Updatable Public-Key Encryption, Revisited

Joël Alwen
AWS Wickr

Georg Fuchsbauer
TU Wien

Marta Mularczyk
AWS Wickr

Updatable KEM

KEM

(pk, sk) ← KGen()

(K, c) ← Enc(pk)

K ← Dec(sk, c)

✗ no forward secrecy: leaked sk leaks all previously encapsulated keys

Updatable KEM

(pk, sk) ← KGen()

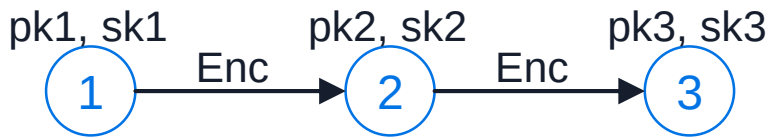
(K, c, pk') ← Enc(pk)

(K, sk') ← Dec(sk, c)

✓ forward secrecy

✓ efficient

✗ requires coordination between senders



Forward-Secure KEM

(pk, sk) ← KGen()

(K, c) ← Enc(pk)

(K, sk') ← Dec(sk, c)

✓ forward secrecy

✗ not efficient

Our Contributions

	New UKEM Application	Application Security	UKEM Security	Assumption	|pk| + |ctxt|
[JMM'19]	2-party messaging	"almost-optimal"	IND-CPA	DH (ROM)	

Our Contributions

	New UKEM Application	Application Security	UKEM Security	Assumption	|pk| + |ctxt|
[JMM'19]	2-party messaging	"almost-optimal"	IND-CPA	DH (ROM)	
[ACDT'20]	group messaging	very restricted	[JMM'19](-ish)	DH (ROM)	

Our Contributions

	New UKEM Application	Application Security	UKEM Security	Assumption	|pk| + |ctxt|
[JMM'19]	2-party messaging	"almost-optimal"	IND-CPA	DH (ROM)	
[ACDT'20]	group messaging	very restricted	[JMM'19](-ish)	DH (ROM)	
[DKW'21]			IND-CCA	DH, LWE	

Our Contributions

	New UKEM Application	Application Security	UKEM Security	Assumption	|pk| + |ctxt|
[JMM'19]	2-party messaging	"almost-optimal"	IND-CPA	DH (ROM)	
[ACDT'20]	group messaging	very restricted	[JMM'19](-ish)	DH (ROM)	
[DKW'21]			IND-CCA	DH, LWE	
[HLP'22]			[DKW'21]	DCR (ROM)	25.5 kB

Our Contributions

	New UKEM Application	Application Security	UKEM Security	Assumption	|pk| + |ctxt|
[JMM'19]	2-party messaging	"almost-optimal"	IND-CPA	DH (ROM)	
[ACDT'20]	group messaging	very restricted	[JMM'19](-ish)	DH (ROM)	
[DKW'21]			IND-CCA	DH, LWE	
[HLP'22]			[DKW'21]	DCR (ROM)	25.5 kB
[EJKM'22]			[DKW'21]	isogenies (ROM)	

Our Contributions

	New UKEM Application	Application Security	UKEM Security	Assumption	|pk| + |ctxt|
[JMM'19]	2-party messaging	"almost-optimal"	IND-CPA	DH (ROM)	
[ACDT'20]	group messaging	very restricted	[JMM'19](-ish)	DH (ROM)	
[DKW'21]			IND-CCA	DH, LWE	
[HLP'22]			[DKW'21]	DCR (ROM)	25.5 kB
[EJKM'22]			[DKW'21]	isogenies (ROM)	
[HPS'23]			[DKW'21]	LWE (ROM)	12.6 kB + |NIZK|

Our Contributions

	New UKEM Application	Application Security	UKEM Security	Assumption	|pk| + |ctxt|
[JMM'19]	2-party messaging	"almost-optimal"	IND-CPA	DH (ROM)	
[ACDT'20]	group messaging	very restricted	[JMM'19](-ish)	DH (ROM)	
[DKW'21]			IND-CCA	DH, LWE	
[HLP'22]			[DKW'21]	DCR (ROM)	25.5 kB
[EJKM'22]			[DKW'21]	isogenies (ROM)	
[HPS'23]			[DKW'21]	LWE (ROM)	12.6 kB + |NIZK|
[AW'23]			[DKW'21]⁻	DH (ROM)	0.38 kB

Our Contributions

	New UKEM Application	Application Security	UKEM Security	Assumption	|pk| + |ctxt|
[JMM'19]	2-party messaging	"almost-optimal"	IND-CPA	DH (ROM)	
[ACDT'20]	group messaging	very restricted	[JMM'19](-ish)	DH (ROM)	
[DKW'21]		more realistic group messaging?	IND-CCA	DH, LWE	
[HLP'22]			[DKW'21]	DCR (ROM)	25.5 kB
[EJKM'22]			[DKW'21]	isogenies (ROM)	
[HPS'23]			[DKW'21]	LWE (ROM)	12.6 kB + |NIZK|
[AW'23]			[DKW'21]—	DH (ROM)	0.38 kB

Our Contributions

	New UKEM Application	Application Security	UKEM Security	Assumption	|pk| + |ctxt|
[JMM'19]	2-party messaging	"almost-optimal"	IND-CPA	DH (ROM)	
[ACDT'20]	group messaging	very restricted	[JMM'19](-ish)	DH (ROM)	
[DKW'21]		more realistic group messaging?	IND-CCA	DH, LWE	
[HLP'22]			[DKW'21]	DCR (ROM)	25.5 kB
[EJKM'22]			[DKW'21]	isogenies (ROM)	
[HPS'23]			[DKW'21]	LWE (ROM)	12.6 kB + |NIZK|
[AW'23]			[DKW'21]⁻	DH (ROM)	0.38 kB
[this work]			IND-CCA-Members	DH (ROM)	0.24 kB
[this work]			IND-CCA-Joiners	DH+pairing (ROM, AGM)	0.24 kB

UKEM Syntax and Security

UKEM Syntax and Security

Basic Syntax [ACDT'20]

(pk1, sk1) ← KGen()

(K, c, pk') ← Enc(pk)

(K, sk') ← Dec(sk, c)

Basic IND-CPA Security [ACDT'20]

- oracles Enc, Chal
- Chal returns c* and real or random key K*

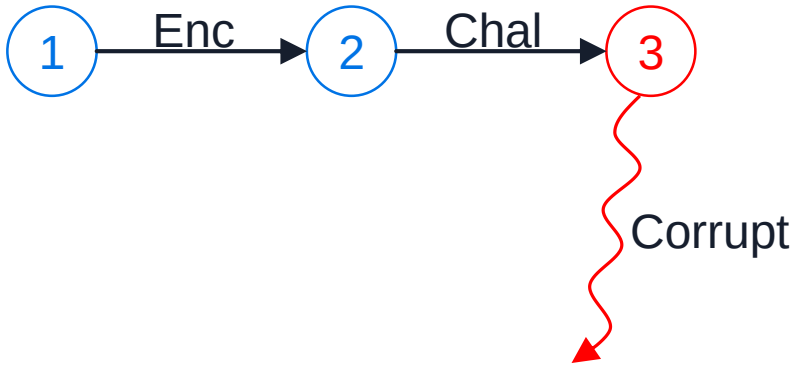
UKEM Syntax and Security

Basic Syntax [ACDT'20]

(pk1, sk1) ← KGen()

(K, c, pk') ← Enc(pk)

(K, sk') ← Dec(sk, c)



Basic IND-CPA Security [ACDT'20]

- oracles Enc, Chal
- Chal returns c* and real or random key K*
- Chal also returns sk *after* decrypting c*

UKEM Syntax and Security

Basic Syntax [ACDT’20]

(pk1, sk1) ← KGen()

(K, c, pk’) ← Enc(pk)

(K, sk’) ← Dec(sk, c)

Basic IND-CCA Security [DKW’21]

UKEM Syntax and Security

Basic Syntax [ACDT'20]

(pk1, sk1) ← KGen()

(K, c, pk') ← Enc(pk)

(K, sk') ← Dec(sk, c)

Basic IND-CCA Security [DKW'21]

add oracle Dec(c', pk')

UKEM Syntax and Security

Extended Syntax [DKW'21]

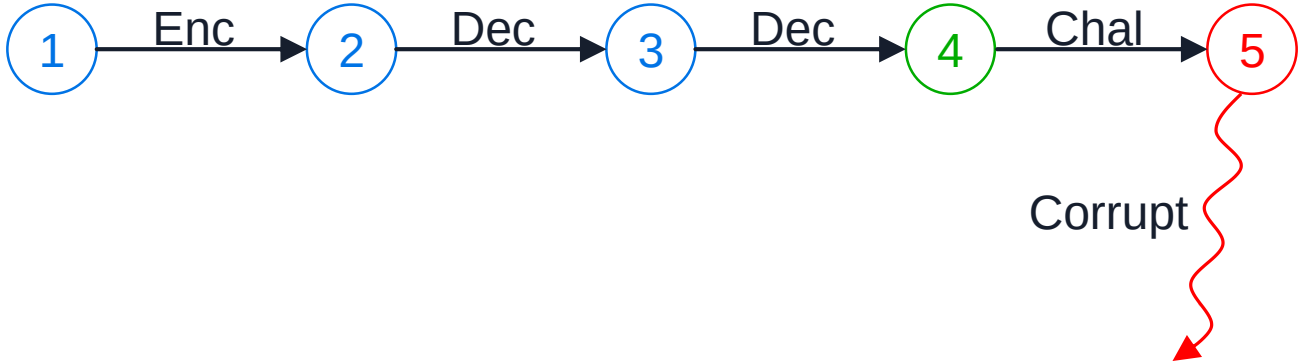
(pk1, sk1) ← KGen()

(K, c, pk', mt') ← Enc(pk)

(K, sk') ← Dec(sk, c)

0/1 ← Verify(pk, pk', mt')

allows a sender to verify a public key *without the secret key*



Basic IND-CCA Security [DKW'21]

add oracle Dec(c', pk', mt')

- if Dec(sk, c') succeeds, create full node
- else if Verify(pk, pk', mt') succeeds, create half node

UKEM Syntax and Security

Extended Syntax [DKW'21]

(pk1, sk1) ← KGen()

(K, c, pk', mt') ← Enc(pk)

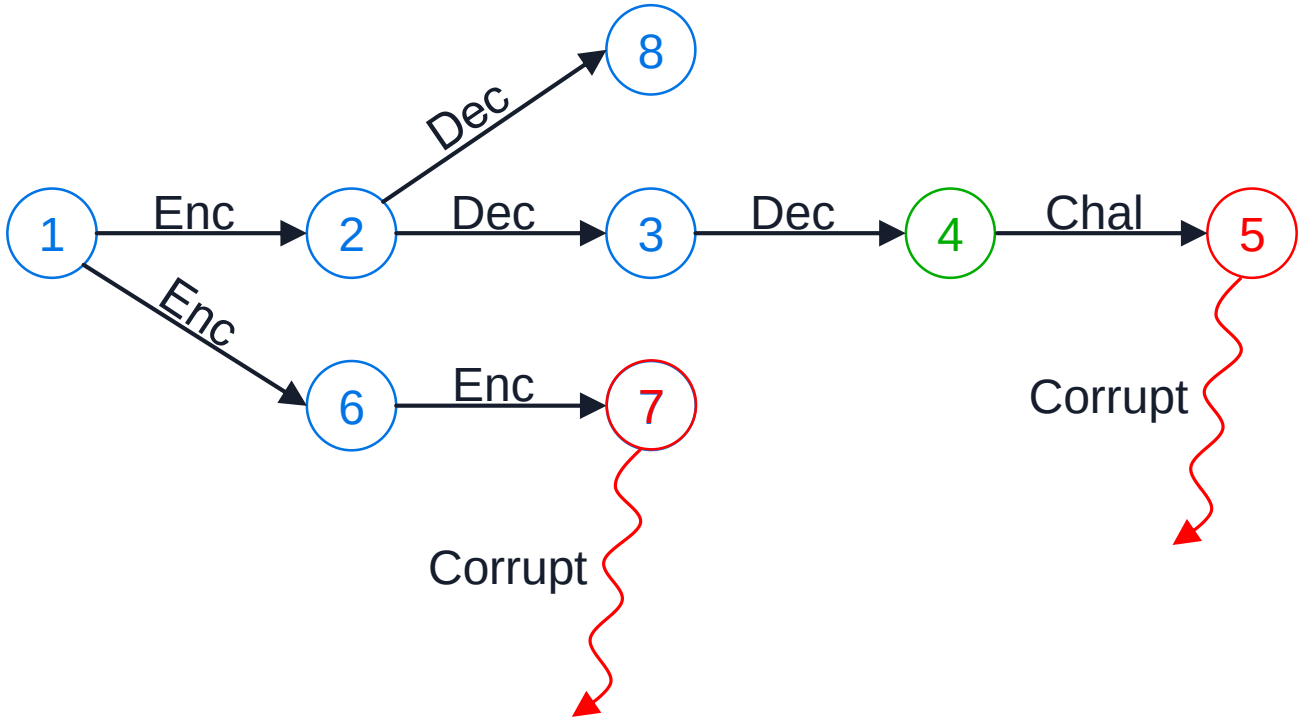
(K, sk') ← Dec(sk, c)

0/1 ← Verify(pk, pk', mt')

IND-CCA-Members [this work]

what do we need for Secure Group Messaging?

- ➔ "Enc-forks"
- ➔ "Dec-forks"
- ➔ multiple corruptions
- ➔ challenge most nodes



UKEM Syntax and Security

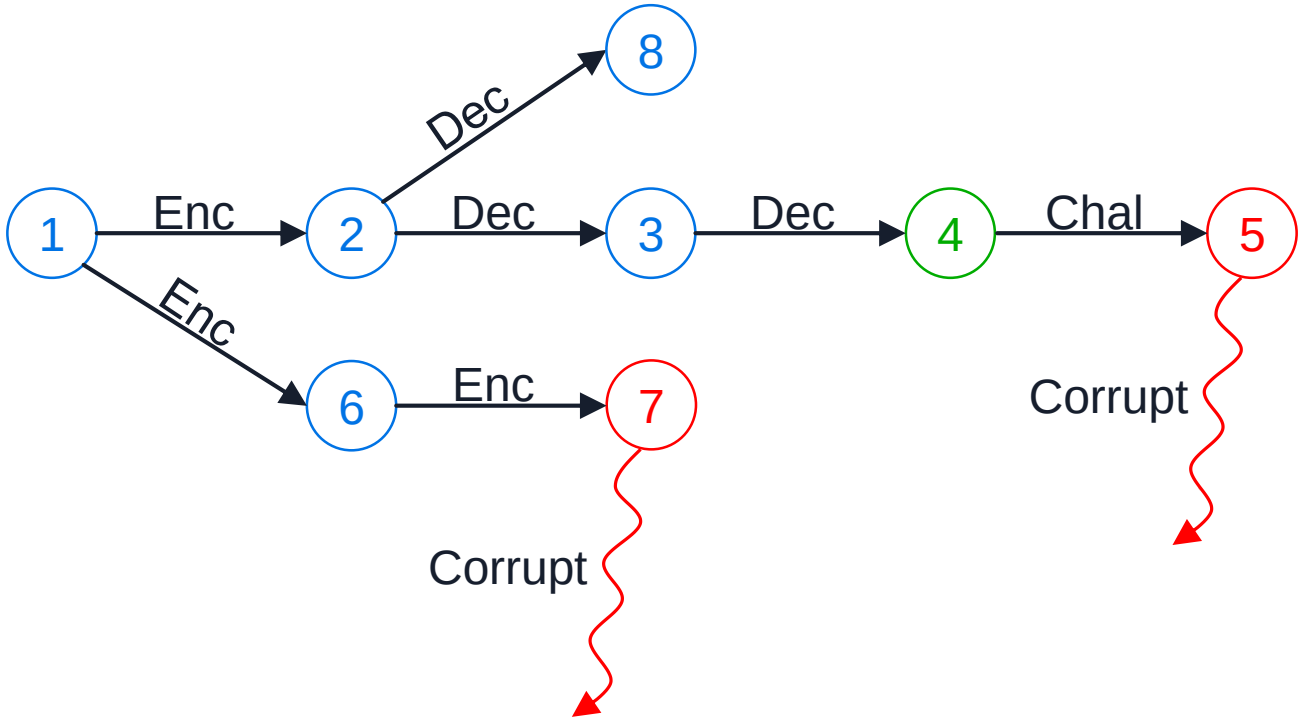
Extended Syntax for Joiner Security [this work]

(pk1, sk1) ← KGen()

(K, c, pk', mt') ← Enc(pk)

(K, sk') ← Dec(sk, c)

0/1 ← Verify(pk, pk', mt')



Motivation

Alice joins mid-session

- everyone else is offline
- keys are at epoch 8
- Alice trusts that epoch 1 is honest
- how can Alice trust pk at epoch 8?

UKEM Syntax and Security

Extended Syntax for Joiner Security [this work]

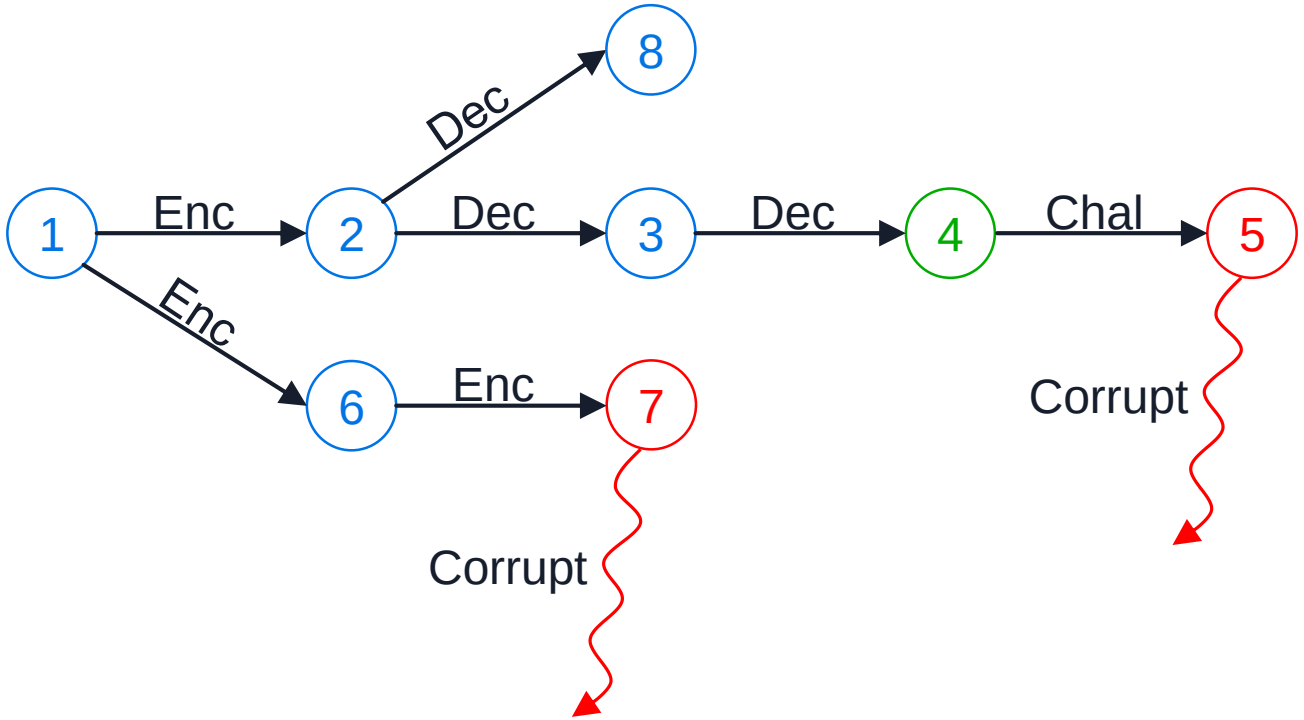
(pk1, sk1, jt1) ← KGen()

(K, c, pk', mt', jt') ← Enc(pk, jt)

(K, sk') ← Dec(sk, c)

0/1 ← Verify(pk, pk', mt')

0/1 ← VerifyJT(pk1, pk', jt')



Motivation

Alice joins mid-session

- everyone else is offline
- keys are at epoch 8
- Alice trusts that epoch 1 is honest
- how can Alice trust pk at epoch 8?

UKEM Syntax and Security

Extended Syntax for Joiner Security [this work]

(pk1, sk1, jt1) ← KGen()

(K, c, pk', mt', jt') ← Enc(pk, jt)

(K, sk') ← Dec(sk, c)

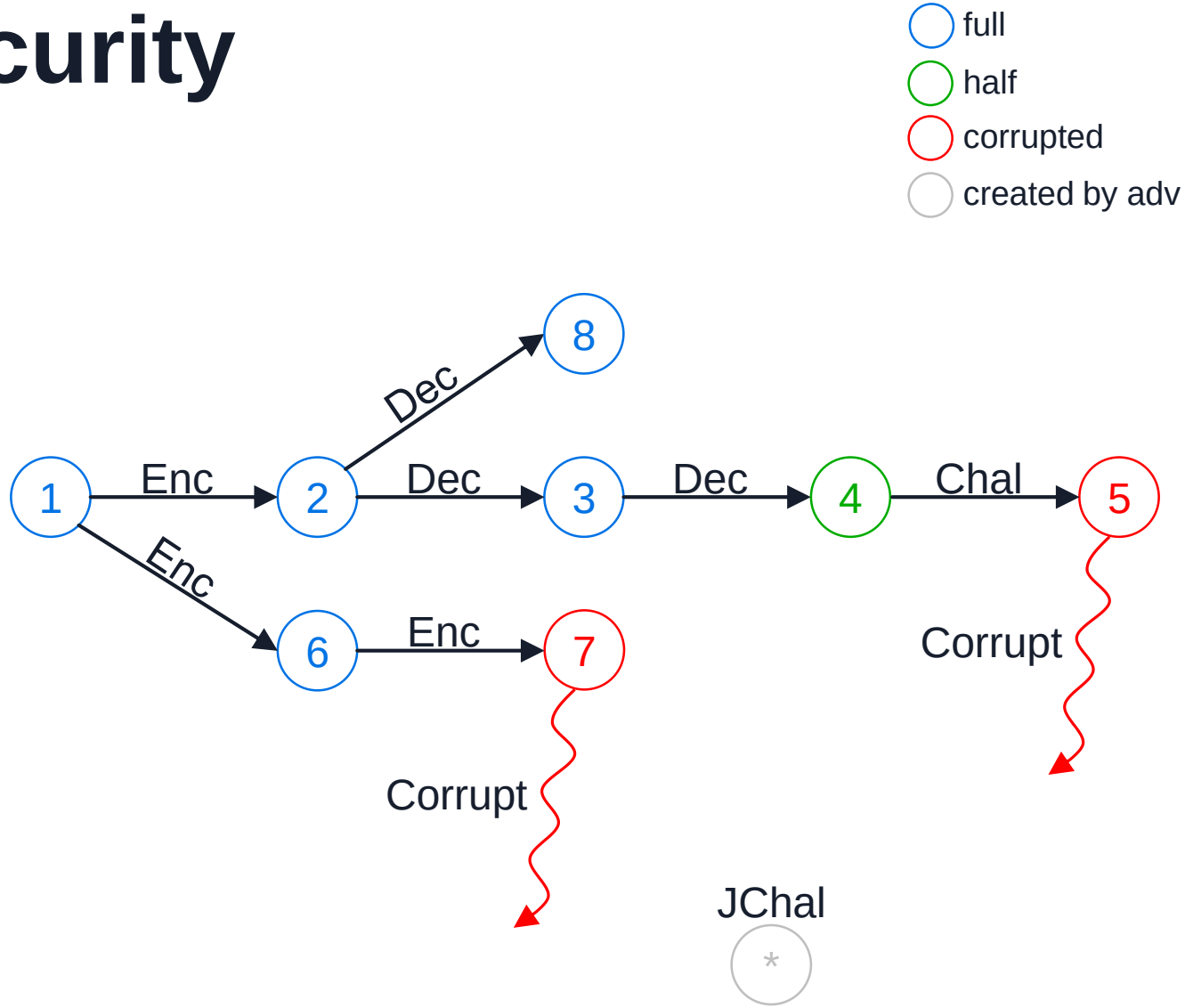
0/1 ← Verify(pk, pk', mt')

0/1 ← VerifyJT(pk1, pk', jt')

IND-CCA-Joiners [this work]

add oracle JChal(pk', jt')

- pk', mt' arbitrary
- if VerifyJT succeeds
  - runs Enc(pk', jt') and returns c*, real or random K* (and other Enc outputs)



Construction

DHIES-KEM

assumes : group G with generator g

key pair : $(x, X = g^x)$

Enc(X)

$r \leftarrow \$$

$R := g^r$

$K := H_1(X^r, X, R)$

return K, R

Construction

DHIES-KEM with key update

assumes : group G with generator g

key pair : $(x, X = g^x)$

Enc(X)

$r \leftarrow \$$

$R \coloneqq g^r$

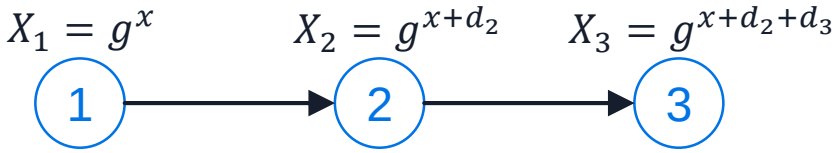
$K \coloneqq H_1(X^r, X, R)$

$d \coloneqq H_2(X^r, X, R)$

$X' \coloneqq X \cdot g^d \quad (= g^{x+d})$

return K, R, X'

using H_2 allows to deal with adaptive corruptions in the proof
→ with linear security loss!



Construction

DHIES-KEM with key update and member tags

assumes : group G with generator g

key pair : $(x, X = g^x)$

Enc(X)

$r \leftarrow \$$

$R := g^r$

$K := H_1(X^r, X, R)$

$d := H_2(X^r, X, R)$

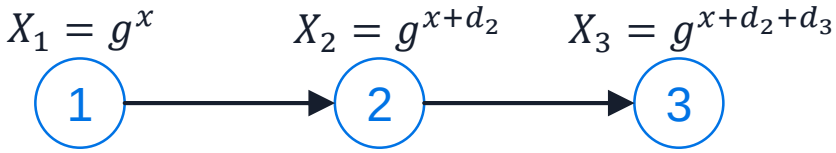
$X' := X \cdot g^d \quad (= g^{x+d})$

$\tau \leftarrow$ Schnorr-ZKPoK(d)

return K, R, X', τ

strong simulation (multi-) extractable

τ_3 proves knowledge of d_3



Construction

DHIES-KEM with key update, member tags and joiner tags

assumes : group G with generator g

key pair : $(x, X = g^x)$

Enc(X)

$r \leftarrow \$$

$R \coloneqq g^r$

$K \coloneqq H_1(X^r, X, R)$

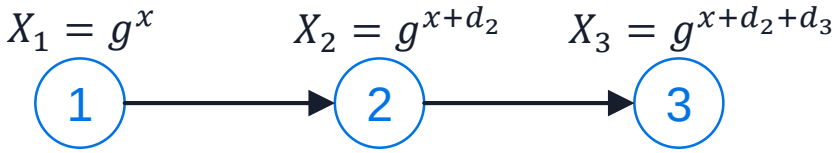
$d \coloneqq H_2(X^r, X, R)$

$X' \coloneqq X \cdot g^d \quad (= g^{x+d})$

$\tau' \leftarrow$ Schnorr-ZKPoK(d)

$\pi' \leftarrow$ ZKPoK$(d_2 + d_3 + \cdots + d)$

return K, R, X', τ, π'



Construction

DHIES-KEM with key update, member tags and joiner tags

assumes : group G with generator g

key pair : $(x, X = g^x)$

Enc(X, π)

$r \leftarrow \$$

$R := g^r$

$K := H_1(X^r, X, R)$

$d := H_2(X^r, X, R)$

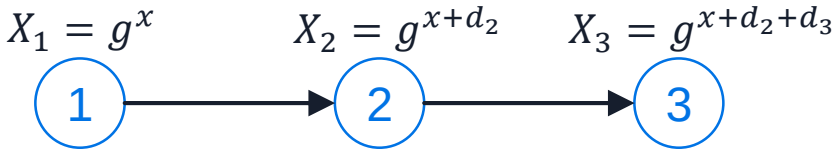
$X' := X \cdot g^d \quad (= g^{x+d})$

$\tau' \leftarrow$ Schnorr-ZKPoK(d)

$\pi' \leftarrow$ ZKPoK$(d_2 + d_3 + \cdots + d)$

return K, R, X', τ, π'

constant-size malleable ZKPoK



Summary

- 2 new notions and constructions of Updatable KEMs

UKEM security	Assumption	|pk| + |ctx|	|joiner tag|
IND-CCA-Members	DH (ROM)	0.24 kB	–
IND-CCA-Joiners	DH + pairing (ROM + AGM)	0.24 kB	0.01 kB

- New tool : malleable ZKPoK