The Pre-Shared Key Modes of HPKE

Joël Alwen[1], Jonas Janneck[2], Eike Kiltz[2], Benjamin Lipp[3]

[1]AWS-Wickr, [2]Ruhr-Universität Bochum, [3]Max Planck Institute for Security and Privacy

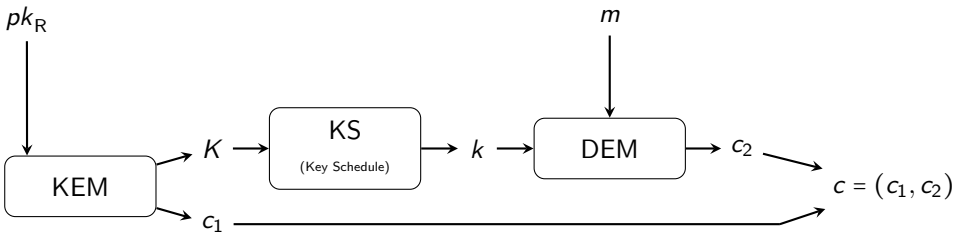
Asiacrypt 2023
December 7, 2023

Overview

1. Hybrid Public Key Encryption (HPKE)
2. Modeling Pre-Shared Key (PSK) Modes of HPKE
3. Security
4. Post-Quantum Security

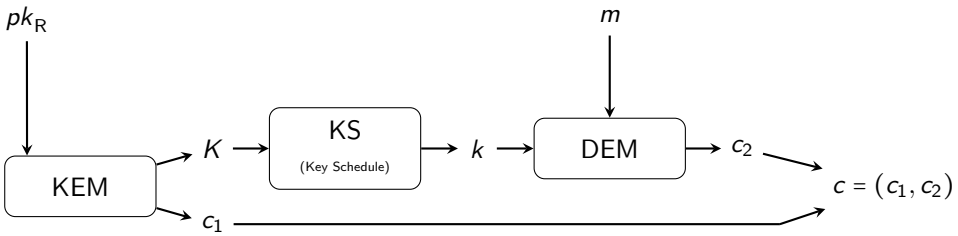
Overview

Hybrid Public Key Encryption (HPKE)



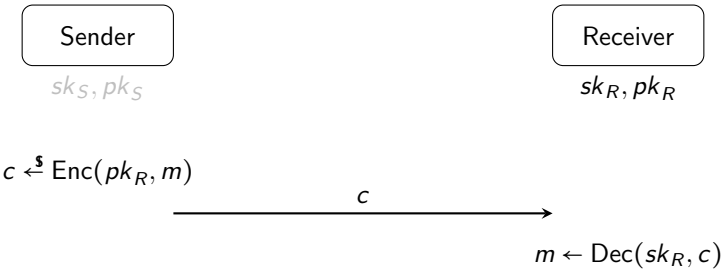
- Follows KEM/DEM paradigm

Hybrid Public Key Encryption (HPKE)

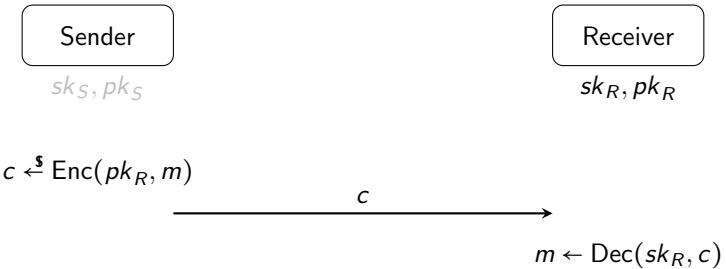


- Follows KEM/DEM paradigm
- Published as RFC 9180 by the Internet Research Task Force [BBLW22]
- Used in TLS 1.3 Encrypted Client Hello Extension, Message Layer Security (MLS), Oblivious DNS over HTTPS, ...

HPKE – Base Mode

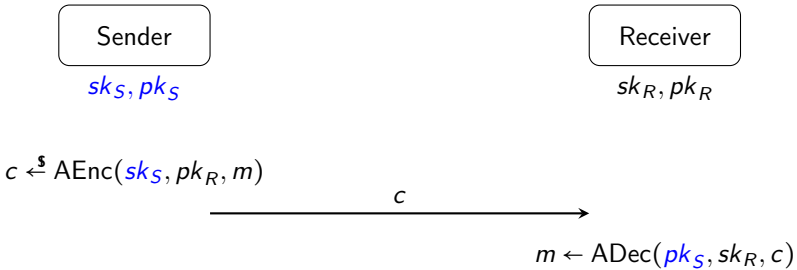


HPKE – Base Mode



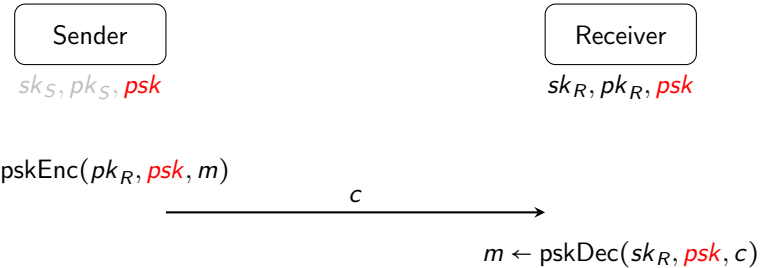
Mode	Sender Key	PSK	Primitive	Security	Source
$\mathrm{HPKE}_{\mathrm{Base}}$	–	–	PKE	CCA	folklore

HPKE – Auth Mode



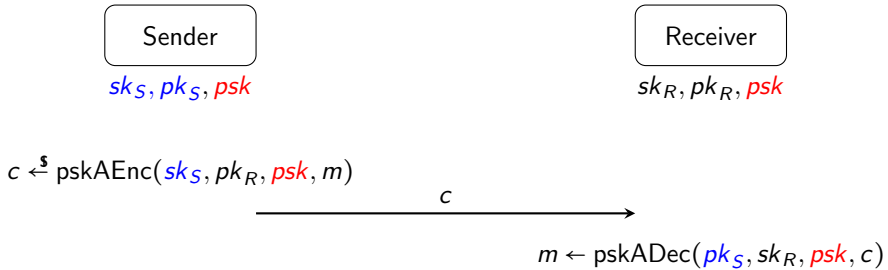
Mode	Sender Key	PSK	Primitive	Security	Source
$\mathsf{HPKE}_{\mathsf{Base}}$	–	–	PKE	CCA	folklore
$\mathsf{HPKE}_{\mathsf{Auth}}$	$\surd$	–	APKE	Insider-CCA & Outsider-Auth	[ABH+21]

HPKE – PSK Mode



Mode	Sender Key	PSK	Primitive	Security	Source
$\mathsf{HPKE}_{\mathsf{Base}}$	–	–	PKE	CCA	folklore
$\mathsf{HPKE}_{\mathsf{Auth}}$	$\surd$	–	APKE	Insider-CCA & Outsider-Auth	[ABH+21]
$\mathsf{HPKE}_{\mathsf{PSK}}$	–	$\surd$	?	?	

HPKE – AuthPSK Mode



Mode	Sender Key	PSK	Primitive	Security	Source
$\text{HPKE}_{\text{Base}}$	–	–	PKE	CCA	folklore
$\text{HPKE}_{\text{Auth}}$	$\surd$	–	APKE	Insider-CCA & Outsider-Auth	[ABH+21]
HPKE_{PSK}	–	$\surd$	?	?	
$\text{HPKE}_{\text{AuthPSK}}$	$\surd$	$\surd$	?	?	

Filling the Gaps

1. Modeling syntax and security of PSK modes
2. Proving security (confidentiality and authenticity)

Mode	Sender Key	PSK	Primitive	Security	Source
$\mathsf{HPKE}_{\mathsf{Base}}$	–	–	PKE	CCA	folklore
$\mathsf{HPKE}_{\mathsf{Auth}}$	$\surd$	–	APKE	Insider-CCA & Outsider-Auth	[ABH+21]
$\mathsf{HPKE}_{\mathsf{PSK}}$	–	$\surd$	pskPKE	CCA & Auth	This work
$\mathsf{HPKE}_{\mathsf{AuthPSK}}$	$\surd$	$\surd$	pskAPKE	Insider-CCA & Outsider-Auth	This work

Overview

Syntax

Mode	Sender Key	PSK	Primitive	Security	Source
$\mathsf{HPKE}_{\mathsf{Base}}$	–	–	PKE	CCA	folklore
$\mathsf{HPKE}_{\mathsf{Auth}}$	$\surd$	–	APKE	Insider-CCA & Outsider-Auth	[ABH+21]
$\mathsf{HPKE}_{\mathsf{PSK}}$	–	$\surd$	pskPKE	CCA & Auth	This work
$\mathsf{HPKE}_{\mathsf{AuthPSK}}$	$\surd$	$\surd$	pskAPKE	Insider-CCA & Outsider-Auth	This work

$\mathsf{pskPKE} \coloneqq (\mathsf{GenSK}, \mathsf{GenPSK}, \mathsf{pskEnc}, \mathsf{pskDec})$

- $(sk, pk) \xleftarrow{\$} \mathsf{GenSK}$
- $psk \xleftarrow{\$} \mathsf{GenPSK}$
- $c \xleftarrow{\$} \mathsf{pskEnc}(pk_R, psk, m)$
- $m \leftarrow \mathsf{pskDec}(sk_R, psk, c)$

Syntax

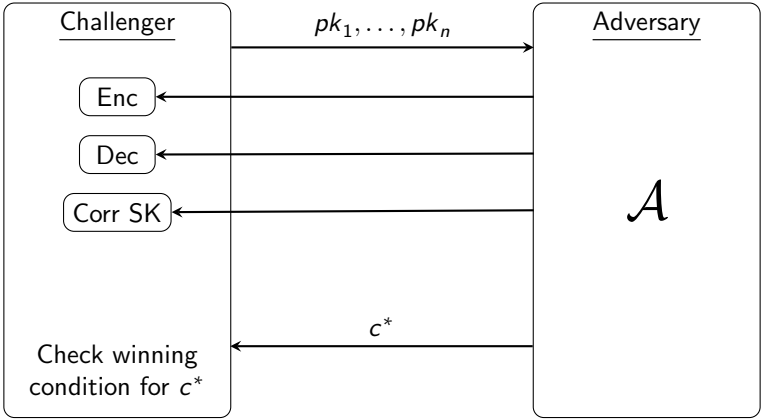
Mode	Sender Key	PSK	Primitive	Security	Source
$\mathsf{HPKE}_{\mathsf{Base}}$	–	–	PKE	CCA	folklore
$\mathsf{HPKE}_{\mathsf{Auth}}$	$\surd$	–	APKE	Insider-CCA & Outsider-Auth	[ABH+21]
$\mathsf{HPKE}_{\mathsf{PSK}}$	–	$\surd$	pskPKE	CCA & Auth	This work
$\mathsf{HPKE}_{\mathsf{AuthPSK}}$	$\surd$	$\surd$	pskAPKE	Insider-CCA & Outsider-Auth	This work

$\mathsf{pskAPKE} \coloneqq (\mathsf{GenSK}, \mathsf{GenPSK}, \mathsf{pskAEnc}, \mathsf{pskADec})$

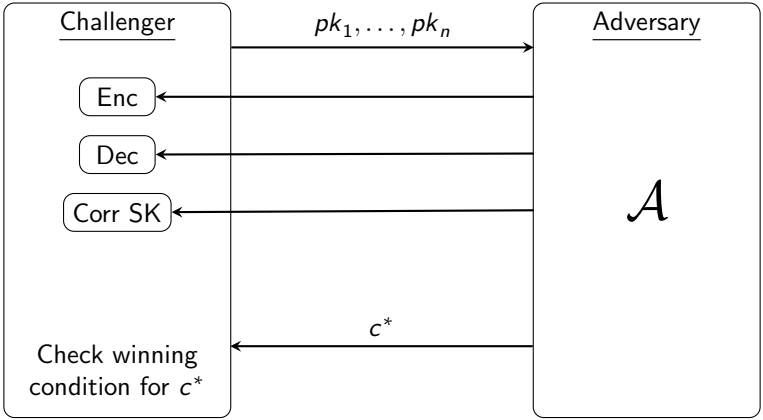
- $(sk, pk) \xleftarrow{\$} \mathsf{GenSK}$
- $psk \xleftarrow{\$} \mathsf{GenPSK}$
- $c \xleftarrow{\$} \mathsf{pskAEnc}(sk_S, pk_R, psk, m)$
- $m \leftarrow \mathsf{pskADec}(pk_S, sk_R, psk, c)$

Outsider-Auth for APKE [ABH+21]

Outsider-Auth for APKE [ABH+21]



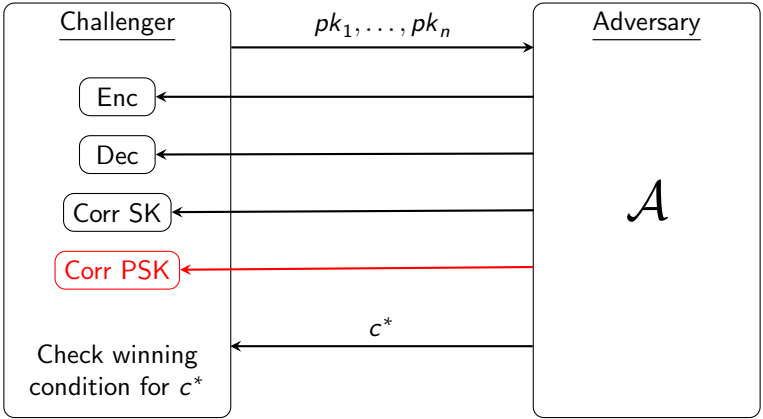
Outsider-Auth for APKE [ABH+21]



Winning condition:

- Fresh and valid ciphertext
- Sender secret key corresponding to c^* is not corrupted

Outsider-Auth for pskAPKE



Winning condition:

- Fresh and valid ciphertext
- Sender secret key and pre-shared key corresponding to c^* are not both corrupted

Overview

Security – Overview

Four generic composition theorems for hybrid constructions

Primitive	Confidentiality	Authenticity
pskPKE		
pskAPKE		

Security – Overview

Four generic composition theorems for hybrid constructions

Primitive	Confidentiality	Authenticity
pskPKE	Thm. 1 **CCA**	Thm. 2 **Auth**
pskAPKE		

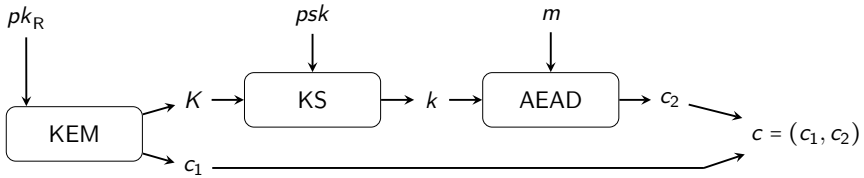
Security – Overview

Four generic composition theorems for hybrid constructions

Primitive	Confidentiality	Authenticity
pskPKE	Thm. 1 **CCA**	Thm. 2 **Auth**
pskAPKE	Thm. 3 **Insider** – **CCA** (implies Outsider-CCA)	Thm. 4 **Outsider** – **Auth**

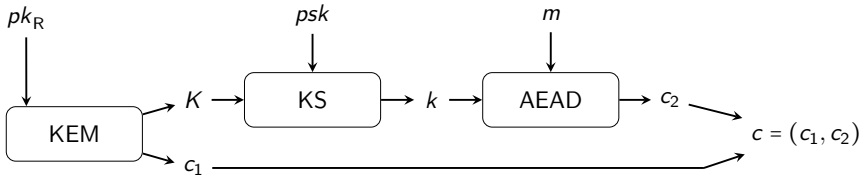
Security – pskPKE

Mode $\mathsf{HPKE}_{\mathsf{PSK}}$:



Security – pskPKE

Mode $\mathsf{HPKE}_{\mathsf{PSK}}$:

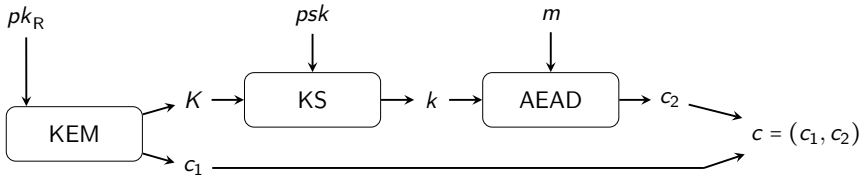


Theorem 1 (CCA security)

KEM **CCA** + KS **dual-PRF** + AEAD **CCA** ⇒ pskPKE **CCA**

Security – pskPKE

Mode $\mathsf{HPKE}_{\mathsf{PSK}}$:



Theorem 1 (CCA security)

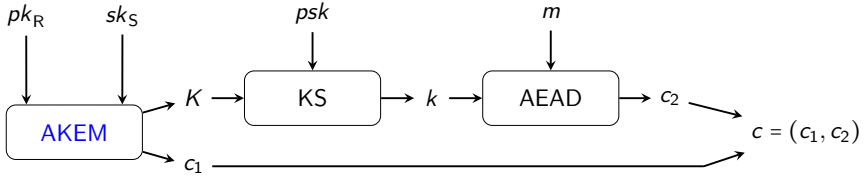
KEM **CCA** + KS **dual-PRF** + AEAD **CCA** ⇒ pskPKE **CCA**

Theorem 2 (Auth security)

KEM **CCA** + KS **dual-PRF** + AEAD **INT-CTXT** ⇒ pskPKE **Auth**

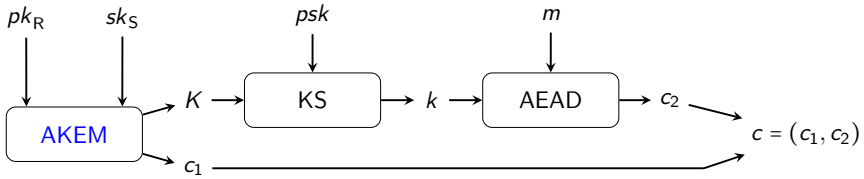
Security – pskAPKE

Mode $\mathsf{HPKE}_{\mathsf{AuthPSK}}$:



Security – pskAPKE

Mode $\mathsf{HPKE}_{\mathsf{AuthPSK}}$:

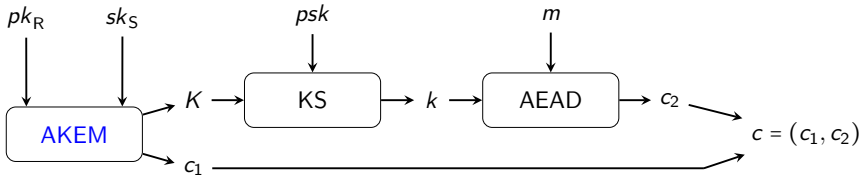


Theorem 3 (Insider-CCA security)

AKEM **Insider-CCA** + KS **dual-PRF** + AEAD **CCA** ⇒ pskAPKE **Insider-CCA**

Security – pskAPKE

Mode $\mathsf{HPKE}_{\mathsf{AuthPSK}}$:



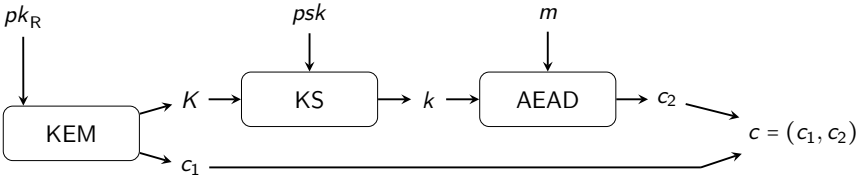
Theorem 3 (Insider-CCA security)

AKEM **Insider-CCA** + KS **dual-PRF** + AEAD **CCA** ⇒ pskAPKE **Insider-CCA**

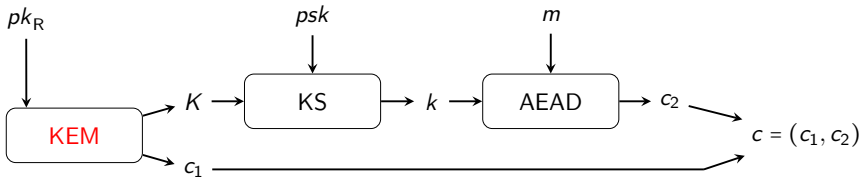
Theorem 4 (Outsider-Auth security)

AKEM **Outsider-CCA** + AKEM **Outsider-Auth** + KS **dual-PRF** + AEAD **INT-CTXT** ⇒ pskAPKE **Outsider-Auth**

RFC Specification: $\mathsf{HPKE}_{\mathsf{PSK}}$

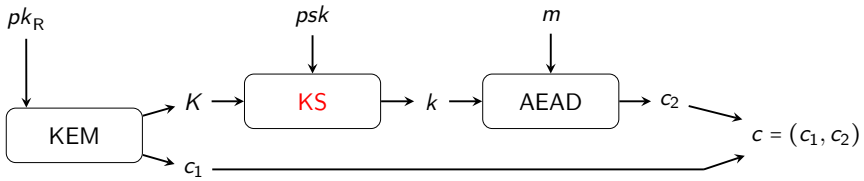


RFC Specification: $\mathsf{HPKE}_{\mathsf{PSK}}$



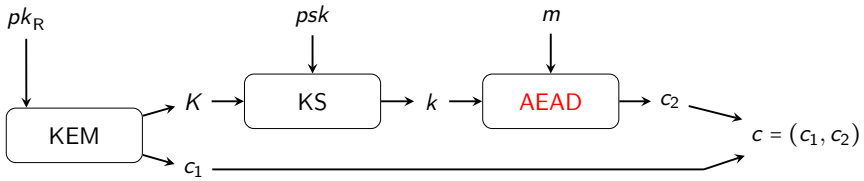
- (1) KEM: basic Diffie-Hellman KEM fulfilling CCA security

RFC Specification: HPKE_{PSK}



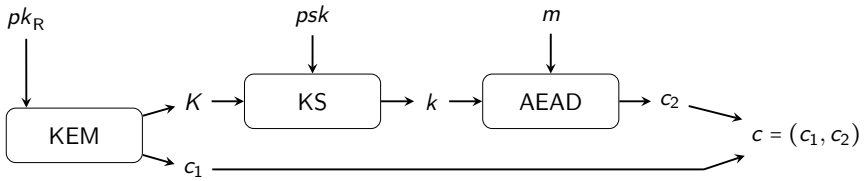
- (1) KEM: basic Diffie-Hellman KEM fulfilling CCA security
- (2) KS: based on HMAC-SHA2, is dual PRF if HMAC is a dual PRF

RFC Specification: $\mathrm{HPKE}_{\mathrm{PSK}}$



- (1) KEM: basic Diffie-Hellman KEM fulfilling CCA security
- (2) KS: based on HMAC-SHA2, is dual PRF if HMAC is a dual PRF
- (3) AEAD: AES-GCM or ChaCha20-Poly1305 fulfilling IND-CPA and INT-CTXT security [BT16, DGGP21]

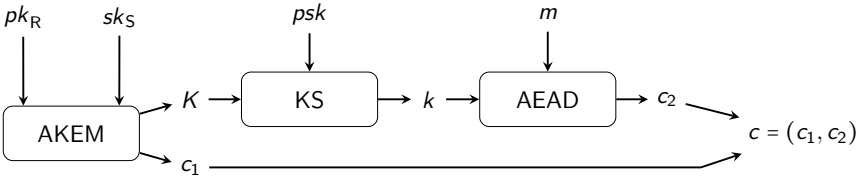
RFC Specification: $\mathsf{HPKE}_{\mathsf{PSK}}$



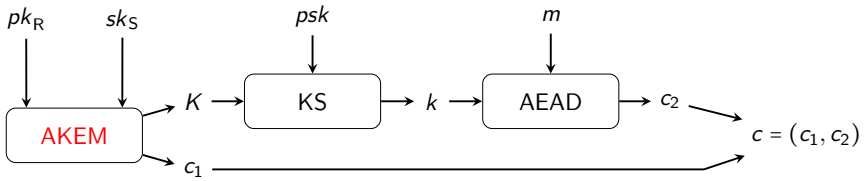
- (1) KEM: basic Diffie-Hellman KEM fulfilling CCA security
- (2) KS: based on HMAC-SHA2, is dual PRF if HMAC is a dual PRF
- (3) AEAD: AES-GCM or ChaCha20-Poly1305 fulfilling IND-CPA and INT-CTXT security [BT16, DGGP21]

$$(\mathbf{1}) + (\mathbf{2}) + (\mathbf{3}) \overset{\text{Thm.1+2}}{\Rightarrow} \textbf{CCA and Auth}$$

RFC Specification: $\mathsf{HPKE}_{\mathsf{AuthPSK}}$

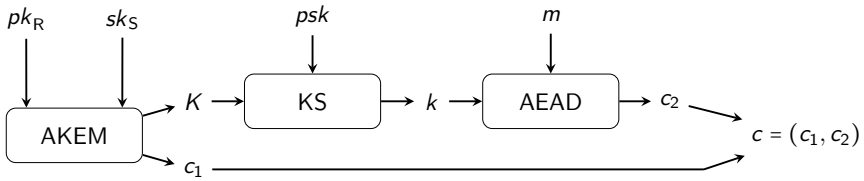


RFC Specification: $\text{HPKE}_{\text{AuthPSK}}$



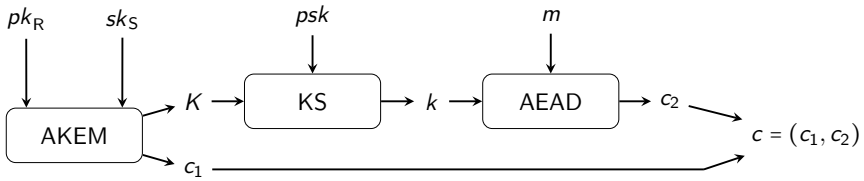
- (1) AKEM: adaption of DH-KEM and proved Insider-CCA and Outsider-Auth-secure under Gap Diffie-Hellmann assumption [ABH+21]

RFC Specification: $\text{HPKE}_{\text{AuthPSK}}$



- (1) AKEM: adaption of DH-KEM and proved Insider-CCA and Outsider-Auth-secure under Gap Diffie-Hellmann assumption [ABH+21]
- (2) KS: as before
- (3) AEAD: as before

RFC Specification: $\text{HPKE}_{\text{AuthPSK}}$



- (1) AKEM: adaption of DH-KEM and proved Insider-CCA and Outsider-Auth-secure under Gap Diffie-Hellmann assumption [ABH+21]
- (2) KS: as before
- (3) AEAD: as before

$$(\mathbf{1}) + (\mathbf{2}) + (\mathbf{3}) \overset{\text{Thm.3+4}}{\Rightarrow} \textbf{Insider-CCA and Outsider-Auth}$$

Overview

Post-Quantum HPKE

- We need the underlying primitives to be post-quantum secure
  - KEM ✓
  - AKEM ?

Post-Quantum HPKE

- We need the underlying primitives to be post-quantum secure
  - KEM ✓
  - AKEM ?
- We introduce two AKEM constructions:
  - KEM + Signature + Hash (PRF)
  - NIKE + Hash (PRF)

Classical/Post-Quantum Hybrid

Classical/Post-Quantum Hybrid

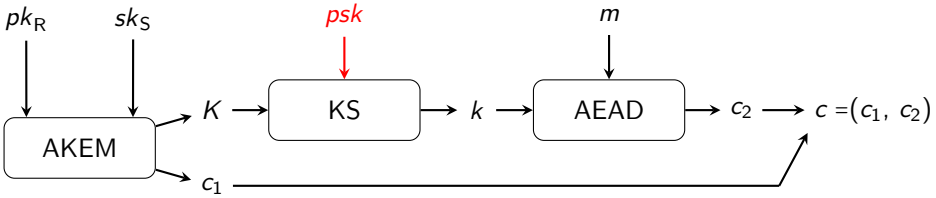
- Goal: Build a classical/post-quantum hybrid (A)PKE
- Relies on classical (C) and post-quantum (PQ) assumptions

Classical/Post-Quantum Hybrid

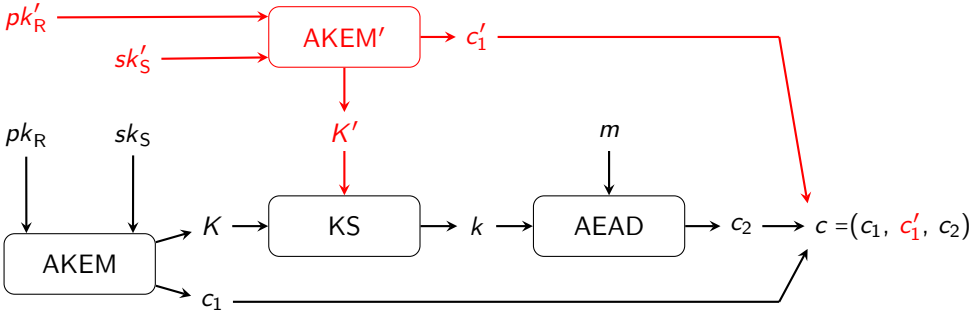
- Goal: Build a classical/post-quantum hybrid (A)PKE
- Relies on classical (C) and post-quantum (PQ) assumptions
- Direct plug-in construction from HPKE PSK modes::

$$\text{PQ KEM} + \text{pskPKE} \Rightarrow \text{C/PQ PKE}$$
$$\text{PQ AKEM} + \text{pskAPKE} \Rightarrow \text{C/PQ APKE}$$

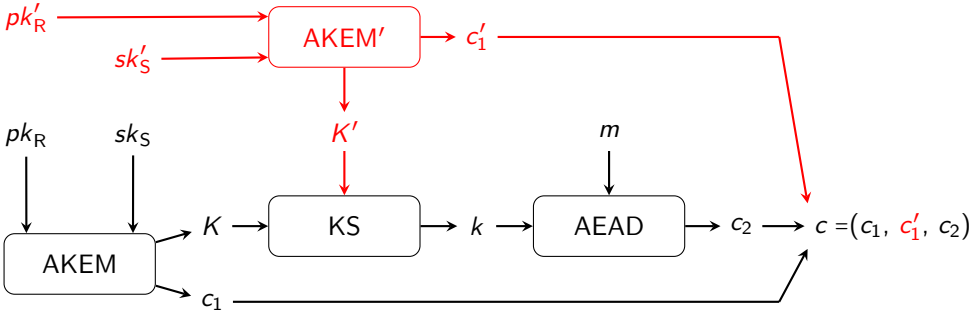
Hybrid From HPKE PSK Modes



Hybrid From HPKE PSK Modes



Hybrid From HPKE PSK Modes



Theorem 5

If KS, AEAD, *and (*AKEM *or* AKEM′*) are secure, then* APKE *is secure.*

Summary

Contributions:

Summary

Contributions:

- Security model for pskPKE and pskAPKE

Summary

Contributions:

- Security model for pskPKE and pskAPKE
- Security proofs of pre-shared key modes of HPKE

Summary

Contributions:

- Security model for pskPKE and pskAPKE
- Security proofs of pre-shared key modes of HPKE
- Two post-quantum AKEM constructions

Summary

Contributions:

- Security model for pskPKE and pskAPKE
- Security proofs of pre-shared key modes of HPKE
- Two post-quantum AKEM constructions
- Post-quantum security and plug-in hybrid construction

Credit: [Mas09]

Summary

Contributions:

- Security model for pskPKE and pskAPKE
- Security proofs of pre-shared key modes of HPKE
- Two post-quantum AKEM constructions
- Post-quantum security and plug-in hybrid construction

ia.cr/2023/1480

jonas.janneck@rub.de

Credit: [Mas09]

References I


Joël Alwen, Bruno Blanchet, Eduard Hauck, Eike Kiltz, Benjamin Lipp, and Doreen Riepel.
Analysing the HPKE standard.
In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part I*, volume 12696 of *LNCS*, pages 87–116. Springer, Heidelberg, October 2021.


Richard L. Barnes, Karthik Bhargavan, Benjamin Lipp, and Christopher A. Wood.
Hybrid public key encryption.
RFC 9180, RFC Editor, February 2022.


Mihir Bellare and Björn Tackmann.
The multi-user security of authenticated encryption: AES-GCM in TLS 1.3.
In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part I*, volume 9814 of *LNCS*, pages 247–276. Springer, Heidelberg, August 2016.

References II

Jean Paul Degabriele, Jérôme Govinden, Felix Günther, and Kenneth G Paterson.
The security of chacha20-poly1305 in the multi-user setting.
In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pages 1981–2003, 2021.

Luca Mascaro.
Cc by-sa 2.0 via wikimedia commons.
https://commons.wikimedia.org/wiki/File:Toyota_Prius_Plug-In_Hybrid_IAA_2009.jpg, 2009.
[Online; accessed 28-November-2023].