric Password Authenticated Key Exchange



PW

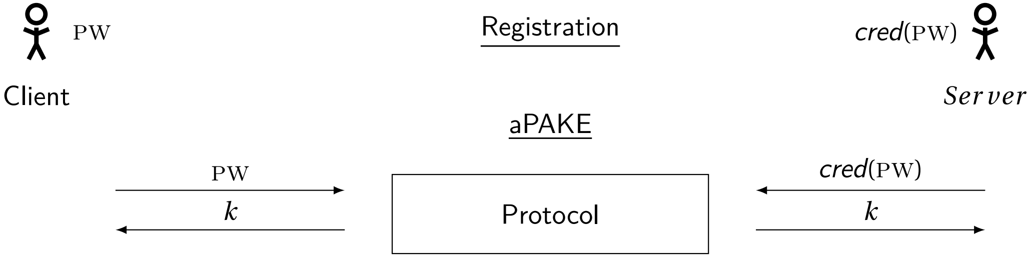
Registration

cred(PW)

Client

$Server$

Asymmetric Password Authenticated Key Exchange



PW

Registration

cred(PW)

Client

$Server$

aPAKE

PW

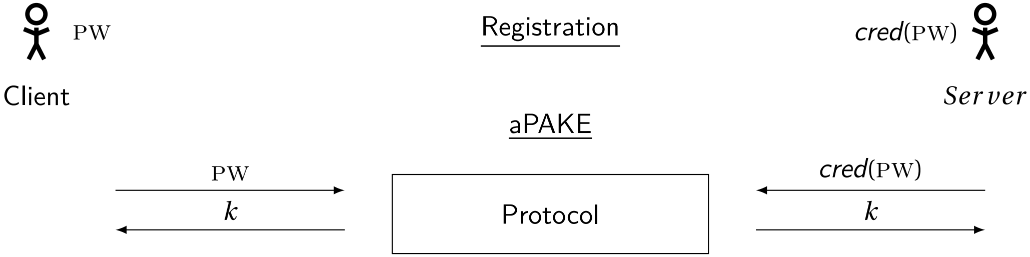
k

Protocol

cred(PW)

k

<u>A</u>symmetric <u>P</u>assword <u>A</u>uthenticated <u>K</u>ey <u>E</u>xchange



PW

Registration

cred(PW)

Client

$Server$

aPAKE

PW

k

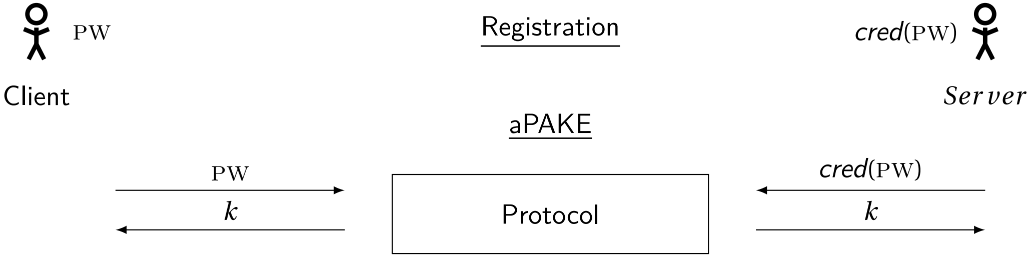
Protocol

cred(PW)

k

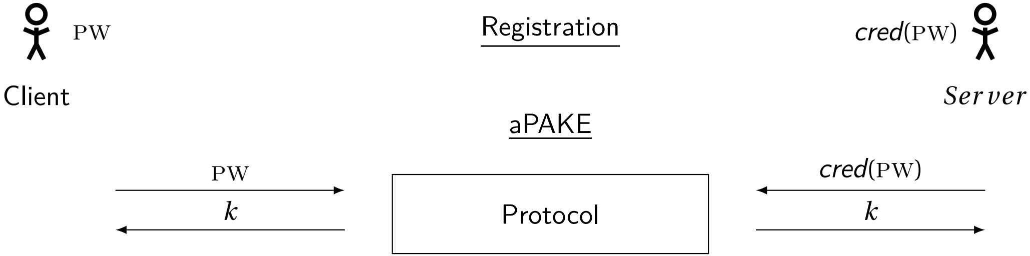
$$\text{Adv} \leq \frac{\text{\#Online Interactions}}{\text{PW-Space}} + \text{Intractability Assumption}$$

Asymmetric Password Authenticated Key Exchange



$$\mathrm{Adv} \leq \frac{\#\text{Online Interactions}}{\textsc{pw}\text{-Space}} + \textsc{Dlog}$$

Asymmetric Password Authenticated Key Exchange



$$\mathsf{Adv} \leq \frac{\#\text{Online Interactions}}{\textsc{pw}\text{-Space}} + \textsc{Dlog}$$

Bad News: *Quantum computers might break* DLOG.

Bad News: *Quantum computers might break* DLOG.

Good News: *Quantum computing appears to be expensive!*

Bad News: *Quantum computers might break* DLOG.

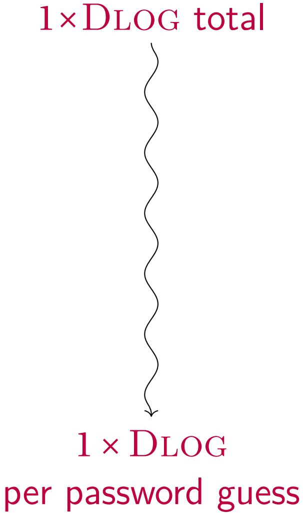
Good News: *Quantum computing appears to be expensive!*

Force adversary to use a lot of quantum computing!

Bad News: *Quantum computers might break* Dlog.

Good News: *Quantum computing appears to be expensive!*

Force adversary to use a lot of quantum computing!



1×Dlog total

1 × Dlog
per password guess

Quantum Annoying'ness [2]

Security

$$\mathsf{Adv} \leq \frac{\#\text{Online Interactions}}{\textsc{pw}\text{-Space}} + \frac{\#\textsc{Dlog}'s}{\textsc{pw}\text{-Space}}$$

Model

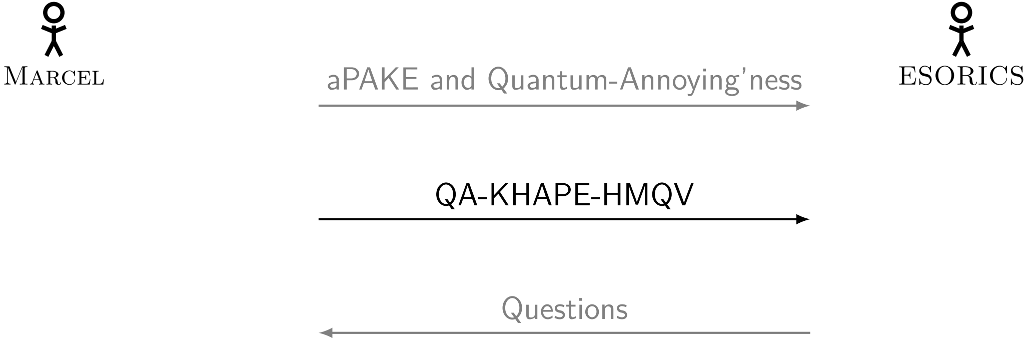
- Dlog Oracle
- GGM
- BPR[1]

Limitations

- Only Dlog oracle
- Multiple Dlog's harder than one Dlog

[2] Eaton and Stebila 2021, "The "Quantum Annoying" Property of Password-Authenticated Key Exchange Protocols"

[1] Bellare, Pointcheval, and Rogaway 2000, "Authenticated Key Exchange Secure against Dictionary Attacks"



Marcel

ESORICS

aPAKE and Quantum-Annoying'ness

QA-KHAPE-HMQV

Questions

KHAPE-HMQV[3] — simplified

Client

Registration

$(a, A), (b, B)$ fresh AKE keys

Server

$e \leftarrow \mathsf{IC}_1.E(\textsc{pw}, a, B, \quad)$

$\textit{store cred}(\textsc{pw}) = (b, A, e \quad)$

[3] Gu, Jarecki, and Krawczyk 2021, "KHAPE: Asymmetric PAKE from Key-Hiding Key Exchange"

KHAPE-HMQV[3] — simplified

Client

Registration

$(a, A), (b, B)$ fresh AKE keys

$e \leftarrow \mathsf{IC}_1.E(\textsc{pw}, a, B, \quad)$

store $\mathit{cred}(\textsc{pw}) = (b, A, e \quad)$

Server

On input: $\textsc{pw}$

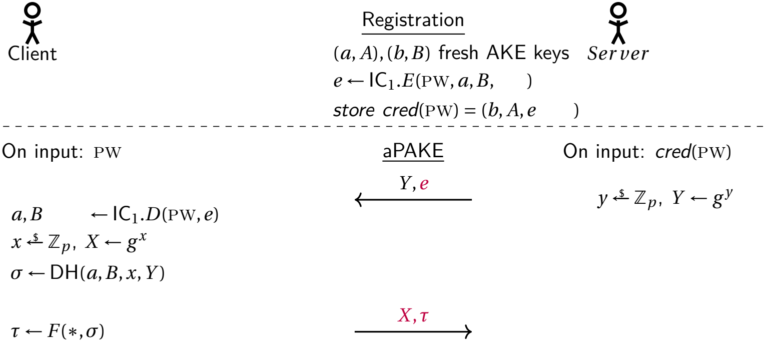
aPAKE

On input: $\mathit{cred}(\textsc{pw})$

$$\xleftarrow{\quad Y, e \quad} \qquad y \xleftarrow{\$} \mathbb{Z}_p,\ Y \leftarrow g^y$$

[3] Gu, Jarecki, and Krawczyk 2021, "KHAPE: Asymmetric PAKE from Key-Hiding Key Exchange"

KHAPE-HMQV[3] — simplified



Client

Registration

$(a, A), (b, B)$ fresh AKE keys

Server

$e \leftarrow \mathsf{IC}_1.E(\textsc{pw}, a, B, \quad)$

store $\mathit{cred}(\textsc{pw}) = (b, A, e \quad)$

On input: $\textsc{pw}$

aPAKE

On input: $\mathit{cred}(\textsc{pw})$

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

$\xleftarrow{Y, e}$

$a, B \qquad \leftarrow \mathsf{IC}_1.D(\textsc{pw}, e)$

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

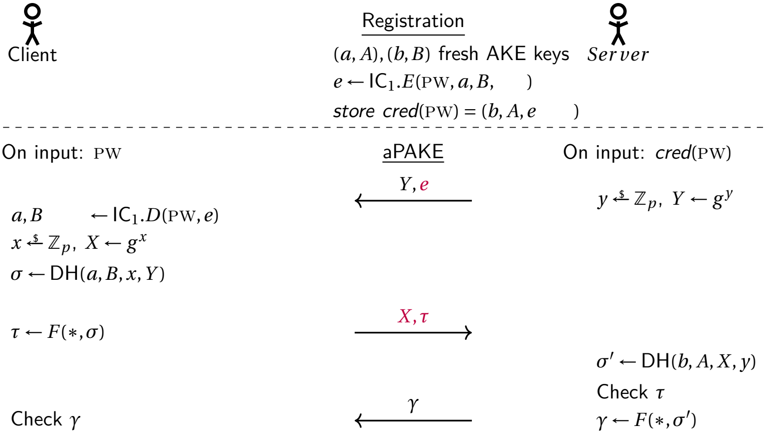
$\sigma \leftarrow \mathsf{DH}(a, B, x, Y)$

$\tau \leftarrow F(*, \sigma)$

$\xrightarrow{X, \tau}$

[3] Gu, Jarecki, and Krawczyk 2021, “KHAPE: Asymmetric PAKE from Key-Hiding Key Exchange”

KHAPE-HMQV[3] — simplified



Client

Registration

$(a, A), (b, B)$ fresh AKE keys

$e \leftarrow \mathsf{IC}_1.E(\textsc{pw}, a, B, \quad)$

store $\mathit{cred}(\textsc{pw}) = (b, A, e \quad)$

$Server$

On input: $\textsc{pw}$

aPAKE

On input: $\mathit{cred}(\textsc{pw})$

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

$\xleftarrow{Y, e}$

$a, B \quad \leftarrow \mathsf{IC}_1.D(\textsc{pw}, e)$

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

$\sigma \leftarrow \mathsf{DH}(a, B, x, Y)$

$\tau \leftarrow F(*, \sigma)$

$\xrightarrow{X, \tau}$

$\sigma' \leftarrow \mathsf{DH}(b, A, X, y)$

Check τ

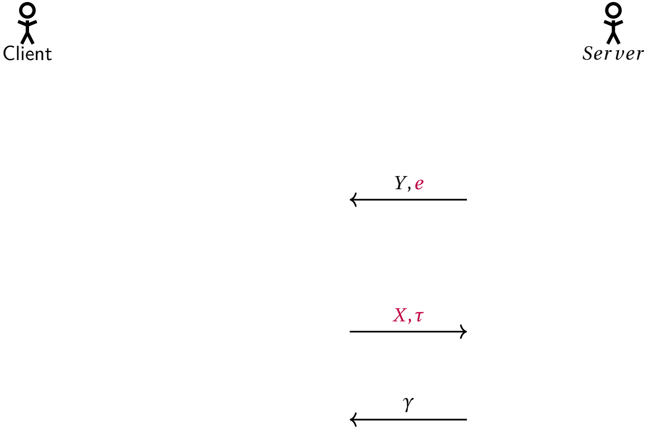
$\gamma \leftarrow F(*, \sigma')$

$\xleftarrow{\gamma}$

Check γ

[3] Gu, Jarecki, and Krawczyk 2021, “KHAPE: Asymmetric PAKE from Key-Hiding Key Exchange”

KHAPE-HMQV[3] — simplified


Client

$Server$

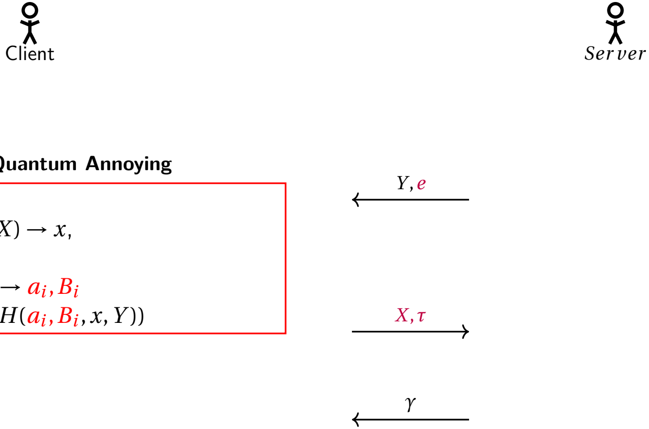
$\xleftarrow{Y, e}$

$\xrightarrow{X, \tau}$

$\xleftarrow{\gamma}$

[3] Gu, Jarecki, and Krawczyk 2021, "KHAPE: Asymmetric PAKE from Key-Hiding Key Exchange"

KHAPE-HMQV[3] — simplified



Not Quantum Annoying

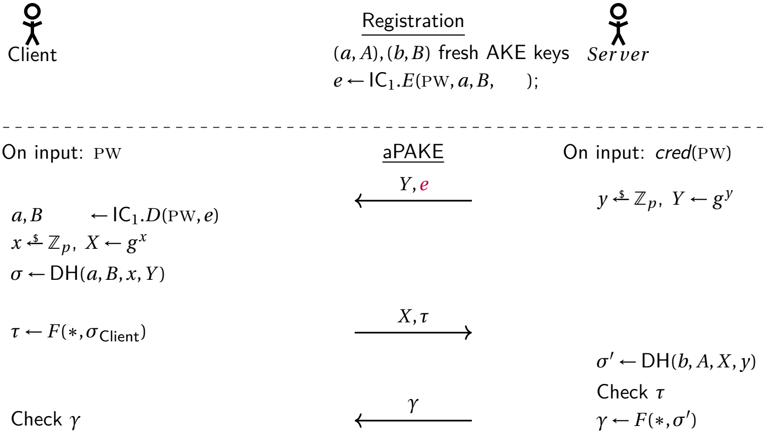
Attacker:

- query $\textsc{DLog}(X) \rightarrow x$,
- check $\textsc{pw}_i$

$\rightsquigarrow$ IC.$D(\textsc{pw}_i, e) \rightarrow a_i, B_i$
until $\tau = F(DH(a_i, B_i, x, Y))$

[3] Gu, Jarecki, and Krawczyk 2021, “KHAPE: Asymmetric PAKE from Key-Hiding Key Exchange”

QA-KHAPE-HMQV – simplified



Client

Registration

$(a, A), (b, B)$ fresh AKE keys

$e \leftarrow \mathsf{IC}_1.E(\textsc{pw}, a, B, \quad);$

Server

On input: $\textsc{pw}$

aPAKE

On input: *cred*$(\textsc{pw})$

$\xleftarrow{Y, e}$

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

$a, B \leftarrow \mathsf{IC}_1.D(\textsc{pw}, e)$

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

$\sigma \leftarrow \mathsf{DH}(a, B, x, Y)$

$\tau \leftarrow F(*, \sigma_{\mathsf{Client}})$

$\xrightarrow{X, \tau}$

$\sigma' \leftarrow \mathsf{DH}(b, A, X, y)$

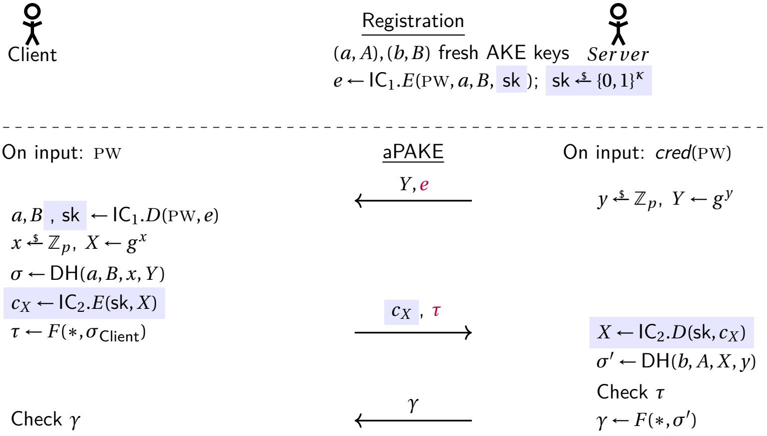
Check τ

$\gamma \leftarrow F(*, \sigma')$

$\xleftarrow{\gamma}$

Check γ

QA-KHAPE-HMQV – simplified



Client

Registration

$(a, A), (b, B)$ fresh AKE keys

Server

$e \leftarrow \mathsf{IC}_1.E(\textsc{pw}, a, B, \mathsf{sk});\ \mathsf{sk} \xleftarrow{\$} \{0,1\}^{\kappa}$

On input: $\textsc{pw}$

aPAKE

On input: *cred*$(\textsc{pw})$

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

$\xleftarrow{\quad Y, e \quad}$

$a, B, \mathsf{sk} \leftarrow \mathsf{IC}_1.D(\textsc{pw}, e)$

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

$\sigma \leftarrow \mathsf{DH}(a, B, x, Y)$

$c_X \leftarrow \mathsf{IC}_2.E(\mathsf{sk}, X)$

$\tau \leftarrow F(*, \sigma_{\mathsf{Client}})$

$\xrightarrow{\quad c_X, \tau \quad}$

$X \leftarrow \mathsf{IC}_2.D(\mathsf{sk}, c_X)$

$\sigma' \leftarrow \mathsf{DH}(b, A, X, y)$

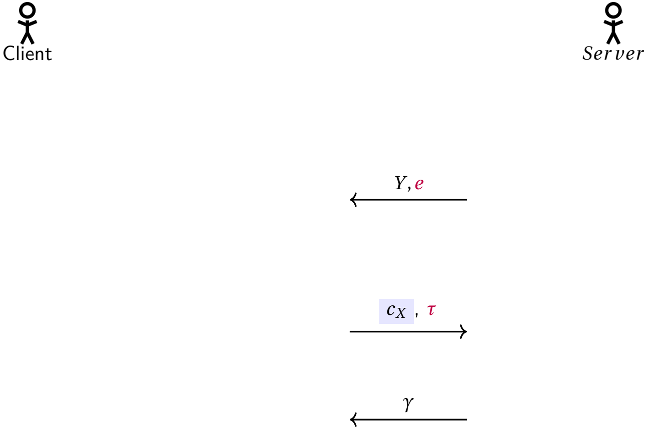
Check τ

$\gamma \leftarrow F(*, \sigma')$

$\xleftarrow{\quad \gamma \quad}$

Check γ

QA-KHAPE-HMQV – simplified



Client

$Server$

Y, e

c_X , τ

γ

QA-KHAPE-HMQV – simplified

Client

Server

~~Not~~ Quantum Annoying

Attacker can

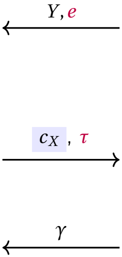
- ~~query $\textsc{DLog}(X) \rightarrow x$~~,
- check $\textrm{PW}_i$

$\rightsquigarrow \mathsf{IC}.D(\textrm{PW}_i, e) \rightarrow a_i, B_i, \mathsf{sk}_i,$

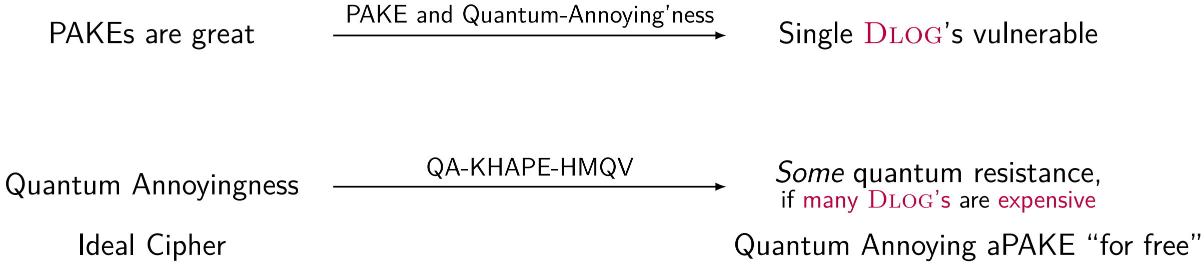
$\mathsf{IC}.D(\mathsf{sk}_i, c_X) \rightarrow X_i,$

query $\textsc{DLog}(X_i) \rightarrow x_i$

until $\tau = F(DH(a_i, B_i, x_i, Y))$



Takeaway



PAKEs are great

PAKE and Quantum-Annoying'ness

Single DLOG's vulnerable

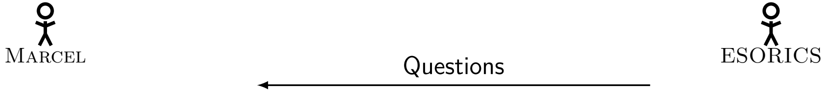
Quantum Annoyingness

QA-KHAPE-HMQV

Some quantum resistance,
if many DLOG's are expensive

Ideal Cipher

Quantum Annoying aPAKE “for free”



“Making an Asymmetric PAKE Quantum-Annoying by Hiding Group Elements”

~~A Short Link to the Paper~~

Marcel Tiepelt, Edward Eaton, Douglas Stebila

marcel.tiepelt@kit.edu