NTNU

Norwegian University of Science and Technology

The Direction of Updatable Encryption does not Matter Much

Yao Jiang

Norwegian University of Science and Technology (NTNU), Norway

NTNU

Updatable Encryption

Problem Motivation: Outsourcing

Problem Motivation: Outsourcing

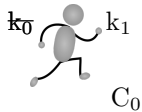
$\mathrm{Dec}_{k_0}(C_0) = m$

— Threats: Key compromise

Problem Motivation: Outsourcing

- Threats: Key compromise
- Solution: Key rotation

Key Rotation: a Standard Approach



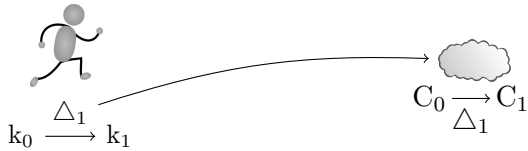
C_0 ← Download

Decrypt m = $Dec_{k_0}(C_0)$

Re-encrypt $Enc_{k_1}(m) = C_1$ → Re-upload → C_1

— Download and re-upload is infeasible
even for moderate storage requirements

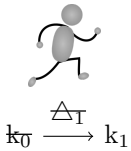
Key Rotation: Updatable Encryption (UE)

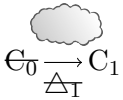


— **Key Homomorphic PRFs and their Applications**
Boneh, Lewi, Montgomery, Raghunathan; CRYPTO '13 (+ ePrint 2015/220)

NTNU

Key Rotation: Updatable Encryption (UE)





— Client only ever needs to store one key

— fresh encryptions, updated ciphertexts and tokens should all reveal nothing about plaintext

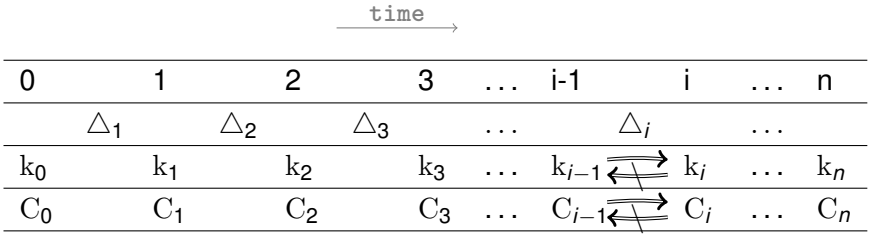
— **Key Homomorphic PRFs and their Applications**
Boneh, Lewi, Montgomery, Raghunathan; CRYPTO '13 (+ ePrint 2015/220)

Epoch-based Model

time →

0	1	2	3	4	5	6	7	...	n
	$\triangle_1$	$\triangle_2$	$\triangle_3$	$\triangle_4$	$\triangle_5$	$\triangle_6$	$\triangle_7$	...	
k_0	k_1	k_2	k_3	k_4	k_5	k_6	k_7	...	k_n
C_0	C_1	C_2	C_3	C_4	C_5	C_6	C_7	...	C_n

Uni-directional Updates



Uni-directional key updates:

- We can only infer k_i from k_{i-1} and $\triangle_i$;
- We can not infer k_{i-1} from k_i and $\triangle_i$;

Uni-directional ciphertext updates:

- We can only infer C_i from C_{i-1} and $\triangle_i$;
- We can not infer C_{i-1} from C_i and $\triangle_i$;

Bi-directional Updates

time →

0		1		2		3	...	i-1		i	...	n
	$\triangle_1$		$\triangle_2$		$\triangle_3$		...		$\triangle_i$		...	
k_0		k_1		k_2		k_3	...	k_{i-1}	⇄	k_i	...	k_n
C_0		C_1		C_2		C_3	...	C_{i-1}	⇄	C_i	...	C_n

Bi-directional key updates:

- We can infer k_i from k_{i-1} and $\triangle_i$;
- We can infer k_{i-1} from k_i and $\triangle_i$;

Bi-directional ciphertext updates:

- We can infer C_i from C_{i-1} and $\triangle_i$;
- We can infer C_{i-1} from C_i and $\triangle_i$;

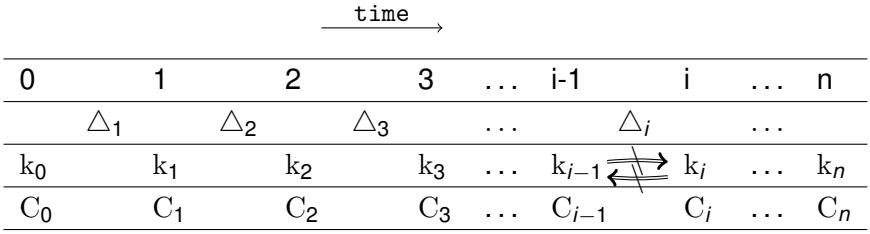
NTNU

Questions

— UE schemes with uni-directional updates leak less information than with bi-directional updates

— Are uni-directional updates better?

No-directional Key Updates



No-directional key updates:

— We can not infer k_i from k_{i-1} and $\triangle_i$;

— We can not infer k_{i-1} from k_i and $\triangle_i$;

NTNU

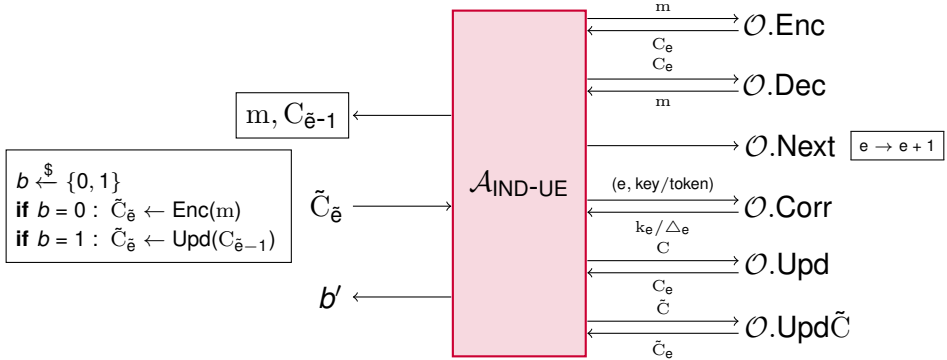
Questions

- UE schemes with no-directional key updates leak the least information
- Are no-directional key updates better?

NTNU

Security Notions

Existing Confidentiality Notions for Updatable Encryption (IND-UE)

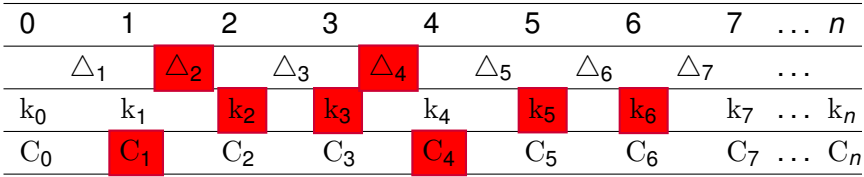


— Challenger checks leaked information to see if the adversary can trivially win

Only in CCA games does an adversary have access to $\mathcal{O}$.Dec

— **Fast and Secure Updatable Encryption**
Boyd, Davies, Gjøsteen, Jiang; Crypto '20

Leakage and Trivial Wins



— Directly obtained information:

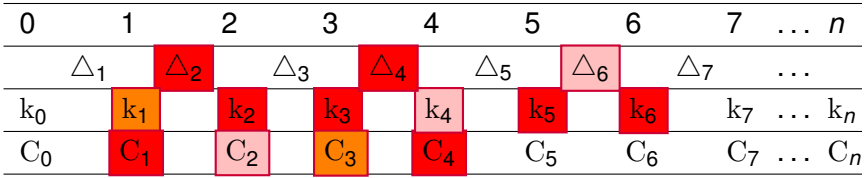
- Adversary adaptively corrupts keys and tokens
- Adversary can asks for ciphertexts

Corrupted information

Inferred information

Inferred information (only in bi-directional updates)

Leakage and Trivial Wins

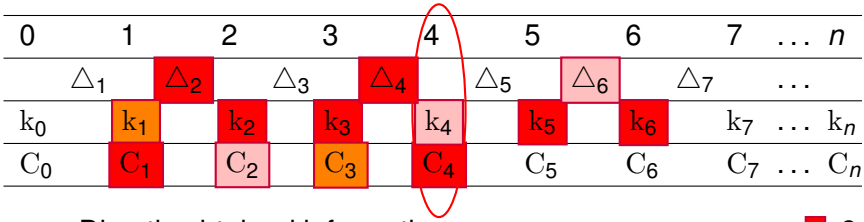


— Directly obtained information:
- Adversary adaptively corrupts keys and tokens
- Adversary can asks for ciphertexts

— Inferred information:
- Assume uni-directional updates: $k_4, \triangle_6, C_2$.
- Assume bi-directional updates: $k_1, k_4, \triangle_6, C_2, C_3$.

Corrupted information
Inferred information
Inferred information (only in bi-directional updates)

Leakage and Trivial Wins

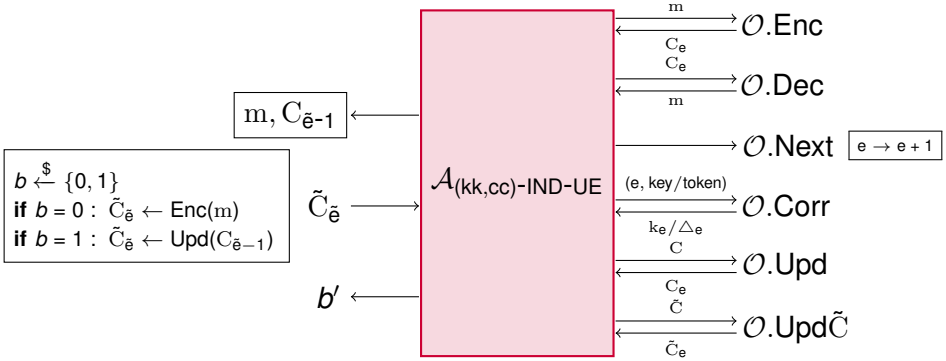


- Directly obtained information:
  - Adversary adaptively corrupts keys and tokens
  - Adversary can asks for ciphertexts
- Inferred information:
  - Assume uni-directional updates: $k_4, \triangle_6, C_2$.
  - Assume bi-directional updates: $k_1, k_4, \triangle_6, C_2, C_3$.
- Adversary can use k_4 to decrypt C_4 to trivially win a security game!

Corrupted information
Inferred information
Inferred information (only in bi-directional updates)

Six Variants of Confidentiality Notions

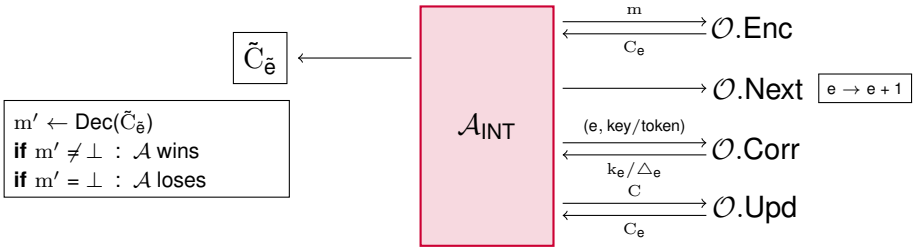
— For kk $\in \{\text{uni}, \text{bi}, \text{no}\}$ and cc $\in \{\text{uni}, \text{bi}\}$, consider UE schemes with kk-directional key updates and cc to cc-directional ciphertext updates.



— Challenger checks leaked information to see if the adversary can trivially win

— Trivial wins depend on the update settings!

Existing Integrity Notions for Updatable Encryption

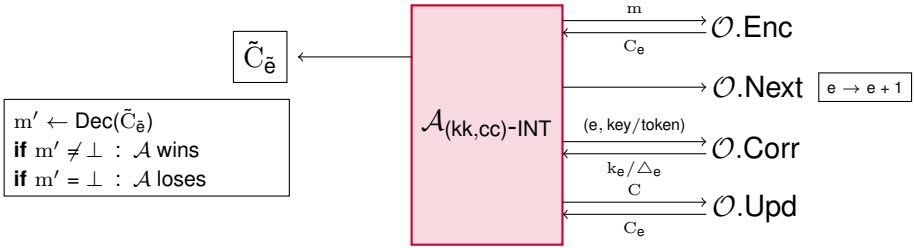


— Challenger checks leaked information to see if the adversary can trivially win

— **(R)CCA secure updatable encryption with integrity protection**
Klooß, Lehmann and Rupp; Eurocrypt '19

Six Variants of Integrity Notions

— For kk $\in \{\text{uni}, \text{bi}, \text{no}\}$ and cc $\in \{\text{uni}, \text{bi}\}$, consider UE schemes with kk-directional key updates and cc to cc-directional ciphertext updates.



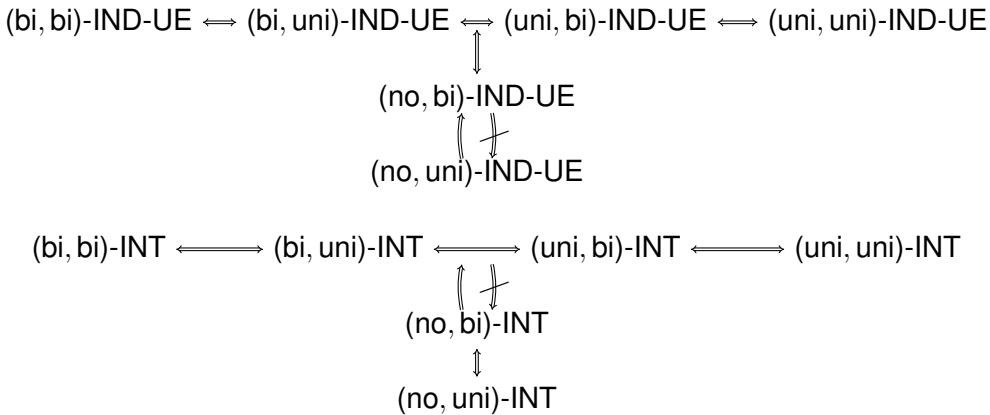
— Challenger checks leaked information to see if the adversary can trivially win

— Trivial wins depend on the update settings!

NTNU

Relations

Relations


(bi, bi)-IND-UE
(bi, uni)-IND-UE
(uni, bi)-IND-UE
(uni, uni)-IND-UE
(no, bi)-IND-UE
(no, uni)-IND-UE
(bi, bi)-INT
(bi, uni)-INT
(uni, bi)-INT
(uni, uni)-INT
(no, bi)-INT
(no, uni)-INT

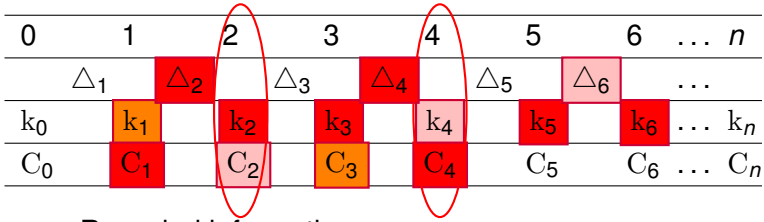
NTNU

How to prove these relations?

— To prove:
  - Security notions with uni- and bi-directional updates are equivalent.

— It suffices to prove:
  - The trivial wins in the uni-directional updates are triggered if and only if the trivial wins in the bi-directional updates are triggered.

Motivation Example | Uni-directional vs. Bi-directional



Corrupted information

Inferred information

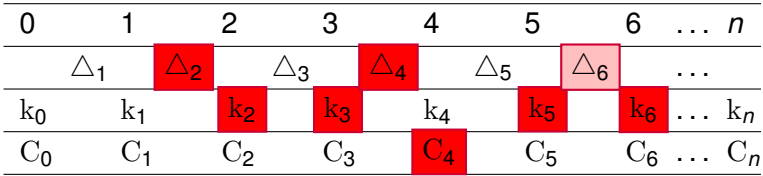
Inferred information (only in bi-directional updates)

— Revealed information:
  - Assume uni-directional updates: $k_2, k_3, k_4, k_5, k_6, \triangle_2, \triangle_4, \triangle_6$.
  - Assume bi-directional updates: $k_1, k_2, k_3, k_4, k_5, k_6, \triangle_2, \triangle_4, \triangle_6$.

— Adversary can trivially win a security game if it asks for one of $C_1, \ldots, C_6$! No matter uni- or bi-directional updates!

— UE schemes with uni-directional updates will not provide more security than UE schemes with bi- directional updates!

Motivation Example | No-directional Key Updates and Uni-directional Ciphertext Updates



Corrupted information
Inferred information
Inferred information (only in bi-directional updates)

— Adversary can not trivialliy win the confidentiality game!

NTNU

UE Constructions

NTNU

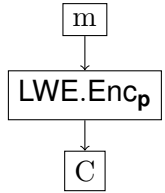
Prior Works

UE schemes	Hard problems	IND-UE
BLMR	DDH or LWE, etc.	✘
RISE	DDH	✓
NYUAE	SXDH	✓?
E&M	DDH	✓?
SHINE	DDH	✓

— Can we find post-quantum secure UE schemes?

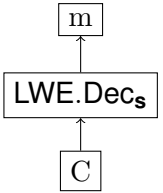
An LWE-based UE scheme (LWEUE)

LWEUE.Enc :



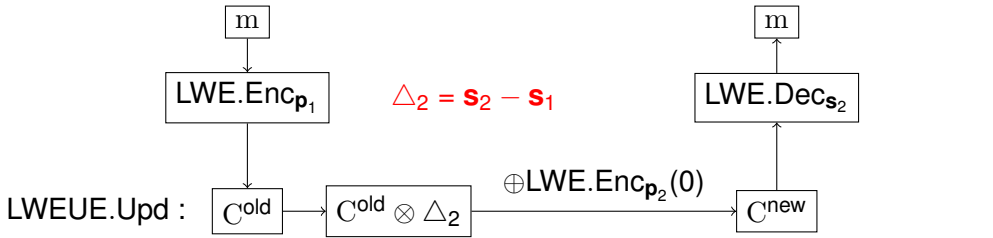
$C = \text{LWE.Enc}_p(m)$

LWEUE.Dec :



$m = \text{LWE.Dec}_s(C)$

An LWE-based UE scheme (LWEUE): Re-randomization



LWEUE is randIND-UE-CPA Secure

Assuming DLWE

NTNU

Summary

NTNU

Summary

- We introduce six-variants of security notions for UE schemes.
- Security notions with uni- and bi-directional updates are equivalent. A surprising result!
- Security notions with no-directional key updates are strictly stronger than uni- and bi- directional update variants of the corresponding notions.
- A post-quantum secure UE scheme: LWEUE

NTNU

Open Problems

— Constructing UE schemes with no-directional key updates.

— Constructing UE schemes with chosen ciphertext post-quantum security.

NTNU

Thank you for your attention!

Questions?