On the Multi-User Security of LWE-based NIKE

Roman Langrehr, ETH Zurich

2023-12-02

Non-Interactive Key Exchange (NIKE) [CKS08, FHKP13]

Alice

Bob

$$\mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda)$$

$$(\mathsf{pk}_A, \mathsf{sk}_A) \leftarrow \mathsf{KeyGen}(\mathsf{pp}) \qquad\qquad (\mathsf{pk}_B, \mathsf{sk}_B) \leftarrow \mathsf{KeyGen}(\mathsf{pp})$$

$$\xrightarrow{\mathsf{pk}_A} \quad \text{PKI} \quad \xleftarrow{\mathsf{pk}_B}$$

$$\xleftarrow[\mathsf{pk}_B]{} \quad \text{PKI} \quad \xrightarrow[\mathsf{pk}_A]{}$$

Non-Interactive Key Exchange (NIKE) [CKS08, FHKP13]

Alice

Bob

$\mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda)$

$(\mathsf{pk}_A, \mathsf{sk}_A) \leftarrow \mathsf{KeyGen}(\mathsf{pp})$

$(\mathsf{pk}_B, \mathsf{sk}_B) \leftarrow \mathsf{KeyGen}(\mathsf{pp})$

$$\text{Alice} \overset{\mathsf{pk}_A}{\longrightarrow} \text{PKI} \overset{\mathsf{pk}_B}{\longleftarrow} \text{Bob}$$

$$\text{Alice} \underset{\mathsf{pk}_B}{\longleftarrow} \text{PKI} \underset{\mathsf{pk}_A}{\longrightarrow} \text{Bob}$$

$K_{AB} \leftarrow \mathsf{SharedKey}(\mathsf{sk}_A, \mathsf{pk}_B)$

$K_{BA} \leftarrow \mathsf{SharedKey}(\mathsf{sk}_B, \mathsf{pk}_A)$

Non-Interactive Key Exchange (NIKE) [CKS08, FHKP13]

Alice

Bob

$$\mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda)$$

$(\mathsf{pk}_A, \mathsf{sk}_A) \leftarrow \mathsf{KeyGen}(\mathsf{pp})$ $\qquad$ $(\mathsf{pk}_B, \mathsf{sk}_B) \leftarrow \mathsf{KeyGen}(\mathsf{pp})$

$$\underset{\xleftarrow[\mathsf{pk}_B]{}}{\xrightarrow{\mathsf{pk}_A}} \quad \text{PKI} \quad \underset{\xrightarrow[\mathsf{pk}_A]{}}{\xleftarrow{\mathsf{pk}_B}}$$

$K_{AB} \leftarrow \mathsf{SharedKey}(\mathsf{sk}_A, \mathsf{pk}_B)$ $\quad = \quad$ $K_{BA} \leftarrow \mathsf{SharedKey}(\mathsf{sk}_B, \mathsf{pk}_A)$

Non-Interactive Key Exchange (NIKE) [CKS08, FHKP13]

Alice

Bob

$$\mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda)$$

$(\mathsf{pk}_A, \mathsf{sk}_A) \leftarrow \mathsf{KeyGen}(\mathsf{pp})$ $\qquad$ $(\mathsf{pk}_B, \mathsf{sk}_B) \leftarrow \mathsf{KeyGen}(\mathsf{pp})$

$$\xrightarrow{\mathsf{pk}_A} \text{ PKI } \xleftarrow{\mathsf{pk}_B}$$

$$\xleftarrow{\mathsf{pk}_B} \text{ PKI } \xrightarrow{\mathsf{pk}_A}$$

$$K_{AB} \leftarrow \mathsf{SharedKey}(\mathsf{sk}_A, \mathsf{pk}_B) \overset{\text{w.h.p.}}{=} K_{BA} \leftarrow \mathsf{SharedKey}(\mathsf{sk}_B, \mathsf{pk}_A)$$

Light security

Adversary

- gets public keys of 2 users and

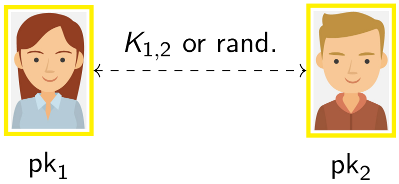
pk_1

pk_2

Light security

Adversary

- gets public keys of 2 users and
- real or random shared key



Adaptive Honest Key Registration (HKR) Security

Adversary can adaptively

- spawn new users

pk_1

pk_2

pk_3

pk_4

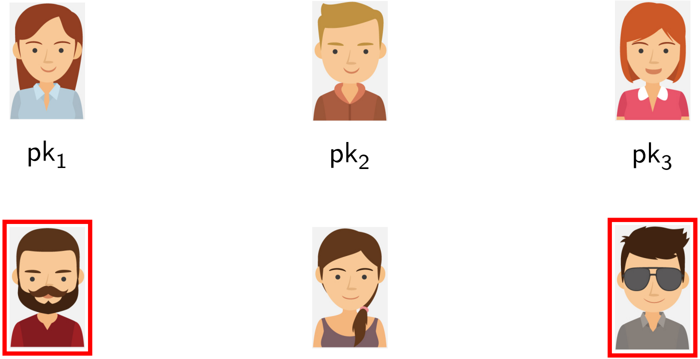
pk_5

pk_6

Adaptive Honest Key Registration (HKR) Security

Adversary can adaptively

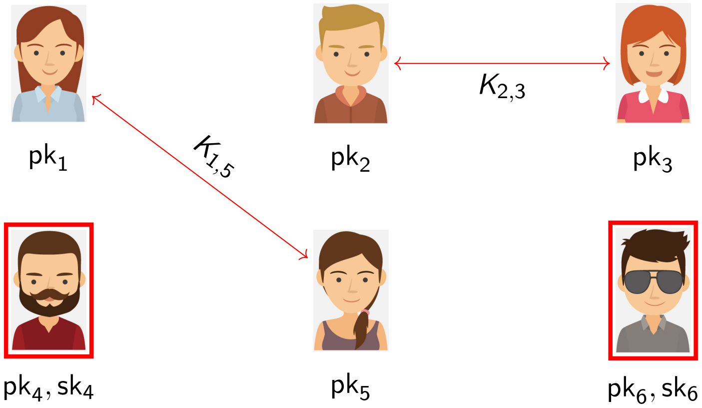
- spawn new users
- corrupt users



Adaptive Honest Key Registration (HKR) Security

Adversary can adaptively

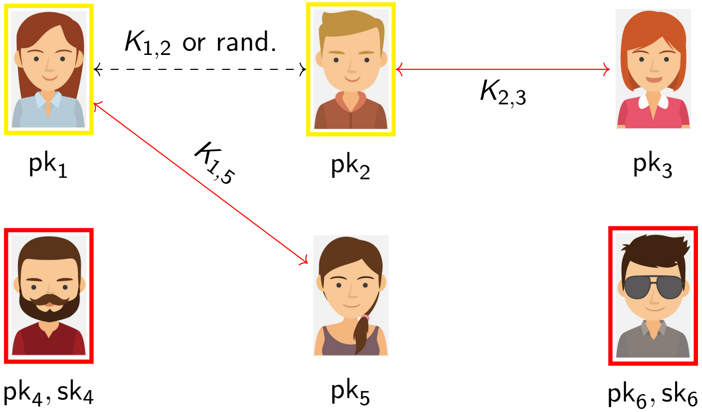
- spawn new users
- corrupt users
- reveal shared keys, even those computed with a challenge users secret key



Adaptive Honest Key Registration (HKR) Security

Adversary can adaptively

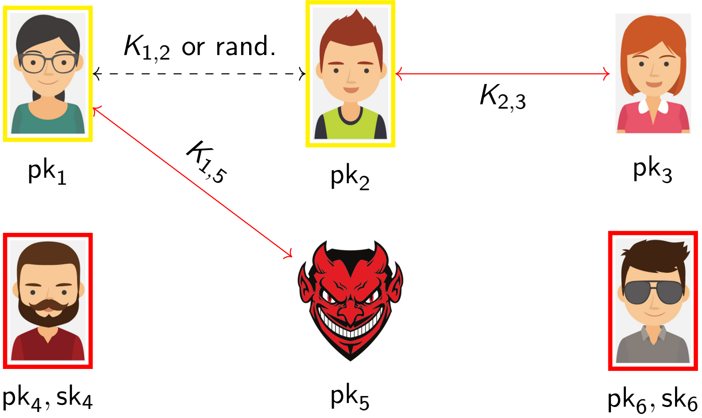
- spawn new users
- corrupt users
- reveal shared keys, even those computed with a challenge users secret key
- get challenged on one uncorrupted shared key



Adaptive Dishonest Key Registration (DKR) Security

Adversary can adaptively

- spawn new users
- corrupt users
- reveal shared keys, even those computed with a challenge users secret key
- get challenged on (one) uncorrupted shared key
- introduce maliciously generated public keys



Relations between these security notions

Light $\leftarrow$ - - - - - - - - - - - Adaptive HKR $\leftarrow$ - - - - - - - Adaptive DKR

Relations between these security notions

For negligible correctness error

$$\begin{tikzcd} \text{Light} \arrow[r, bend left, "\text{[FHKP13]}"] & \text{Adaptive HKR} \arrow[l, dashed] & \text{Adaptive DKR} \arrow[l, dashed] \end{tikzcd}$$

Relations between these security notions

This work: This is necessary for a generic argument

For negligible correctness error

$$\begin{tikzcd} \text{Light} \arrow[r, bend left, "\text{[FHKP13]}"] & \text{Adaptive HKR} \arrow[l, dashed] & \text{Adaptive DKR} \arrow[l, dashed] \end{tikzcd}$$

Relations between these security notions

This work: This is necessary for a generic argument

For negligible correctness error

For perfect correctness

$$\begin{tikzcd}[column sep=huge]
\text{Light} \arrow[r, bend left, "\text{[FHKP13]}"] & \text{Adaptive HKR} \arrow[l, dashed] \arrow[r, bend left, "\substack{\text{[HHK18]} \\ +\ \text{NIZKPoK}}"] & \text{Adaptive DKR} \arrow[l, dashed]
\end{tikzcd}$$

LWE-based NIKE

Alice

Bob

$$\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n \times n}$$

$\mathbf{s}_A \xleftarrow{\$} \{0,1\}^n$; $\mathbf{e}_A \xleftarrow{\$} \mathcal{E}^n$

$\mathrm{pk}_A := \mathbf{s}_A^\top \mathbf{A} + \mathbf{e}_A^\top, \mathrm{sk}_A := \mathbf{s}_A$

$\mathbf{s}_B \xleftarrow{\$} \{0,1\}^n$; $\mathbf{e}_B \xleftarrow{\$} \mathcal{E}^n$

$\mathrm{pk}_B := \mathbf{A}\mathbf{s}_B + \mathbf{e}_B, \mathrm{sk}_A := \mathbf{s}_B$

$$\xrightarrow[\mathrm{pk}_B]{\mathrm{pk}_A} \text{PKI} \xrightarrow[\mathrm{pk}_A]{\mathrm{pk}_B}$$

LWE-based NIKE

Alice

Bob

$$\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times n}$$

$\mathbf{s}_A \xleftarrow{\$} \{0,1\}^n$; $\mathbf{e}_A \xleftarrow{\$} \mathcal{E}^n$

$\mathsf{pk}_A := \mathbf{s}_A^\top \mathbf{A} + \mathbf{e}_A^\top, \mathsf{sk}_A := \mathbf{s}_A$

$\mathbf{s}_B \xleftarrow{\$} \{0,1\}^n$; $\mathbf{e}_B \xleftarrow{\$} \mathcal{E}^n$

$\mathsf{pk}_B := \mathbf{A}\mathbf{s}_B + \mathbf{e}_B, \mathsf{sk}_A := \mathbf{s}_B$

$$\text{Alice} \underset{\mathsf{pk}_B}{\overset{\mathsf{pk}_A}{\rightleftarrows}} \text{PKI} \underset{\mathsf{pk}_A}{\overset{\mathsf{pk}_B}{\rightleftarrows}} \text{Bob}$$

$e'_A \xleftarrow{\$} \mathcal{E}$

$e'_B \xleftarrow{\$} \mathcal{E}$

$$K_{AB} := \mathbf{s}_A^\top \mathsf{pk}_B + e'_A = \mathbf{s}_A^\top \mathbf{A}\mathbf{s}_B + \mathbf{s}_A^\top \mathbf{e}_B + e'_A$$

$$K_{BA} := \mathsf{pk}_A \mathbf{s}_B + e'_B = \mathbf{s}_A^\top \mathbf{A}\mathbf{s}_B + \mathbf{e}_A^\top \mathbf{s}_B + e'_B$$

LWE-based NIKE

Alice

Bob

$$\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n \times n}$$

$\mathbf{s}_A \xleftarrow{\$} \{0,1\}^n$; $\mathbf{e}_A \xleftarrow{\$} \mathcal{E}^n$
$\mathsf{pk}_A := \mathbf{s}_A^\top \mathbf{A} + \mathbf{e}_A^\top, \mathsf{sk}_A := \mathbf{s}_A$

$\mathbf{s}_B \xleftarrow{\$} \{0,1\}^n$; $\mathbf{e}_B \xleftarrow{\$} \mathcal{E}^n$
$\mathsf{pk}_B := \mathbf{A}\mathbf{s}_B + \mathbf{e}_B, \mathsf{sk}_A := \mathbf{s}_B$

$$\text{Alice} \underset{\mathsf{pk}_B}{\overset{\mathsf{pk}_A}{\rightleftarrows}} \text{PKI} \underset{\mathsf{pk}_A}{\overset{\mathsf{pk}_B}{\rightleftarrows}} \text{Bob}$$

$e'_A \xleftarrow{\$} \mathcal{E}$
$$K_{AB} := \mathbf{s}_A^\top \mathsf{pk}_B + e'_A = \boxed{\mathbf{s}_A^\top \mathbf{A} \mathbf{s}_B} + \mathbf{s}_A^\top \mathbf{e}_B + e'_A$$

$e'_B \xleftarrow{\$} \mathcal{E}$
$$K_{BA} := \mathsf{pk}_A \mathbf{s}_B + e'_B = \boxed{\mathbf{s}_A^\top \mathbf{A} \mathbf{s}_B} + \mathbf{e}_A^\top \mathbf{s}_B + e'_B$$

LWE-based NIKE

Alice

Bob

$$\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n \times n}$$

$\mathbf{s}_A \xleftarrow{\$} \{0,1\}^n$; $\mathbf{e}_A \xleftarrow{\$} \mathcal{E}^n$

$\mathsf{pk}_A := \mathbf{s}_A^\top \mathbf{A} + \mathbf{e}_A^\top, \mathsf{sk}_A := \mathbf{s}_A$

$\mathbf{s}_B \xleftarrow{\$} \{0,1\}^n$; $\mathbf{e}_B \xleftarrow{\$} \mathcal{E}^n$

$\mathsf{pk}_B := \mathbf{A}\mathbf{s}_B + \mathbf{e}_B, \mathsf{sk}_A := \mathbf{s}_B$

$\xrightarrow{\mathsf{pk}_A}$ PKI $\xrightarrow{\mathsf{pk}_B}$

$\xleftarrow[\mathsf{pk}_B]{}$ PKI $\xleftarrow[\mathsf{pk}_A]{}$

$e'_A \xleftarrow{\$} \mathcal{E}$

$$K_{AB} := \mathbf{s}_A^\top \mathsf{pk}_B + e'_A = \boxed{\mathbf{s}_A^\top \mathbf{A} \mathbf{s}_B} + \boxed{\mathbf{s}_A^\top \mathbf{e}_B + e'_A}$$

$e'_B \xleftarrow{\$} \mathcal{E}$

$$K_{BA} := \mathsf{pk}_A \mathbf{s}_B + e'_B = \boxed{\mathbf{s}_A^\top \mathbf{A} \mathbf{s}_B} + \boxed{\mathbf{e}_A^\top \mathbf{s}_B + e'_B}$$

LWE-based NIKE

Alice

Bob

$$\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n \times n}$$

$\mathbf{s}_A \xleftarrow{\$} \{0,1\}^n$; $\mathbf{e}_A \xleftarrow{\$} \mathcal{E}^n$

$\mathsf{pk}_A := \mathbf{s}_A^\top \mathbf{A} + \mathbf{e}_A^\top, \mathsf{sk}_A := \mathbf{s}_A$

$\mathbf{s}_B \xleftarrow{\$} \{0,1\}^n$; $\mathbf{e}_B \xleftarrow{\$} \mathcal{E}^n$

$\mathsf{pk}_B := \mathbf{A}\mathbf{s}_B + \mathbf{e}_B, \mathsf{sk}_A := \mathbf{s}_B$

$$\text{Alice} \underset{\mathsf{pk}_B}{\overset{\mathsf{pk}_A}{\rightleftarrows}} \text{PKI} \underset{\mathsf{pk}_A}{\overset{\mathsf{pk}_B}{\rightleftarrows}} \text{Bob}$$

$e'_A \xleftarrow{\$} \mathcal{E}$ $\qquad$ $e'_B \xleftarrow{\$} \mathcal{E}$

$$K_{AB} := \mathbf{s}_A^\top \mathsf{pk}_B + e'_A = \boxed{\mathbf{s}_A^\top \mathbf{A}\mathbf{s}_B} + \boxed{\mathbf{s}_A^\top \mathbf{e}_B + e'_A} \approx K_{BA} := \mathsf{pk}_A \mathbf{s}_B + e'_B = \boxed{\mathbf{s}_A^\top \mathbf{A}\mathbf{s}_B} + \boxed{\mathbf{e}_A^\top \mathbf{s}_B + e'_B}$$

LWE-based NIKE

Alice

Bob

$$\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times n}$$

$\mathbf{s}_A \xleftarrow{\$} \{0,1\}^n$; $\mathbf{e}_A \xleftarrow{\$} \mathcal{E}^n$

$\mathsf{pk}_A := \mathbf{s}_A^\top \mathbf{A} + \mathbf{e}_A^\top, \mathsf{sk}_A := \mathbf{s}_A$

$\mathbf{s}_B \xleftarrow{\$} \{0,1\}^n$; $\mathbf{e}_B \xleftarrow{\$} \mathcal{E}^n$

$\mathsf{pk}_B := \mathbf{A}\mathbf{s}_B + \mathbf{e}_B, \mathsf{sk}_A := \mathbf{s}_B$

$$\text{Alice} \underset{\mathsf{pk}_B}{\overset{\mathsf{pk}_A}{\rightleftarrows}} \text{PKI} \underset{\mathsf{pk}_A}{\overset{\mathsf{pk}_B}{\rightleftarrows}} \text{Bob}$$

$e'_A \xleftarrow{\$} \mathcal{E}$ $\qquad$ $e'_B \xleftarrow{\$} \mathcal{E}$

$$K_{AB} := \mathbf{s}_A^\top \mathsf{pk}_B + e'_A = \boxed{\mathbf{s}_A^\top \mathbf{A}\mathbf{s}_B} + \boxed{\mathbf{s}_A^\top \mathbf{e}_B + e'_A} \approx K_{BA} := \mathsf{pk}_A \mathbf{s}_B + e'_B = \boxed{\mathbf{s}_A^\top \mathbf{A}\mathbf{s}_B} + \boxed{\mathbf{e}_A^\top \mathbf{s}_B + e'_B}$$

$\mathsf{Round}(K_{AB})$ $\qquad$ $\mathsf{Round}(K_{BA})$

LWE-based NIKE

Alice

Bob

$$\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times n}$$

$\mathbf{s}_A \xleftarrow{\$} \{0,1\}^n;\ \mathbf{e}_A \xleftarrow{\$} \mathcal{E}^n$

$\mathsf{pk}_A := \mathbf{s}_A^\top \mathbf{A} + \mathbf{e}_A^\top, \mathsf{sk}_A := \mathbf{s}_A$

$\mathbf{s}_B \xleftarrow{\$} \{0,1\}^n;\ \mathbf{e}_B \xleftarrow{\$} \mathcal{E}^n$

$\mathsf{pk}_B := \mathbf{A}\mathbf{s}_B + \mathbf{e}_B, \mathsf{sk}_A := \mathbf{s}_B$

$$\text{Alice} \xrightarrow{\mathsf{pk}_A} \text{PKI} \xrightarrow{\mathsf{pk}_B} \text{Bob}$$

$$\text{Alice} \xleftarrow{\mathsf{pk}_B} \text{PKI} \xleftarrow{\mathsf{pk}_A} \text{Bob}$$

$e'_A \xleftarrow{\$} \mathcal{E}$

$e'_B \xleftarrow{\$} \mathcal{E}$

$$K_{AB} := \mathbf{s}_A^\top \mathsf{pk}_B + e'_A = \boxed{\mathbf{s}_A^\top \mathbf{A}\mathbf{s}_B} + \boxed{\mathbf{s}_A^\top \mathbf{e}_B + e'_A} \approx K_{BA} := \mathsf{pk}_A \mathbf{s}_B + e'_B = \boxed{\mathbf{s}_A^\top \mathbf{A}\mathbf{s}_B} + \boxed{\mathbf{e}_A^\top \mathbf{s}_B + e'_B}$$

$$\mathrm{Round}(K_{AB}) \overset{\text{w.h.p.}}{=} \mathrm{Round}(K_{BA})$$

LWE-based NIKE & Our results

polynomial modulus-to-noise ratio $\implies$ non-neglible correctness error

LWE-based NIKE & Our results

$$\begin{aligned} \text{polynomial modulus-to-noise ratio} \quad &\implies \quad \text{non-neglible correctness error} \\ \text{super-polynomial modulus-to-noise ratio} \quad &\implies \quad \text{neglible correctness error} \end{aligned}$$

LWE-based NIKE & Our results

$$\begin{aligned} \text{polynomial modulus-to-noise ratio} &\implies \text{non-neglible correctness error} \\ \text{super-polynomial modulus-to-noise ratio} &\implies \text{neglible correctness error} \end{aligned}$$

This correctness error is inherent [GKRS20]

LWE-based NIKE & Our results

$$\begin{aligned} \text{polynomial modulus-to-noise ratio} \quad &\Longrightarrow \quad \text{non-neglible correctness error} \\ \text{super-polynomial modulus-to-noise ratio} \quad &\Longrightarrow \quad \text{neglible correctness error} \end{aligned}$$

This correctness error is inherent [GKRS20]
Potential errors can be corrected with one bit of interaction [DXL12, Pei14]

LWE-based NIKE & Our results

polynomial modulus-to-noise ratio $\Longrightarrow$ non-neglible correctness error
super-polynomial modulus-to-noise ratio $\Longrightarrow$ neglible correctness error

This correctness error is inherent [GKRS20]
Potential errors can be corrected with one bit of interaction [DXL12, Pei14]

m-t-n ratio	Light security	Adaptive HKR security	Adaptive DKR security with NIZKPoK
poly.			
super-poly.			

LWE-based NIKE & Our results

polynomial modulus-to-noise ratio $\Longrightarrow$ non-neglible correctness error
super-polynomial modulus-to-noise ratio $\Longrightarrow$ neglible correctness error

This correctness error is inherent [GKRS20]
Potential errors can be corrected with one bit of interaction [DXL12, Pei14]

m-t-n ratio	Light security	Adaptive HKR security	Adaptive DKR security with NIZKPoK
poly.	✓		
super-poly.	✓		

[DXL12, Pei14]

LWE-based NIKE & Our results

polynomial modulus-to-noise ratio $\implies$ non-neglible correctness error
super-polynomial modulus-to-noise ratio $\implies$ neglible correctness error

This correctness error is inherent [GKRS20]
Potential errors can be corrected with one bit of interaction [DXL12, Pei14]

m-t-n ratio	Light security	Adaptive HKR security	Adaptive DKR security with NIZKPoK
poly.	✓		
super-poly.	✓	Generic ✓	

LWE-based NIKE & Our results

polynomial modulus-to-noise ratio	$\Longrightarrow$	non-neglible correctness error
super-polynomial modulus-to-noise ratio	$\Longrightarrow$	neglible correctness error

This correctness error is inherent [GKRS20]
Potential errors can be corrected with one bit of interaction [DXL12, Pei14]

m-t-n ratio	Light security	Adaptive HKR security	Adaptive DKR security with NIZKPoK
poly.	✓		
super-poly.	✓	✓	✓ with (Q)ROM

Concurrent work [GdKQ$^+$23]

LWE-based NIKE & Our results

polynomial modulus-to-noise ratio $\implies$ non-neglible correctness error
super-polynomial modulus-to-noise ratio $\implies$ neglible correctness error

This correctness error is inherent [GKRS20]
Potential errors can be corrected with one bit of interaction [DXL12, Pei14]

m-t-n ratio	Light security	Adaptive HKR security	Adaptive DKR security with NIZKPoK
poly.	✓	✓ (bounded) ? (unbounded)	
super-poly.	✓	✓	✓ with (Q)ROM

LWE-based NIKE & Our results

polynomial modulus-to-noise ratio $\implies$ non-neglible correctness error
super-polynomial modulus-to-noise ratio $\implies$ neglible correctness error

This correctness error is inherent [GKRS20]
Potential errors can be corrected with one bit of interaction [DXL12, Pei14]

m-t-n ratio	Light security	Adaptive HKR security	Adaptive DKR security with NIZKPoK
poly.	✓	✓ (bounded) ? (unbounded)	✗
super-poly.	✓	✓	✓ with (Q)ROM

LWE-based NIKE & Our results

polynomial modulus-to-noise ratio	$\Longrightarrow$	non-neglible correctness error
super-polynomial modulus-to-noise ratio	$\Longrightarrow$	neglible correctness error

This correctness error is inherent [GKRS20]
Potential errors can be corrected with one bit of interaction [DXL12, Pei14]

m-t-n ratio	Light security	Adaptive HKR security	Adaptive DKR security with NIZKPoK
poly.	✓	✓ (bounded) ? (unbounded)	✗
super-poly.	✓	✓	✗ poly. noise ✓ super-poly. noise ✓ with (Q)ROM

Alice

$\boxed{\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times n}}$

Bob

$\mathbf{s}_A \xleftarrow{\$} \{0,1\}^n;\ \mathbf{e}_A \xleftarrow{\$} \mathcal{E}^n$

$\boxed{\mathsf{pk}_A := \mathbf{s}_A^\top \mathbf{A} + \mathbf{e}_A^\top}, \mathsf{sk}_A := \mathbf{s}_A$

$\mathbf{s}_B \xleftarrow{\$} \{0,1\}^n;\ \mathbf{e}_B \xleftarrow{\$} \mathcal{E}^n$

$\boxed{\mathsf{pk}_B := \mathbf{A}\mathbf{s}_B + \mathbf{e}_B}, \mathsf{sk}_A := \mathbf{s}_B$

$\boxed{\mathsf{Round}(K_{AB})}$ where $K_{AB} := \mathbf{s}_A^\top \mathsf{pk}_B + e'_A = \mathbf{s}_A^\top \mathbf{A}\mathbf{s}_B + \mathbf{s}_A^\top \mathbf{e}_B + e'_A,\ \ e'_A \xleftarrow{\$} \mathcal{E}$

G_0 Real light security game

Light security [DXL12, Pei14]

Alice

$\boxed{\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times n}}$

Bob

$\mathbf{s}_A \xleftarrow{\$} \{0,1\}^n;\ \mathbf{e}_A \xleftarrow{\$} \mathcal{E}^n$

$\boxed{\mathsf{pk}_A := \mathbf{s}_A^\top \mathbf{A} + \mathbf{e}_A^\top}, \mathsf{sk}_A := \mathbf{s}_A$

$\cancel{\mathbf{s}_B \xleftarrow{\$} \{0,1\}^n;\ \mathbf{e}_B \xleftarrow{\$} \mathcal{E}^n}$

$\cancel{\boxed{\mathsf{pk}_B := \mathbf{A}\mathbf{s}_B + \mathbf{e}_B}, \mathsf{sk}_A := \mathbf{s}_B}$

$\boxed{\mathsf{pk}_B \xleftarrow{\$} \mathbb{Z}_q^n}$

$\boxed{\mathsf{Round}(K_{AB})}$ where $K_{AB} := \mathbf{s}_A^\top \mathsf{pk}_B + e'_A = \mathbf{s}_A^\top \mathbf{A}\mathbf{s}_B + \mathbf{s}_A^\top \mathbf{e}_B + e'_A,\ \ e'_A \xleftarrow{\$} \mathcal{E}$

G_0 Real light security game

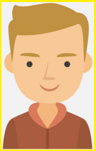
G_1 pk_B is uniformly random

LWE: $\mathbf{A}\mathbf{s}_B + \mathbf{e}_B \approx_c$ uniform

Light security [DXL12, Pei14]

Alice

$\boxed{\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times n}}$



Bob

$\cancel{\mathbf{s}_A \xleftarrow{\$} \{0,1\}^n;\ \mathbf{e}_A \xleftarrow{\$} \mathcal{E}^n \quad \boxed{\mathrm{pk}_A := \mathbf{s}_A^\top \mathbf{A} + \mathbf{e}_A^\top}, \mathrm{sk}_A := \mathbf{s}_A}$ $\boxed{\mathrm{pk}_A \xleftarrow{\$} \mathbb{Z}_q^n}$

$\cancel{\mathbf{s}_B \xleftarrow{\$} \{0,1\}^n;\ \mathbf{e}_B \xleftarrow{\$} \mathcal{E}^n \quad \boxed{\mathrm{pk}_B := \mathbf{A}\mathbf{s}_B + \mathbf{e}_B}, \mathrm{sk}_A := \mathbf{s}_B}$ $\boxed{\mathrm{pk}_B \xleftarrow{\$} \mathbb{Z}_q^n}$

$\boxed{\mathrm{Round}(K_{AB})}$ where $\cancel{K_{AB} := \mathbf{s}_A^\top \mathrm{pk}_B + e'_A = \mathbf{s}_A^\top \mathbf{A}\mathbf{s}_B + \mathbf{s}_A^\top \mathbf{e}_B + e'_A,\ e'_A \xleftarrow{\$} \mathcal{E}}$ $K_{AB} \xleftarrow{\$} \mathbb{Z}_q$

- G_0 Real light security game
- G_1 pk_B is uniformly random
- G_2 pk_A and K_{AB} are uniformly random

LWE: $\mathbf{A}\mathbf{s}_B + \mathbf{e}_B \approx_c$ uniform

LWE: $\begin{pmatrix} \mathbf{A}^\top \\ \mathrm{pk}_B^\top \end{pmatrix} \mathbf{s}_A + \begin{pmatrix} \mathbf{e}_A \\ e'_A \end{pmatrix} \approx_c$ uniform

Adaptive HKR security

- Reduction guesses the two challenge users

Adaptive HKR security

- Reduction guesses the two challenge users
- Problem: Shared key queries with a challenge users secret key

Alice

$\boxed{\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n \times n}}$

Charlie

$\mathbf{s}_A \xleftarrow{\$} \{0,1\}^n$; $\mathbf{e}_A \xleftarrow{\$} \mathcal{E}^n$

$\boxed{\mathsf{pk}_A := \mathbf{s}_A^\top \mathbf{A} + \mathbf{e}_A^\top}$, $\mathsf{sk}_A := \mathbf{s}_A$

$\mathbf{s}_C \xleftarrow{\$} \{0,1\}^n$; $\mathbf{e}_C \xleftarrow{\$} \mathcal{E}^n$

$\boxed{\mathsf{pk}_C := \mathbf{A}\mathbf{s}_C + \mathbf{e}_C}$, $\boxed{\mathsf{sk}_C := \mathbf{s}_C}$

$\boxed{\mathsf{Round}(K_{AC})}$ where $K_{AC} := \mathbf{s}_A^\top \mathsf{pk}_C + e'_A = \mathbf{s}_A^\top \mathbf{A}\mathbf{s}_C + \mathbf{s}_A^\top \mathbf{e}_C + e'_A$, $e'_A \xleftarrow{\$} \mathcal{E}$

Trick 1: Using leakage

Needed: $K_{AC} := \mathbf{s}_A^\top \mathsf{pk}_C + e'_A = \mathbf{s}_A^\top \mathbf{A}\mathbf{s}_C + \ \mathbf{s}_A^\top \mathbf{e}_C \ + e'_A, \ e'_A \xleftarrow{\$} \mathcal{E}$

Trick 1: Using leakage

Needed: $K_{AC} := \mathbf{s}_A^\top \mathsf{pk}_C + e'_A = \mathbf{s}_A^\top \mathbf{A}\mathbf{s}_C + \ \mathbf{s}_A^\top \mathbf{e}_C \ + e'_A,\ e'_A \xleftarrow{\$} \mathcal{E}$

Known: $K_{CA} := \mathsf{pk}_A^\top \mathbf{s}_C + e'_C = \mathbf{s}_A^\top \mathbf{A}\mathbf{s}_C + \ \ \mathbf{e}_A^\top \mathbf{s}_C \ + e'_C\ ,\ e'_C \xleftarrow{\$} \mathcal{E}$

Trick 1: Using leakage

$$\text{Needed: } K_{AC} := \mathbf{s}_A^\top \mathsf{pk}_C + e'_A = \mathbf{s}_A^\top \mathbf{A}\mathbf{s}_C + \boxed{\mathbf{s}_A^\top \mathbf{e}_C} + e'_A,\ e'_A \xleftarrow{\$} \mathcal{E}$$

$$\text{Known: } K_{CA} := \mathsf{pk}_A^\top \mathbf{s}_C + e'_C = \mathbf{s}_A^\top \mathbf{A}\mathbf{s}_C + \boxed{\mathbf{e}_A^\top \mathbf{s}_C} + e'_C,\ e'_C \xleftarrow{\$} \mathcal{E}$$

Trick 1: Using leakage

Leakage about $\mathbf{s}_A$ (e.g. justified by [BD20])

$$\text{Needed: } K_{AC} := \mathbf{s}_A^\top \mathrm{pk}_C + e'_A = \mathbf{s}_A^\top \mathbf{A}\mathbf{s}_C + \boxed{\mathbf{s}_A^\top \mathbf{e}_C} + e'_A,\; e'_A \xleftarrow{\$} \mathcal{E}$$

$$\text{Known: } K_{CA} := \mathrm{pk}_A^\top \mathbf{s}_C + e'_C = \mathbf{s}_A^\top \mathbf{A}\mathbf{s}_C + \boxed{\mathbf{e}_A^\top \mathbf{s}_C} + e'_C\,,\; e'_C \xleftarrow{\$} \mathcal{E}$$

Trick 1: Using leakage

Leakage about $\mathbf{s}_A$ (e.g. justified by [BD20])

$$\text{Needed:}\quad K_{AC} := \mathbf{s}_A^\top \mathrm{pk}_C + e'_A = \mathbf{s}_A^\top \mathbf{A}\mathbf{s}_C + \boxed{\mathbf{s}_A^\top \mathbf{e}_C} + e'_A,\quad e'_A \xleftarrow{\$} \mathcal{E}$$

$$\text{Known:}\quad K_{CA} := \mathrm{pk}_A^\top \mathbf{s}_C + e'_C = \mathbf{s}_A^\top \mathbf{A}\mathbf{s}_C + \boxed{\boxed{\mathbf{e}_A^\top \mathbf{s}_C} + e'_C},\quad e'_C \xleftarrow{\$} \mathcal{E}$$

Noisy linear leakage about $\mathbf{e}_A$ (e.g. justified by [DKL$^+$23])

Trick 1: Using leakage

Leakage about $\mathbf{s}_A$ (e.g. justified by [BD20])

$$\text{Needed: } K_{AC} := \mathbf{s}_A^\top \mathrm{pk}_C + e'_A = \mathbf{s}_A^\top \mathbf{A}\mathbf{s}_C + \boxed{\mathbf{s}_A^\top \mathbf{e}_C} + e'_A, \; e'_A \xleftarrow{\$} \mathcal{E}$$

$$\text{Known: } K_{CA} := \mathrm{pk}_A^\top \mathbf{s}_C + e'_C = \mathbf{s}_A^\top \mathbf{A}\mathbf{s}_C + \boxed{\boxed{\mathbf{e}_A^\top \mathbf{s}_C} + e'_C}, \; e'_C \xleftarrow{\$} \mathcal{E}$$

Noisy linear leakage about $\mathbf{e}_A$ (e.g. justified by [DKL$^+$23])

n has to grow linear with the number of users

Trick 2: Using leakage more economically

- We don't need K_{AC}, Round(K_{AC}) is sufficient

Trick 2: Using leakage more economically

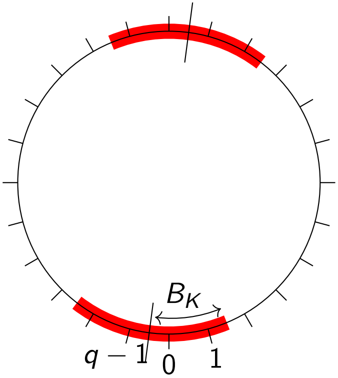
- We don't need K_{AC}, $\text{Round}(K_{AC})$ is sufficient
- Often $\text{Round}(K_{AC}) = \text{Round}(K_{CA})$

Trick 2: Using leakage more economically

- We don't need K_{AC}, $\text{Round}(K_{AC})$ is sufficient
- Often $\text{Round}(K_{AC}) = \text{Round}(K_{CA})$
  - Leakage can be avoided then

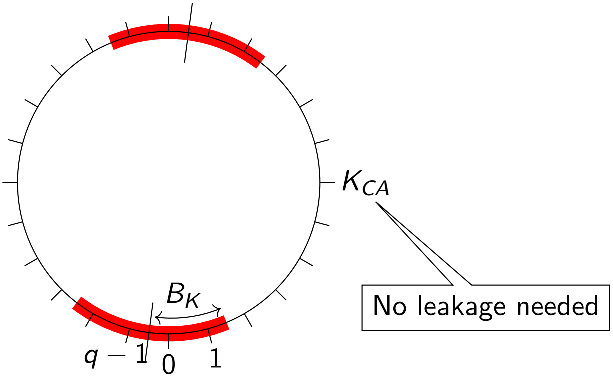
Trick 2: Using leakage more economically

- We don't need K_{AC}, Round(K_{AC}) is sufficient
- Often Round(K_{AC}) = Round(K_{CA})
  - Leakage can be avoided then



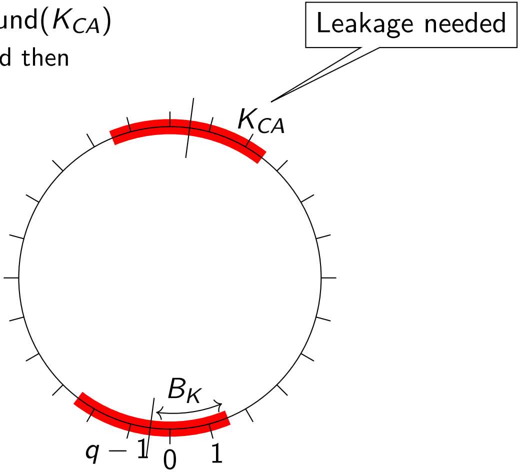
Trick 2: Using leakage more economically

- We don't need K_{AC}, $\mathrm{Round}(K_{AC})$ is sufficient
- Often $\mathrm{Round}(K_{AC}) = \mathrm{Round}(K_{CA})$
  - Leakage can be avoided then



Trick 2: Using leakage more economically

- We don't need K_{AC}, Round(K_{AC}) is sufficient
- Often Round(K_{AC}) = Round(K_{CA})
  - Leakage can be avoided then



Trick 2: Using leakage more economically

The difficulty:

- Leakage on $\mathbf{s}_A$ must not depend on $\mathbf{A}$

Trick 2: Using leakage more economically

The difficulty:

- Leakage on $\mathbf{s}_A$ must not depend on $\mathbf{A}$
- Whether K_{CA} is in the red zone does depend on $\mathbf{A}$

Trick 2: Using leakage more economically

The difficulty:

- Leakage on $\mathbf{s}_A$ must not depend on $\mathbf{A}$
- Whether K_{CA} is in the red zone does depend on $\mathbf{A}$

The solution:

- We need leakage $\mathbf{s}_A^\top \mathbf{e}_C$

Trick 2: Using leakage more economically

The difficulty:

- Leakage on $\mathbf{s}_A$ must not depend on $\mathbf{A}$
- Whether K_{CA} is in the red zone does depend on $\mathbf{A}$

The solution:

- We need leakage $\mathbf{s}_A^\top \mathbf{e}_C$
- $\mathbf{e}_C$ has only small influence on K_{CA}.

Trick 2: Using leakage more economically

The difficulty:

- Leakage on $\mathbf{s}_A$ must not depend on $\mathbf{A}$
- Whether K_{CA} is in the red zone does depend on $\mathbf{A}$

The solution:

- We need leakage $\mathbf{s}_A^\top \mathbf{e}_C$
- $\mathbf{e}_C$ has only small influence on K_{CA}.

$$\Longrightarrow \text{number of users can grow polynomially in } n$$

Summary

m-t-n ratio	Light security	Adaptive HKR security	Adaptive DKR security with NIZKPoK
poly.	✓	✓ (bounded) ? (unbounded)	✗
super-poly.	✓	✓	✗ poly. noise ✓ super-poly. noise ✓ with (Q)ROM

References I

Zvika Brakerski and Nico Döttling.
Hardness of LWE on general entropic distributions.
In Anne Canteaut and Yuval Ishai, editors, EUROCRYPT 2020, Part II, volume 12106 of LNCS, pages 551–575. Springer, Heidelberg, May 2020.
doi:10.1007/978-3-030-45724-2_19.

David Cash, Eike Kiltz, and Victor Shoup.
The twin Diffie-Hellman problem and applications.
In Nigel P. Smart, editor, EUROCRYPT 2008, volume 4965 of LNCS, pages 127–145. Springer, Heidelberg, April 2008.
doi:10.1007/978-3-540-78967-3_8.

References II

Nico Döttling, Dimitris Kolonelos, Russell W. F. Lai, Chuanwei Lin, Giulio Malavolta, and Ahmadreza Rahimi.
Efficient laconic cryptography from learning with errors.
In Carmit Hazay and Martijn Stam, editors, EUROCRYPT 2023, Part III, volume 14006 of LNCS, pages 417–446. Springer, Heidelberg, April 2023.
doi:10.1007/978-3-031-30620-4_14.

Jintai Ding, Xiang Xie, and Xiaodong Lin.
A simple provably secure key exchange scheme based on the learning with errors problem.
Cryptology ePrint Archive, Report 2012/688, 2012.
https://eprint.iacr.org/2012/688.

References III

Eduarda S. V. Freire, Dennis Hofheinz, Eike Kiltz, and Kenneth G. Paterson.
Non-interactive key exchange.
In Kaoru Kurosawa and Goichiro Hanaoka, editors, PKC 2013, volume 7778 of LNCS, pages 254–271. Springer, Heidelberg, February / March 2013.
doi:10.1007/978-3-642-36362-7_17.

Phillip Gajland, Bor de Kock, Miguel Quaresma, Giulio Malavolta, and Peter Schwabe.
Swoosh: Practical lattice-based non-interactive key exchange.
Cryptology ePrint Archive, Report 2023/271, 2023.
https://eprint.iacr.org/2023/271.

References IV

Siyao Guo, Pritish Kamath, Alon Rosen, and Katerina Sotiraki.
Limits on the efficiency of (ring) LWE based non-interactive key exchange.
In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, PKC 2020, Part I, volume 12110 of LNCS, pages 374–395. Springer, Heidelberg, May 2020.
doi:10.1007/978-3-030-45374-9_13.

Julia Hesse, Dennis Hofheinz, and Lisa Kohl.
On tightly secure non-interactive key exchange.
In Hovav Shacham and Alexandra Boldyreva, editors, CRYPTO 2018, Part II, volume 10992 of LNCS, pages 65–94. Springer, Heidelberg, August 2018.
doi:10.1007/978-3-319-96881-0_3.

References V

Chris Peikert.
Lattice cryptography for the internet.
In Michele Mosca, editor, Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014, pages 197–219. Springer, Heidelberg, October 2014.
doi:10.1007/978-3-319-11659-4_12.

Pictures

Alice, Bob, and other faces: freepik.com
Devil face: vecteezy.com

Trick 2: Using leakage more economically (Full detail)

The difficulty:

- Leakage on $\mathbf{s}_A$ must not depend on $\mathbf{A}$
- Whether K_{CA} is in the red zone does depend on $\mathbf{A}$

The solution:

- We need leakage $\mathbf{s}_A^\top \mathbf{e}_C$
- $\mathbf{e}_C$ has only small influence on K_{CA}.
- Use leakage $\mathbf{s}_A^\top \mathbf{e}_i$ for several $\mathbf{e}_i \xleftarrow{\$} \mathcal{E}^n$
- If $\mathbf{s}_A^\top \mathbf{A} \mathbf{s}_C$ is in the red zone $\Rightarrow$ use one of the $\mathbf{e}_i$ as Charlie's error vector.
- Otherwise sample a fresh error vector for Charlie

$$\implies \text{number of users can grow polynomially in } n$$

DKR insecurity

Use of NIZKPoKs $\Rightarrow \mathcal{A}$ can register malicious public key only with a valid secret key.

- Adversary can create $(\mathsf{pk}, \mathsf{sk})$ s.t. $\mathbf{s}_A^\top \mathsf{pk} \approx 0$

$\Rightarrow$ High likelihood of correctness error with Alice

Example:

- Assume for simplicity Alice does not add noise to the shared key before rounding
- Register for $i \in [n]$ user with $\mathsf{pk}_i = -e_i$, $\mathsf{sk}_i = \mathbf{0}$
- If $(\mathbf{s}_A)_i = 0$, $\mathsf{Round}(K_{A,i}) = \mathsf{Round}(0) = 0$
- If $(\mathbf{s}_A)_i = 1$, $\mathsf{Round}(K_{A,i}) = \mathsf{Round}(q-1) = 1$

$\Rightarrow \mathcal{A}$ can extract $\mathbf{s}_A$ with n malicious users

- Attack can be extended to
  - shared keys with noise
  - different distributions of LWE secrets
  - different rounding functions (with polynomial modulus-to-noise ratio)

DKR security

For malicious user Charlie:

- Extract sk_C from NIZKPoK
- Compute K_{CA} with sk_C
- B: maximum difference between K_{AC} and K_{CA}
- Use noise super-polynomial in B for the shared keys

$\Rightarrow$ $K_{AC} \approx_s K_{CA}$