Provable Security Analysis for the Password Authenticated Key Exchange Problem

Ph.D. Thesis Presentation

Presenter: M. Sc. Jose Becerra

Supervisors: Prof. Peter Y. A. Ryan
Dr. Dimiter Ostrev

UNIVERSITÉ DU LUXEMBOURG

May 14, 2019
Esch-sur-Alzette, Luxembourg

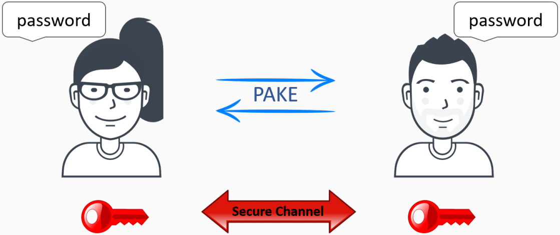
securityandtrust.lu

Table of Contents

Introduction

What is a PAKE

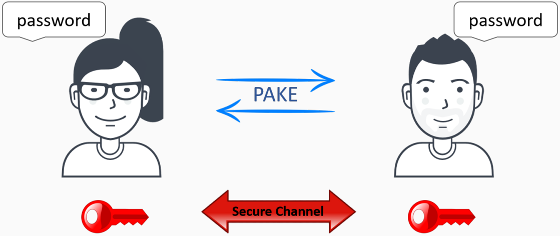
- Password Authenticated Key-Exchange protocol.
- Goal: Establishment of strong cryptographic session keys from low entropy secrets.



- Attacks should be limited to online dictionary attacks only.
  - $\mathcal{A}$ may test at most one password per session during an active attack.

What is a PAKE

- Password Authenticated Key-Exchange protocol.
- Goal: Establishment of strong cryptographic session keys from low entropy secrets.

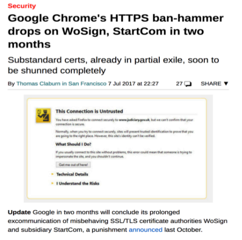


- Attacks should be limited to online dictionary attacks only.
    - $\mathcal{A}$ may test at most one password per session during an active attack.

PAKEs Application I

Build secure channels relying only on shared passwords.

- No need of PKI.



Security

Google Chrome's HTTPS ban-hammer drops on WoSign, StartCom in two months

Substandard certs, already in partial exile, soon to be shunned completely

By Thomas Claburn in San Francisco 7 Jul 2017 at 22:27 27 SHARE ▼

This Connection is Untrusted

You have asked Firefox to connect securely to **www.judiciary.gov.uk**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Update Google in two months will conclude its prolonged excommunication of misbehaving SSL/TLS certificate authorities WoSign and subsidiary StartCom, a punishment announced last October.

Google to Fully Distrust WoSign/StartCom SSL Certs in Chrome 61

Author:
Michael Mimoso
July 10, 2017 / 2:28 pm
2 minute read

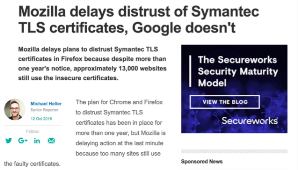
Google has put websites signed with WoSign/StartCom SSL certificates on notice that it will no longer trust certs from the Chinese CA starting in Chrome 61.

Google to punish Symantec for issuing bogus certs

By Juha Saarinen
Mar 24 2017
12:20PM

Will distrust all Symantec certificates gradually, forcing reissue.

Google is tightening the thumbscrews on Symantec for its repeated misissuance of digital certificates via a range of proposed penalty measures.



Mozilla delays distrust of Symantec TLS certificates, Google doesn't

Mozilla delays plans to distrust Symantec TLS certificates in Firefox because despite more than one year's notice, approximately 13,000 websites still use the insecure certificates.

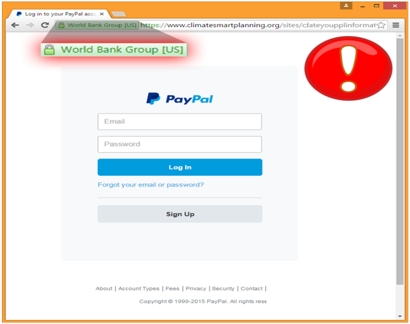
Michael Heller
Senior Reporter
12 Oct 2018

The plan for Chrome and Firefox to distrust Symantec TLS certificates has been in place for more than one year, but Mozilla is delaying action at the last minute because too many sites still use the faulty certificates.

PAKEs Application II

Login scenarios while intrinsically protecting the user's password.

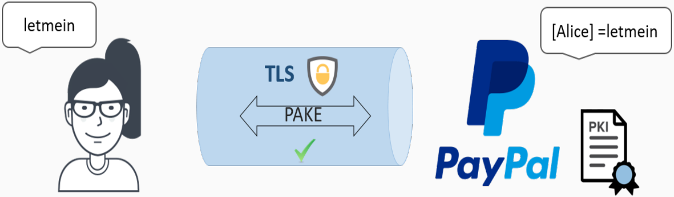
- In 2018, 49% of phishing attacks where performed in https web pages (marked as secure by the browser).
- PAKEs prevent the compromise of the user's password.



PAKEs Application II

Login scenarios while intrinsically protecting the user's password.

- In 2018, 49% of phishing attacks where performed in https web pages (marked as secure by the browser).
- PAKEs prevent the compromise of the user's password.



Motivation and Research Objectives

Our aim is to facilitate the adoption of PAKEs in real-world applications.

1. Examine whether the simulation-based and indistinguishability-based security notions for PAKEs are equivalent.
2. Investigate whether the SPAKE2 protocol provably satisfies some meaningful notion of forward secrecy.
3. Investigate the relevance of tight security reductions for PAKE protocols.

We consider the computational-complexity approach in our analysis.

Relation between SIM-based and IND-based security models

Security Models for PAKEs

IND-based

1. Find then Guess (IND-FtG) [BPR00]
2. Real or Random (IND-RoR) [AFP05]

SIM-based

- Boyko Mackenzie and Patel (SIM-BMP) [BMP00]
- Universally Composable PAKEs (UC) [CHKM05]

Security Models for PAKEs

$$\begin{tikzcd}
\mathit{IND\text{-}RoR} \arrow[d] & \mathit{SIM\text{-}BMP} \\
\mathit{IND\text{-}FtG} & \mathit{SIM\text{-}UC} \arrow[l]
\end{tikzcd}$$

Fig. 1: Known relations between PAKE security definitions.

Security Models for PAKEs

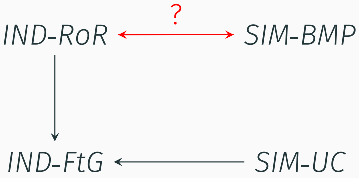


Fig. 2: Known relations between PAKE security definitions.

Real or Random Security Model (IND-RoR)

- Security defined by a game played $\mathcal{CH}$ and $\mathcal{A}$.

$b \in \{0,1\}$

- initUser (U)
- initInstance (U, i, pid)
- Send (U, i, m)
- Execute (U, i, U', i')
- Corrupt (U)
- Test (U, i)
    - if $b = 1$ *real* session key.
    - if $b = 0$ *random* string.

Definition

Protocol P satisfies RoR security if ∀ PPT $\mathcal{A}$:

$$Adv_P^{RoR}(\mathcal{A}) \leq \frac{k}{|D|} + \ negl(\lambda)$$

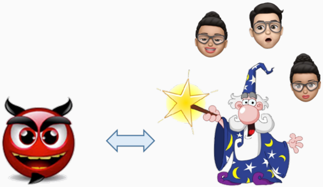
---

k: number of active instances

D: password dictionary

Simulation-based Security Model (SIM-BMP) I

Real World



- Real execution of the protocol.
- The adversary controls the network.

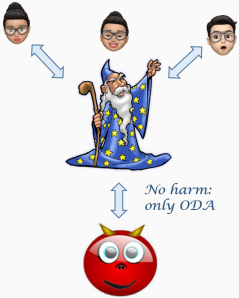
RW adv. is given access to the following queries:

- initUser (U).
- initInstance (U, i, pid).
- Send (U, i, m).
- Corrupt(U)
- Application (f, U, i).

Transcript: $RW(B)$

Simulation-based Security Model (SIM-BMP) II

Ideal World



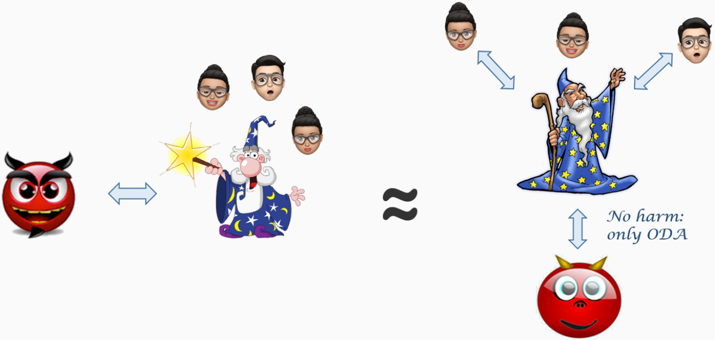
- Defines the ideal functionality for a PAKE.
- Secure by definition.

IW adv. (or simulator) is given access to the following queries:

- initUser (U).
- initInstance (U, i, pid).
- Abort user instance (U, i).
- Test instance password (U, i, π').
- Start session (U, i).
- Application (f, U, i).
- Implementation.

Transcript: $IW(B^*)$

Simulation-based Security Model (SIM-BMP) III



Definition

Protocol P is SIM-BMP secure if:

$$\forall B \;\; \exists B^* \;\; s.t. \;\; RW(B) \approx_c IW(B^*)$$

No assumption is made about the distribution of passwords.

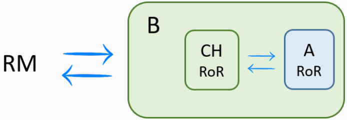
SIM-BMP → IND-RoR I

Theorem (SIM-BMP → IND-RoR)

If protocol P satisfies SIM-BMP security, then P also satisfies IND-RoR security.

SIM-BMP → IND-RoR II

- We construct B from $\mathcal{A}$.

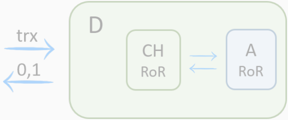


- The output is $RW(B)$.

By SIM-BMP security definition:

$$\forall B \;\; \exists B^{*} \;\; s.t. \;\; RW(B) \approx_{c} IW(B^{*})$$

- Build a distinguisher $\mathcal{D}(trx)$.



$1 \leftarrow \mathcal{D}(\cdot)$ if real-world trx.
$0 \leftarrow \mathcal{D}(\cdot)$ if ideal-world trx.

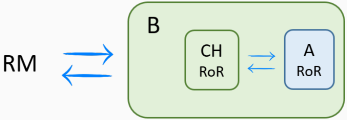
$$Adv_{P}^{RoR}(\mathcal{A}) \leq \frac{k}{|D|} + \;\; negl(\lambda)$$

$\cdots$ then P is IND-RoR secure.

B, B^{*} are real-world and ideal-world adv. in SIM-BMP.
$\mathcal{A}$ is the adv. in RoR.

SIM-BMP → IND-RoR II

- We construct B from $\mathcal{A}$.

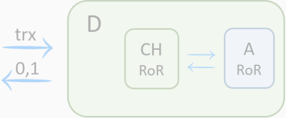


- The output is $RW(B)$.

By SIM-BMP security definition:

$$\forall B \ \ \exists B^* \ \ s.t. \ \ RW(B) \approx_c IW(B^*)$$

- Build a distinguisher $\mathcal{D}(trx)$.



$1 \leftarrow \mathcal{D}(\cdot)$ if real-world trx.
$0 \leftarrow \mathcal{D}(\cdot)$ if ideal-world trx.

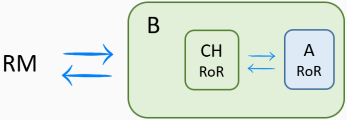
$$Adv_P^{RoR}(\mathcal{A}) \leq \frac{k}{|D|} + \ \ negl(\lambda)$$

$\cdots$ then P is IND-RoR secure.

B, B^* are real-world and ideal-world adv. in SIM-BMP.
$\mathcal{A}$ is the adv. in RoR.

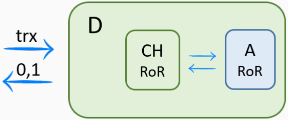
SIM-BMP → IND-RoR II

- We construct B from $\mathcal{A}$.



- The output is $RW(B)$.

- Build a distinguisher $\mathcal{D}(trx)$.



$1 \leftarrow \mathcal{D}(\cdot)$ if real-world trx.
$0 \leftarrow \mathcal{D}(\cdot)$ if ideal-world trx.

By SIM-BMP security definition:

$$\forall B \;\; \exists B^* \;\; s.t. \;\; RW(B) \approx_c IW(B^*)$$

$$Adv_P^{RoR}(\mathcal{A}) \leq \frac{k}{|D|} + \; negl(\lambda)$$

$\cdots$ then P is IND-RoR secure.

B, B^* are real-world and ideal-world adv. in SIM-BMP.
$\mathcal{A}$ is the adv. in RoR.

IND-RoR vs SIM-BMP

$$\begin{tikzcd}
\mathit{IND\text{-}RoR} \arrow[r, dashed, "?"] \arrow[d] & \mathit{SIM\text{-}BMP} \\
\mathit{IND\text{-}FtG} & \mathit{SIM\text{-}UC} \arrow[l]
\end{tikzcd}$$

Fig. 3: Could not prove by contradiction the implication.

SIM Security: Online Dictionary Attacks

SIM-BMP

1. Incorporate in the IW, the non-negligible probability of an adversary guessing the password.
   - **test instance password** (U, i, π').

P is SIM-BMP secure if $\forall\mathcal{D}$:

$$\forall B \;\; \exists B^* \;\; s.t. \;\; RW(B) \approx_c IW(B^*)$$

---

k: number of active instances
D: password dictionary

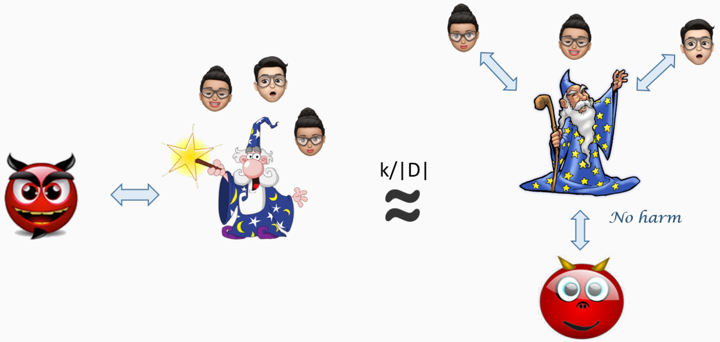
SIM-BMP’

2. Do not incorporate in the IW the non-negligible probability of guessing the password.
   - Relax the indistinguishability requirement.

P is SIM-BMP’ secure if $\forall\mathcal{D}$:

$$\forall B \;\; \exists B^* \;\; s.t. \;\; RW(B) \overset{k/|D|}{\approx} IW(B^*)$$

SIM-BMP' Security Model



Definition

Protocol P is SIM-BMP' secure if:

$$\forall B \ \ \exists B^* \ \ s.t. \ \ RW(B) \overset{k/|D|}{\approx} IW(B^*)$$

SIM-BMP’ Security Model II

Theorem (SIM-BMP’ → IND-RoR)

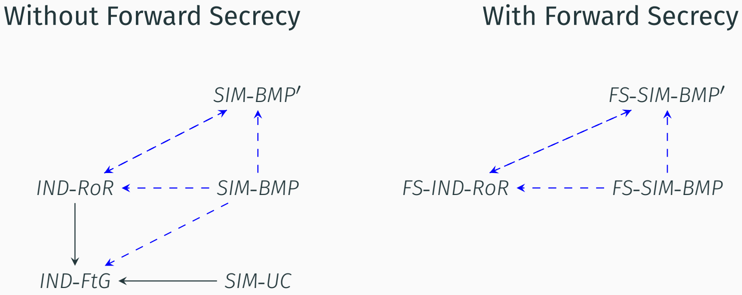
If protocol P satisfies SIM-BMP’ security, then P also satisfies IND-RoR security.

Theorem (IND-RoR → SIM-BMP’)

If protocol P satisfies IND-RoR security, then P also satisfies SIM-BMP’ security.

IND vs SIM Comparison Results

Our results (in blue) are summarized in the following diagram:



Without Forward Secrecy

$$\begin{tikzcd}
 & \mathit{SIM\text{-}BMP'} \arrow[dl, dashed, leftrightarrow] \\
\mathit{IND\text{-}RoR} \arrow[d] & \mathit{SIM\text{-}BMP} \arrow[u, dashed] \arrow[l, dashed] \arrow[dl, dashed] \\
\mathit{IND\text{-}FtG} & \mathit{SIM\text{-}UC} \arrow[l]
\end{tikzcd}$$

With Forward Secrecy

$$\begin{tikzcd}
 & \mathit{FS\text{-}SIM\text{-}BMP'} \arrow[dl, dashed, leftrightarrow] \\
\mathit{FS\text{-}IND\text{-}RoR} & \mathit{FS\text{-}SIM\text{-}BMP} \arrow[u, dashed] \arrow[l, dashed]
\end{tikzcd}$$

Fig. 4: Relation between PAKE security definitions.

Forward Secrecy for SPAKE2

SPAKE2

- PAKE protocol by Abdalla and Pointcheval (CT-RSA 2005).
- One round protocol.
- Currently in the process of standardization by the IEFT.
- Proven secure in the IND-FtG security model (BPR).

... but without *forward secrecy*.

SPAKE2 - Description

Public: $M, N \in \mathbb{G}$; Secret: $\pi \in \mathbb{Z}_q$

$$\begin{array}{rcl}
\text{Client C} & & \text{Server S} \\
x \overset{\$}{\leftarrow} \mathbb{Z}_q, X := g^x & & y \overset{\$}{\leftarrow} \mathbb{Z}_q, Y := g^y \\
X^* := X \cdot M^\pi & & Y^* = Y \cdot N^\pi \\
& \xrightarrow{\quad X^* \quad} & \\
& \xleftarrow{\quad Y^* \quad} & \\
\sigma := (\frac{Y^*}{N^\pi})^x & & \sigma := (\frac{X^*}{M^\pi})^y \\
sk := H(C, S, X^*, Y^*, \sigma, \pi) & & sk := H(C, S, X^*, Y^*, \sigma, \pi)
\end{array}$$

Fig. 5: SPAKE2 protocol.

Forward Secrecy

“It ensures the protection of session keys even if the long-term secret of the participants gets later compromised” [DOW92].

- **Weak Forward Secrecy (wFS).**
  Session keys generated without the active intervention of $\mathcal{A}$, should remain secret to $\mathcal{A}$, regardless any Corrupt query.
- **Perfect Forward Secrecy (PFS).**
  Session keys established **before** any Corrupt (U) query should remain secret to the adversary.
- It is difficult to prove PFS for 1-round protocols with only *implicit authentication.*

Forward Secrecy

“It ensures the protection of session keys even if the long-term secret of the participants gets later compromised” [DOW92].

- **Weak Forward Secrecy (wFS).**
  Session keys generated without the active intervention of $\mathcal{A}$, should remain secret to $\mathcal{A}$, regardless any Corrupt query.
- **Perfect Forward Secrecy (PFS).**
  Session keys established **before** any Corrupt (U) query should remain secret to the adversary.
- It is difficult to prove PFS for 1-round protocols with only *implicit authentication.*

Perfect vs week Forward Secrecy

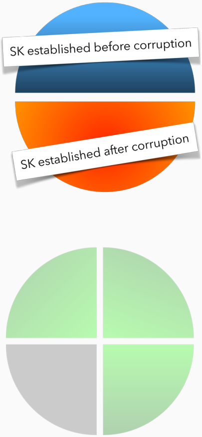


Fig. 6: Sessions protected with PFS.

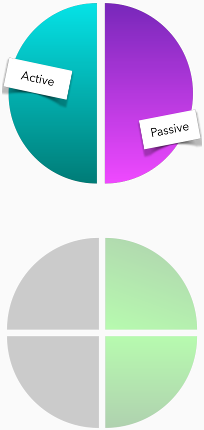


Fig. 7: Sessions protected with wFS.

Perfect vs week Forward Secrecy

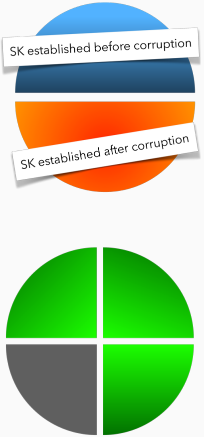


Fig. 6: Sessions protected with PFS.

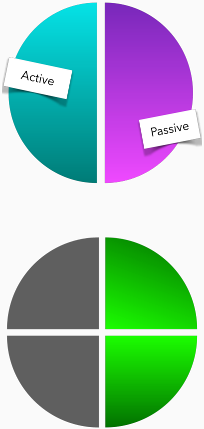


Fig. 7: Sessions protected with wFS.

SPAKE2 - Problematic Scenario

$$\begin{array}{ccc}
\text{Adv. } \mathcal{A}(C) & & \text{Server S} \\
x \overset{\$}{\leftarrow} \mathbb{Z}_q, X := g^x & & y \overset{\$}{\leftarrow} \mathbb{Z}_q, Y := g^y \\
X^* := X \cdot M^{\pi_1} & \xrightarrow{\quad X^* \quad} & Y^* = Y \cdot N^{\pi_c} \\
 & & \sigma := (\frac{X^*}{M^{\pi_c}})^y \\
 & \xleftarrow{\quad Y^* \quad} & sk := H(C, S, X^*, Y^*, \sigma, \pi_c)
\end{array}$$

- An active adversary tries to impersonate C to S.
- Only implicit authentication : Server accepts (and might use) sk without confirming its intended partner.

SPAKE2 - Problematic Scenario

Adv. $\mathcal{A}(C)$ — Server S

$x \leftarrow \mathbb{Z}_q, X := g^x$ — $y \leftarrow \mathbb{Z}_q, Y := g^y$

$X^* := X \cdot M^{\pi_1}$ $\xrightarrow{X^*}$ $Y^* = Y \cdot N^{\pi_c}$

$\sigma := \left(\frac{X^*}{M^{\pi_c}}\right)^y$

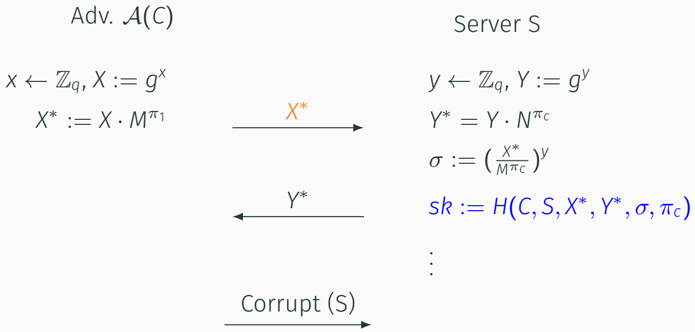
$\xleftarrow{Y^*}$ $sk := H(C, S, X^*, Y^*, \sigma, \pi_c)$

$\vdots$

$\xrightarrow{\text{Corrupt (S)}}$

1. Perfect Forward Secrecy.
    - *sk* must be secret to $\mathcal{A}$.
2. Weak Forward Secrecy.
    - Does not guarantee the secrecy of *sk*.

SPAKE2 - Problematic Scenario



Adv. $\mathcal{A}(C)$

$x \leftarrow \mathbb{Z}_q, X := g^x$

$X^* := X \cdot M^{\pi_1}$

$\xrightarrow{X^*}$

Server S

$y \leftarrow \mathbb{Z}_q, Y := g^y$

$Y^* = Y \cdot N^{\pi_c}$

$\sigma := (\frac{X^*}{M^{\pi_c}})^y$

$\xleftarrow{Y^*}$

$sk := H(C, S, X^*, Y^*, \sigma, \pi_c)$

$\vdots$

$\xrightarrow{\text{Corrupt (S)}}$

1. Perfect Forward Secrecy.
    - sk must be secret to $\mathcal{A}$.
2. Weak Forward Secrecy.
    - Does not guarantee the secrecy of sk.

SPAKE2 - weak Forward Secrecy

Theorem

SPAKE2 is secure in the BPR model with weak Forward Secrecy under the CDH and CSDH assumptions:

$$\mathrm{Adv}_{P}^{\mathrm{wFS\text{-}FtG}}(\mathcal{A}) \leq \frac{n_{se}}{|D|} + \mathcal{O}\left(\frac{(n_{se}+n_{ex})(n_{se}+n_{ex}+n_{ro})}{q} + n_{ro}\cdot\mathrm{Adv}_{\mathbb{G}}^{\mathsf{CDH}}(\mathcal{B}^{\mathcal{A}}) + n_{se}n_{ro}\cdot\mathrm{Adv}_{\mathbb{G}}^{\mathsf{CDH}}(\hat{\mathcal{B}}^{\mathcal{A}}) + (n_{ro})^2\cdot\mathrm{Adv}_{\mathbb{G}}^{\mathsf{CSDH}}(\tilde{\mathcal{B}}^{\mathcal{A}})\right).$$

D: password dictionary

n_{se}: number of Send queries

n_{ex}: number of Execute queries

n_{ro}: number of random oracle queries

PFS-SPAKE2

- Incorporating key-confirmation codes to SPAKE2 results in PFS-SPAKE2.
    - Explicit mutual authentication.
    - Remove one CRS.
    - Computationally more efficient (client side).

PFS-SPAKE2 Description

Public: $M \in \mathbb{G}$; Secret: $\pi \in \mathbb{Z}_q, \pi \neq 0$

$$
\begin{array}{rcl}
\text{Client C} & & \text{Server S} \\
x \overset{\$}{\leftarrow} \mathbb{Z}_q, X := g^x & & \\
X^* := X \cdot M^\pi & \xrightarrow{\quad C, X^* \quad} & y \overset{\$}{\leftarrow} \mathbb{Z}_q, Y := g^y \\
 & & \sigma := \left(\frac{X^*}{M^\pi}\right)^y \\
\sigma := Y^x & \xleftarrow{\quad Y, k \quad} & k := H_1(C, S, X^*, Y, \sigma, \pi) \\
k \overset{?}{=} H_1(C, S, X^*, Y, \sigma, \pi) & & \\
k' := H_2(C, S, X^*, Y, \sigma, \pi) & & \\
sk := H_3(C, S, X^*, Y, \sigma, \pi) & \xrightarrow{\quad k' \quad} & k' \overset{?}{=} H_2(C, S, X^*, Y, \sigma, \pi) \\
 & & sk := H_3(C, S, X^*, Y, \sigma, \pi)
\end{array}
$$

PFS-SPAKE2 - Security

Theorem

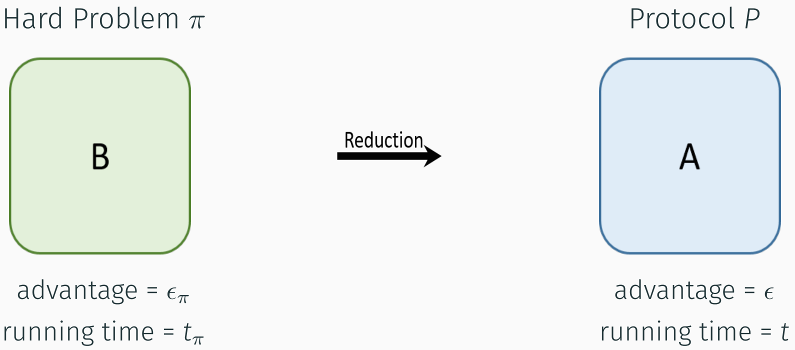
PFS-SPAKE2 is secure in the BPR model with Perfect Forward Secrecy under the CDH assumption:

$$\mathrm{Adv}_P^{\mathrm{wFS\text{-}FtG}}(\mathcal{A}) \leq \frac{n_{se}}{|D|} + \mathcal{O}\left(\frac{(n_{se}+n_{ex})(n_{se}+n_{ex}+n_{ro})}{q} + n_{ro}\cdot\mathrm{Adv}_{\mathbb{G}}^{\mathsf{CDH}}(\mathcal{B}^{\mathcal{A}}) \;+\; n_{se}n_{ro}\cdot\mathrm{Adv}_{\mathbb{G}}^{\mathsf{CDH}}(\hat{\mathcal{B}}^{\mathcal{A}}) + (n_{ro})^2\cdot\mathrm{Adv}_{\mathbb{G}}^{\mathsf{CDH}}(\tilde{\mathcal{B}}^{\mathcal{A}})\right).$$

D: password dictionary
n_{se}: number of Send queries
n_{ex}: number of Execute queries
n_{ro}: number of random oracle queries

Tight Security Reductions

Tight Reductions


Hard Problem π

Protocol P

advantage = ϵ_π

running time = t_π

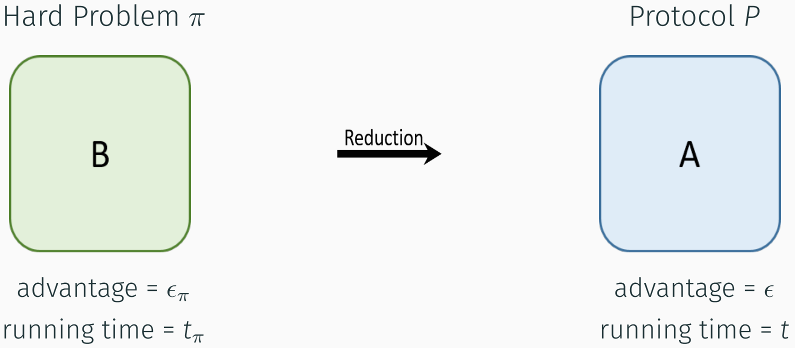
advantage = ϵ

running time = t

An **adversary** running in time t with advantage ϵ give us a π**-solver** running in time t_π with advantage ϵ_π.

- The protocol is secure if such solver does not exist.

Tight Reductions


Hard Problem π

Protocol P

advantage = ϵ_π

running time = t_π

advantage = ϵ

running time = t

The reduction is tight if

$$\frac{\epsilon}{t} = c \cdot \frac{\epsilon_\pi}{t_\pi}.$$

- Preserve strength of hardness assumption.

Why Tight Reductions?

The reduction is not tight if: $\epsilon >> \epsilon_\pi$ or $t_\pi >> t$.

- $\epsilon \leq L \cdot \epsilon_\pi$, for large L: security degradation factor.

For instance consider:

- Desired security level of 150 bits for the protocol.
- L = 2^{40} degradation factor.

$$\epsilon \leq L \cdot \epsilon_\pi$$

$$2^{-150} = 2^{40} \cdot 2^{-190}$$

- Then the hardness assumption needs to provide at least 190 bits of security → larger parameters and less efficient impl.

PAK Protocol

- Boyko, Mackenzie and Patel 2001.
- PAKE protocol with explicit mutual authentication.
- Low computation and communication cost.
- Satisfies forward secrecy.
- Currently under consideration by IETF for standardization.
  - Patent expired in 2017.

Initialization

Public: $\mathbb{G}, g, q; \quad H : \{0,1\}^* \to \mathbb{G};$

$H_1, H_2, H_3 : \{0,1\}^* \to \{0,1\}^k;$

Client		Server
Secret: π		$\pi_S[C] = (H(\pi_C))^{-1}$
$x \xleftarrow{\$} \mathbb{Z}_q, \alpha := g^x$		
$\gamma := H_1(\pi)$		
$m := \alpha \cdot \gamma$	$\xrightarrow{C, m}$	$y \xleftarrow{\$} \mathbb{Z}_q, \mu := g^y$
		$\gamma' := \pi_S[C]$
		$\sigma := (m \cdot \gamma')^y$, i.e. $\sigma = DH(\alpha, \mu)$
		$k := H_2(C, S, m, \mu, \sigma, \gamma')$
		$k'' := H_3(C, S, m, \mu, \sigma, \gamma')$
$\sigma := \mu^x$, i.e. $\sigma = DH(\alpha, \mu)$	$\xleftarrow{\mu, k}$	$sk := H_4(C, S, m, \mu, \sigma, \gamma')$
$\gamma' := \gamma^{-1}$		
abort if $k \neq H_2(C, S, m, \mu, \sigma, \gamma')$		
$k' := H_3(C, S, m, \mu, \sigma, \gamma')$		
$sk := H_4(C, S, m, \mu, \sigma, \gamma')$	$\xrightarrow{k'}$	abort if $k' \neq k''$

Fig. 8: PAK protocol.

Non-tight Reduction in PAK I

PAK security proof is not tight:

$$\mathrm{Adv}_{\mathbb{G}}^{PAK}(\mathcal{A}) \leq \frac{n_{se}}{|D|} + \mathcal{O}\left(n_{se} \cdot (n_{ro})^2 \cdot \mathrm{Adv}_{\mathbb{G}}^{\mathsf{CDH}}(\mathcal{B}^{\mathcal{A}})\right)$$

We consider realistic parameters:

- $\mathbb{G}$ has order $q = 2^{256} \rightarrow \mathrm{Adv}_{\mathbb{G}}^{\mathsf{CDH}} \leq 2^{-128}$.
- $n_{se} \approx 2^{30}$: Number of Send queries.
- $n_{ro} \approx 2^{63}$: Number of random oracle queries.

$n_{se} \cdot (n_{ro})^2 \cdot \mathrm{Adv}_{\mathbb{G}}^{\mathsf{CDH}}(\mathcal{B}^{\mathcal{A}}) >> 1$ ... is meaningless.

Non-tight Reduction in PAK II

- Instantiation over prime order groups.
    - Both CDH and DDH are hard.
- Security proof relies on the CDH assumption and RO model.
- Construct a CDH-solver algorithm:

$$H(m, \mu, \cdots, \sigma_1, \pi)$$

$$H(m, \mu, \cdots, \sigma_2, \pi)$$

$$\vdots$$

$$H(m, \mu, \cdots, \sigma_{ro}, \pi)$$

How can the simulator choose the correct σ s.t.

$$\sigma = DH\left(\frac{m}{H(\pi)}, \mu\right)$$

$\cdots$ possible with a DDH-oracle.

Non-tight Reduction in PAK II

- Instantiation over prime order groups.
    - Both CDH and DDH are hard.
- Security proof relies on the CDH assumption and RO model.
- Construct a CDH-solver algorithm:

$$H(m, \mu, \cdots, \sigma_1, \pi)$$

$$H(m, \mu, \cdots, \sigma_2, \pi)$$

$$\vdots$$

$$H(m, \mu, \cdots, \sigma_{ro}, \pi)$$

How can the simulator choose the correct σ s.t.

$$\sigma = DH\left(\frac{m}{H(\pi)}, \mu\right)$$

$\cdots$ possible with a DDH-oracle.

Non-tight Reduction in PAK II

- Instantiation over prime order groups.
  - Both CDH and DDH are hard.
- Security proof relies on the CDH assumption and RO model.
- Construct a CDH-solver algorithm:

$$H(m, \mu, \cdots, \sigma_1, \pi)$$

$$H(m, \mu, \cdots, \sigma_2, \pi)$$

$$\vdots$$

$$H(m, \mu, \cdots, \sigma_{ro}, \pi)$$

How can the simulator choose the correct σ s.t.

$$\sigma = DH\left(\frac{m}{H(\pi)}, \mu\right)$$

$\cdots$ possible with a DDH-oracle.

Tightly-secure PAK

Our solution:

- Instantiate PAK over Gap Diffie-Hellman groups, e.g. *billinear groups*.
- Tight reduction from Gap-DH.

Theorem

$$Adv^{PAK}(\mathcal{A}) \leq \frac{n_{se}}{|D|} + 8 \cdot Adv_{\mathbb{G}}^{Gap\text{-}DH}(\mathcal{B}^{\mathcal{A}})$$

More efficient implementations.

- PAK and $\mathbb{G}$ provide the same security level w.r.t. the Gap-DH problem.

Tightly-secure PAK

Our solution:

- Instantiate PAK over Gap Diffie-Hellman groups, e.g. *billinear groups*.
- Tight reduction from Gap-DH.

Theorem

$$Adv^{PAK}(\mathcal{A}) \leq \frac{n_{se}}{|D|} + 8 \cdot Adv_{\mathbb{G}}^{Gap\text{-}DH}(\mathcal{B}^{\mathcal{A}})$$

More efficient implementations.

- PAK and $\mathbb{G}$ provide the same security level w.r.t. the Gap-DH problem.

Summary

Summary of our Contributions

- Proved that the original SPAKE2 satisfies weak Forward Secrecy.
    - SPAKE2 with key-confirmation codes satisfies Perfect Forward Secrecy.
- Tight security reduction for the PAK protocol.
    - The same technique could be applied to other EKE-based protocols, e.g. PPK, SPAKE2.
- Comparison between SIM-BMP and IND-RoR security models for PAKEs.
    - SIM-BMP $\longrightarrow$ IND-RoR.
    - SIM-BMP' $\longleftrightarrow$ IND-RoR.

Q & A

Thanks !!!